Cyber Protect Cloud

23.02

Panduan Administrator untuk Mitra

REVISI: 28/02/2023

Daftar isi

Tentang dokumen ini

Dokumen ini ditujukan bagi administrator mitra yang ingin menggunakan Cyber Protect Cloud untuk memberikan layanan kepada klien mereka.

Dokumen ini menjelaskan cara menyiapkan dan mengelola layanan yang tersedia di Cyber Protect Cloud menggunakan portal manajemen.

Tentang Cyber Protect

Cyber Protect adalah platform awan yang memungkinkan penyedia layanan, reseller, dan distributor untuk memberikan layanan perlindungan data kepada mitra dan pelanggan mereka.

Layanan ini disediakan pada tingkat mitra, hingga tingkat perusahaan pelanggan dan pengguna akhir.

Manajemen layanan tersedia di aplikasi web yang disebut **konsol layanan**. Manajemen penyewa dan akun pengguna tersedia di aplikasi web yang disebut **portal manajemen**.

Portal manajemen memungkinkan administrator untuk:

- Memantau penggunaan layanan dan mengakses konsol layanan
- Mengelola penyewa
- Mengelola akun pengguna
- Mengonfigurasi layanan dan kuota bagi penyewa
- Mengelola penyimpanan
- Mengelola branding
- Membuat laporan tentang penggunaan layanan

Layanan Cyber Protect

Bagian ini menjelaskan set fitur yang diperkenalkan pada Maret 2021 dengan model penagihan baru. Baca selengkapnya tentang kelebihan model penagihan baru di lembar data Cyber Protect.

Set layanan dan fitur berikut tersedia di Cyber Protect Cloud:

- **Cyber Protect**
  - **Perlindungan** - Perlindungan siber lengkap dengan fungsionalitas keamanan dan manajemen yang termasuk di dalam produk dasarnya, serta pemulihan bencana, pencadangan dan pemulihan, otomatisasi, dan keamanan email yang tersedia dalam fitur bayar sesuai pemakaian. Fungsi ini dapat diperluas dengan paket perlindungan tingkat lanjut yang dikenakan biaya tambahan.
    Paket perlindungan tingkat lanjut adalah set fitur unik yang mengatasi skenario yang lebih canggih dalam area fungsional tertentu, misalnya, Cadangan Tingkat Lanjut, Keamanan Tingkat Lanjut, dan lainnya. Paket tingkat lanjut memperluas fungsi yang tersedia dalam layanan Cyber Protect standar.
    Untuk informasi selengkapnya mengenai Paket Perlindungan Tingkat Lanjut, lihat "Paket Perlindungan Tingkat Lanjut" (hlm. 122).
  - **File Sync & Share** - solusi untuk berbagi konten perusahaan dengan aman dari mana pun, kapan pun, dan pada perangkat apa pun.
  - **Pengiriman Data Fisik** - solusi yang membantu Anda menghemat waktu dan lalu lintas

jaringan dengan mengirim data ke pusat data awan pada hard drive.
  - **Notary** - solusi berbasi blockchain yang memastikan keaslian konten yang dibagikan.
- **SPLA Cyber Infrastructure**

Dalam portal manajemen, Anda dapat memilih set layanan dan fitur yang akan disediakan untuk penyewa Anda. Konfigurasi dilakukan per penyewa, jika Anda menyediakan atau mengedit penyewa, seperti yang dijelaskan dalam Membuat penyewa.

Mode penagihan untuk Cyber Protect

Mode penagihan adalah skema untuk akuntansi dan penagihan untuk penggunaan layanan dan fiturnya. Mode penagihan menentukan unit apa yang akan digunakan sebagai dasar penghitungan harga. Mode penagihan dapat diatur oleh mitra di tingkat Pelanggan.

Mesin pelisensian secara otomatis mendapatkan item penawaran bergantung pada fitur yang diminta dalam rencana proteksi. Pengguna dapat mengoptimalkan tingkat perlindungan dan biaya dengan menyesuaikan rencana proteksi.

Catatan
Anda hanya dapat menggunakan mode penagihan per penyewa Pelanggan.

Mode penagihan untuk komponen Perlindungan

Perlindungan memiliki dua mode penagihan:

- Per beban kerja
- Per gigabyte

Set fitur untuk kedua mode penagihan sama.

Dalam kedua mode penagihan, layanan Perlindungan menyertakan fitur perlindungan standar yang mencakup sebagian besar risiko keamanan cyber. Pengguna dapat menggunakannya tanpa biaya tambahan. Penggunaan fitur yang disertakan akan dihitung, tetapi tidak akan ditagih. Untuk daftar lengkap item penawaran yang disertakan dan dapat ditagih, lihat "Layanan Cyber Protect" (hlm. 6).

Meskipun paket tingkat lanjut diaktifkan untuk pelanggan, penagihan hanya akan dimulai setelah pelanggan mulai menggunakan fitur paket tersebut dalam rencana proteksi. Ketika fitur tingkat lanjut diterapkan dalam rencana proteksi, mesin pelisensian secara otomatis menetapkan lisensi yang diperlukan ke beban kerja yang diproteksi.

Ketika fitur tingkat lanjut tidak lagi digunakan, lisensi dibatalkan dan penagihan dihentikan. Mesin pelisensian secara otomatis menetapkan lisensi yang mencerminkan penggunaan fitur yang sebenarnya.

Anda dapat menetapkan lisensi hanya untuk fitur layanan Cyber Protect standar. Fitur tingkat lanjut ditagih berdasarkan penggunaan dan lisensinya tidak dapat diubah secara manual. Mesin pelisensian menetapkan dan membatalkan permintaan lisensi secara otomatis. Anda dapat

mengubah tipe lisensi untuk beban kerja secara manual, tetapi lisensi akan ditetapkan ulang ketika rencana proteksi untuk beban kerja tersebut diubah oleh pengguna.

Catatan
Penagihan untuk fitur perlindungan tingkat lanjut tidak dimulai ketika Anda mengaktifkannya. Penagihan akan dimulai hanya setelah pelanggan mulai menggunakan fitur tingkat lanjut dalam rencana proteksi. Set fitur yang diaktifkan akan dihitung dan disertakan dalam laporan penggunaan, tetapi tidak akan ditagih, kecuali fitur digunakan.

Mode penagihan untuk File Sync & Share

File Sync & Share memiliki mode penagihan berikut:

- Per pengguna
- Per gigabyte

Anda juga dapat menetapkan aturan penagihan dari edisi File Sync & Share legasi.

Catatan
Penagihan untuk File Sync & Share Tingkat Lanjut tidak dimulai ketika Anda mengaktifkannya. Penagihan akan dimulai hanya setelah pelanggan mulai menggunakan fitur tingkat lanjutnya. Set fitur tingkat lanjut yang diaktifkan akan dihitung dan disertakan dalam laporan penggunaan, tetapi tidak akan ditagih, kecuali jika fiturnya digunakan.

Penagihan untuk Pengiriman Data Fisik

Penagihan untuk Pengiriman Data Fisik mengikuti model bayar sesuai pemakaian.

Penagihan untuk Notary

Penagihan untuk Notary mengikuti model bayar sesuai pemakaian.

Menggunakan mode penagihan dengan edisi legasi

Jika Anda belum memigrasikan model penagihan terkini, gunakan item penawaran dibawah salah satu mode penagihan untuk menggantikan edisi legasi. Mesin pelisensian akan secara otomatis mengoptimalkan lisensi yang ditetapkan ke pelanggan untuk meminimalkan jumlah yang dapat ditagih.

Catatan
Anda tidak dapat mencampurkan edisi dengan mode penagihan.

Beralih dari edisi legasi ke model pelisensian terkini

Anda dapat mengalihkan item penawaran untuk penyewa Anda secara manual dengan mengedit profil mereka dan memilih item penawaran bagi mereka. Untuk informasi lebih lanjut tentang proses pengalihan, lihat "Beralih antara edisi dan mode penagihan" (hlm. 9).

Untuk beralih dari edisi ke mode penagihan untuk beberapa pelanggan, Pengalihan edisi massal untuk beberapa pelanggan (67942).

Beralih antara edisi dan mode penagihan

Di portal manajemen, Anda dapat mengubah akun penyewa untuk mengalihkan item penawaran antara mode penagihan (per beban kerja menjadi per gigabyte dan sebaliknya) serta antara mode penagihan dan edisi lama.

Untuk informasi tentang pengalihan penyewa massal, lihat Pengalihan edisi massal untuk beberapa pelanggan (67942).

Proses pengalihan mencakup langkah-langkah berikut.

1. Menyediakan item penawaran baru untuk penyewa pelanggan (pengaktifan item penawaran dan pengaturan kuota) untuk mencocokkan dengan fungsi yang tersedia dalam item penawaran asli.
2. Membatalkan item penawaran yang tidak digunakan dan menetapkan item penawaran ke beban kerja sesuai fitur yang digunakan dalam rencana proteksi (rekonsiliasi penggunaan).

Tabel berikut mengilustrasikan proses dalam kedua arah.

	Arah pengalihan	
	Edisi > Mode penagihan	**Mode penagihan > Mode penagihan**
Pengalihan item penawaran	Mangaktifkan item penawaran untuk memenuhi fungsi yang tersedia dalam edisi sumber.	Set item penawaran yang sama akan diaktifkan.
Pengalihan kuota	Kuota akan direplikasi dari item penawaran sumber ke item penawaran tujuan. Sumber Standar → tujuan produk Standar. Sumber Standar → tujuan paket. **Catatan** Jika Anda beralih dari edisi dengan sub-edisi (misalnya, "Cyber Protect (per beban kerja)"), kuota akan diringkas.	Kuota akan direplikasi dari item penawaran sumber ke item penawaran tujuan.
Pengalihan penggunaan	Item penawaran akan ditetapkan ulang ke beban kerja sesuai fitur yang diminta dalam rencana proteksi yang ditetapkan pada beban kerja tersebut.	

Contoh: Mengalihkan Cyber Protect edisi Advanced ke Penagihan per beban kerja

Dalam skenario ini, seorang penyewa pelanggan memiliki Cyber Protect edisi Advanced yang digunakan pada 8 stasiun kerja, dan kuota diatur untuk 10 beban kerja. 3 stasiun kerja

menggunakan inventaris perangkat lunak dan manajemen patch dalam rencana proteksi, 2 stasiun kerja mengaktifkan pemfilteran URL dalam rencana proteksi, dan satu mesin menggunakan perlindungan data berkelanjutan. Tabel berikut mengilustrasikan konversi edisi ke item penawaran baru.

Item penawaran sumber - penggunaan/kuota	Item penawaran tujuan - penggunaan/kuota
Cyber Protect Stasiun kerja tingkat lanjut 8/10	• Stasiun Kerja - 8/10 • Keamanan Tingkat Lanjut - 2/10 • Stasiun kerja Cadangan Tingkat Lanjut - 1/10 • Manajemen Tingkat Lanjut - 3/10

Langkah-langkah berikut dilakukan selama pengalihan:

1. Item penawaran yang mencakup fungsi yang tersedia dalam edisi sumber diaktifkan secara otomatis.
2. Kuota direplikasi pada item penawaran baru.
3. Penggunaan direkonsiliasi sesuai penggunaan sebenarnya dalam rencana proteksi: tiga beban kerja menggunakan fitur paket Manajemen Tingkat Lanjut, dua menggunakan fitur paket Keamanan Tingkat Lanjut, dan satu menggunakan fitur paket Cadangan Tingkat Lanjut.

Contoh: Cyber Protect per edisi beban kerja menjadi Penagihan per beban kerja

Dalam contoh ini, pelanggan menetapkan beberapa edisi pada beban kerja. Setiap beban kerja hanya dapat memiliki satu edisi atau satu mode penagihan.

Item penawaran sumber - penggunaan/kuota	Item penawaran tujuan - penggunaan/kuota
Cyber Protect Workstation Essentials - 6/12	• Stasiun Kerja - 14/42 • Stasiun kerja Cadangan Tingkat Lanjut - 2/42 • Keamanan Tingkat Lanjut - 13/42 • Manajemen Tingkat Lanjut - 5/42
Cyber Protect Workstation Standard - 5/10	
Cyber Protect Advanced Workstation - 2/10	
Stasiun Kerja Cyber Backup Standard - 1/10	

Langkah-langkah berikut dilakukan selama pengalihan:

1. Item penawaran yang mencakup fungsionalitas yang tersedia di semua edisi sumber telah diaktifkan secara otomatis. Dengan mode penagihan, beberapa item penawaran dapat ditetapkan ke satu beban kerja sesuai kebutuhan.
2. Kuota diringkas dan direplikasi.
3. Penggunaan direkonsiliasi sesuai rencana proteksi.

Mengubah mode penagihan untuk penyewa mitra

Cara mengubah mode penagihan untuk penyewa mitra

1. Di portal manajemen, buka **Klien**.
2. Pilih penyewa mitra yang mode penagihannya ingin Anda ubah, klik ikon elipsis , lalu klik **Konfigurasi**.
3. Pada tab **Cyber Protect**, pilih layanan yang ingin Anda ubah mode penagihannya dan klik **Edit**.
4. Pilih mode penagihan yang diinginkan lalu aktifkan atau nonaktifkan item penawaran yang tersedia sesuai kebutuhan.
5. Klik **Simpan**.

Mengubah mode penagihan untuk penyewa pelanggan

Anda dapat mengubah penagihan untuk penyewa pelanggan dengan:

- Mengedit mode penagihan asli, dengan mengaktifkan atau menonaktifkan item penawaran.
- Beralih ke mode penagihan baru.

Untuk informasi lebih lanjut tentang cara mengedit item penawaran yang tersedia, lihat Mengaktifkan atau menonaktifkan item penawaran.

Cara beralih mode penagihan untuk penyewa pelanggan

1. Di portal manajemen, buka **Klien**.
2. Pilih penyewa pelanggan yang edisinya ingin Anda ubah, klik ikon elipsis  , lalu klik **Konfigurasikan**.
3. Di tab **Konfigurasi**, di bagian **Layanan**, pilih mode penagihan baru.
   Pop-up dialog muncul untuk memberi tahu Anda mengenai konsekuensi perubahan ke mode penagihan baru.
4. Masukkan nama pengguna untuk mengonfirmasi pilihan Anda.

Catatan
Perubahan ini dapat memakan waktu hingga 10 menit.

Item penawaran dan manajemen kuota

Bagian ini menjelaskan hal berikut:

- Apa itu layanan dan item penawaran?
- Bagaimana item penawaran diaktifkan atau dinonaktifkan?
- Apa itu mode penagihan?
- Apa itu Paket perlindungan tingkat lanjut?
- Apa itu edisi legasi dan sub-edisi?
- Apa definisi kuota lunak dan kuota keras?

- Kapan kuota keras dapat terlampaui?
- Apa definisi transformasi kuota cadangan?
- Bagaimana ketersediaan item penawaran memengaruhi ketersediaan penginstal dalam konsol layanan?

Layanan dan item penawaran

Layanan

Layanan awan adalah serangkaian fungsi yang di-host oleh mitra, atau di awan privat pelanggan akhir. Biasanya, layanan dijual sebagai langganan atau dengan bayar sesuai pemakaian.

Layanan Cyber Protect mengintegrasikan keamanan cyber, perlindungan data, dan manajemen untuk melindungi titik akhir, sistem, dan data Anda dari ancaman keamanan cyber. Layanan Cyber Protect terdiri dari beberapa komponen: Perlindungan, File Sync & Share, Notary, dan Pengiriman Data Fisik. Beberapa komponen ini dapat diperluas dengan fungsi tingkat lanjut dengan menggunakan paket Perlindungan tingkat lanjut. Untuk informasi detail tentang fitur tingkat lanjut dan yang disertakan, lihat "Layanan Cyber Protect" (hlm. 6).

Item penawaran

 Item penawaran adalah set fitur layanan yang dikelompokkan menurut tipe beban kerja atau fungsi tertentu, misalnya, penyimpanan, infrastruktur pemulihan bencana, dan lainnya. Dengan mengaktifkan item penawaran tertentu, Anda menentukan beban kerja yang dapat dilindungi, berapa banyak beban kerja yang dapat dilindungi (dengan mengatur kuota), dan tingkat perlindungan yang akan tersedia untuk mitra, pelanggan, dan pengguna akhir mereka (dengan mengaktifkan atau menonaktifkan paket perlindungan tingkat lanjut).

Fungsi yang tidak diaktifkan akan disembunyikan dari pelanggan dan pengguna, kecuali Anda mengonfigurasi skenario upsell. Untuk informasi lebih lanjut tentang skenario upsell, lihat "Mengonfigurasi skenario upsell untuk pelanggan Anda" (hlm. 63).

Penggunaan fitur dikumpulkan dari layanan dan tercermin pada item penawaran, yang digunakan dalam laporan dan penagihan lebih lanjut.

Mode penagihan dan edisi

Dengan edisi legasi, Anda dapat menetapkan satu item penawaran per beban kerja. Dengan mode penagihan, fungsi terbagi sehingga Anda dapat mengaktifkan beberapa item penawaran (fitur layanan dan paket tingkat lanjut) per beban kerja untuk memenuhi kebutuhan pelanggan dengan lebih baik dan menerapkan penagihan yang lebih akurat, hanya untuk fitur yang memang digunakan pelanggan Anda.

Untuk informasi lebih lanjut tentang mode penagihan untuk Cyber Protect, lihat "Mode penagihan untuk Cyber Protect" (hlm. 7).

Anda dapat menggunakan mode penagihan atau edisi untuk mengonfigurasi layanan yang tersedia untuk penyewa Anda. Anda dapat menggunakan satu mode penagihan atau satu edisi per penyewa Pelanggan. Hasilnya, untuk menerapkan mode penagihan yang berbeda untuk fitur layanan yang berbeda, Anda perlu membuat beberapa penyewa untuk satu pelanggan. Misalnya, jika pelanggan ingin memiliki kotak surat Microsoft 365 dalam mode penagihan Per gigabyte, dan Teams dalam mode penagihan Per beban kerja, Anda harus membuat dua penyewa pelanggan yang berbeda untuk pelanggan ini.

Untuk membatasi penggunaan layanan dalam item penawaran, Anda dapat menentukan kuota untuk item penawaran tersebut. Lihat "Kuota lunak dan kuota keras" (hlm. 14).

Mengaktifkan atau menonaktifkan item penawaran

Anda dapat mengaktifkan semua item penawaran yang tersedia untuk edisi atau model penagihan tertentu, seperti yang dijelaskan dalam Membuat penyewa.

Catatan
Menonaktifkan semua item penawaran layanan tidak menonaktifkan layanan secara otomatis.

Ada beberapa batasan untuk menonaktifkan item penawaran, yang dicantumkan dalam tabel berikut.

Item penawaran	Menonaktifkan	Hasil
Penyimpanan cadangan	Dapat dinonaktifkan jika penggunaan sama dengan nol.	Penyimpanan awan tidak akan tersedia sebagai tujuan pencadangan dalam penyewa pelanggan.
Cadangan lokal	Dapat dinonaktifkan jika penggunaan sama dengan nol.	Penyimpanan lokal tidak akan tersedia sebagai tujuan pencadangan dalam penyewa pelanggan.
Sumber data (termasuk Microsoft 365 dan Google Workspace)	Dapat dinonaktifkan jika penggunaan sama dengan nol.	Cadangan dan pemulihan sumber data (termasuk Microsoft 365 dan Google Workspace) akan menjadi tidak tersedia dalam penyewa pelanggan.
Semua item penawaran Disaster Recovery	Dapat dinonaktifkan jika penggunaan lebih dari nol.	Lihat detailnya di "Kuota lunak dan keras".
Semua item penawaran Notaris	Dapat dinonaktifkan jika penggunaan sama dengan nol.	Layanan Notaris tidak akan tersedia di dalam penyewa pelanggan.
Semua item penawaran File Sync & Share	Item penawaran tidak dapat diaktifkan atau dinonaktifkan secara terpisah.	Layanan File Sync & Share tidak akan tersedia di dalam penyewa pelanggan.

Semua item penawaran Pengiriman Data Fisik	Dapat dinonaktifkan jika penggunaan sama dengan nol.	Layanan Pengiriman Data Fisik tidak akan tersedia di dalam penyewa pelanggan.

Untuk item penawaran yang tidak dapat dinonaktifkan saat penggunaannya lebih dari nol, Anda dapat menghapus penggunaan secara manual, lalu menonaktifkan item penawaran terkait.

Kuota lunak dan kuota keras

Kuota memungkinkan Anda untuk membatasi kemampuan penyewa untuk menggunakan layanan. Untuk menentukan kuota, pilih klien pada tab **Klien**, pilih tab layanan, lalu klik **Edit**.

Ketika kuota melebihi batas, pemberitahuan akan dikirim ke alamat email pengguna. Jika Anda tidak menetapkan kelebihan kuota, kuota akan dianggap sebagai "**lunak.**" Artinya, pembatasan penggunaan layanan Cyber Protection tidak diterapkan.

Ketika Anda menentukan kelebihan kuota, maka kuota dianggap "**keras.**" **Kelebihan** memungkinkan pengguna untuk melampaui kuota sebesar nilai yang ditentukan. Ketika kelebihan terlampaui, pembatasan penggunaan layanan diterapkan.

Contoh

Kuota lunak: Anda telah menentukan kuota untuk stasiun kerja sama dengan 20. Ketika jumlah stasiun kerja terlindungi milik pelanggan mencapai 20, pelanggan akan menerima pemberitahuan melalui email, tapi layanan Cyber Protection akan tetap tersedia.

Kuota keras: Jika Anda sudah menentukan kuota untuk stasiun kerja sama dengan 20 dan kelebihannya adalah 5, pelanggan Anda akan menerima pemberitahuan melalui email saat jumlah stasiun kerja terlindungi mencapai 20, dan layanan Cyber Protection akan dinonaktifkan saat jumlah tersebut mencapai 25.

Ketika kuota keras tercapai, layanan menjadi terbatas (Mustahil untuk melindungi beban kerja lain atau menggunakan lebih banyak penyimpanan). Ketika kuota keras terlampaui, pemberitahuan akan dikirim ke alamat email pengguna.

Level untuk menentukan kuota

Kuota dapat diatur pada level yang tercantum dalam tabel di bawah ini.

Penyewa/Pengguna	Kuota lunak (kuota saja)	Kuota keras (kuota dan kelebihan)
Mitra	ya	tidak
Folder	ya	tidak
Pelanggan	ya	ya
Unit	tidak	tidak
Pengguna	ya	ya

Kuota lunak dapat diatur pada level mitra dan folder. Pada level unit, tidak ada kuota yang dapat diatur. Kuota keras dapat ditentukan di level pelanggan dan pengguna.

Jumlah total kuota keras yang ditentukan pada level pengguna tidak dapat melebihi kuota keras pelanggan terkait.

Mengatur kuota lunak dan kuota keras

Cara mengatur kuota untuk klien Anda

1. Di portal manajemen, buka **Klien**.
2. Pilih klien yang ingin Anda atur kuotanya.
3. Pilih tab **Perlindungan**, lalu klik **Edit**.
4. Pilih jenis kuota yang ingin diatur. Misalnya, pilih **Stasiun kerja** atau **Server**.
5. Klik tautan **Tidak terbatas** di sebelah kanan untuk membuka jendela **Pengeditan kuota**.
   - Jika Anda ingin memberi tahu klien tentang kuota dan tidak ingin membatasi kemampuan klien untuk menggunakan layanan, atur nilai kuota di bidang **Kuota lunak**.
     Klien akan menerima email pemberitahuan setelah mencapai batas kuota, tetapi layanan Cyber Protection akan tetap tersedia.
   - Jika Anda ingin membatasi kemampuan klien untuk menggunakan layanan, pilih **Kuota keras** dan tetapkan nilai kuota pada bidang di bawah **Kuota keras**.
     Klien akan menerima email pemberitahuan setelah mencapai batas kuota, dan layanan Cyber Protection akan dinonaktifkan.
6. Di jendela **Pengeditan kuota**, klik **Selesai**, lalu klik **Simpan**.

Kuota Backup

Anda dapat menentukan kuota penyimpanan awan, kuota untuk pencadangan lokal, dan jumlah maksimum mesin/perangkat/situs web pengguna yang dapat dilindungi. Kuota berikut tersedia.

Kuota untuk perangkat

- **Stasiun Kerja**
- **Server**
- **Mesin virtual**
- **Perangkat seluler**
- **Server hosting web** (Server fisik atau virtual berbasis Linux yang menjalankan panel kontrol Plesk, cPanel, DirectAdmin, VirtualMin, atau ISPManager)
- **Situs web**

Sebuah mesin/perangkat/situs web dianggap terlindungi selama setidaknya ada satu rencana proteksi yang diterapkan pada ketiganya. Perangkat seluler menjadi terlindungi setelah pencadangan pertama.

Saat kelebihan untuk sejumlah perangkat terlampaui, pengguna tidak dapat menerapkan rencana proteksi ke lebih banyak perangkat.

Kuota untuk sumber data awan

- **Kursi Microsoft 365**

  Kuota ini diterapkan oleh penyedia layanan ke seluruh perusahaan. Administrator perusahaan dapat melihat kuota dan penggunaan pada portal manajemen.

  Pelisensian kursi Microsoft 365 tergantung pada mode penagihan terpilih untuk Cyber Protection.

  Dalam mode penagihan **Per beban kerja**, kuota **kursi Microsoft 365** dihitung per pengguna unik. Pengguna unik adalah pengguna yang memiliki setidaknya salah satu hal berikut:

  - Kotak surat yang dilindungi
  - OneDrive yang dilindungi
  - Akses ke setidaknya satu sumber daya level perusahaan yang dilindungi: situs Microsoft 365 SharePoint Online, atau Microsoft 365 Teams.
    Untuk mempelajari cara memeriksa jumlah anggota situs Microsoft 365 SharePoint atau Teams, lihat artikel basis pengetahuan ini.

  Catatan
  Pengguna Microsoft 365 yang diblokir yang tidak memiliki kotak surat pribadi atau OneDrive yang dilindungi, dan hanya dapat mengakses sumber daya yang dibagikan (kotak surat bersama, situs SharePoint, serta Microsoft Teams), tidak dikenakan biaya.

  Pengguna yang diblokir adalah mereka yang tidak memiliki login valid dan tidak dapat mengakses layanan Microsoft 365. Pelajari cara memblokir semua pengguna tanpa lisensi di organisasi Microsoft 365, lihat "Mencegah pengguna Microsoft 365 tanpa lisensi untuk masuk" (hlm. 18).)

  Kursi Microsoft 365 berikut tidak dikenakan biaya dan tidak memerlukan lisensi per kursi:

  - Kotak surat bersama
  - Ruangan dan perlengkapan
  - Pengguna eksternal dengan akses ke situs SharePoint dan/atau Microsoft Teams yang dicadangkan

  Untuk informasi lebih lanjut tentang opsi pelisensian dengan mode penagihan per gigabyte, lihat Cyber Protect Cloud: pelisensian Microsoft 365 per GB.

  Untuk informasi lebih lanjut tentang opsi pelisensian dengan mode penagihan per beban kerja, lihat Cyber Protect Cloud: pelisensian Microsoft 365 dan perubahan harga.

- **Microsoft 365 Teams**

  Kuota ini diterapkan oleh penyedia layanan ke seluruh perusahaan. Kuota ini mengaktifkan atau menonaktifkan kemampuan untuk melindungi Microsoft 365 Teams dan mengatur jumlah maksimum tim yang dapat dilindungi. Diperlukan satu kuota untuk melindungi satu tim, berapa

pun jumlah anggota atau salurannya. Administrator perusahaan dapat melihat kuota dan penggunaan pada portal manajemen.

- **Microsoft 365 SharePoint Online**

  Kuota ini diterapkan oleh penyedia layanan ke seluruh perusahaan. Kuota ini mengaktifkan atau menonaktifkan kemampuan untuk melindungi situs SharePoint Online dan mengatur jumlah maksimum kumpulan situs dan situs grup yang dapat dilindungi.

  Administrator perusahaan dapat melihat kuota ini pada portal manajemen. Mereka juga dapat melihat kuota, beserta jumlah penyimpanan yang digunakan oleh cadangan SharePoint Online, dalam laporan penggunaan.
- **Kursi Google Workspace**

  Kuota ini diterapkan oleh penyedia layanan ke seluruh perusahaan. Perusahaan diperbolehkan untuk melindungi kotak surat **Gmail** (termasuk kalender dan kontak), file **Google Drive**, atau keduanya. Administrator perusahaan dapat melihat kuota dan penggunaan pada portal manajemen.
- **Shared Drive Google Workspace**

  Kuota ini diterapkan oleh penyedia layanan ke seluruh perusahaan. Kuota ini mengaktifkan atau menonaktifkan kemampuan untuk melindungi Shared Drive Google Workspace. Jika kuota diaktifkan, drive Shared dalam jumlah berapa pun dapat dilindungi. Administrator perusahaan tidak dapat melihat kuota di portal manajemen, namun dapat melihat jumlah penyimpanan yang digunakan oleh cadangan drive Shared dalam laporan penggunaan.

  Mencadangkan Shared Drive Google Workspace hanya tersedia untuk pelanggan yang memiliki setidaknya satu kuota Kursi Google Workspace tambahan. Kuota ini hanya diverifikasi dan tidak akan digunakan.

Kursi Microsoft 365 dianggap terlindungi selama setidaknya satu rencana proteksi diterapkan pada kotak surat atau OneDrive pengguna. Kursi Google Workspace dianggap terlindungi selama setidaknya ada satu rencana proteksi yang diterapkan pada kotak surat atau Google Drive pengguna.

Saat kelebihan untuk sejumlah tempat terlampaui, administrator perusahaan tidak dapat menerapkan rencana proteksi ke lebih banyak tempat.

Kuota untuk penyimpanan

- **Cadangan lokal**

  Kuota **Cadangan lokal** membatasi ukuran total cadangan lokal yang dibuat menggunakan infrastruktur awan. Kelebihan tidak dapat ditetapkan untuk kuota ini.
- **Sumber daya awan**

  Kuota **Sumber daya awan** menggabungkan kuota untuk penyimpanan cadangan dan kuota untuk pemulihan bencana. Kuota penyimpanan cadangan membatasi ukuran total cadangan yang terletak di penyimpanan awan. Saat kelebihan kuota penyimpanan cadangan terlampaui, pencadangan akan gagal.

Melampaui kuota untuk penyimpanan cadangan

Kuota penyimpanan cadangan tidak dapat terlampaui. Sertifikat agen proteksi memiliki kuota teknis yang sama dengan kuota cadangan + kelebihan penyewa. Cadangan tidak dapat dimulai jika kuota terlampaui. Jika kuota dalam sertifikat tercapai selama pembuatan cadangan, tapi belum mencapai kelebihan, pencadangan akan berhasil sepenuhnya. Pencadangan akan gagal jika kelebihan tercapai selama pencadangan.

Contoh:

Penyewa pengguna memiliki ruang bebas sebesar 1 TB dalam kuotanya, dan kelebihan yang dikonfigurasi untuk pengguna ini adalah 5 TB. Pengguna memulai pencadangan. Jika ukuran cadangan yang dibuat adalah, misalnya 3 TB, pencadangan tidak akan berhasil sepenuhnya karena kelebihan terlampaui. Jika ukuran cadangan yang dibuat lebih besar dari 6 TB, cadangan akan gagal jika kelebihan terlampaui.

Transformasi kuota cadangan

Secara umum, seperti inilah cara mendapatkan kuota cadangan dan pemetaan item penawaran ke jenis sumber daya: sistem membandingkan item penawaran yang tersedia dengan jenis sumber daya, lalu mendapatkan kuota untuk item penawaran yang cocok.

Terdapat juga kemampuan untuk menetapkan kuota item penawaran lainnya, meksipun tidak benar-benar cocok dengan jenis sumber daya. Ini disebut **transformasi kuota cadangan**. Jika tidak ada item penawaran yang sesuai, sistem akan mencoba mencari kuota yang lebih tepat dan mahal untuk jenis sumber daya (transformasi kuota cadangan otomatis). Jika tidak ditemukan sesuatu yang sesuai, Anda dapat secara manual menetapkan kuota layanan ke jenis sumber daya dalam konsol layanan.

Contoh

Anda ingin mencadangkan mesin virtual (stasiun kerja, berbasis agen).

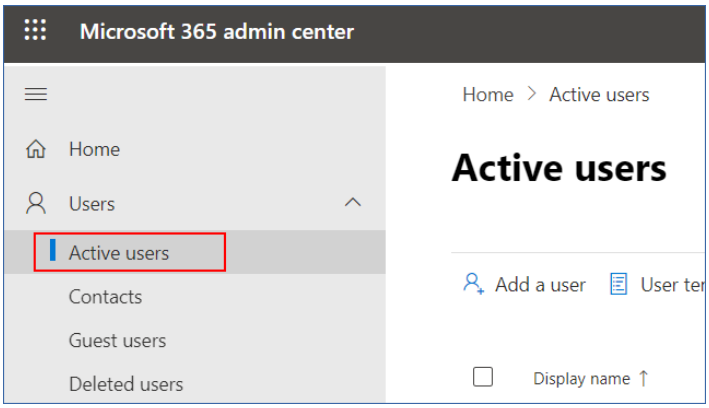
Pertama, sistem akan memeriksa jika ada kuota **Mesin virtual** yang dialokasikan. Jika tidak ditemukan, sistem secara otomatis mencoba untuk memperoleh kuota **Stasiun Kerja**. Jika kuota tersebut tidak ditemukan juga, kuota lain tidak akan diperoleh secara otomatis. Jika Anda memiliki kuota memadai yang lebih mahal dari kuota **Mesin virtual** dan berlaku untuk mesin virtual, Anda dapat login ke konsol layanan dan menetapkan kuota **Server** secara manual.

Mencegah pengguna Microsoft 365 tanpa lisensi untuk masuk

Anda dapat mencegah semua pengguna tanpa lisensi di organisasi Microsoft 365 Anda untuk masuk dengan mengedit status masuk mereka.

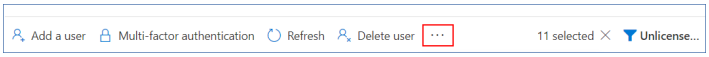
Untuk mencegah pengguna tanpa lisensi yang masuk

1. Masuk ke pusat admin Microsoft 365 (https://admin.microsoft.com) sebagai administrator global.
2. Di menu navigasi, buka **Pengguna** > **Pengguna Aktif**.



3. Klik **Filter**, kemudian pilih **Pengguna tanpa lisensi**.

4. Pilih kotak centang di samping nama pengguna, kemudian klik ikon elipsis (...).



5. Dari menu, pilih **Edit status masuk**.
6. Pilih kotak centang **Blokir pengguna untuk masuk**, kemudian klik **Simpan**.

Kuota Disaster Recovery

Catatan
Item penawaran Pemulihan Bencana hanya tersedia dengan add-on Pemulihan Bencana.

Kuota ini diberlakukan oleh penyedia layanan ke seluruh perusahaan. Administrator perusahaan dapat melihat kuota dan penggunaan pada portal manajemen, namun tidak dapat menetapkan kuota bagi pengguna.

- **Penyimpanan pemulihan bencana**
  Penyimpanan Pemulihan Bencana menunjukkan ukuran penyimpanan dingin dari server yang dilindungi dengan Pemulihan Bencana. Penyimpanan ini dihitung mulai dari saat server pemulihan dibuat, terlepas dari apakah server sedang berjalan atau tidak. Jika kelebihan kuota ini tercapai, membuat server primer dan pemulihan atau menambah/memperpanjang disk dari server primer yang ada tidak mungkin dilakukan. Jika kelebihan untuk kuota ini terlampaui, memulai failover atau memulai server yang dihentikan tidak mungkin dilakukan. Server yang sedang berjalan akan tetap berjalan.
- **Titik komputasi**
  Kuota ini membatasi sumber daya CPU dan RAM yang dikonsumsi oleh server utama dan pemulihan selama masa penagihan. Jika kelebihan untuk kuota ini terlampaui, semua server utama dan pemulihan akan dimatikan. Penggunaan server tersebut tidak dimungkinkan hingga awal masa penagihan berikutnya. Masa pembayaran default adalah satu bulan kalender penuh. Ketika kuota dinonaktifkan, server tidak dapat digunakan terlepas dari periode pembayarannya.
- **Alamat IP publik**

Kuota ini membatasi jumlah alamat IP publik yang dapat ditetapkan ke server utama dan pemulihan. Jika kelebihan untuk kuota ini terlampaui, tidak dimungkinkan untuk mengaktifkan alamat IP publik untuk lebih banyak server. Anda dapat menolak server untuk menggunakan alamat IP publik, dengan mengosongkan kotak centang **Alamat IP publik** pada pengaturan server. Setelah itu, Anda dapat mengizinkan server lain untuk menggunakan alamat IP publik, yang biasanya tidak akan sama.

Ketika kuota dinonaktifkan, semua server akan berhenti menggunakan alamat IP publik, sehingga tidak dapat lagi dijangkau dari internet.

- **Server awan**

  Kuota ini membatasi jumlah total server utama dan pemulihan. Jika kelebihan untuk kuota ini terlampaui, pembuatan server utama atau server pemulihan tidak dimungkinkan.

  Ketika kuota dinonaktifkan, server akan terlihat pada konsol layanan, namun operasi yang tersedia hanyalah **Hapus**.
- **Akses internet**

  Kuota ini mengaktifkan atau menonaktifkan akses internet dari server utama dan pemulihan.

  Ketika kuota dinonaktifkan, server utama dan pemulihan tidak akan dapat terhubung dengan internet.

Kuota File Sync & Share

Anda dapat menentukan kuota File Sync & Share berikut untuk penyewa:

- **Pengguna**

  Kuota menentukan jumlah pengguna yang dapat mengakses layanan ini.

  Akun Administrator tidak dihitung sebagai bagian dari kuota ini.
- **Penyimpanan awan**

  Ini adalah penyimpanan awan untuk menyimpan file-file pengguna. Kuota menentukan ruang yang dialokasikan bagi penyewa dalam penyimpanan awan.

Kuota Pengiriman Data Fisik

Kuota layanan Pengiriman Data Fisik digunakan atas dasar per drive. Anda dapat menyimpan cadangan awal dari beberapa mesin di satu hard drive.

Anda dapat menentukan kuota Pengiriman Data Fisik berikut untuk penyewa:

- **Menuju awan**

  Mengizinkan pengiriman cadangan awal ke pusat data awan menggunakan drive hard disk. Kuota ini menentukan jumlah maksimal drive yang akan dikirim ke pusat data awan.

Kuota Notary

Anda dapat menentukan kuota Notary berikut untuk penyewa:

- **Penyimpanan notaris**

  Penyimpanan notaris adalah penyimpanan awan tempat file yang dinotariskan, ditandatangani, dan file yang sedang berlangsung dinotariskan atau ditandatangi disimpan. Kuota ini menentukan ruang maksimum yang dapat ditempati oleh file-file ini.

  Untuk mengurangi penggunaan kuota ini, Anda dapat menghapus file yang sudah diaktakan atau ditandatangani dari penyimpanan notaris.
- **Notarisasi**

  Kuota ini menentukan jumlah maksimum file yang dapat diaktakan dengan menggunakan layanan notaris. Sebuah file dianggap diaktakan segera setelah diunggah ke penyimpanan notaris dan status notariasinya berubah menjadi Sedang berlangsung.

  Jika file yang sama diaktakan berkali-kali, setiap notarisasi dihitung sebagai yang baru.
- **eSignature**

  Kuota ini menentukan jumlah maksimum file yang dapat ditandatangani dengan menggunakan layanan notaris. Sebuah file dianggap ditandatangani segera setelah dikirim untuk ditandatangani.

Mengubah kuota layanan mesin

Tingkat perlindungan mesin ditentukan dengan kuota layanan yang berlaku. Kuota layanan yang berkaitan dengan item penawaran yang tersedia untuk penyewa dengan mesin terdaftar.

Kuota layanan ditugaskan secara otomatis ketika rencana proteksi diterapkan ke mesin untuk pertama kalinya.

Kuota yang paling sesuai akan ditugaskan, bergantung kepada jenis mesin yang diproteksi, sistem operasinya, tingkat proteksi yang diperlukan, dan ketersedian kuota. Jika kuota yang paling sesuai tidak tersedia di organisasi Anda, kuota kedua terbaiklah yang akan ditugaskan. Misalnya, jika kuota yang paling sesuai adalah **Server Hosting Web** tapi kuota ini tidak tersedia, kuota **Server** yang akan ditugaskan.

Contoh penugasan kuota:

- Mesin fisik yang menjalankan Server Windows atau sistem operasi Linux ditugaskan kuota **Server**.
- Mesin fisik yang menjalankan sistem operasi Windows desktop ditugaskan kuota **Stasiun Kerja**.
- Mesin fisik yang menjalankan Windows 10 dengan mengaktifkan Hyper-V ditugaskan kuota **Stasiun Kerja**.
- Mesin desktop yang berjalan pada infrastruktur desktop virtual dan yang agen proteksinya diinstal di dalam sistem operasi tamu (misalnya, Agen untuk Windows), ditugaskan kuota **Mesin virtual**. Mesin jenis ini juga dapat menggunakan kuota **Stasiun Kerja** jika kuota **Mesin virtual** tidak tersedia.
- Mesin desktop yang berjalan pada infrastruktur desktop virtual dan yang agen proteksinya diinstal di dalam sistem operasi tamu (misalnya, Agen untuk VMware atau Agen untuk Hyper-V), ditugaskan kuota **Mesin virtual**.
- Server Hyper-V atau vSphere ditugaskan kuota **Server**.

- Server dengan cPanel atau Plesk ditugaskan kuota **Server Hosting Web**. Server jenis ini juga dapat menggunakan kuota **Mesin virtual** atau kuota **Server**, tergantung kepada jenis mesin lokasi server web berjalan, jika kuota **Server Hosting Web** tidak tersedia.
- Cadangan keberadaan aplikasi memerlukan kuota **Server**, bahkan untuk sebuah stasiun kerja.

Anda dapat secara manual mengubah tugas asli. Misalnya, untuk menerapkan rencana proteksi lanjutan ke mesin yang sama, Anda mungkin perlu meningkatkan kuota layanan mesin. Jika fitur yang diperlukan oleh rencana proteksi ini tidak didukung dengan kuota layanan yang saat ini ditugaskan, rencana proteksi akan gagal.

Atau, Anda dapat mengubah kuota layanan jika Anda membeli kuota yang lebih sesuai setelah kuota asli ditetapkan. Misalnya, kuota **Stasiun Kerja** ditugaskan ke mesin virtual. Setelah membeli kuota **Mesin virtual**, Anda dapat menugaskan kuota ini secara manual ke mesin, daripada ke kuota **Stasiun Kerja** asli.

Anda juga dapat merilis kuota layanan yang saat ini ditetapkan, lalu menetapkannya ke mesin lain.

Anda dapat mengubah kuota layanan dari masing-masing mesin atau untuk sekelompok mesin.

Untuk mengubah kuota layanan dari masing-masing mesin

1. Di konsol layanan Cyber Protection, buka **Perangkat**.
2. Pilih mesin yang diinginkan, lalu klik **Detail**.
3. Di bagian **Kuota layanan**, klik **Ubah**.
4. Di jendela **Ubah lisensi**, pilih kuota layanan yang diinginkan atau **Tidak ada kuota**, lalu klik **Ubah**.

Untuk mengubah kuota layanan untuk sekelompok mesin

1. Di konsol layanan Cyber Protection, buka **Perangkat**.
2. Pilih lebih dari satu mesin, lalu klik **Tetapkan kuota**.
3. Di jendela **Ubah lisensi**, pilih kuota layanan yang diinginkan atau **Tidak ada kuota**, lalu klik **Ubah**.

Kebergantungan penginstal agen pada item penawaran

Bergantung pada item penawaran yang diperbolehkan, penginstal agen terkait akan tersedia di bagian **Tambah perangkat** di konsol layanan. Dalam tabel di bawah ini, Anda dapat melihat penginstal agen dan ketersediaannya di konsol layanan bergantung pada item penawaran yang diaktifkan.

Mengaktifkan item penawaran	**Server**	**Stasiun Kerja**	**Mesin virtual**	**Kursi Microsoft 365**	**Kursi Google Workspace**	**Perangkat seluler**	**Server web hosting**	**Situs web**
Penginstal agen								

Stasiun kerja – Agen untuk Windows		+	+					+
Stasiun kerja – Agen untuk Mac OS		+	+					+
Server – Agen untuk Windows	+		+				+	+
Server – Agen untuk Linux	+		+				+	+
Agen untuk Hyper-V			+					
Agen untuk VMware			+					
Agen untuk Virtuozzo			+					
Agen untuk SQL	+		+					
Agen untuk Exchange	+		+					
Agen untuk Active Directory	+		+					
Agen untuk Microsoft 365				+				
Agen untuk Google Workspace					+			
Penginstal lengkap untuk Windows	+	+	+				+	+
Seluler (iOS dan Android)						+		

Menggunakan portal manajemen

Langkah berikut akan memandu Anda melalui penggunaan dasar portal manajemen.

Browser web yang didukung

Antarmuka web mendukung browser web berikut:

- Google Chrome 29 ke atas
- Mozilla Firefox 23 ke atas
- Opera 16 ke atas
- Microsoft Edge 25 ke atas
- Safari 8 ke atas yang berjalan di sistem operasi macOS dan iOS

Di browser web lain (termasuk browser Safari yang berjalan di sistem operasi lain), antarmuka pengguna mungkin akan ditampilkan dengan tidak tepat atau beberapa fungsi mungkin tidak tersedia.

Mengaktifkan akun administrator

Setelah menandatangani perjanjian kemitraan, Anda akan menerima pesan email yang berisi informasi berikut:

- **Login Anda.** Ini adalah nama pengguna yang Anda gunakan untuk masuk. Login Anda juga ditampilkan di halaman aktivasi akun.
- Tombol **Aktifkan akun**. Klik tombol dan atur kata sandi untuk akun Anda. Pastikan kata sandi Anda setidaknya sepanjang sembilan karakter. Untuk informasi lebih lanjut tentang kata sandi, lihat "Persyaratan kata sandi" (hlm. 24).

Persyaratan kata sandi

Panjang maksimum kata sandi untuk akun pengguna adalah 9 karakter. Kata sandi juga diperiksa kerumitannya, dan masuk ke dalam salah satu dari kategori berikut:

- Lemah
- Sedang
- Kuat

Anda tidak bisa menyimpan kata sandi yang lemah, meskipun berisi 9 karakter atau lebih. Kata sandi yang menggunakan nama pengguna, login, surel pengguna, atau nama penyewa pemilik akun pengguna selalu dianggap lemah. Sebagian besar kata sandi paling umum juga dianggap lemah.

Untuk memperkuat kata sandi, tambahkan lebih banyak karakter. Menggunakan jenis karakter yang berbeda, seperti digit, huruf besar dan huruf kecil, dan karakter khusus tidak diwajibkan, tetapi akan menghasilkan kata sandi yang kuat dan juga lebih pendek.

Mengakses portal manajemen

1. Buka halaman masuk layanan.
   Alamat halaman masuk disertakan dalam pesan email aktivasi yang Anda terima.
2. Ketik login, lalu klik **Lanjutkan**.
3. Ketik kata sandi, lalu klik **Lanjutkan**.

   Catatan
   Untuk mencegah Cyber Protect Cloud terkena serangan brute-force, portal akan mengunci Anda setelah upaya masuk gagal sebanyak 10x. Periode penguncian adalah 5 menit. Jumlah upaya masuk yang gagal akan diatur ulang setelah 15 menit.

4. Gunakan menu di sebelah kanan untuk menavigasi portal manajemen.

Periode tunggu sewa untuk portal manajemen adalah 24 jam untuk sesi aktif dan 1 jam untuk sesi idle.

Beberapa layanan sudah mencakup kemampuan untuk beralih ke portal manajemen dari konsol layanan.

Mengonfigurasi kontak di wizard profil Perusahaan

Anda dapat mengonfigurasi informasi kontak untuk perusahaan Anda. Kami akan mengirimkan pembaruan fitur baru dan perubahan penting lainnya di platform ke kontak yang Anda berikan.

Saat Anda masuk ke portal manajemen untuk pertama kalinya, wizard profil Perusahaan memandu Anda melalui informasi dasar tentang perusahaan dan kontak yang akan diberikan.

Anda dapat membuat kontak dari pengguna yang sudah ada di platform Cyber Protect atau menambah informasi kontak dari pihak yang tidak memiliki akses ke layanan.

Untuk mengonfigurasi kontak perusahaan menggunakan panduan profil Perusahaan

1. Di **Informasi perusahaan**, tentukan detail berikut mengenai perusahaan Anda:
   - **Nama resmi perusahaan (secara hukum)**
   - **Alamat resmi perusahaan (alamat kantor pusat)**
     - **Negara**
     - **Kode pos**
2. Klik **Berikutnya**.
3. Dalam **Kontak perusahaan**, konfigurasi kontak untuk tujuan berikut:
   - **Kontak penagihan** — Kontak yang akan mendapatkan pembaruan tentang perubahan penting dalam pelaporan penggunaan di platform.
   - **Kontak bisnis**—Kontak yang akan mendapatkan pembaruan tentang perubahan penting terkait bisnis di platform.

- **Kontak teknis**—Kontak yang akan mendapatkan pembaruan tentang perubahan teknis penting di platform.

Anda dapat menggunakan kontak untuk lebih dari satu tujuan.

Pilih opsi untuk membuat kontak.

- **Buat dari pengguna yang sudah ada**. Pilih pengguna dari daftar tarik-turun.
- **Buat kontak baru**. Berikan informasi kontak berikut:
  - **Nama depan** — Nama depan narahubung. Bidang ini wajib diisi.
  - **Nama belakang** — Nama belakang narahubung. Bidang ini wajib diisi.
  - **Surel bisnis** — Alamat surel narahubung. Bidang ini wajib diisi.
  - **Telepon bisnis** — Bidang ini opsional.
  - **Jabatan** — Bidang ini opsional.

4. Jika Anda berencana menggunakan kontak Penagihan sebagai kontak bisnis atau teknis, pilih tanda yang sesuai dalam bagian **Kontak penagihan**:
   - **Gunakan kontak yang sama untuk kontak Bisnis**
   - **Gunakan kontak yang sama untuk kontak Teknis**
5. Klik **Selesai**.

   Hasilnya, kontak dibuat. Anda dapat mengedit informasi dan mengonfigurasi kontak lain di bagian **Manajemen Perusahaan > Profil perusahaan** dari konsol manajemen, seperti yang dijelaskan di Mengonfigurasi kontak perusahaan.

Mengakses konsol Cyber Protection dari portal manajemen

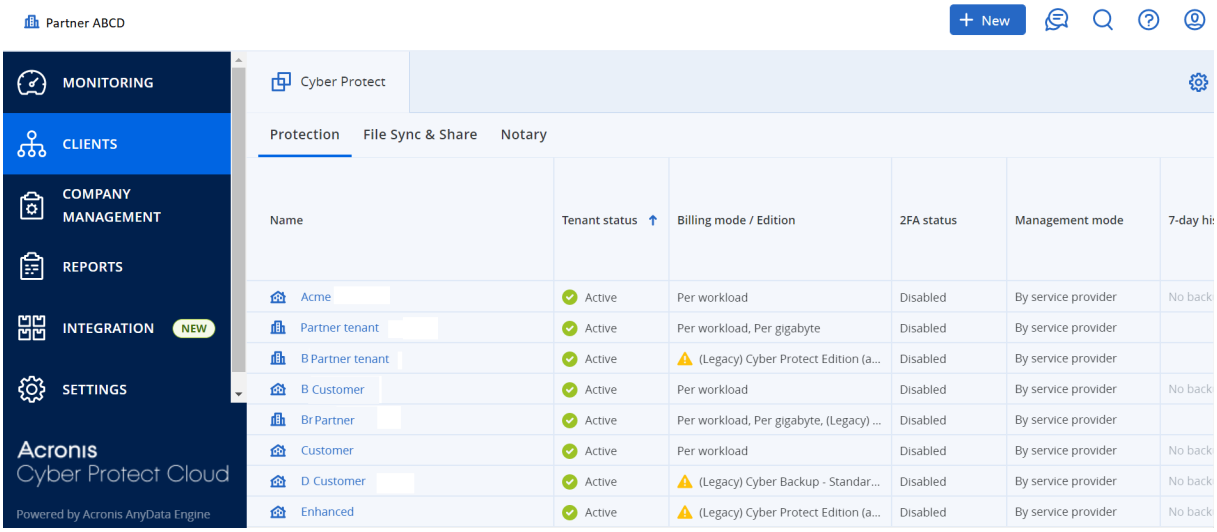
1. Di portal manajemen, buka **Pemantauan** > **Penggunaan**.
2. Di bawah **Perlindungan Cyber**, pilih **Perlindungan**, dan kemudian klik **Kelola layanan**.
   Atau, di bawah **Klien**, pilih pelanggan, lalu klik **Kelola layanan**.

Hasilnya, Anda dialihkan ke konsol Cyber Protection.

Navigasi di portal manajemen

Ketika menggunakan portal manajemen, pada waktu tertentu Anda beroperasi di dalam penyewa. Nama penyewa ini ditunjukkan di pojok kiri atas.

Secara default, tingkat hierarki tertinggi tersedia untuk Anda dipilih. Klik nama penyewa dalam daftar untuk menelusuri hierarki. Untuk menavigasi kembali ke tingkat atas, klik namanya di sudut kiri atas.



Semua bagian antarmuka pengguna hanya menampilkan dan memengaruhi penyewa yang saat ini Anda operasikan. Misalnya:

- Tab **Klien** hanya menampilkan penyewa yang merupakan turunan langsung dari penyewa yang saat ini Anda operasikan.
- Tab **Manajemen Perusahaan** menampilkan profil perusahaan dan akun pengguna yang ada di penyewa tempat Anda beroperasi saat ini.
- Dengan menggunakan tombol **Baru**, Anda dapat membuat penyewa atau akun pengguna baru hanya di penyewa yang saat ini Anda operasikan.

Membatasi akses ke antarmuka web

Administrator dapat membatasi akses ke antarmuka web dengan menentukan daftar alamat IP dari anggota penyewa yang diizinkan masuk.

Pembatasan ini juga berlaku untuk mengakses portal manajemen melalui API.

Pembatasan ini hanya berlaku pada tingkat yang ditetapkan. Pembatasan ini *tidak* diterapkan pada anggota penyewa turunan.

Untuk membatasi akses ke antarmuka web

1. Masuk ke portal manajemen.
2. Navigasikan ke penyewa yang ingin Anda batasi aksesnya.
3. Klik **Pengaturan** > **Keamanan**.
4. Aktifkan switch **Kontrol login**.
5. Pada **Alamat IP yang diizinkan**, tentukan alamat IP yang diizinkan.
   Anda dapat masukkan parameter berikut, dipisah dengan titik koma:
   - Alamat IP, misalnya: 192.0.2.0
   - Rentang IP, misalnya: 192.0.2.0-192.0.2.255

- Subnet, misalnya: 192.0.2.0/24

6. Klik **Simpan**.

Catatan
Untuk penyedia layanan yang menggunakan Cyber Infrastructure (model hybrid):

Jika tombol **Kontrol login** diaktifkan di menu **Pengaturan** > **Keamanan** di portal manajemen, tambahkan alamat IP publik eksternal dari simpul Cyber Infrastructure ke daftar **Alamat IP yang diizinkan**.

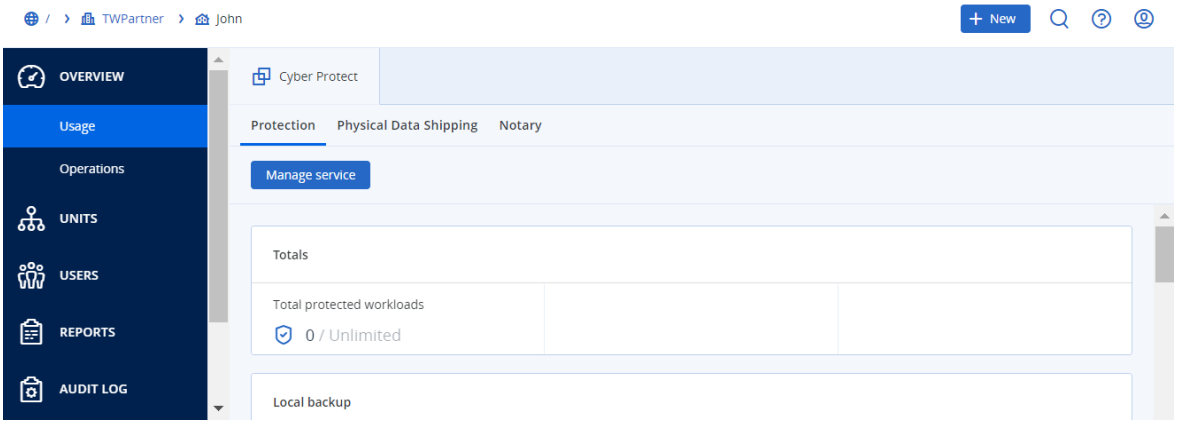
Mengakses layanan

Tab Ikhtisar

Bagian **Ikhtisar** > **Penggunaan** menyajikan ikhtisar penggunaan layanan dan memungkinkan Anda untuk mengakses layanan pada penyewa yang Anda operasikan.

Untuk mengelola layanan bagi penyewa menggunakan tab Ikhtisar

1. Arahkan ke penyewa yang ingin Anda kelola layanannya, lalu klik **Ikhtisar** > **Penggunaan**.
   Harap dicatat bahwa beberapa layanan dapat dikelola pada tingkat penyewa mitra dan penyewa pelanggan, sementara layanan lainnya dapat dikelola hanya pada tingkat penyewa pelanggan.
2. Klik nama layanan yang ingin Anda kelola, lalu klik **Kelola layanan** atau **Konfigurasi layanan**.
   Untuk informasi tentang cara menggunakan layanan, lihat panduan pengguna yang tersedia pada konsol layanan.

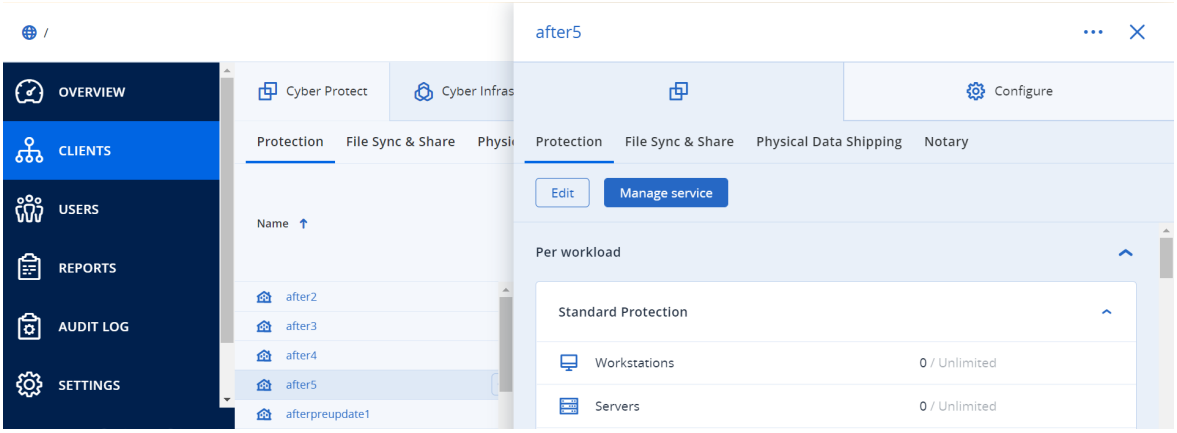


Tab Klien

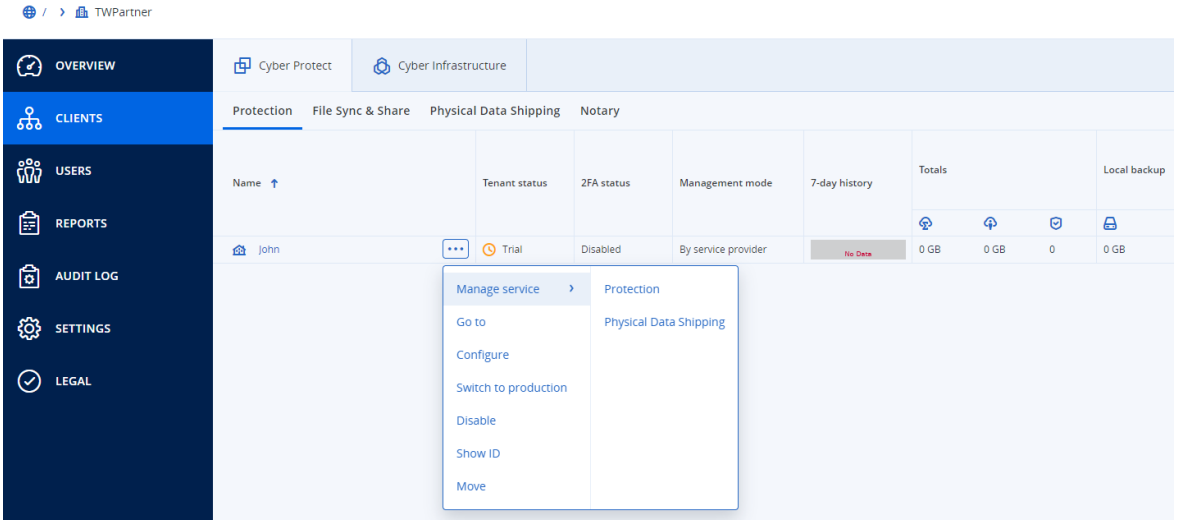
Tab **Klien** menampilkan penyewa turunan dari penyewa yang Anda operasikan dan memungkinkan Anda untuk mengakses layanan mereka.

Untuk mengelola layanan bagi penyewa menggunakan tab Klien

1. Lakukan salah satu langkah berikut:
   - Klik **Klien**, pilih penyewa yang layanannya ingin Anda kelola, klik nama atau ikon layanan yang ingin Anda kelola, lalu klik **Kelola layanan** atau **Konfigurasi layanan**.



   - Klik **Klien**, klik ikon elipsis di samping nama penyewa yang layanannya ingin Anda kelola, klik **Kelola layanan**, lalu pilih layanan yang ingin Anda kelola.



   Harap dicatat bahwa beberapa layanan dapat dikelola pada tingkat penyewa mitra dan penyewa pelanggan, sementara layanan lainnya dapat dikelola hanya pada tingkat penyewa pelanggan. Untuk informasi tentang cara menggunakan layanan, lihat panduan pengguna yang tersedia pada konsol layanan.

Bilah riwayat 7 hari

Pada layar **Klien**, bilah **Riwayat 7 hari** menampilkan status cadangan beban kerja untuk setiap penyewa pelanggan selama tujuh hari terakhir. Bilah dibagi menjadi 168 baris berwarna. Setiap baris merepresentasikan interval satu jam, dan menampilkan status terburuk suatu cadangan dengan interval satu jam yang terkait.

Tabel berikut ini memberikan informasi tentang arti setiap warna baris tersebut.

Warna	Deskripsi
merah	setidaknya salah satu cadangan selama periode satu jam tersebut gagal
jingga	setidaknya salah satu cadangan selama periode satu jam tersebut selesai dengan peringatan, namun tanpa kesalahan cadangan
hijau	terdapat setidaknya satu cadangan yang sukses selama periode satu jam tersebut, tanpa peringatan dan kesalahan cadangan
abu-abu	tidak ada cadangan yang selesai selama periode satu jam tersebut

Bilah **Riwayat 7 hari** menunjukkan "Tidak ada cadangan" hingga statistik terkait dikumpulkan.

Untuk mitra penyewa, bilah **Riwayat 7 hari** kosong, karena statistik agregat tidak didukung.

Akun pengguna dan penyewa

Terdapat dua jenis akun pengguna: akun administrator dan akun pengguna.

- **Administrator** memiliki akses ke portal manajemen. Mereka memiliki hak administrator pada semua layanan.
- **Pengguna** tidak memiliki akses ke portal manajemen. Akses mereka ke layanan dan peran mereka pada layanan ditentukan oleh administrator.

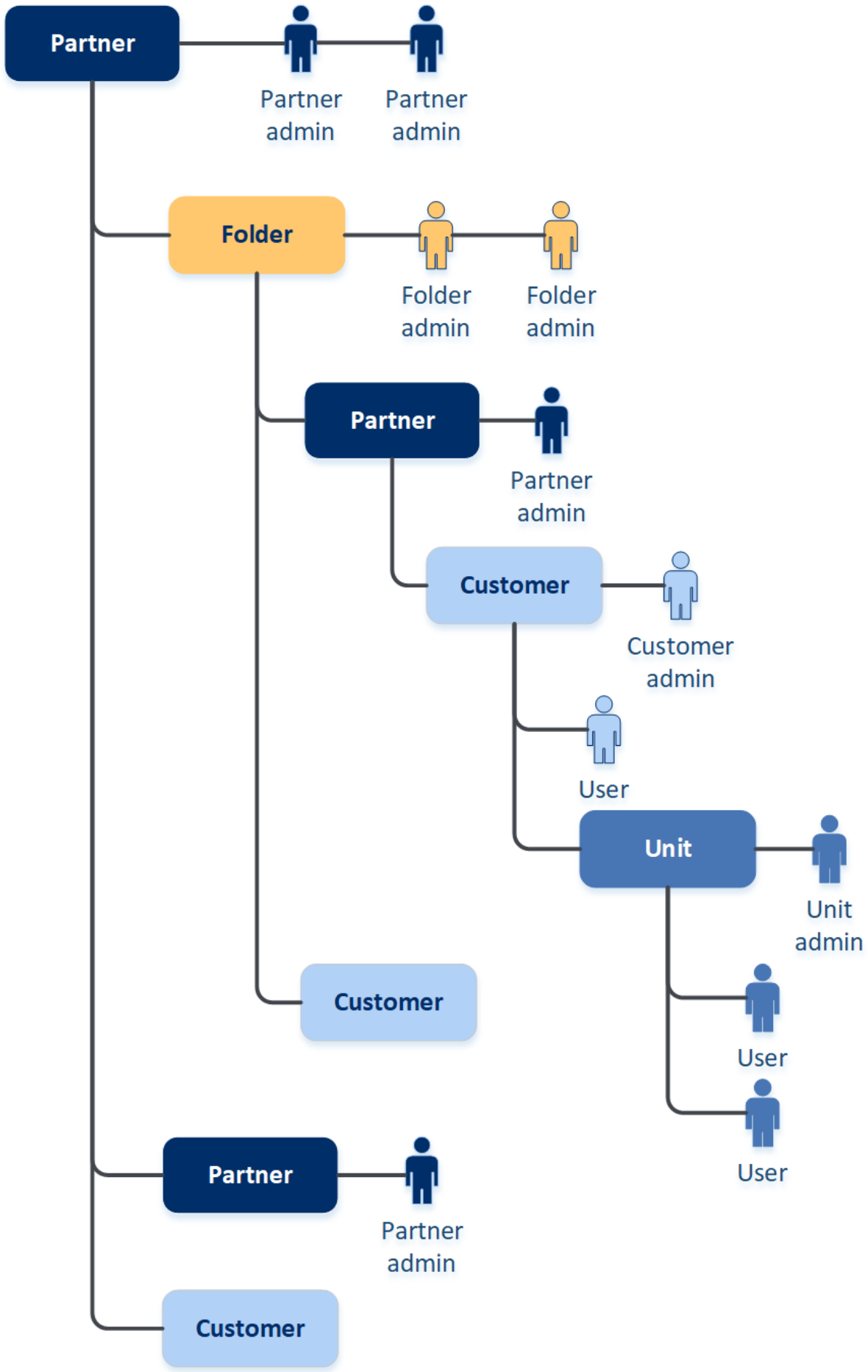
Setiap akun dimiliki penyewa. Penyewa adalah bagian sumber daya portal manajemen (seperti akun pengguna dan penyewa turunan) dan penawaran layanan (layanan yang diaktifkan dan item penawaran di dalamnya) yang didedikasikan untuk mitra atau pelanggan. Hierarki penyewa seharusnya sesuai dengan hubungan klien/vendor antara pengguna layanan dan penyedia layanan.

- Jenis penyewa **Mitra** biasanya sesuai dengan penyedia layanan yang menjual kembali layanan.
- Jenis penyewa **Folder** adalah penyewa tambahan yang biasanya digunakan oleh administrator mitra untuk mitra dan pelanggan grup untuk mengonfigurasi penawaran terpisah dan/atau branding yang berbeda.
- Jenis penyewa **Pelanggan** biasanya sesuai dengan organisasi yang menggunakan layanan.
- Jenis penyewa **Unit-unit** biasanya sesuai dengan unit atau departemen di dalam organisasi.

Administrator dapat membuat dan mengelola penyewa, akun administrator, dan akun pengguna dan atau di bawah tingkat hierarki mereka.

Administrator dari penyewa induk jenis **Mitra** dapat bertindak sebagai administrator tingkat rendah dalam penyewa jenis **Pelanggan** atau **Mitra**, yang mode pengelolaannya **Dikelola oleh penyedia layanan**. Oleh karena itu, administrator tingkat mitra dapat, misalnya, mengelola akun penguna dan layanan, atau mengakses cadangan dan sumber daya lain dalam penyewa turunan. Namun, adminstrator di tingkat rendah dapat membatasi akses ke penyewanya untuk administrator tingkat tinggi.

Diagram berikut menggambarkan contoh hierarki penyewa mitra, folder, pelanggan, dan unit.


Partner
Partner admin
Partner admin
Folder
Folder admin
Folder admin
Partner
Partner admin
Customer
Customer admin
User
Unit
Unit admin
User
User
Customer
Partner
Partner admin
Customer

Tabel berikut merangkum operasi yang dapat dilakukan oleh administrator dan pengguna.

Operasi	Pengguna	Administrator pelanggan dan unit	Administrator mitra dan folder
Membuat penyewa	Tidak	Iya	Iya
Buat akun	Tidak	Iya	Iya
Unduh dan instal perangkat lunak	Iya	Iya	Tidak*
Mengelola layanan	Iya	Iya	Iya
Buat laporan tentang penggunaan layanan	Tidak	Iya	Iya
Mengonfigurasi branding	Tidak	Tidak	Iya

*Administrator mitra yang perlu melakukan operasi ini dapat membuat administrator pelanggan atau akun pengguna untuk dirinya sendiri.

Mengelola penyewa

Penyewa berikut tersedia di Cyber Protect:

- Penyewa **Mitra** biasanya dibuat untuk setiap mitra yang menandatangani perjanjian kemitraan.
- Penyewa **Folder** biasanya dibuat untuk mitra dan pelanggan grup untuk mengonfigurasi penawaran terpisah dan/atau branding berbeda.
- Penyewa **Pelanggan** biasanya dibuat untuk setiap organisasi yang mendaftar layanan.
- Penyewa **Unit** dibuat dalam penyewa pelanggan untuk memperluas layanan ke unit organisasi baru.

Langkah-langkah untuk membuat dan mengonfigurasi penyewa bervariasi menurut penyewa yang Anda buat, tetapi secara umum prosesnya terdiri dari langkah-langkah berikut:

1. Buat penyewa.
2. Pilih layanan untuk penyewa.
3. Konfigurasikan item penawaran untuk penyewa.

Membuat penyewa

1. Masuk ke portal manajemen.
2. Navigasikan ke penyewa di mana Anda ingin membuat penyewa.
3. Di sudut kanan atas, klik **Baru**, lalu klik salah satu dari pilihan berikut, tergantung pada jenis penyewa yang ingin Anda buat:

- Penyewa **Mitra** biasanya dibuat untuk setiap mitra yang menandatangani perjanjian kemitraan.
- Penyewa **Folder** biasanya dibuat untuk mitra dan pelanggan grup untuk mengonfigurasi penawaran terpisah dan/atau branding berbeda.
- Penyewa **Pelanggan** biasanya dibuat untuk setiap organisasi yang mendaftar layanan.
- Penyewa **Unit** dibuat dalam penyewa pelanggan untuk memperluas layanan ke unit organisasi baru.

4. Di bagian **Nama**, tentukan nama penyewa baru.
5. [Hanya saat membuat mitra penyewa] Masukkan **Nama resmi perusahaan (legal)** (wajib diisi) dan **Nomor registrasi Perusahaan/nomor PPN/ID PAJAK** (opsional).
6. [Hanya ketika membuat penyewa pelanggan] Di bagian **Mode**, pilih apakah penyewa menggunakan layanan dalam mode percobaan atau dalam mode produksi. Laporan penggunaan layanan bulanan tidak termasuk data penggunaan untuk penyewa mode percobaan.

   Penting
   Jika Anda mengalihkan mode dari percobaan ke produksi di pertengahan bulan, seluruh bulan akan dimasukkan dalam laporan penggunaan layanan bulanan. Untuk alasan ini, kami sarankan Anda untuk mengalihkan mode di hari pertama setiap bulan. Mode secara otomatis beralih ke produksi saat penyewa tetap dalam mode percobaan selama satu bulan penuh.
   Ada dua kemungkinan skenario untuk mengalihkan mode percobaan penyewa ke mode produksi:
   - Di pertengahan bulan, yang berarti seluruh bulan ***berikutnya*** juga akan dimasukkan dalam laporan penggunaan layanan bulanan.
   - [Opsi yang direkomendasikan] Pada hari pertama setiap bulan – hanya bulan saat ini yang akan dihitung.

7. Dalam **Mode manajemen**, pilih salah satu dari mode berikut untuk mengelola akses ke penyewa:
   - **Layanan mandiri** – mode ini membatasi akses ke penyewa ini untuk administrator penyewa induk: administrator hanya dapat memodifikasi properti penyewa, tetapi tidak dapat mengakses atau mengelola apa pun di dalamnya (misalnya penyewa, pengguna, layanan, cadangan, dan sumber daya lainnya).
   - **Dikelola oleh penyedia layanan** – mode ini memberikan akses penuh ke penyewa untuk administrator penyewa induk: memodifikasi properti; mengelola penyewa, pengguna, dan layanan; mengakses cadangan, dan sumber daya lainnya.

   Hanya administrator penyewa yang Anda buat yang akan dapat mengubah mode Manajemen jika sedang dalam mode **Layanan mandiri**. Untuk ini, administrator dari penyewa yang dibuat dapat membuka **Pengaturan** > **Keamanan** dan mengatur switch **Akses dukungan**.
   Anda dapat memeriksa mode Manajemen yang terpilih untuk penyewa turunan Anda di tab **Klien**.

8. Dalam **Keamanan**, aktifkan atau nonaktifkan autentikasi dua faktor untuk penyewa.
   Jika diaktifkan, semua pengguna pada penyewa ini akan diwajibkan mengatur autentikasi dua faktor untuk akun mereka demi akses yang lebih aman. Pengguna harus menginstal aplikasi autentikasi untuk perangkat faktor kedua mereka dan menggunakan kode TOTP yang dibuat satu kali beserta login dan kata sandi tradisional untuk masuk ke konsol. Untuk detail selengkapnya, lihat "Mengatur autentikasi dua faktor". Untuk melihat status autentikasi dua faktor bagi pelanggan Anda, buka **Klien**.
9. [Hanya saat membuat penyewa pelanggan di Mode keamanan yang ditingkatkan] Di **Keamanan**, pilih kotak centang **Mode keamanan yang ditingkatkan**.
   Dengan mode ini, hanya cadangan yang terenkripsi yang diperbolehkan. Kata sandi enkripsi harus diatur pada perangkat yang dilindungi dan tanpanya, pencadangan akan gagal. Semua operasi yang memerlukan penyediaan kata sandi enkripsi ke layanan awan tidak tersedia. Untuk detail lebih lanjut, lihat "Mode keamanan yang ditingkatkan" (hlm. 35).

   Penting
   Anda tidak dapat menonaktifkan Mode keamanan yang ditingkatkan setelah penyewa dibuat.

10. Di **Buat administrator**, konfigurasikan akun administrator.

    Catatan
    Pembuatan administrator wajib bagi penyewa pelanggan dan penyewa mitra dengan **Mode manajemen** yang diatur menjadi **Layanan mandiri**.

    a. Masukkan nama log masuk dan surel untuk akun administrator. Bidang yang tersisa bersifat opsional, tapi berikan saluran komunikasi lebih lanjut jika seandainya kami memerlukan kontak administrator.
    b. Pilih bahasa.
       Jika Anda tidak memilih bahasa, Bahasa Inggris akan digunakan secara default.
    c. Tentukan kontak perusahaan.
       - **Penagihan**—kontak yang akan mendapatkan pembaruan tentang perubahan penting terkait laporan penggunaan di platform.
       - **Teknis**—kontak yang akan mendapatkan pembaruan tentang perubahan penting terkait teknis di platform.
       - **Bisnis**—kontak yang akan mendapatkan pembaruan tentang perubahan penting terkait bisnis di platform.

         Anda dapat menetapkan lebih dari satu kontak perusahaan ke pengguna.
11. Di **Bahasa**, ubah bahasa default pemberitahuan, laporan, dan perangkat lunak yang akan digunakan dalam penyewa ini.
12. Lakukan salah satu langkah berikut:
    - Untuk menyelesaikan pembuatan penyewa, klik **Simpan dan tutup**. Dengan ini, semua layanan akan diaktifkan untuk penyewa. Mode penagihan untuk layanan Perlindungan akan diatur ke per beban kerja.

- Untuk memilih layanan bagi penyewa, klik **Berikutnya**. Lihat "Memilih layanan untuk penyewa" (hlm. 36).

Mode keamanan yang ditingkatkan

Mode keamanan yang ditingkatkan menyediakan pengaturan spesial untuk klien dengan permintaan keamanan yang ditingkatkan. Mode ini memerlukan enkripsi wajib untuk semua cadangan dan hanya mengizinkan kata sandi enkripsi yang diatur secara lokal.

Administrator mitra dapat mengaktifkan Mode keamanan yang ditingkatkan hanya ketika membuat penyewa pelanggan baru dan tidak dapat menonaktifkan mode ini nantinya. Mustahil untuk mengaktifkan Mode keamanan yang ditingkatkan bagi penyewa yang sudah ada.

Dengan Mode keamanan yang ditingkatkan, semua cadangan yang dibuat di penyewa pelanggan dan unitnya secara otomatis dienkripsi dengan algoritme AES dan kunci 256-bit. Pengguna dapat mengatur kata sandi enkripsi hanya di perangkat terlindungi, dan tidak dapat mengaturnya dalam rencana proteksi.

Layanan awan tidak dapat mengakses kata sandi enkripsi. Karena batasan ini, fitur berikut tidak tersedia untuk penyewa di Mode keamanan yang ditingkatkan:

- Pemulihan melalui konsol layanan
- Penelusuran cadangan di tingkat file melalui konsol layanan
- Pencadangan awan ke awan
- Pencadangan situs web
- Cadangan aplikasi
- Pencadangan perangkat seluler
- Pemindaian antimalware pada cadangan
- Pemulihan aman
- Pembuatan daftar putih korporat otomatis
- Peta perlindungan data
- Pemulihan bencana
- Laporan dan dasbor yang terkait ke fitur yang tidak tersedia

Pembatasan

- Mode keamanan yang ditingkatkan hanya cocok dengan agen yang versinya 15.0.26390 atau lebih tinggi.
- Mode keamanan yang ditingkatkan tidak tersedia untuk perangkat yang menjalankan Red Hat Enterprise LInux 4.x atau 5.x, dan turunannya.

Memilih layanan untuk penyewa

Saat membuat penyewa baru, semua layanan diaktifkan secara default. Anda dapat memilih layanan yang akan tersedia bagi pengguna dalam penyewa dan penyewa turunannya.

Anda juga dapat memilih dan mengaktifkan layanan untuk beberapa penyewa yang ada dalam satu tindakan. Untuk informasi lebih lanjut, lihat "Mengaktifkan layanan untuk beberapa penyewa yang ada" (hlm. 37).

Prosedur ini tidak berlaku untuk penyewa unit.

Untuk memilih layanan bagi penyewa

1. Dalam bagian **Pilih layanan** dialog buat/edit penyewa, pilih mode penagihan atau edisi.
   - Pilih mode penagihan **Per beban kerja** atau **Per gigabyte**, lalu kosongkan kotak centang untuk layanan yang ingin Anda nonaktifkan untuk penyewa.
     Set layanan untuk kedua mode penagihan sama.

     Untuk Pemulihan Bencana Tingkat Lanjut, jika Anda mendaftarkan lokasi pemulihan bencana sendiri di bawah akun Anda, Anda dapat memilih lokasi untuk pemulihan bencana dari daftar drop-down.
   - Untuk menggunakan edisi legasi, pilih tombol radio **Edisi Legasi**, dan pilih edisi dari daftar drop-down.

   Layanan yang dinonaktifkan akan disembunyikan dari pengguna di dalam penyewa dan penyewa turunannya.
2. Lakukan salah satu langkah berikut:
   - Untuk menyelesaikan pembuatan penyewa, klik **Simpan dan tutup**. Dalam hal ini, semua item penawaran untuk layanan terpilih akan diaktifkan untuk penyewa dengan kuota tidak terbatas.
   - Untuk mengonfigurasi item penawaran untuk penyewa, klik **Berikutnya**. Lihat "Mengonfigurasi item penawaran untuk penyewa" (hlm. 36).

Mengonfigurasi item penawaran untuk penyewa

Saat membuat penyewa baru, semua item penawaran untuk layanan terpilih diaktifkan. Anda dapat memilih item penawaran yang akan tersedia bagi pengguna dalam penyewa dan penyewa turunannya, serta mengatur kuota untuk mereka.

Prosedur ini tidak berlaku untuk penyewa unit.

Untuk mengonfigurasi item penawaran untuk penyewa

1. Pada bagian **Layanan konfigurasi** dialog buat/edit penyewa, di bawah setiap tab layanan, hapus kotak centang untuk item penawaran yang ingin Anda nonaktifkan.
   Fungsi yang terkait dengan item penawaran yang dinonaktifkan tidak akan tersedia bagi pengguna dalam penyewa dan penyewa turunannya.

Catatan
Anda dapat menonaktifkan item penawaran yang terkait dengan fungsi perlindungan tingkat lanjut, tetapi item tersebut akan diaktifkan kembali secara otomatis ketika pengguna mengaktifkan fitur tingkat lanjut dalam rencana proteksi.

2. Untuk beberapa layanan, Anda dapat memilih penyimpanan yang akan tersedia untuk penyewa baru. Penyimpanan dikelompokkan berdasarkan lokasi. Anda dapat memilih dari daftar lokasi dan penyimpanan yang ada untuk penyewa Anda.
   - Saat membuat penyewa mitra/folder, Anda dapat memilih beberapa lokasi dan penyimpanan untuk setiap layanan.
   - Saat membuat penyewa pelanggan, Anda harus memilih satu lokasi, lalu memilih satu penyimpanan per layanan dalam lokasi ini. Penyimpanan yang ditetapkan untuk pelanggan dapat diubah kemudian, tetapi hanya jika penggunaannya 0 GB – yaitu, baik sebelum pelanggan mulai menggunakan penyimpanan atau setelah pelanggan menghapus semua cadangan dari penyimpanan ini. Informasi tentang penggunaan ruang penyimpanan tidak diperbarui secara real-time. Tunggu hingga 24 jam agar informasi diperbarui.

   Untuk detail tentang penyimpanan, lihat "Mengelola lokasi dan penyimpanan".
3. Guna menetapkan kuota untuk item, klik tautan **Tak terbatas** di sebelah item penawaran. Kuota ini "lunak". Jika ada nilai yang terlampaui, pemberitahuan email akan dikirim ke administrator penyewa dan administrator penyewa induk. Pembatasan penggunaan layanan tidak diterapkan. Untuk penyewa mitra, diharapkan agar penggunaan item penawaran dapat melebihi kuota karena kelebihan tidak dapat diatur saat membuat penyewa mitra.
4. [Hanya ketika membuat penyewa pelanggan] Tentukan kelebihan kuota.
   Kelebihan memungkinkan penyewa pelanggan untuk melebihi kuota dari nilai yang ditentukan. Saat kelebihan terlampaui, pembatasan penggunaan layanan yang sesuai akan diterapkan.
5. Klik **Simpan dan tutup**.

Penyewa yang baru dibuat akan muncul di tab **Klien** konsol manajemen.

Jika Anda ingin mengedit pengaturan penyewa atau mengubah administrator, pilih penyewa di tab **Klien**, lalu klik ikon pensil di bagian yang ingin Anda edit.

Mengaktifkan layanan untuk beberapa penyewa yang ada

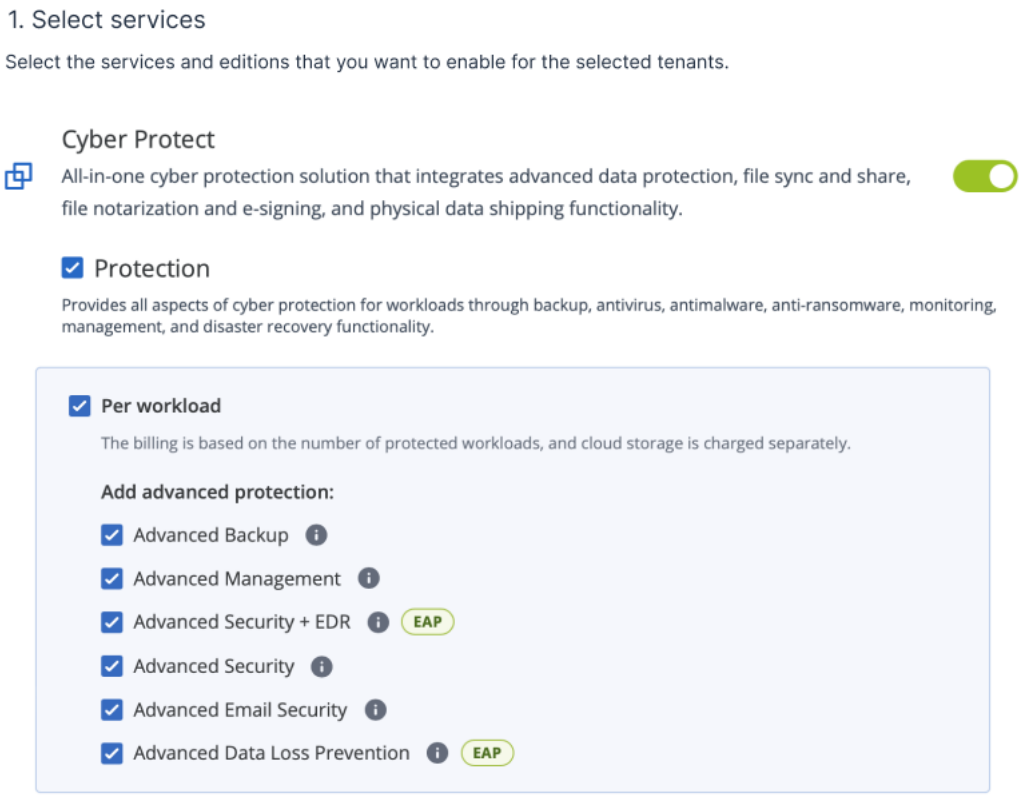
Anda dapat mengaktifkan layanan, edisi, paket, dan item penawaran secara massal untuk beberapa penyewa (hingga maksimum 100 penyewa dalam satu sesi).

Prosedur ini berlaku untuk sub-root, mitra, folder, dan penyewa pelanggan. Penyewa dari jenis yang berbeda ini dapat dipilih secara bersamaan.

Untuk mengaktifkan layanan untuk beberapa penyewa

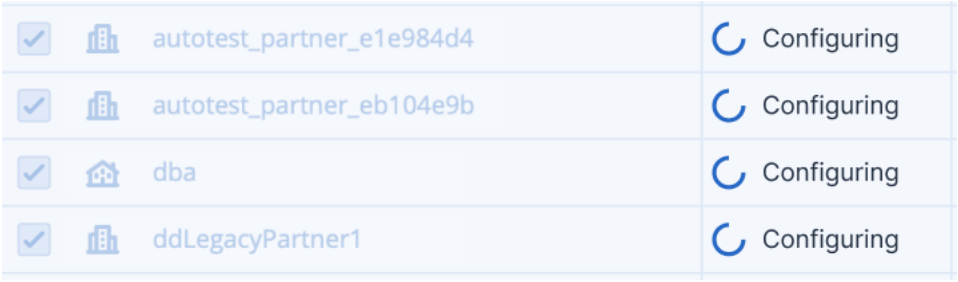
1. Di portal manajemen, buka **Klien**.
2. Di pojok kanan atas, klik **Konfigurasikan layanan**.

3. Pilih setiap penyewa yang ingin Anda aktifkan layanannya dengan mengisi kotak centang di samping nama penyewa, lalu klik **Berikutnya**.
4. Di bagian **Pilih layanan**, pilih layanan terkait yang ingin Anda terapkan ke semua penyewa yang dipilih, lalu klik **Berikutnya**.



Catatan
Anda tidak dapat menonaktifkan layanan yang sebelumnya diaktifkan di layar ini. Semua layanan, edisi, dan item penawaran yang dipilih sebelum Anda memulai prosedur ini akan tetap diaktifkan.

5. Di bagian **Konfigurasi layanan**, pilih fitur layanan dan item penawaran yang ingin Anda aktifkan untuk penyewa yang dipilih, lalu klik **Berikutnya**.
6. Di bagian **Ringkasan**, tinjau perubahan yang akan diterapkan pada penyewa yang dipilih.
   Anda dapat mengeklik **Perluas semua** untuk melihat semua layanan pilihan penyewa dan item penawaran yang akan diterapkan. Atau, Anda dapat memperluas setiap penyewa untuk melihat layanan yang dipilih dan item penawaran khusus untuk penyewa tersebut.
7. Klik **Terapkan perubahan**. Saat layanan dikonfigurasikan untuk setiap penyewa, penyewa dinonaktifkan, dan kolom **Status penyewa** menunjukkan layanan dan item penawaran sedang dikonfigurasi, seperti yang ditampilkan di bawah ini.



8. Saat konfigurasi layanan dan item penawaran berhasil diterapkan ke penyewa yang dipilih, pesan konfirmasi akan ditampilkan.
   Jika karena alasan tertentu layanan dan item penawaran tidak dapat diterapkan ke penyewa, kolom **Status penyewa** menampilkan **Tidak diterapkan**. Klik **Coba lagi** untuk meninjau konfigurasi penyewa yang dipilih.

Mengaktifkan pemberitahuan pemeliharaan

Sebagai pengguna Mitra, Anda dapat mengizinkan penyewa anak (mitra dan pelanggan) untuk menerima surel pemberitahuan pemeliharaan langsung dari pusat data Cyber Protect, dan menerima pemberitahuan pemeliharaan dalam produk di dalam portal Manajemen. Ini akan membantu Anda mengurangi jumlah panggilan dukungan terkait pemeliharaan.

Catatan
Surel pemberitahuan pemeliharaan di-branding oleh pusat data. Branding kustom tidak didukung untuk pemberitahuan ini.

Untuk mengaktifkan pemberitahuan pelanggan untuk mitra atau pelanggan anak

1. Masuk ke portal manajemen sebagai pengguna Mitra, klik **Klien**, dan klik nama mitra atau penyewa pelanggan yang ingin Anda aktifkan pemberitahuan pemeliharaannya.
2. Klik **Konfigurasi**.
3. Di tab **Pengaturan umum**, cari opsi **Pemberitahuan pemeliharaan** dan aktifkan.
   Jika tidak melihat opsi **Pemberitahuan pemeliharaan**, hubungi penyedia layanan.

Catatan
Pemberitahuan pemeliharaan diaktifkan, tetapi tidak akan dikirim hingga penyewa yang dipilih mengaktifkan pemberitahuan untuk pengguna mereka atau menyebarkan opsi ini lebih lanjut ke mitra atau pelanggan anak untuk mengaktifkan pemberitahuan bagi penggunanya.

Untuk mengaktifkan pemberitahuan pemeliharaan untuk pengguna

1. Masuk ke portal manajemen sebagai pengguna Mitra atau Administrator Perusahaan.
   Sebagai Mitra, Anda dapat mengakses pengguna untuk semua penyewa yang Anda kelola.
2. Buka **Manajemen Perusahaan** > **Pengguna** , dan klik nama pengguna yang ingin Anda aktifkan pemberitahuan pemeliharaannya.

3. Pada tab **Layanan**, di bagian **Pengaturan**, klik pensil untuk mengedit opsi.
4. Pilih kotak centang **Pemberitahuan pemeliharaan** dan klik **Selesai**.

Pengguna yang dipilih akan menerima pemberitahuan surel untuk aktivitas pemeliharaan yang akan datang di pusat data.

Mengonfigurasi profil pelanggan yang dikelola sendiri

Sebagai mitra, Anda dapat mengonfigurasi profil pelanggan yang dikelola sendiri untuk penyewa Anda kelola. Opsi ini memungkinkan Anda mengontrol visibilitas profil penyewa dan informasi kontak untuk setiap pelanggan Anda.

Cara mengonfigurasi profil pelanggan yang dikelola sendiri

1. Di portal manajemen, buka **Klien**.
2. Pilih klien pemilik profil pelanggan yang dikelola sendiri yang ingin Anda konfigurasi.
3. Pilih tab **Konfigurasikan**, lalu pilih tab **Pengaturan umum**.
4. Aktifkan atau nonaktifkan tombol **Aktifkan profil pelanggan yang dikelola sendiri**.

Ketika profil pelanggan yang dikelola sendiri diaktifkan, klien ini akan melihat bagian **Profil perusahaan** di menu navigasi dan bidang terkait kontak di wizard pembuatan pengguna (**Telepon kantor**, **Kontak perusahaan**, dan **Jabatan**).

Ketika profil pelanggan yang dikelola sendiri dinonaktifkan, bagian **Profil perusahaan** di menu navigasi dan bidang terkait kontak di wizard pembuatan pengguna akan disembunyikan.

Mengonfigurasi kontak perusahaan

Sebagai mitra, Anda dapat mengonfigurasi informasi kontak untuk perusahaan Anda dan untuk penyewa yang dikelola oleh Anda. Kami akan mengirimkan pembaruan fitur baru dan perubahan penting lainnya di platform ke kontak dalam daftar ini.

Anda dapat menambahkan beberapa kontak dan menetapkan kontak perusahaan, bergantung pada peran pengguna. Anda dapat membuat kontak dari pengguna yang sudah ada di platform Cyber Protect atau menambah informasi kontak dari pihak yang tidak memiliki akses ke layanan.

Untuk mengonfigurasi kontak untuk perusahaan Anda

1. Di konsol manajemen, buka **Manajemen Perusahaan** > **Profil perusahaan**.
2. Di bagian **Kontak**, klik **+**.
3. Pilih opsi untuk membuat kontak.
   - **Buat dari pengguna yang sudah ada**
     - Pilih pengguna dari daftar drop-down.
     - Pilih kontak perusahaan.
       - **Penagihan**—kontak yang akan mendapatkan pembaruan tentang perubahan penting terkait laporan penggunaan di platform.

        - **Teknis**—kontak yang akan mendapatkan pembaruan tentang perubahan penting terkait teknis di platform.
        - **Bisnis**—kontak yang akan mendapatkan pembaruan tentang perubahan penting terkait bisnis di platform.

        Anda dapat menetapkan lebih dari satu kontak perusahaan ke pengguna.

      Jika Anda menghapus kontak yang terkait dengan pengguna dari daftar kontak di profil Perusahaan, pengguna tidak akan dihapus. Sistem akan membatalkan penetapan semua kontak perusahaan untuk pengguna, sehingga tidak akan muncul lagi di kolom **Kontak perusahaan** di daftar **Pengguna**.

      Jika Anda perlu mengubah alamat surel kontak yang terkait dengan pengguna, sistem akan meminta verifikasi dari alamat baru yang ditetapkan. Sebuah surel akan dikirim ke alamat ini, dan pengguna harus mengonfirmasi perubahan tersebut.
- **Buat kontak baru**
  - Berikan informasi kontak.
    - **Nama depan**—Nama depan narahubung. Bidang ini wajib diisi.
    - **Nama belakang**—Nama belakang narahubung. Bidang ini wajib diisi.
    - **Surel bisnis**—Alamat surel narahubung. Bidang ini wajib diisi.
    - **Telepon bisnis**—Bidang ini opsional.
    - **Jabatan**—Bidang ini opsional.
  - Pilih **Kontak perusahaan**.
    - **Penagihan**—kontak yang akan mendapatkan pembaruan tentang perubahan penting terkait laporan penggunaan di platform.
    - **Teknis**—kontak yang akan mendapatkan pembaruan tentang perubahan penting terkait teknis di platform.
    - **Bisnis**—kontak yang akan mendapatkan pembaruan tentang perubahan penting terkait bisnis di platform.

      Anda dapat menetapkan lebih dari satu kontak perusahaan ke pengguna.
4. Klik **Tambah**.

Untuk mengonfigurasi kontak untuk penyewa

Catatan
Jika Anda memodifikasi informasi kontak untuk penyewa turunan, perubahan Anda akan terlihat ke penyewa.

1. Di portal manajemen, buka **Klien**.
2. Klik penyewa, dan klik **Konfigurasi**.
3. Di bagian **Kontak**, klik **+**.
4. Pilih opsi untuk membuat kontak.

- **Buat dari pengguna yang sudah ada**
  - Pilih pengguna dari daftar drop-down.
  - Pilih kontak perusahaan.
    - **Penagihan**—kontak yang akan mendapatkan pembaruan tentang perubahan penting terkait laporan penggunaan di platform.
    - **Teknis**—kontak yang akan mendapatkan pembaruan tentang perubahan penting terkait teknis di platform.
    - **Bisnis**—kontak yang akan mendapatkan pembaruan tentang perubahan penting terkait bisnis di platform.

      Anda dapat menetapkan lebih dari satu kontak perusahaan ke pengguna.

    Jika Anda menghapus kontak yang terkait dengan pengguna dari daftar kontak di profil Perusahaan, pengguna tidak akan dihapus. Sistem akan membatalkan penetapan semua kontak perusahaan untuk pengguna, sehingga tidak akan muncul lagi di kolom **Kontak perusahaan** di daftar **Pengguna**.

    Jika Anda perlu mengubah alamat surel kontak yang terkait dengan pengguna, sistem akan meminta verifikasi dari alamat baru yang ditetapkan. Sebuah surel akan dikirim ke alamat ini, dan pengguna harus mengonfirmasi perubahan tersebut.
- **Buat kontak baru**
  - Berikan informasi kontak.
    - **Nama depan**—Nama depan narahubung. Bidang ini wajib diisi.
    - **Nama belakang**—Nama belakang narahubung. Bidang ini wajib diisi.
    - **Surel bisnis**—Alamat surel narahubung. Bidang ini wajib diisi.
    - **Telepon bisnis**—Bidang ini opsional.
    - **Jabatan**—Bidang ini opsional.
  - Pilih **Kontak perusahaan**.
    - **Penagihan**—kontak yang akan mendapatkan pembaruan tentang perubahan penting terkait laporan penggunaan di platform.
    - **Teknis**—kontak yang akan mendapatkan pembaruan tentang perubahan penting terkait teknis di platform.
    - **Bisnis**—kontak yang akan mendapatkan pembaruan tentang perubahan penting terkait bisnis di platform.

      Anda dapat menetapkan lebih dari satu kontak perusahaan ke pengguna.

5. Klik **Tambah**.

Refreshing data penggunaan untuk penyewa

Secara default, data penggunaan di-refresh pada interval tetap. Anda dapat me-refresh data penggunaan untuk penyewa secara manual.

1. Pada manajemen konsol manajemen, buka **Klien**.
2. Klik penyewa, dan klik elipsis pada baris penyewa.

3. Pilih **Refresh penggunaan**.

   Catatan
   Mengambil data dapat memerlukan waktu hingga 10 menit.

4. Muat ulang halaman untuk melihat data yang diperbarui.

Menonaktifkan dan mengaktifkan penyewa

Anda dapat menonaktifkan penyewa untuk sementara. Misalnya, apabila penyewa Anda ragu-ragu untuk menggunakan layanan.

Untuk menonaktifkan penyewa

1. Di portal manajemen, buka **Klien**.
2. Pilih penyewa yang ingin Anda nonaktifkan, lalu klik ikon elipsis > **Nonaktifkane**.
3. Konfirmasi tindakan Anda dengan mengklik **Nonaktifkan**.

Hasilnya:

- Penyewa dan semua subpenyewanya akan dinonaktifkan, layanan mereka akan dihentikan.
- Penagihan dari penyewa dan sub-penyewanya akan dilanjutkan karena data mereka akan dipertahankan dan disimpan di Cyber Protect Cloud.
- Semua klien API dalam penyewa dan subpenyewa akan dinonaktifkan dan semua integrasi menggunakan klien ini akan berhenti bekerja.

Untuk mengaktifkan penyewa, pilih di daftar klien, lalu klik ikon elipsis > **Aktifkan**.

Memindahkan penyewa ke penyewa lain

Portal manajemen memungkinkan Anda untuk memindahkan penyewa dari satu penyewa induk ke penyewa induk lainnya. Ini mungkin berguna jika Anda ingin mentransfer pelanggan dari satu mitra ke mitra lain, atau jika Anda membuat penyewa folder untuk mengelola klien Anda dan ingin memindahkan beberapa dari mereka ke penyewa folder yang baru dibuat.

Jenis penyewa yang dapat dipindahkan

Jenis penyewa	Dapat dipindahkan	Penyewa target
Mitra	Iya	Mitra atau Folder
Folder	Iya	Mitra atau Folder
Pelanggan	Iya	Mitra atau Folder
Unit	Tidak	Tidak ada

Persyaratan dan pembatasan

- Anda dapat memindahkan penyewa hanya jika penyewa induk target memiliki kumpulan layanan yang sama atau lebih besar dan item penawaran sebagai penyewa induk asli.
- Ketika memindahkan penyewa pelanggan, semua penyimpanan yang ditetapkan kepada penyewa pelanggan di penyewa induk asli harus ada di penyewa induk target. Hal ini diperlukan karena data yang terkait layanan pelanggan tidak dapat dipindahkan dari satu penyimpanan ke penyimpanan lain.
- Di penyewa pelanggan yang dikelola oleh penyedia layanan, mungkin ada rencana yang diterapkan pada beban kerja pelanggan dari tingkat penyedia layanan (misalnya, paket skrip). Ketika memindahkan pelanggan penyewa, rencana penyedia layanan akan dibatalkan dari beban kerja pelanggan dan semua layanan yang terkait dengan rencana ini akan berhenti bekerja untuk pelanggan ini.
- Anda dapat memindahkan penyewa dalam hierarki akun mitra. Anda juga dapat memindahkan penyewa pelanggan ke pelanggan target di luar hirarki akun mitra Anda. Untuk mempelajari apakah operasi tersebut dapat dilakukan, hubungi manajer akun Anda di .
- Hanya administrator (seperti Administrator di Portal Manajemen atau administrator Perusahaan) yang dapat memindahkan penyewa ke induk penyewa yang berbeda.

Cara memindahkan penyewa

1. Masuk ke portal manajemen.
2. Dapatkan dan salin **ID Internal** mitra target atau penyewa folder yang penyewanya ingin Anda pindahkan. Lakukan langkah berikut:
   a. Di tab **Klien**, pilih penyewa target yang menjadi tujuan pemindahan penyewa Anda.
   b. Di panel properti penyewa, klik ikon elipsis vertikal, lalu klik **Tampilkan ID**.
   c. Salin string teks yang ditunjukkan dalam bidang **ID Internal**, lalu klik **Batalkan**.
3. Pilih penyewa yang ingin Anda pindahkan, kemudian pindahkan ke mitra/folder target. Lakukan langkah berikut:
   a. Pada tab **Klien**, pilih penyewa yang ingin Anda pindahkan.
   b. Di panel properti penyewa, klik ikon elipsis vertikal, lalu klik **Pindah**.
   c. Tempelkan pengidentifikasi internal penyewa target, lalu klik **Pindah**.

Operasi segera dimulai dan dapat memerlukan waktu hingga 10 menit.

Jika penyewa yang Anda pindahkan memiliki anak penyewa (misalnya, penyewa folder atau mitra dengan penyewa pelanggan di dalamnya), seluruh sub penyewa akan dipindahkan ke penyewa target.

Mengonversikan penyewa mitra ke penyewa folder dan sebaliknya

Portal manajemen memungkinkan Anda untuk mengonversikan penyewa mitra ke penyewa folder.

Hal ini mungkin berguna jika Anda menggunakan penyewa mitra untuk tujuan pengelompokan kemudian ingin mengelola infrastruktur penyewa Anda dengan benar. Hal ini juga berguna jika Anda ingin dasbor operasional menyertakan informasi agregat tentang penyewa.

Anda juga dapat mengonversikan penyewa folder ke penyewa mitra.

Catatan
Konversi ini merupakan operasi yang aman dan tidak memengaruhi pengguna dalam penyewa dan data terkait layanan apa pun.

Untuk mengonversikan penyewa

1. Masuk ke portal manajemen.
2. Pada tab **Klien**, pilih penyewa yang ingin Anda konversikan.
3. Lakukan salah satu langkah berikut:
   - Klik ikon elipsis di samping nama penyewa.
   - Pilih penyewa, lalu klik ikon elipsis pada panel properti penyewa.
4. Klik **Konversikan ke folder** atau **Konversikan ke mitra**.
5. Konfirmasi keputusan Anda.

Membatasi akses ke penyewa Anda

Administrator di tingkat pelanggan dan yang lebih tinggi dapat membatasi akses ke penyewa mereka untuk administrator tingkat yang lebih tinggi.

Jika akses ke penyewa dibatasi, administrator penyewa induk hanya dapat memodifikasi properti penyewa. Mereka sama sekali tidak dapat melihat akun dan penyewa turunan.

Untuk mencegah administrator tingkat yang lebih tinggi mengakses penyewa Anda

1. Masuk ke portal manajemen.
2. Buka **Pengaturan** > **Keamanan**.
3. Nonaktifkan switch **Akses dukungan**.

Akibatnya, administrator penyewa induk akan memiliki akses terbatas ke penyewa Anda. Mereka hanya dapat memodifikasi properti penyewa, tetapi tidak dapat mengakses atau mengelola apa pun di dalamnya (mis. penyewa, pengguna, layanan, cadangan, dan sumber daya lainnya).

Jika switch **Akses dukungan** diaktifkan, administrator penyewa induk akan memiliki akses penuh ke penyewa Anda. Administrator tersebut akan dapat melakukan hal berikut: memodifikasi properti; mengelola penyewa, pengguna, dan layanan; mengakses cadangan, dan sumber daya lainnya.

Menghapus penyewa

Anda mungkin ingin menghapus penyewa untuk membebaskan sumber daya yang digunakannya. Statistik penggunaan akan diperbarui dalam satu hari setelah penghapusan. Untuk penyewa besar

mungkin memerlukan waktu lebih lama.

Sebelum menghapus penyewa, Anda harus menonaktifkannya. Untuk informasi lebih lanjut tentang cara melakukan ini, lihat Menonaktifkan dan mengaktifkan penyewa.

Penting
Menghapus penyewa tidak dapat diubah!

Untuk menghapus penyewa

1. Di portal manajemen, buka **Klien**.
2. Pilih penyewa yang dinonaktifkan yang ingin Anda hapus, lalu klik ikon elipsis > **Hapus**.
3. Untuk mengonfirmasi tindakan Anda, masukkan login Anda, lalu klik **Hapus**.

Hasilnya:

- Penyewa dan subpenyewa tersebut akan dihapus.
- Semua layanan yang diaktifkan dalam penyewa dan subpenyewa akan dihentikan.
- Semua pengguna dalam penyewa dan subpenyewa tersebut akan dihapus.
- Semua mesin dalam penyewa dan subpenyewa tersebut akan menjadi tidak terdaftar.
- Semua data terkait layanan, misalnya cadangan dan file yang disinkronkan, di penyewa dan subpenyewanya akan dihapus.
- Semua klien API dalam penyewa dan subpenyewa akan dihapus dan semua integrasi menggunakan klien ini akan berhenti bekerja.

Mengelola pengguna

Administrator Mitra, Administrator Pelanggan, dan Administrator Unit dapat mengonfigurasi serta mengelola akun pengguna di bawah penyewa yang dapat diakses untuk mereka.

Membuat akun pengguna

Anda mungkin ingin membuat akun tambahan dalam kasus berikut:

- Akun administrator mitra/folder — untuk membagikan tugas manajemen layanan dengan orang lain.
- Akun administrator pelanggan/prospek/unit — untuk mendelegasikan manajemen layanan kepada orang lain yang izin aksesnya akan sangat dibatasi pada pelanggan/prospek/unit yang sesuai.
- Akun pengguna dalam pelanggan atau penyewa unit — untuk memungkinkan pengguna mengakses hanya sebagian layanan.

Perlu diketahui bahwa akun yang ada tidak dapat dipindahkan antar penyewa. Pertama, Anda harus membuat penyewa, lalu mengisinya dengan akun.

Untuk membuat akun pengguna

1. Masuk ke portal manajemen.
2. Navigasikan ke penyewa di mana Anda ingin membuat akun pengguna. Lihat "Navigasi di portal manajemen" (hlm. 26).
3. Di sudut kanan atas, klik **Baru** > **Pengguna**.

   Atau, buka **Manajemen perusahaan > Pengguna**, dan klik **+ Baru**.
4. Tentukan informasi kontak berikut untuk akun:
   - **Masuk**

     Penting
     Setiap akun harus memiliki alamat masuk unik.
   - **Email**

     Penting
     Jika pengguna terdaftar di layanan File Sync & Share, berikan email yang digunakan untuk registrasi File Sync & Share.

     Perhatikan bahwa setiap akun pengguna pelanggan harus memiliki alamat email unik.
   - **Nama depan**
   - **Nama belakang**
   - [Opsional] **Telepon bisnis**

     Catatan
     Kolom seperti **Telepon bisnis**, **Jabatan pekerjaan**, dan **Kontak perusahaan** ditampilkan di panduan pembuatan pengguna hanya jika mitra induk telah mengaktifkan opsi **Aktifkan profil pelanggan yang dikelola sendiri** untuk penyewa pelanggan. Jika tidak, bidang ini tidak ditampilkan.
   - [Opsional] **Jabatan pekerjaan**
   - Di bagian **Bahasa**, ubah bahasa default pemberitahuan, laporan, dan perangkat lunak yang akan digunakan untuk akun ini.
5. [Opsional] Tentukan kontak perusahaan.
   - **Penagihan**—kontak yang akan mendapatkan pembaruan tentang perubahan penting terkait laporan penggunaan di platform.
   - **Teknis**—kontak yang akan mendapatkan pembaruan tentang perubahan penting terkait teknis di platform.
   - **Bisnis**—kontak yang akan mendapatkan pembaruan tentang perubahan penting terkait bisnis di platform.

     Anda dapat menetapkan lebih dari satu kontak perusahaan ke pengguna.

   Anda dapat melihat kontak perusahaan yang ditetapkan untuk pengguna di daftar **Pengguna**, di kolom **Kontak perusahaan**, dan edit akun pengguna untuk mengubah kontak perusahaan jika diperlukan.

6. [Tidak tersedia saat membuat akun di penyewa mitra/folder] Pilih layanan yang akses dan perannya di setiap layanan akan diberikan kepada pengguna.
   Layanan yang tersedia bergantung pada layanan yang diaktifkan untuk penyewa yang akun penggunanya dibuat.
   - Jika Anda memilih kotak centang **Administrator perusahaan**, pengguna akan memiliki akses ke portal manajemen dan peran administrator di semua layanan yang saat ini diaktifkan untuk penyewa. Pengguna juga akan memiliki peran administrator di semua layanan yang akan diaktifkan untuk penyewa di waktu mendatang.
   - Jika Anda memilih kotak centang **administrator Unit**, pengguna akan memiliki akses ke portal manajemen, dan mungkin atau tidak memiliki peran administrator layanan, tergantung pada layanan.
   - Jika tidak, pengguna akan memiliki peran yang Anda tentukan di layanan yang Anda pilih.
7. Klik **Buat**.

Akun pengguna yang baru dibuat muncul di tab **Pengguna** di bawah **Manajemen Perusahaan**.

Jika Anda ingin mengedit pengaturan pengguna atau menentukan pengaturan pemberitahuan dan kuota (tidak tersedia untuk administrator mitra/folder) untuk pengguna, pilih pengguna di tab **Pengguna**, lalu klik ikon pensil di bagian yang ingin Anda edit.

Untuk mengatur ulang kata sandi pengguna

1. Di portal manajemen, buka **Manajemen Perusahaan** > **Pengguna**.
2. Pilih pengguna yang kata sandinya ingin Anda atur ulang, lalu klik ikon elipsis > **Atur ulang kata sandi**.
3. Konfirmasi tindakan Anda dengan mengeklik **Atur ulang**.

Sekarang pengguna dapat menyelesaikan proses pengaturan ulang dengan mengikuti instruksi dalam email yang diterima.

Untuk layanan yang tidak mendukung autentikasi dua faktor (misalnya, registrasi di Cyber Infrastructure), Anda mungkin perlu mengonversi akun pengguna menjadi *Akun layanan* — akun yang tidak memerlukan autentikasi dua faktor.

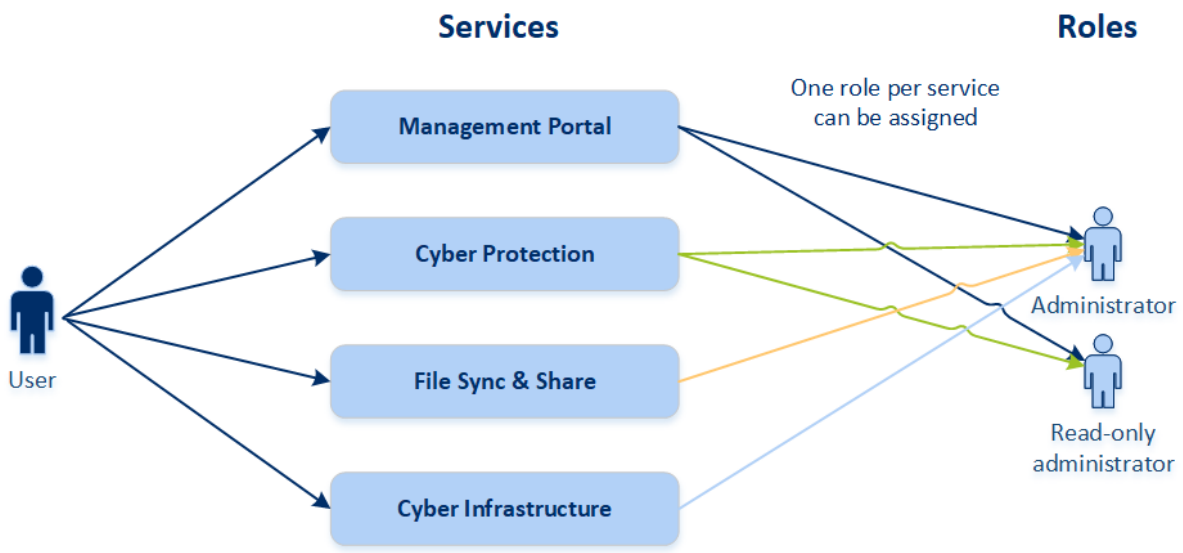
Cara mengonversi akun pengguna menjadi jenis akun layanan

1. Di portal manajemen, buka **Manajemen Perusahaan** > **Pengguna**.
2. Pilih pengguna yang akunnya ingin Anda konversi ke jenis akun layanan, lalu klik ikon elipsis > **Tandai sebagai akun layanan**.
3. Di jendela konfirmasi, masukkan kode autentikasi dua faktor dan konfirmasi tindakan Anda.

Sekarang akun dapat digunakan untuk layanan yang tidak mendukung autentikasi dua faktor.

Peran pengguna yang tersedia untuk setiap layanan

Satu pengguna dapat memiliki beberapa peran, tetapi hanya satu peran per layanan.



Untuk setiap layanan, Anda dapat menentukan peran mana yang akan ditetapkan untuk pengguna.

Layanan	Peran	Deskripsi
n/a	Administrator perusahaan	Peran ini memberikan hak administrator penuh untuk semua layanan. Peran ini memberikan akses ke daftar izin perusahaan. Jika add-on Pemulihan Bencana layanan Cyber Protection diaktifkan untuk perusahaan, peran ini juga memberikan akses ke fungsi pemulihan bencana.
Portal Manajemen	Administrator	Peran ini memberikan akses ke portal manajemen tempat administrator dapat mengelola pengguna dalam seluruh organisasi.
	Administrator hanya baca Level mitra	Peran ini memberikan akses hanya baca ke semua objek di portal manajemen mitra dan portal manajemen semua pelanggan mitra ini. Pengguna tersebut dapat mengakses data pengguna lain dari organisasi dalam mode hanya baca.
	Administrator hanya baca Layanan pelanggan	Peran ini memberikan akses hanya baca ke semua objek di portal manajemen seluruh perusahaan. Pengguna tersebut dapat mengakses data pengguna lain pada organisasi dalam mode hanya baca.
	Administrator hanya baca Level unit	Peran ini menyediakan akses hanya baca ke semua objek di portal manajemen unit dan sub-unit perusahaan. Pengguna tersebut dapat mengakses data pengguna lain pada organisasi dalam mode hanya baca.
Cyber Protection	Administrator cyber	Selain hak peran Administrator, peran ini memungkinkan mengonfigurasi dan mengelola layanan Cyber Protection, serta menyetujui tindakan dalam Pembuatan Skrip Cyber.

		Peran administrator Cyber hanya tersedia untuk penyewa dengan paket Manajemen Tingkat Lanjut yang diaktifkan.
	Administrator	Peran ini memungkinkan untuk mengonfigurasi dan mengelola Cyber Protection bagi pelanggan Anda. Peran ini dibutuhkan untuk mengonfigurasi dan mengelola fungsi Pemulihan Bencana dan daftar izin perusahaan.
	Administrator hanya baca	Peran ini memberikan akses hanya baca untuk semua objek pada layanan Cyber Protection. Pengguna tersebut dapat mengakses data pengguna lain pada organisasi dalam mode hanya baca. Administrator hanya baca tidak dapat mengonfigurasi dan mengelola fungsi Pemulihan Bencana atau daftar izin perusahaan.
	Pulihkan operator	Peran tersebut memberi akses ke cadangan organisasi Microsoft 365 dan Google Workspace, serta memungkinkan pemulihan cadangan tersebut sekaligus membatasi akses ke konten sensitif.
File Sync & Share	Administrator	Peran ini memungkinkan untuk mengonfigurasi dan mengelola File Sync & Share bagi pengguna Anda.
Cyber Infrastructure	Administrator	Peran ini memungkinkan untuk mengonfigurasi dan mengelola Infrastruktur Cyber bagi pengguna Anda.

Peran administrator hanya baca

Akun dengan peran ini memiliki akses hanya baca ke Cyber Protection konsol web dan dapat melakukan hal berikut:

- Mengumpulkan data diagnostik seperti laporan sistem.
- Melihat titik pemulihan cadangan, tetapi tidak dapat menelusuri isi cadangan dan tidak dapat melihat file, folder, atau email.

Administrator hanya baca tidak dapat melakukan hal berikut:

- Memulai atau menghentikan tugas apa pun.
  Misalnya, administrator hanya baca tidak dapat memulai pemulihan atau menghentikan cadangan yang berjalan.
- Mengakses sistem file pada sumber atau mesin target.
  Misalnya, administrator hanya baca tidak dapat melihat file, folder, atau email pada mesin yang dicadangkan.
- Mengganti pengaturan apa pun.
  Misalnya, administrator hanya baca tidak dapat membuat rencana proteksi atau mengubah pengaturan apa pun.
- Membuat, memperbarui, atau menghapus data apa pun.
  Misalnya, administrator hanya baca tidak dapat menghapus cadangan.

Semua objek UI yang tidak dapat diakses untuk administrator hanya baca tersembunyi, kecuali untuk pengaturan default rencana proteksi. Pengaturan ini ditampilkan, tetapi tombol **Simpan** tidak aktif.

Perubahan apa pun yang berkaitan dengan akun dan peran ditampilkan pada tab **Aktivitas** dengan detail berikut:

- Apa yang berubah
- Siapa yang menerapkan perubahan
- Tanggal dan waktu perubahan

Pulihkan peran operator

Peran ini tersedia hanya di layanan Cyber Protection dan dibatasi untuk cadangan Microsoft 365 dan Google Workspace.

Operator pemulihan dapat melakukan hal berikut:

- Melihat peringatan dan aktivitas.
- Menjelajahi dan me-refresh daftar cadangan.
- Jelajahi cadangan tanpa mengakses kontennya. Operator pemulihan dapat melihat nama file yang dicadangkan serta subyek dan pengirim email yang dicadangkan.
- Cari cadangan (pencarian teks lengkap tidak didukung).
- Pulihkan cadangan awan-ke-awan ke lokasi aslinya dalam organisasi Microsoft 365 atau Google Workspace asli.

Operator pemulihan tidak dapat melakukan hal berikut:

- Hapus peringatan.
- Tambah atau hapus organisasi Microsoft 365 atau Google Workspace.
- Tambah, hapus, atau ganti nama lokasi cadangan.
- Hapus atau ganti nama cadangan.
- Buat, hapus, atau ganti nama folder saat memulihkan cadangan ke lokasi khusus.
- Terapkan rencana pencadangan atau jalankan pencadangan.
- Akses file yang dicadangkan atau konten email yang dicadangkan.
- Unduh file atau lampiran email yang dicadangkan.
- Kirim sumber daya awan yang dicadangkan, seperti email atau item kalender, sebagai email.
- Lihat atau pulihkan percakapan Microsoft 365 Teams.
- Pulihkan cadangan awan-ke-awan ke lokasi yang tidak asli, seperti kotak surat yang berbeda, OneDrive, Google Drive, atau Microsoft 365 Teams.

Peran pengguna dan hak Pembuatan Skrip Cyber

Tindakan yang tersedia dengan skrip dan rencana skrip bergantung pada status skrip dan peran pengguna Anda.

Administrator dapat mengelola objek di penyewa mereka sendiri dan di penyewa anak. Mereka tidak dapat melihat atau mengakses objek pada level administrasi atas, jika ada.

Administrator level bawah hanya memiliki akses hanya baca ke rencana skrip yang diterapkan pada beban kerja mereka oleh administrator level atas.

Peran berikut memberikan hak terkait dengan Pembuatan Skrip Cyber:

- Administrator perusahaan

  Peran ini memberikan hak administrator penuh di semua layanan. Terkait dengan Pembuatan Skrip Cyber, peran ini memberikan hak yang sama dengan peran administrator Cyber.

- Administrator cyber

  Peran ini memberikan izin penuh, termasuk persetujuan skrip yang dapat digunakan di penyewa, dan kemampuan untuk menjalankan skrip dengan status **Pengujian**.
- Administrator

  Peran ini memberikan izin sebagian, dengan kemampuan untuk menjalankan skrip yang disetujui serta membuat dan menjalankan rencana skrip yang menggunakan skrip yang disetujui.
- Administrator hanya baca

  Peran ini memberikan izin terbatas, dengan kemampuan untuk melihat skrip dan rencana proteksi yang digunakan di penyewa.
- Pengguna

  Peran ini memberikan izin sebagian, dengan kemampuan untuk menjalankan skrip yang disetujui serta membuat dan menjalankan rencana skrip yang menggunakan skrip yang disetujui, tetapi hanya pada mesin milik pengguna.

Tabel berikut merangkum semua tindakan yang tersedia, bergantung pada status skrip dan peran pengguna.

Peran	Objek	Status skrip		
		Draf	Pengujian	Disetujui
Administrator cyber Administrator perusahaan	Rencana skrip	Edit (Hapus draf skrip dari rencana) Hapus Mencabut Nonaktifkan Hentikan	Buat Edit Terapkan Aktifkan Jalankan Hapus	Buat Edit Terapkan Aktifkan Jalankan Hapus

			Mencabut Nonaktifkan Hentikan	Mencabut Nonaktifkan Hentikan
	Skrip	Buat Edit Ubah status Klona Hapus Batalkan yang sedang berjalan	Buat Edit Ubah status Jalankan Klona Hapus Batalkan yang sedang berjalan	Buat Edit Ubah status Jalankan Klona Hapus Batalkan yang sedang berjalan
Administrator Pengguna (untuk beban kerja mereka sendiri)	Rencana skrip	Tampilan Mencabut Nonaktifkan Hentikan	Tampilan Batalkan jalankan	Buat Edit Terapkan Aktifkan Jalankan Hapus Mencabut Nonaktifkan Hentikan
	Skrip	Buat Edit Klona Hapus Batalkan yang sedang berjalan	Tampilan Klona Batalkan yang sedang berjalan	Jalankan Klona Batalkan yang sedang berjalan
Administrator hanya baca	Rencana skrip	Tampilan	Tampilan	Tampilan
	Skrip	Tampilan	Tampilan	Tampilan

Mengubah pengaturan pemberitahuan untuk pengguna

Untuk mengubah pengaturan pemberitahuan bagi pengguna, buka **Manajemen Perusahaan** > **Pengguna**. Pilih pengguna yang ingin Anda konfigurasikan notifikasinya, lalu klik ikon pensil di

bagian **Pengaturan**. Pengaturan notifikasi berikut tersedia jika layanan Cyber Protection diaktifkan untuk penyewa di mana pengguna dibuat:

- **Pemberitahuan kuota berlebih** (diaktifkan secara default)
  Notifikasi tentang penggunaan kuota yang terlampaui.
- **Laporan penggunaan terjadwal** (diaktifkan secara default)
  Laporan penggunaan dikirim pada tanggal satu setiap bulannya.
- **Pemberitahuan merek URL** (dinonaktifkan secara default)
  Pemberitahuan tentang berakhirnya masa berlaku sertifikat yang akan datang yang digunakan untuk URL khusus layanan Cyber Protect Cloud. Pemberitahuan dikirim ke semua administrator penyewa yang dipilih - 30 hari, 15 hari, 7 hari, 3 hari, dan 1 hari sebelum berakhirnya masa berlaku sertifikat.
- **Notifikasi kegagalan**, **Pemberitahuan peringatan**, dan **Pemberitahuan sukses** (dinonaktifkan secara default)
  Notifikasi tentang hasil eksekusi rencana proteksi dan hasil operasi pemulihan bencana untuk setiap perangkat.
- **Rekap harian tentang peringatan aktif** (diaktifkan secara default)
  Rekap harian dibuat berdasarkan daftar peringatan aktif yang ada dalam konsol layanan pada saat rekap dibuat. Rekap dibuat dan dikirim satu kali sehari, antara pukul 10.00 dan 23.59 UTC. Waktu saat laporan dibuat dan dikirim bergantung pada beban kerja di pusat data. Jika tidak ada peringatan aktif pada saat itu, rekap tidak dikirim. Rekap tidak termasuk informasi untuk peringatan lampau yang tidak aktif lagi. Contohnya, jika pengguna menemukan cadangan yang gagal dan menghapus peringatannya, atau pencadangan dicoba lagi dan berhasil sebelum rekap dibuat, peringatan tidak akan ada lagi dan tidak akan termasuk dalam rekap.
- **Notifikasi kontrol perangkat** (nonaktif secara default)
  Notifikasi tentang upaya untuk menggunakan perangkat periferal dan port yang dibatasi rencana proteksi dengan modul kontrol perangkat diaktifkan.
- **Notifikasi pemulihan** (diaktifkan secara default)
  Notifikasi tentang tindakan pemulihan pada sumber daya berikut: pesan email dan keseluruhan kotak surat pengguna, folder umum, OneDrive/GoogleDrive: keseluruhan OneDrive dan file atau folder, file SharePoint, Teams: Channel, keseluruhan Team, pesan email, dan situs Team.
  Dalam konteks notifikasi ini, tindakan berikut dianggap sebagai tindakan pemulihan: kirim sebagai email, unduh, atau mulai operasi pemulihan.
- **Notifikasi pencegahan kehilangan data** (dinonaktifkan secara default)
  Notifikasi tentang peringatan pencegahan kehilangan data terkait dengan aktivitas pengguna ini di jaringan.
- **Notifikasi insiden keamanan** (dinonaktifkan secara default)
  Notifikasi tentang malware yang terdeteksi selama pemindaian pada saat diakses, dieksekusi, dan diminta serta tentang deteksi dari mesin perilaku dan mesin pemfilteran URL.
  Terdapat dua opsi yang tersedia: **Dimitigasi** dan **Tidak dimitigasi**. Opsi-opsi ini relevan untuk peringatan insiden Deteksi dan Tanggapan Titik Akhir (Endpoint Detection and Response/EDR),

peringatan EDR dari umpan ancaman, dan peringatan tersendiri (untuk beban kerja yang tidak memiliki EDR yang aktif).

Saat peringatan EDR dibuat, email dikirim ke pengguna yang relevan. Jika status ancaman insiden berubah, email baru akan dikirim. Email tersebut menyertakan tombol tindakan yang memungkinkan pengguna melihat detail insiden (jika dimitigasi), atau untuk menyelidiki dan memulihkan insiden (jika tidak dimitigasi).

- **Pemberitahuan infrastruktur** (dinonaktifkan secara default)
  Pemberitahuan tentang masalah dengan infrastruktur Pemulihan Bencana: saat infrastruktur Pemulihan Bencana tidak tersedia, atau terowongan VPN tidak tersedia.

Semua pemberitahuan dikirim ke alamat email pengguna.

Pemberitahuan yang diterima oleh peran pengguna

Pemberitahuan yang dikirim oleh Cyber Protection bergantung pada peran pengguna.

Tipe pemberitahuan/Peran pengguna	Pengguna	Administrator Pelanggan
Pemberitahuan untuk perangkat sendiri	Iya	Iya
Pemberitahuan untuk semua perangkat di organisasi	n/a	Ya (kecuali **Pemberitahuan insiden keamanan**)
Pemberitahuan untuk Microsoft 365, Google Workspace, dan cadangan berbasis awan lainnya	n/a	Iya

Tipe pemberitahuan/Peran pengguna	Pengguna	Administrator pelanggan dan unit	Administrator mitra dan folder
Pemberitahuan untuk perangkat sendiri	Iya	Iya	n/a*
Pemberitahuan untuk semua perangkat pada penyewa anak	n/a	Iya	Iya
Pemberitahuan untuk Microsoft 365, Google Workspace, dan cadangan berbasis awan lainnya	n/a	Iya	Iya

* Administrator mitra tidak dapat mendaftarkan perangkatnya sendiri, namun dapat membuat akun administrator pelanggan mereka sendiri dan menggunakan akun tersebut untuk menambah perangkat mereka. Lihat Akun pengguna dan penyewa.

Menonaktifkan dan mengaktifkan akun pengguna

Anda mungkin perlu menonaktifkan akun pengguna untuk sementara waktu membatasi aksesnya ke platform awan.

Untuk menonaktifkan akun pengguna

1. Di portal manajemen, buka **Pengguna**.
2. Pilih akun pengguna yang ingin Anda nonaktifkan, lalu klik ikon elipsis > **Nonaktifkan**.
3. Konfirmasi tindakan Anda dengan mengeklik **Nonaktifkan**.

Akibatnya, pengguna ini tidak akan dapat menggunakan platform awan atau menerima pemberitahuan apa pun.

Untuk mengaktifkan akun pengguna yang dinonaktifkan, pilih di daftar pengguna, lalu klik ikon elipsis > **Aktifkan**.

Menghapus akun pengguna

Anda mungkin perlu menghapus akun pengguna secara permanen untuk membebaskan sumber daya yang digunakannya — seperti ruang penyimpanan atau lisensi. Statistik penggunaan akan diperbarui dalam satu hari setelah penghapusan. Untuk akun dengan banyak data, bisa membutuhkan waktu yang lebih lama.

Sebelum menghapus akun pengguna, Anda harus menonaktifkannya. Untuk informasi lebih lanjut tentang cara melakukan ini, lihat Menonaktifkan dan mengaktifkan akun pengguna.

Penting
Menghapus akun pengguna tidak dapat diubah!

Untuk menghapus akun pengguna

1. Di portal manajemen, buka **Pengguna**.
2. Pilih akun pengguna yang dinonaktifkan, lalu klik ikon elipsis > **Hapus**.
3. Untuk mengonfirmasi tindakan Anda, masukkan login Anda, lalu klik **Hapus**.

Hasilnya:

- Akun pengguna ini akan dihapus.
- Semua data milik akun pengguna ini akan dihapus.
- Semua mesin yang berkaitan dengan akun pengguna ini akan menjadi tidak terdaftar.

Mentransfer kepemilikan akun pengguna

Anda mungkin perlu mentransfer kepemilikan akun pengguna jika Anda ingin menjaga akses ke data pengguna yang dibatasi.

Penting
Anda tidak dapat menetapkan kembali konten dari akun yang dihapus.

Untuk mentransfer kepemilikan akun pengguna:

1. Di portal manajemen, buka **Pengguna**.
2. Pilih akun pengguna yang kepemilikannya ingin Anda transfer, lalu klik ikon pensil di bagian **Informasi umum**.
3. Ganti email yang ada dengan email pemilik akun selanjutnya, lalu klik **Selesai**.
4. Konfirmasi tindakan Anda dengan mengklik **Ya**.
5. Biarkan pemilik akun selanjutnya memverifikasi alamat email mereka dengan mengikuti petunjuk yang dikirim ke sana.
6. Pilih akun pengguna yang kepemilikannya Anda transfer, lalu klik ikon elipsis > **Atur ulang kata sandi**.
7. Konfirmasi tindakan Anda dengan mengeklik **Atur ulang**.
8. Biarkan pemilik akun selanjutnya mengatur ulang kata sandi dengan mengikuti petunjuk yang dikirim ke alamat email mereka.

Pemilik baru sekarang dapat mengakses akun ini.

Mengatur autentikasi dua faktor

Autentikasi dua faktor (2FA) adalah suatu jenis autentikasi multifaktor yang memeriksa identitas pengguna menggunakan kombinasi dua faktor berbeda:

- Sesuatu yang diketahui pengguna (PIN atau kata sandi)
- Sesuatu yang dimiliki pengguna (token)
- Sesuatu yang ada dalam diri pengguna (biometrik)

Autentikasi dua faktor memberikan perlindungan ekstra dari akses tidak sah ke akun Anda.

Platform tersebut mendukung autentikasi **Kata Sandi Satu Kali Berbasis Waktu (TOTP)**. Jika autentikasi TOTP diaktifkan dalam sistem, pengguna harus memasukkan kata sandi tradisionalnya dan kode TOTP satu kali untuk mengakses sistem. Dengan kata lain, pengguna memasukkan kata sandi (faktor pertama) dan kode TOTP (faktor kedua). Kode TOTP dihasilkan dalam aplikasi autentikasi pada perangkat faktor kedua milik pengguna pada basis waktu terkini dan rahasia (kode QR atau alfanumerik) yang diberikan platform.

Cara kerjanya

1. Anda mengaktifkan autentikasi dua faktor pada level organisasi Anda.
2. Semua pengguna organisasi Anda harus menginstal aplikasi autentikasi pada perangkat faktor kedua mereka (ponsel, laptop, desktop, atau tablet). Aplikasi ini akan digunakan untuk menghasilkan kode TOTP satu kali. Rekomendasi pengautentikasi:
   - Google Authenticator
     Versi aplikasi iOS (https://apps.apple.com/app/google-authenticator/id388497605)

Versi Android (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2)

- Microsoft Authenticator

  Versi aplikasi iOS (https://apps.apple.com/app/microsoft-authenticator/id983156458)

  Versi Android (https://play.google.com/store/apps/details?id=com.azure.authenticator)

Penting
Pengguna harus memastikan bahwa waktu pada perangkat yang memiliki aplikasi autentikasi diatur dengan benar dan menunjukkan waktu terkini yang sebenarnya.

3. Pengguna organisasi Anda harus masuk kembali ke sistem.
4. Setelah mengisi informasi masuk dan kata sandi, mereka akan diminta untuk mengatur autentikasi dua faktor untuk akun pengguna mereka.
5. Mereka harus memindai kode QR menggunakan aplikasi autentikasi mereka. Jika kode QR tidak dapat dipindai, mereka dapat menggunakan kode TOTP yang ditunjukkan di bawah kode QR dan menambahkannya secara manual ke aplikasi autentikasi.

Penting
Sangatlah direkomendasikan untuk menyimpannya (cetak kode QR, tulis kode TOTP, gunakan aplikasi yang mendukung pencadangan kode di awan). Anda akan membutuhkan kode TOTP untuk mengatur ulang autentikasi dua faktor jika perangkat faktor kedua hilang.

6. Kode TOTP satu kali akan dihasilkan dalam aplikasi autentikasi. Kode tersebut dihasilkan secara otomatis setiap 30 detik.
7. Pengguna harus memasukkan kode TOTP pada layar "Atur autentikasi dua faktor" setelah memasukkan kata sandi mereka.
8. Hasilnya, autentikasi dua faktor untuk pengguna akan siap.

Sekarang, saat pengguna masuk ke dalam sistem, mereka akan diminta untuk mengisi informasi masuk dan kata sandi, serta kode TOTP satu kali yang dihasilkan dari aplikasi autentikasi. Pengguna dapat memberi tanda tepercaya pada browser saat mereka masuk ke sistem, sehingga kode TOTP tidak akan diminta pada saat masuk berikutnya melalui browser ini.

Propagasi pengaturan dua faktor lintas level penyewa

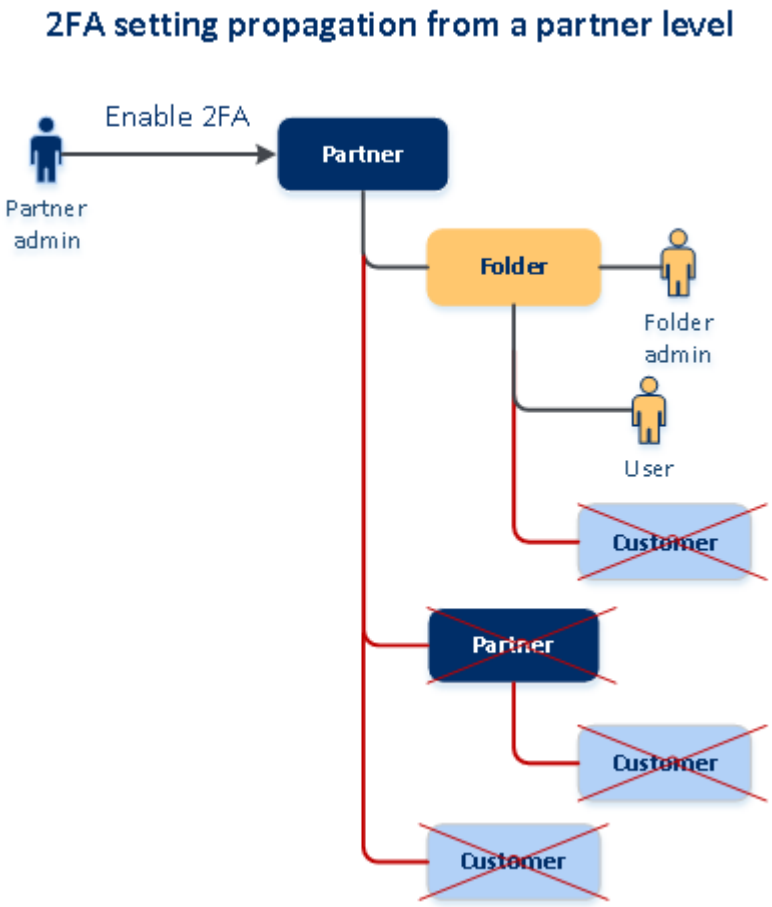
Autentikasi dua faktor diatur pada level **organisasi**. Anda dapat mengaktifkan atau menonaktifkan autentikasi dua faktor:

- Untuk organisasi Anda.
- Untuk penyewa anak Anda (hanya jika opsi **Akses dukungan** diaktifkan dalam penyewa anak).

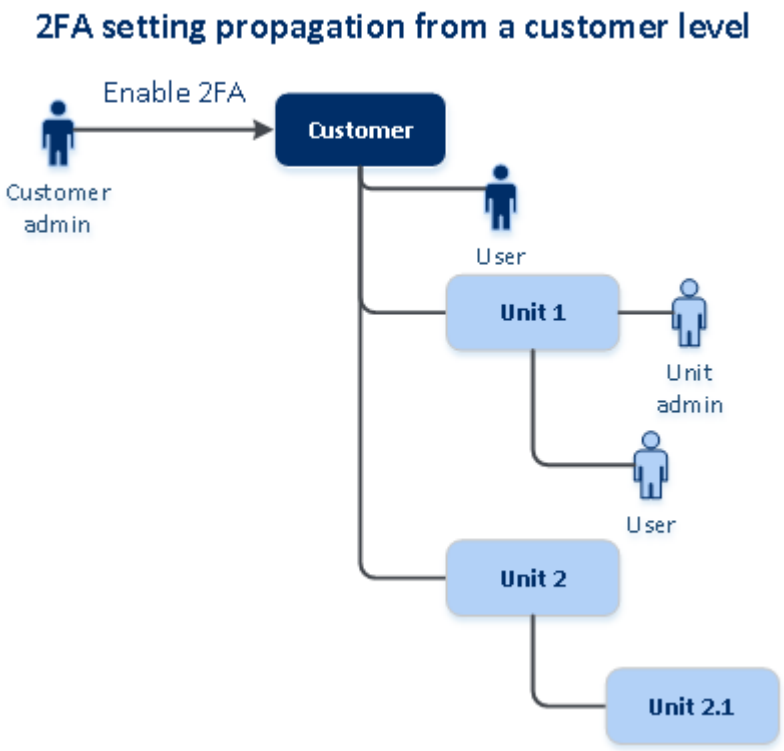
Pengaturan autentikasi dua faktor dipropagasi lintas level pengguna sebagai berikut:

- Folder-folder mewarisi secara otomatis pengaturan autentikasi dua faktor dari organisasi mitra mereka. Dalam skema di bawah ini, garis merah berarti bahwa propagasi pengaturan autentikasi

dua faktor tidak dimungkinkan.



- Unit-unit mewarisi secara otomatis pengaturan autentikasi dua faktor dari organisasi pelanggan mereka.



Catatan

1. Anda dapat mengaktifkan atau menonaktifkan autentikasi dua faktor untuk organisasi anak hanya jika opsi **Akses dukungan** diaktifkan dalam organisasi anak itu.
2. Anda dapat mengelola pengaturan autentikasi dua faktor untuk pengguna dari organisasi anak hanya jika opsi **Akses dukungan** diaktifkan dalam organisasi anak itu.
3. Mengatur autentikasi dua faktor di level folder atau unit tidak dimungkinkan.
4. Anda dapat mengonfigurasi pengaturan autentikasi dua faktor meskipun organisasi induk Anda tidak mengaktifkan pengaturan ini.

Mengatur autentikasi dua faktor untuk penyewa Anda

Sebagai administrator, Anda dapat mengaktifkan autentikasi dua faktor untuk organisasi Anda.

Untuk mengaktifkan autentikasi dua faktor bagi penyewa Anda

1. Di portal manajemen, buka **Pengaturan** > **Keamanan**.
2. Geser toggle **Autentikasi dua faktor**, lalu klik **Aktifkan**.

Kini semua pengguna dalam organisasi harus mengatur autentikasi dua faktor dalam akun mereka. Mereka akan diminta untuk melakukan ini pada saat berikutnya mereka mencoba masuk atau ketika sesi terkini mereka berakhir.

Bilah progres di bawah toggle menunjukkan jumlah pengguna yang telah mengatur autentikasi dua faktor untuk akun mereka. Untuk memeriksa pengguna mana yang telah mengonfigurasi akun mereka, buka tab **Manajemen Perusahaan** > **Pengguna** dan periksa kolom **status 2FA**. Status 2FA

pada pengguna yang belum mengonfigurasi autentikasi dua faktor untuk akun mereka adalah **Pengaturan Diperlukan**.

Setelah berhasil mengonfigurasi autentikasi dua faktor, pengguna harus memasukkan informasi login, kata sandi, dan kode TOTP setiap kali mereka log in ke konsol layanan.

Untuk menonaktifkan autentikasi dua faktor bagi penyewa Anda

1. Di portal manajemen, buka **Pengaturan** > **Keamanan**.
2. Untuk menonaktifkan autentikasi dua faktor, matikan toggle, lalu klik **Nonaktifkan**.
3. [Jika setidaknya satu pengguna mengonfigurasikan autentikasi dua faktor dalam organisasi] Masukkan kode TOTP yang dihasilkan aplikasi autentikasi Anda di perangkat seluler.

Sebagai hasilnya, autentikasi dua faktor dinonaktifkan untuk organisasi Anda, semua rahasia akan dihapus, dan semua browser tepercaya akan dilupakan. Semua pengguna akan masuk ke sistem menggunakan hanya informasi masuk dan kata sandi mereka. Di tab **Manajemen Perusahaan** > **Pengguna**, kolom **status 2FA** akan disembunyikan.

Mengelola autentikasi dua faktor untuk pengguna

Anda dapat memantau pengaturan autentikasi dua faktor untuk semua pengguna Anda dan mengatur ulang pengaturan di portal manajemen, di bawah tab **Manajemen Perusahaan** > **Pengguna**.

Pemantauan

Di portal manajemen, di bawah **Manajemen Perusahaan** > **Pengguna**, Anda dapat melihat daftar semua pengguna di organisasi Anda. **Status 2FA** menunjukkan apakah konfigurasi dua faktor diatur untuk pengguna.

Untuk mengatur ulang autentikasi dua faktor bagi pengguna

1. Di portal manajemen, buka **Manajemen Perusahaan** > **Pengguna**.
2. Di tab **Pengguna**, temukan pengguna yang ingin Anda ubah pengaturannya, lalu klik ikon elipsis.
3. Klik **Atur ulang autentikasi dua faktor**.
4. Masukkan kode TOTP yang dihasilkan di aplikasi autentikasi pada perangkat faktor kedua Anda lalu klik **Atur ulang**.

Hasilnya, pengguna akan dapat mengatur autentikasi dua faktor kembali.

Untuk mengatur ulang browser tepercaya bagi pengguna

1. Di portal manajemen, buka **Manajemen Perusahaan** > **Pengguna**.
2. Di tab **Pengguna**, temukan pengguna yang ingin Anda ubah pengaturannya, lalu klik ikon elipsis.
3. Klik **Atur ulang semua browser tepercaya**.

4. Masukkan kode TOTP yang dihasilkan di aplikasi autentikasi pada perangkat faktor kedua Anda lalu klik **Atur ulang**.

Pengguna yang telah Anda atur ulang semua browser tepercayanya harus mengisi kode TOTP saat masuk berikutnya.

Pengguna dapat mereset semua browser tepercaya dan mereset pengaturan autentikasi dua faktor sendiri. Hal ini dapat selesai jika masuk ke sistem, dengan mengklik tautan yang sesuai dan memasukkan kode TOTP untuk memgonfirmasikan operasi.

Untuk menonaktifkan autentikasi dua faktor bagi pengguna

Kami tidak menyarankan menonaktifkan autentikasi dua faktor karena ini menciptakan potensi pelanggaran dalam keamanan penyewa.

Sebagai pengecualian, Anda dapat menonaktifkan autentikasi dua faktor untuk pengguna dan mempertahankan autentikasi dua faktor untuk semua pengguna penyewa lainnya. Ini adalah solusi untuk kasus ketika autentikasi dua faktor diaktifkan dalam penyewa di mana integrasi awan dikonfigurasi, dan integrasi ini memberi otorisasi ke platform melalui akun pengguna (kata sandi masuk). Untuk terus menggunakan integrasi, sebagai solusi sementara, pengguna dapat diubah menjadi akun layanan yang autentikasi dua faktornya tidak berlaku.

Penting
Mengalihkan pengguna biasa ke pengguna layanan untuk menonaktifkan autentikasi dua faktor tidak disarankan karena menimbulkan risiko bagi keamanan penyewa.

Solusi aman yang disarankan untuk menggunakan integrasi awan tanpa menonaktifkan autentikasi dua faktor untuk penyewa adalah membuat klien API dan mengonfigurasi integrasi awan Anda agar berfungsi dengan klien tersebut.

1. Di portal manajemen, buka **Manajemen Perusahaan** > **Pengguna**.
2. Di tab **Pengguna**, temukan pengguna yang ingin Anda ubah pengaturannya, lalu klik ikon elipsis.
3. Klik **Tandai sebagai akun layanan**. Hasilnya, pengguna akan mendapatkan status autentikasi dua faktor khusus yang disebut **Akun layanan.**
4. [Jika setidaknya seorang pengguna dalam satu penyewa telah mengonfigurasi autentikasi dua faktor] Masukkan kode TOTP yang dihasilkan di aplikasi autentikasi pada perangkat faktor kedua Anda untuk mengonfirmasi penonaktifan.

Untuk mengaktifkan autentikasi dua faktor bagi pengguna

Anda mungkin perlu mengaktifkan autentikasi dua faktor untuk pengguna tertentu yang sebelumnya sudah Anda nonaktifkan.

1. Di portal manajemen, buka **Manajemen Perusahaan** > **Pengguna**.
2. Di tab **Pengguna**, temukan pengguna yang ingin Anda ubah pengaturannya, lalu klik ikon elipsis.

3. Klik **Tandai sebagai akun reguler**. Akibatnya, pengguna harus mengatur autentikasi dua faktor atau mengisi kode TOTP saat memasuki sistem.

Mengatur ulang autentikasi dua faktor jika perangkat faktor kedua hilang

Untuk mengatur ulang akses ke akun Anda apabila perangkat faktor kedua hilang, lakukan salah satu pendekatan berikut ini:

- Kembalikan kode TOTP (kode QR atau kode alfanumerik) Anda dari cadangan.
  Gunakan perangkat faktor kedua lainnya dan tambahkan kode TOTP yang disimpan ke aplikasi autentikasi yang diinstal di perangkat ini.
- Mintalah administrator Anda untuk mengatur ulang pengaturan autentikasi dua faktor bagi Anda.

Perlindungan brute-force

Serangan brute-force merupakan serangan saat penyusup mencoba mendapatkan akses ke sistem dengan memasukkan banyak kata sandi, dengan harapan salah satu benar.

Mekanisme perlindungan brute-force dari platform didasarkan atas cookie perangkat.

Pengaturan untuk perlindungan brute-force yang digunakan ditetapkan sebelumnya:

Parameter	Memasukkan kata sandi	Memasukkan TOTP Kode
Batas upaya	10	5
Periode batas upaya (batas direset setelah waktu habis)	15 men (900 det)	15 men (900 det)
Penguncian terjadi pada	Batas upaya + 1 (upaya ke-11)	Batas upaya
Periode penguncian	5 men (300 det)	5 men (300 det)

Jika Anda memiliki autentikasi dua faktor, cookie perangkat dihasilkan ke klien (browser) hanya setelah autentikasi berhasil menggunakan kedua faktor (kata sandi dan kode TOTP).

Untuk browser tepercaya, cookie perangkat dikeluarkan setelah autentikasi berhasil menggunakan satu faktor saja (kata sandi).

Upaya memasukkan kode TOTP didaftarkan per pengguna, bukan per perangkat. Hal ini berarti bahwa meskipun upaya untuk memasukkan kode TOTP menggunakan perangkat yang berbeda, akan tetap terblokir.

Mengonfigurasi skenario upsell untuk pelanggan Anda

Upselling adalah teknik untuk mengundang pelanggan agar membeli fitur tambahan.

Cyber Protection memiliki beberapa edisi legasi, semuanya memiliki fungsi dan harga yang berbeda. Anda mungkin ingin mempromosikan edisi yang lebih mahal dengan kemampuan lebih canggih untuk pelanggan yang sudah ada yang menggunakan edisi dasar.

Anda dapat mengaktifkan atau menonaktifkan kemampuan upsell bagi pelanggan. Secara default, opsi upsell dinonaktifkan. Jika Anda mengaktifkan upsell untuk pelanggan, mereka akan melihat fungsi tambahan yang tidak tersedia hingga pelanggan membeli edisi yang dipromosikan. Fungsi tambahan ini ditandai dengan label yang menunjukkan nama atau ikon edisi yang dipromosikan, yang semuanya disorot dengan warna oranye. Poin upsell ini akan ditunjukkan kepada pelanggan, untuk memotivasi mereka agar membeli edisi yang lebih mahal. Saat mengeklik poin upsell ini, pelanggan akan melihat dialog yang menyarankan untuk membeli edisi yang lebih mahal guna mengaktifkan fungsi yang diinginkan.

Item tindakan bergantung pada jenis pengguna pelanggan. Jenis pengguna (pembeli atau bukan pembeli) dapat dikonfigurasi menggunakan API platform, untuk perinciannya lihat dokumentasi API. Untuk informasi lebih lanjut tentang item tindakan yang ditampilkan bagi pelanggan Anda, lihat tabel di bawah ini:

Jenis pengguna dalam penyewa pelanggan	Item tindakan
Administrator; pembeli	Tombol **Beli sekarang** ditampilkan di antarmuka pengguna.*
Administrator; bukan pembeli	Pesan "Hubungi mitra Anda untuk meningkatkan edisi" ditampilkan di antarmuka pengguna.
Pengguna; pembeli	Pesan "Hubungi mitra Anda untuk meningkatkan edisi" ditampilkan di antarmuka pengguna.
Pengguna; bukan pembeli	Pesan "Hubungi mitra Anda untuk meningkatkan edisi" ditampilkan di antarmuka pengguna.

* Tautan ke tombol **Beli sekarang**, yang akan mengalihkan pelanggan ke situs web untuk membeli edisi yang lebih lanjut, dapat dikonfigurasi di **Pengaturan** > **Branding**. Di bagian **Upsell**, Anda dapat menentukan **Beli URL**. Pengaturan branding akan diterapkan ke semua mitra/folder turunan dan pelanggan penyewa yang bersifat langsung dan tidak langsung di mana branding dikonfigurasi.

Untuk mengaktifkan atau menonaktifkan kemampuan upsell bagi pelanggan

1. Di portal manajemen, buka **Klien**.
2. Pilih pelanggan, buka panel kanan, lalu klik tab **Konfigurasi**.
3. Di bagian **Upsell**, lakukan hal berikut:
   - Aktifkan **Promosikan edisi lanjutan lain**, untuk mengaktifkan skenario upsell bagi pelanggan.
   - Nonaktifkan **Promosikan edisi lanjutan lain**, untuk menonaktifkan skenario upsell bagi pelanggan.

Poin upsell yang ditampilkan ke pelanggan

Daftar kerentanan

Di konsol layanan, daftar kerentanan dapat ditemukan di **Manajemen perangkat lunak** > **Kerentanan**. Saat pengguna mengeklik ikon jahitan, dialog promosi edisi akan terbuka untuk mendorong pengguna membeli edisi yang lebih mahal.

Membuat atau mengedit rencana proteksi

Di konsol layanan, ini dapat ditemukan di **Rencana** > **Proteksi**. Klik **Buat rencana**. Edisi Cyber Backup hanya memiliki modul aktif **Cadangan** dan **Kerentanan**; modul lainnya tersedia hanya dalam edisi Cyber Protect. Pelanggan Anda akan dapat memperoleh semua modulnya diaktifkan setelah membeli satu edisi Cyber Protect.

Wizard penemuan otomatis

Di konsol layanan, wizard ini dapat ditemukan dalam **Perangkat** > **Semua perangkat**. Pelanggan Anda harus meluncurkan wizard penemuan otomatis dengan mengklik **Tambah**, lalu beralih ke bagian **Beberapa perangkat**, lalu mengklik **hanya Windows**. Metode penemuan mesin otomatis akan tersedia hanya dalam edisi Lanjutan.

Tindakan dalam daftar Perangkat

Di konsol layanan, daftar ini dapat ditemukan dalam **Perangkat** > **Semua perangkat**. Pelanggan Anda harus memilih mesin dan dua opsi tambahan akan ditampilkan di panel kiri:

- **Sambungkan melalui klien HTML5**
- **Patch**

Opsi ini akan tersedia hanya jika pelanggan membeli edisi yang lebih mahal dari edisi yang ada.

Mengelola lokasi dan penyimpanan

Bagian **Pengaturan** > **Lokasi** menampilkan infrastruktur penyimpanan awan dan pemulihan bencana yang dapat Anda gunakan untuk menyediakan layanan **Cyber Protection** dan **File Sync & Share** bagi mitra dan pelanggan Anda.

Penyimpanan yang dikonfigurasi untuk layanan lain akan ditampilkan di bagian **Lokasi** pada rilis mendatang.

Lokasi

Lokasi adalah kontainer yang memungkinkan Anda untuk mengelompokkan penyimpanan awan dan infrastruktur pemulihan bencana dengan mudah. Lokasi ini dapat merepresentasikan apa pun yang Anda pilih, seperti pusat data spesifik atau lokasi geografis komponen infrastruktur Anda.

Anda dapat membuat sejumlah lokasi dan mengisinya dengan penyimpanan cadangan, infrastruktur pemulihan bencana, dan penyimpanan **File Sync & Share**. Lokasi dapat berisi beberapa penyimpanan awan, namun hanya satu infrastruktur pemulihan bencana.

Untuk informasi tentang operasi dan penyimpanan, lihat "Mengelola penyimpanan".

Memilih lokasi dan penyimpanan untuk mitra dan pelanggan

Ketika membuat penyewa mitra/folder, Anda dapat memilih beberapa lokasi dan beberapa penyimpanan per layanan di dalamnya yang akan disediakan bagi penyewa baru.

Saat membuat penyewa pelanggan, Anda harus memilih satu lokasi, lalu memilih satu penyimpanan per layanan dalam lokasi ini. Penyimpanan yang ditetapkan untuk pelanggan dapat diubah kemudian, tetapi hanya jika penggunaannya 0 GB – yaitu, baik sebelum pelanggan mulai menggunakan penyimpanan atau setelah pelanggan menghapus semua cadangan dari penyimpanan ini.

Informasi tentang penyimpanan yang ditetapkan kepada penyewa pelanggan ditampilkan pada panel detail penyewa ketika penyewa memilih di tab **Klien**. Informasi tentang penggunaan ruang penyimpanan tidak diperbarui secara real-time. Tunggu hingga 24 jam agar informasi diperbarui.

Operasi dengan lokasi

Untuk membuat lokasi baru, klik **Tambah lokasi**, lalu tentukan nama lokasi.

Untuk memindahkan penyimpanan atau infrastruktur pemulihan bencana ke lokasi lain, pilih penyimpanan atau infrastruktur, klik ikon pensil di bidang **Lokasi**, lalu pilih lokasi target.

Untuk mengganti nama lokasi, klik ikon elipsis di sebelah nama lokasi, klik **Ganti nama**, lalu tentukan nama lokasi baru.

Untuk menghapus lokasi, klik ikon elipsis di sebelah nama lokasi, klik **Hapus**, lalu konfirmasi keputusan Anda. Hanya lokasi kosong yang dapat dihapus.

Mengelola penyimpanan

Menambahkan penyimpanan baru

- Layanan **Cyber Protection** :
  - Secara default, penyimpanan cadangan berada di pusat data .
  - Jika item penawaran **Penyimpanan cadangan milik mitra** diaktifkan untuk penyewa mitra oleh administrator tingkat atas, administrator mitra dapat mengelola penyimpanan di pusat data mitra sendiri, menggunakan perangkat lunak Cyber Infrastructure. Klik **Tambah penyimpanan pencadangan** di bagian **Lokasi** untuk menemukan informasi tentang mengatur penyimpanan cadangan di pusat data Anda sendiri.
  - Jika item penawaran **Infrastruktur pemulihan bencana yang dimiliki mitra** diaktifkan untuk penyewa mitra oleh administrator tingkat atas, administrator mitra dapat mengelola

infrastruktur pemulihan bencana di pusat data mitra sendiri. Untuk informasi tentang menambahkan infrastruktur pemulihan bencana, hubungi dukungan teknis.

Catatan
Validasi cadangan tidak memungkinkan dengan penyimpanan objek awan publik seperti Amazon S3, Microsoft Azure, Google Cloud Storage, dan Wasabi, yang digunakan oleh pusat data . Validasi cadangan tidak memungkinkan dengan penyimpanan objek awan publik yang digunakan oleh mitra . Namun, mengaktifkannya tidak disarankan karena operasi validasi meningkatkan lalu lintas keluar dari penyimpanan objek publik dan dapat mengarah ke biaya lebih besar.

- Untuk informasi tentang menambahkan penyimpanan yang akan digunakan oleh layanan lain, hubungi dukungan teknis.

Menghapus penyimpanan

Anda dapat menghapus penyimpanan yang telah Anda atau penyewa turunan Anda tambahkan.

Jika penyimpanan ditetapkan ke penyewa pelanggan mana pun, Anda harus menonaktifkan layanan yang menggunakan penyimpanan untuk semua penyewa pelanggan, sebelum menghapus penyimpanan.

Untuk menghapus penyimpanan

1. Masuk ke portal manajemen.
2. Navigasikan ke penyewa tempat penyimpanan ditambahkan.
3. Klik **Pengaturan** > **Lokasi**.
4. Pilih penyimpanan yang ingin Anda hapus.
5. Di panel properti penyimpanan, klik ikon elipsis, lalu klik **Hapus penyimpanan**.
6. Konfirmasi keputusan Anda.

Mengonfigurasi penyimpanan yang tidak dapat diubah

Anda dapat mengonfigurasikan penyimpanan yang tidak dapat diubah pada tingkat mitra dan pada tingkat pelanggan.

Untuk penyewa mitra, tidak ada pilihan mode penyimpanan yang tidak dapat diubah. Administrator dapat menonaktifkan dan mengaktifkan penyimpanan yang tidak dapat diubah, serta mengubah mode dan periode retensinya.

Untuk penyewa pelanggan, penyimpanan yang tidak dapat diubah tersedia dalam mode berikut:

- **Mode tata kelola**
  Dalam mode ini, administrator dapat menonaktifkan dan mengaktifkan penyimpanan yang tidak dapat diubah, serta mengubah mode dan periode retensinya.
- **Mode kepatuhan**

Setelah mode ini dipilih, penyimpanan yang tidak dapat diubah tidak dapat dinonaktifkan, dan mode atau periode retensinya tidak dapat diubah lagi.

Ketika tidak ada pengaturan kustom yang diterapkan ke penyewa turunan, penyewa turunan mewarisi pengaturan penyewa induknya.

Anda dapat mengonfigurasi pengaturan penyimpanan yang tidak dapat diubah hanya jika autentikasi dua faktor diaktifkan untuk penyewa yang memiliki akun administrator.

Cadangan yang dihapus dalam penyimpanan yang tidak dapat diubah masih menggunakan ruang penyimpanan dan dikenakan biaya yang sesuai.

Catatan
Terhitung sejak rilis 21.12, penyimpanan yang tidak dapat diubah dengan periode retensi 14 hari diaktifkan secara default untuk penyewa mitra. Untuk penyewa yang sudah ada, Anda perlu mengaktifkan penyimpanan yang tidak dapat diubah secara manual.

Cara mengaktifkan penyimpanan yang tidak dapat diubah untuk penyewa mitra

1. Masuk ke portal manajemen sebagai administrator lalu buka **Pengaturan** > **Keamanan**.
2. Aktifkan switch **Penyimpanan yang tidak dapat diubah**.
3. Tentukan periode retensi dalam rentang 14 hingga 999 hari.
   Periode retensi default adalah 14 hari. Periode retensi yang lebih lama dapat menyebabkan peningkatan penggunaan penyimpanan.
4. Klik **Simpan**.

Cara menonaktifkan penyimpanan yang tidak dapat diubah untuk penyewa mitra

1. Masuk ke portal manajemen sebagai administrator lalu buka **Pengaturan** > **Keamanan**.
2. Nonaktifkan switch **Penyimpanan yang tidak dapat diubah**.

   Peringatan!
   Perubahan ini akan diambil oleh semua penyewa turunan yang tidak menggunakan pengaturan kustom untuk penyimpanan yang tidak dapat diubah. Semua cadangan yang dihapus akan terhapus secara permanen. Menghapus cadangan baru juga akan menjadi permanen.

3. Konfirmasi pilihan Anda dengan mengeklik **Nonaktifkan**.

Cara mengaktifkan penyimpanan yang tidak dapat diubah untuk penyewa pelanggan

1. Masuk ke portal manajemen sebagai administrator lalu buka **Klien**.
2. Untuk mengedit pengaturan bagi penyewa pelanggan, klik namanya.
3. Di menu navigasi, buka **Pengaturan** > **Keamanan**.
4. Aktifkan switch **Penyimpanan yang tidak dapat diubah**.
5. Tentukan periode retensi dalam rentang 14 hingga 999 hari.

Periode retensi default adalah 14 hari. Periode retensi yang lebih lama dapat menyebabkan peningkatan penggunaan penyimpanan.

6. Pilih mode penyimpanan yang tidak dapat diubah.

   Peringatan!
   Pemilihan **Mode kepatuhan** tidak dapat dibatalkan. Anda tidak lagi dapat menonaktifkan penyimpanan yang tidak dapat diubah dan tidak dapat mengubah mode atau periode retensinya.

7. Klik **Simpan**.

Cara menonaktifkan penyimpanan yang tidak dapat diubah untuk penyewa pelanggan

1. Masuk ke portal manajemen sebagai administrator lalu buka **Klien**.
2. Untuk mengedit pengaturan bagi penyewa pelanggan, klik namanya.
3. Di menu navigasi, buka **Pengaturan** > **Keamanan**.
4. Nonaktifkan switch **Penyimpanan yang tidak dapat diubah**.

   Catatan
   Anda hanya dapat menonaktifkan penyimpanan yang tidak dapat diubah di mode Tata Kelola.

   Peringatan!
   Jika Anda menonaktifkan penyimpanan yang tidak dapat diubah, semua cadangan yang terhapus akan dihapus secara permanen. Menghapus cadangan baru juga akan menjadi permanen.

5. Konfirmasi pilihan Anda dengan mengeklik **Nonaktifkan**.

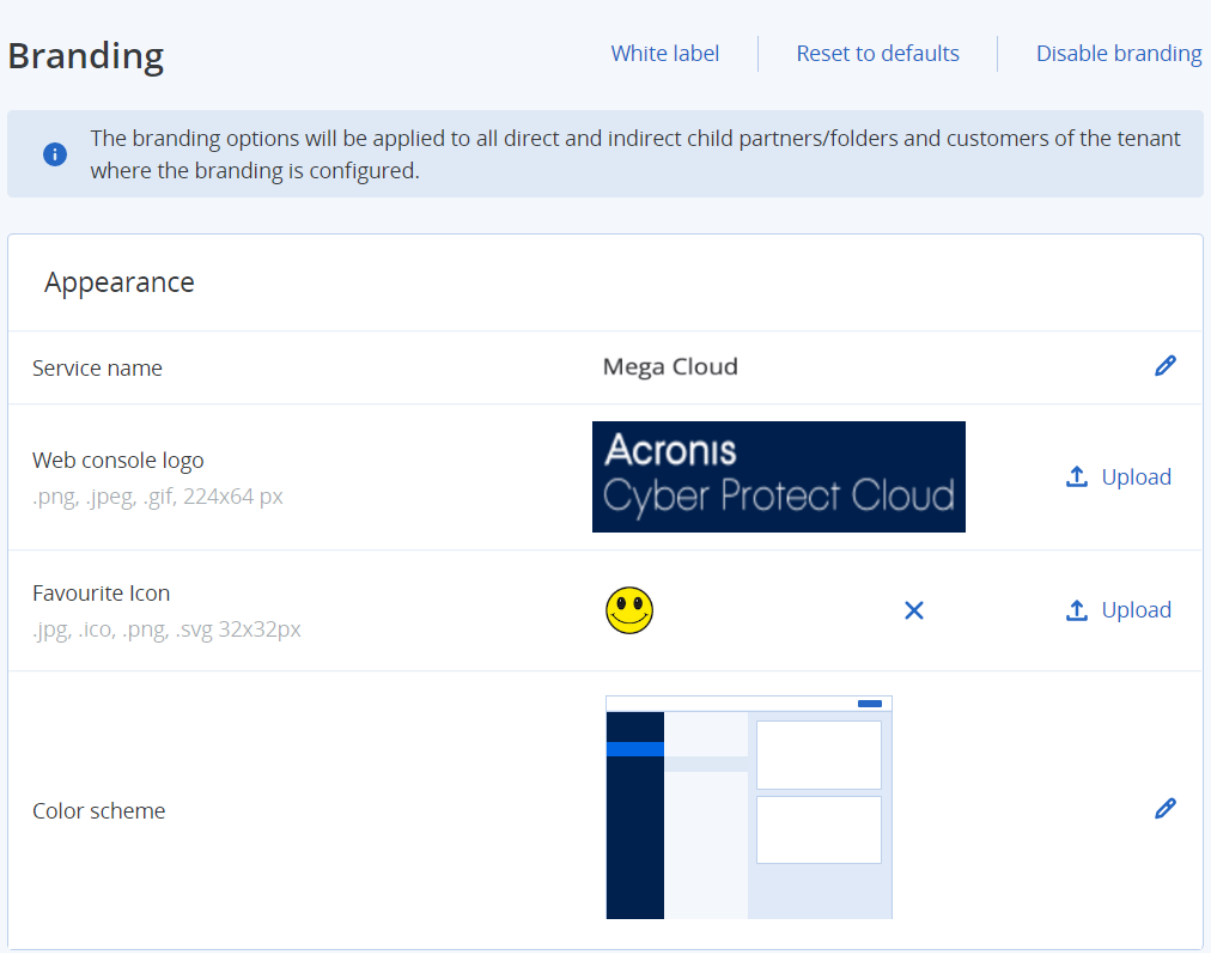
Pembatasan

- Penyimpanan yang tidak dapat diubah tersedia untuk penyimpanan yang dihosting Acronis dan dihosting mitra yang menggunakan Acronis Cyber Infrastructure versi 4.7.1 atau yang lebih baru. Penyimpanan yang tidak dapat diubah mengharuskan port TCP 40440 terbuka untuk layanan Gateway Cadangan di Acronis Cyber Infrastructure. Dalam versi 4.7.1 dan yang lebih baru, port TCP 40440 secara otomatis dibuka dengan jenis lalu lintas **Cadangan (ABGW) publik**. Untuk informasi lebih lanjut tentang jenis lalu lintas, lihat dokumentasi Acronis Cyber Infrastructure.
- Penyimpanan yang tidak dapat diubah memerlukan agen proteksi versi 21.12 (build 15.0.28532) atau versi lebih baru.
- Hanya cadangan TIBX (Versi 12) yang didukung.

Mengonfigurasi branding dan label putih

Bagian **Pengaturan** > **Branding** memungkinkan administrator mitra untuk menyesuaikan antarmuka pengguna pada portal manajemen dan layanan **Cyber Protection** untuk menghapus

setiap hubungan dengan mitra pada level lebih tinggi.



Branding dapat dikonfigurasi pada tingkat mitra dan folder. Branding diterapkan ke semua mitra/folder turunan dan pelanggan penyewa yang bersifat langsung dan tidak langsung di mana branding dikonfigurasi.

Layanan lain menyediakan kemampuan branding terpisah di konsol layanan mereka. Untuk informasi lebih lanjut, lihat panduan pengguna layanan terkait.

Item branding

Tampilan

- **Nama layanan**. Nama ini digunakan dalam semua pesan email yang dikirim oleh portal manajemen dan Layanan awan (pesan aktivasi akun, pesan email pemberitahuan layanan), pada layar **Selamat Datang** setelah login pertama, dan sebagai nama tab browser portal manajemen.
- **Logo konsol web**. Logo ditampilkan pada portal manajemen dan layanan. Klik **Unggah** untuk mengunggah file profil.
- **Ikon Favorit** [Hanya tersedia jika URL kustom dikonfigurasi]. Favicon ditampilkan di sebelah judul halaman di tab browser. Klik **Unggah** untuk mengunggah file profil.

- **Skema warna**. Skema warna menetapkan kombinasi warna yang digunakan untuk semua unsur antarmuka pengguna.

Catatan
Klik **Tinjau skema di tab baru** untuk melihat akan seperti apa tampilan antarmuka pada penyewa turunan Anda. Branding tidak akan diterapkan sampai Anda mengklik **Selesai** pada panel **Pilih skema warna**.

Branding agen dan penginstal

Anda dapat menyesuaikan branding file instalasi agen dan monitor tray untuk Windows dan macOS.

Catatan
Untuk mengaktifkan fungsi branding ini, Anda harus memperbarui agen Cyber Protection ke versi 15.0.28816 (Rilis 22.01) atau yang lebih baru.

- **Nama file penginstal agen**. Nama file instalasi yang diunduh pada beban kerja yang dilindungi.
- **Logo penginstal agen**. Logo yang ditampilkan di wizard Pengaturan selama instalasi agen. Klik **Unggah** untuk mengunggah file profil.
- **Nama agen**. Nama yang ditampilkan di wizard Pengaturan selama instalasi agen.
- **Nama monitor tray**. Nama yang ditampilkan di atas jendela monitor tray.

Dokumentasi dan dukungan

- **URL Beranda**. Halaman ini terbuka saat pengguna mengklik nama perusahaan pada panel **Tentang**.
- **URL dukungan**. Halaman ini terbuka saat pengguna mengklik tautan **Hubungi dukungan** pada panel **Tentang** atau pada pesan email yang dikirimkan oleh portal manajemen.
- **Telepon dukungan**. Nomor telepon ini ditampilkan pada panel **Tentang**.
- **URL basis pengetahuan**. Halaman ini terbuka saat pengguna mengklik tautan **Basis Pengetahuan** pada pesan eror.
- **Panduan administrator Portal Manajemen**. Halaman ini terbuka saat pengguna mengeklik ikon tanda tanya pada sudut kanan atas antarmuka pengguna portal manajemen, lalu mengeklik **Tentang** > **Panduan administrator**.
- **Bantuan administrator Portal Manajemen**. Halaman ini terbuka saat pengguna mengeklik ikon tanda tanya pada sudut kanan atas antarmuka pengguna portal manajemen, lalu mengeklik **Bantuan**.

URL untuk layanan Cyber Protect Cloud

Anda dapat menyediakan layanan Cyber Protect Cloud dari domain kustom Anda. Klik **Konfigurasi** untuk mengatur URL kustom untuk pertama kalinya, atau klik **Konfigurasi ulang** untuk mengubah yang sudah ada. Untuk menggunakan URL default (https://cloud.acronis.com), klik **Atur ulang ke**

default. Untuk informasi selengkapnya tentang URL kustom, lihat "Mengonfigurasi URL antarmuka web kustom".

Pengaturan dokumen hukum

- **URL Perjanjian Lisensi Pengguna Akhir (EULA)**. Halaman ini terbuka saat pengguna mengklik tautan **Perjanjian lisensi pengguna akhir** pada panel **Tentang**, pada layar **Selamat Datang** setelah masuk pertama, dan pada File Sync & Share halaman arahan Unggah Permintaan.
- **URL persyaratan platform**. Halaman ini terbuka saat administrator mitra mengklik tautan **Persyaratan platform** pada panel **Tentang** atau layar **Selamat Datang** setelah masuk pertama.
- **URL Pernyataan privasi**. Halaman ini terbuka saat pengguna mengeklik tautan **Pernyataan privasi** pada layar **Selamat Datang** setelah masuk pertama, dan pada File Sync & Share halaman arahan Unggah Permintaan.

Penting
Jika Anda tidak ingin dokumen muncul di layar Selamat Datang, jangan memasukkan URL untuk dokumen tersebut.

Catatan
Untuk informasi lebih lanjut Tentang File Sync & Share Unggah Permintaan, lihat Cyber Files Cloud Panduan Pengguna.

Upsell

- **Beli URL**. Halaman ini terbuka jika pengguna mengeklik **Beli sekarang** untuk meningkatkan versi ke edisi yang lebih lanjut dari layanan Cyber Protection. Untuk informasi selengkapnya tentang skenario upsell, lihat "Mengonfigurasi skenario upsell untuk pelanggan Anda".

Aplikasi seluler

- **App Store**. Halaman ini terbuka saat pengguna mengeklik **Tambah** > **iOS** pada layanan **Cyber Protection**.
- **Google Play**. Halaman ini terbuka saat pengguna mengeklik **Tambah** > **Android** pada layanan **Cyber Protection**.

Pengaturan email

Anda dapat menentukan server email kustom yang akan digunakan untuk mengirim pemberitahuan email dari portal manajemen dan layanan. Untuk menentukan server email kustom, klik **Sesuaikan**, lalu tentukan pengaturan berikut:

- Pada bagian **Dari**, masukkan nama yang akan ditampilkan pada bidang **Dari** pemberitahuan email.
- Pada bagian **SMTP**, masukkan nama server email keluar (SMTP).
- Pada bagian **Port**, masukkan port server email keluar. Secara default, port diatur ke 25.

- Pada bagian **Enkripsi**, pilih enkripsi SSL atau TLS. Pilih **Tidak ada** untuk menonaktifkan enkripsi.
- Pada bagian **Nama pengguna** dan **Kata sandi**, tentukan kredensial akun yang akan digunakan untuk mengirim pesan.

Mengonfigurasi branding

1. Masuk ke portal manajemen.
2. Navigasikan ke penyewa yang ingin Anda konfigurasikan branding-nya.
3. Klik **Pengaturan** > **Branding**.
4. [Jika branding belum diaktifkan] Klik **Aktifkan branding**.
5. Konfigurasikan item branding yang telah dijelaskan di atas.

Memulihkan pengaturan branding default

Anda dapat mengatur ulang semua item branding ke nilai defaultnya.

1. Masuk ke portal manajemen.
2. Navigasikan ke penyewa yang ingin Anda mulai ulang brandingnya.
3. Klik **Pengaturan** > **Branding**.
4. Di kanan atas, klik **Pulihkan ke default**.

Menonaktifkan branding

Anda dapat menonaktifkan branding untuk akun Anda dan semua penyewa anak.

1. Masuk ke portal manajemen.
2. Navigasikan ke penyewa yang ingin Anda nonaktifkan brandingnya.
3. Klik **Pengaturan** > **Branding**.
4. Di kanan atas, klik **Nonaktifkan branding**.

Label putih

Anda dapat mengontrol apakah agen Cyber Protection (untuk Windows, macOS, dan Linux) dan Monitor Cyber Protection (untuk Windows, macOS, dan Linux) akan diberi merek atau label putih untuk semua mitra anak dan pelanggan Anda. Jika Anda mengaktifkan label putih, agen dan monitor tray akan diberi label putih. Pengaturan ini juga akan mempengaruhi nama dan logo yang digunakan dalam penginstal dan Monitor Cyber Protection.

Menerapkan label putih

1. Masuk ke portal manajemen.
2. Navigasikan ke penyewa tempat Anda ingin menerapkan label putih.

3. Klik **Pengaturan** > **Branding**.
4. Di pojok atas jendela, Klik **Label putih** untuk menghapus semua item branding, kecuali untuk **Nama layanan**, **URL perjanjian Lisensi Pengguna Akhir (EULA)**, **Panduan administrator portal manajemen**, **Bantuan administrator portal manajemen**, dan **Pengaturan server email**.

Mengonfigurasi URL antarmuka web kustom

Catatan
URL yang dikustomisasi akan mengarah ke alamat IP yang berbeda dibandingkan dengan URL default. Ingatlah hal ini saat mengonfigurasi kebijakan firewall.

Untuk mengonfigurasi URL antarmuka web untuk layanan Cyber Protect Cloud

1. Di portal manajemen, klik **Pengaturan** > **Branding**.
2. Di bagian **URL untuk layanan Cyber Protect Cloud**:
   - Klik **Konfigurasi** untuk mengatur URL kustom untuk pertama kalinya.
   - Klik **Konfigurasi ulang** untuk mengubah URL kustom yang ada.
3. Pada langkah **Pengaturan Domain**, siapkan domain dan data CNAME Anda.
   Untuk menggunakan URL kustom, Anda harus memiliki nama domain aktif dan data CNAME yang dikonfigurasi untuk mengarah ke pusat data tempat akun Anda berada. Konfigurasi data CNAME dilakukan oleh pencatat DNS Anda dan mungkin memerlukan waktu hingga 48 jam untuk disebarkan.
   Untuk menemukan nama domain pusat data Anda dan meminta konfigurasi data CNAME Anda, lihat artikel URL Konsol Web Branding (58275).
4. Pada langkah **Periksa URL Anda**, verifikasi bahwa URL kustom Anda dapat diakses, dan bahwa data CNAME Anda dikonfigurasi dengan benar. Untuk melakukannya, masukkan nama URL utama dan klik **Periksa**. Jika menggunakan sertifikat SSL wildcard, Anda dapat menambahkan hingga sepuluh nama domain alternatif. Jika Anda menggunakan sertifikat "Let's Encrypt", nama domain alternatif akan diabaikan.
5. Pada langkah **Sertifikat SSL**, Anda dapat melakukan salah satu hal berikut:
   - Buat sertifikat "Let's Encrypt". Untuk melakukannya, klik **Sertifikat SSL gratis dengan "Let's Encrypt"**. Opsi ini menggunakan sertifikat "Let's Encrypt" yang dikeluarkan oleh entitas pihak ketiga. Penyedia layanan tidak bertanggung jawab atas masalah apa pun yang disebabkan oleh penggunaan berbagai sertifikat gratis ini. Untuk informasi lebih lanjut tentang istilah "Let's Encrypt", lihat https://letsencrypt.org/repository/.
   - Unggah sertifikat wildcard Anda. Untuk melakukannya, klik **Unggah sertifikat wildcard**, lalu berikan sertifikat wildcard dan kunci privat.
6. Klik **Kirim** untuk menerapkan perubahan.

Untuk mereset URL kustom ke default

1. Di portal manajemen, klik **Pengaturan** > **Branding**.
2. Di bagian **URL untuk layanan Acronis Cyber Protect Cloud**, klik **Reset ke default** untuk menggunakan URL default (https://cloud.acronis.com).

Memperbarui agen secara otomatis

Cyber Protect memiliki tiga jenis agen yang dapat diinstal di mesin terproteksi: Agen untuk Windows, Agen untuk Linux, dan Agen untuk Mac.

Cyber Files Cloud memiliki Agen desktop versi Windows dan MacOS untuk File Sync & Share, yang memungkinkan sinkronisasi file dan folder antara mesin dan area penyimpanan awan File Sync & Share pengguna untuk mendukung kerja offline, serta praktik kerja WFH (Work From Home/Kerja Dari Rumah) dan BYOD (Bring Your Own Device/Bawa Perangkat Anda Sendiri).

Untuk memfasilitasi manajemen beberapa beban kerja, Anda dapat mengonfigurasi (dan menonaktifkan) pembaruan otomatis tanpa pengawasan untuk semua agen di semua mesin.

Penting
Saat ini, hanya mitra dan pelanggan yang mengaktifkan Perlindungan yang memiliki akses ke fungsionalitas manajemen pembaruan agen.

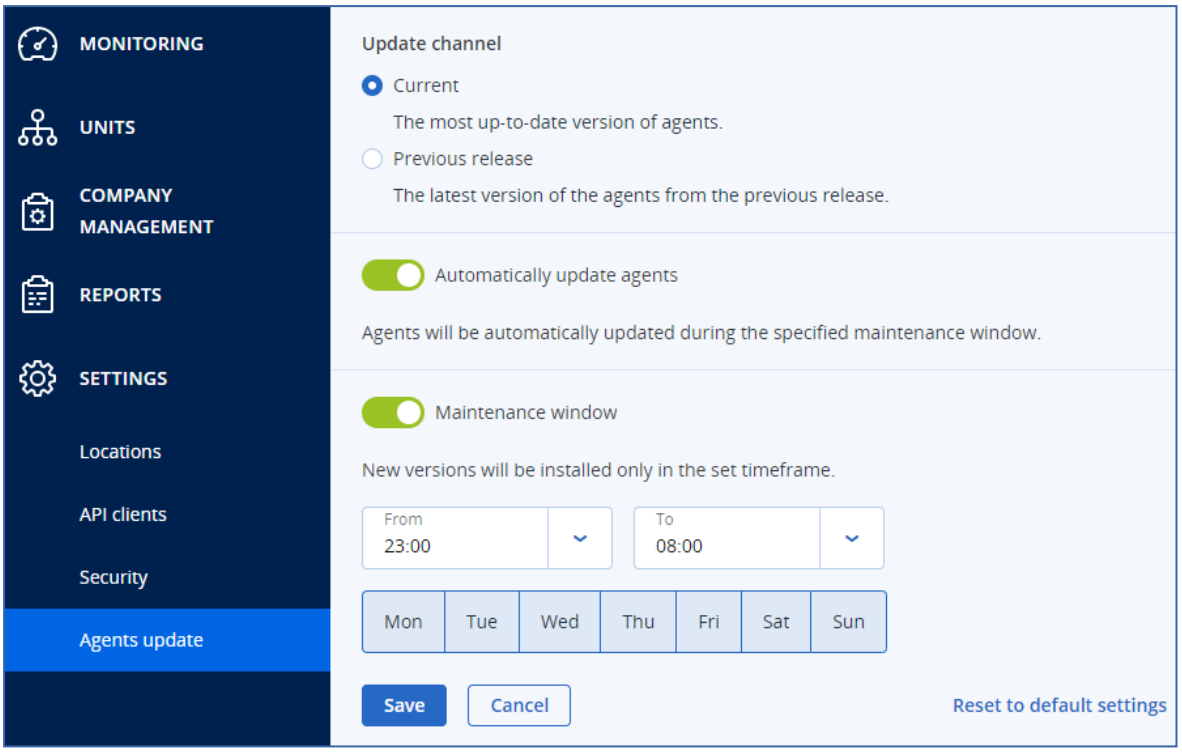
Catatan
Untuk mengelola agen di mesin masing-masing, dan menyesuaikan pengaturan pembaruan otomatis, lihat bagian Panduan Pengguna Cyber Protect di Memperbarui Agen.

Untuk memperbarui agen secara otomatis

Catatan
Pengaturan untuk memperbarui Agen secara otomatis untuk File Sync & Share diambil oleh mitra dan pelanggan yang tidak mengaktifkan Proteksi.

Untuk mengatur pembaruan agen otomatis dari halaman awal Portal Manajemen

1. Pilih **Pengaturan > Pembaruan agen**.



2. Pilih versi yang akan dideteksi untuk pembaruan otomatis: **Saat ini** atau **Rilis sebelumnya**. (Default-nya adalah **Saat ini**.)
3. Aktifkan **Perbarui agen secara otomatis**. Default-nya adalah **aktif**.)
4. Atur jangka waktu pemeliharaan. (Default-nya adalah dari pukul 23.00 hingga 08.00.)

   Catatan
   Meskipun proses pembaruan agen dirancang agar cepat dan lancar, sebaiknya pilih jangka waktu yang akan menimbulkan paling sedikit gangguan untuk pengguna, karena pengguna tidak dapat mencegah atau menunda pembaruan otomatis.

5. [Opsional] Pilih hari tertentu untuk melakukan pembaruan otomatis.
6. Pilih **Simpan.**

Catatan
Pembaruan otomatis hanya tersedia untuk:

- Agen Cyber Protect versi 15.0.26986 (dirilis pada Maret 2021) atau yang lebih baru.
- Agen Desktop untuk File Sync & Share, versi 15.0.30370 atau versi lebih baru.

Agen yang lebih lama harus diperbarui secara manual terlebih dahulu ke versi terbaru, sebelum pembaruan otomatis berlaku.

Untuk memantau pembaruan agen

Penting
Pembaruan agen hanya dapat dipantau oleh administrator mitra dan pelanggan yang mengaktifkan modul Proteksi.

Untuk memantau pembaruan agen, lihat bagian Peringatan dan Aktivitas Panduan Pengguna Cyber Protect.

Pemantauan

Untuk mengakses informasi tentang penggunaan dan pengoperasian layanan, klik **Pemantauan**.

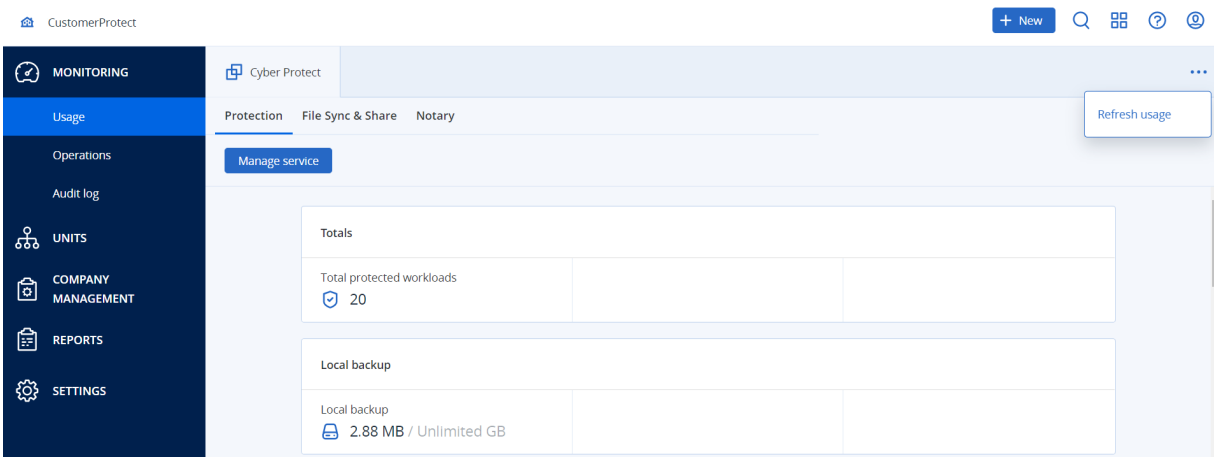
Penggunaan

Tab **Penggunaan** memberikan ikhtisar tentang penggunaan layanan dan memungkinkan Anda untuk mengakses layanan di dalam penyewa tempat Anda beroperasi.

Data penggunaan mencakup fitur standar dan fitur tingkat lanjut.

Untuk me-refresh data penggunaan yang ditampilkan di tab, klik elipsis di bagian kanan atas layar dan pilih **Refresh penggunaan**.

Catatan
Mengambil data dapat memerlukan waktu hingga 10 menit. Muat ulang halaman untuk melihat data yang diperbarui.



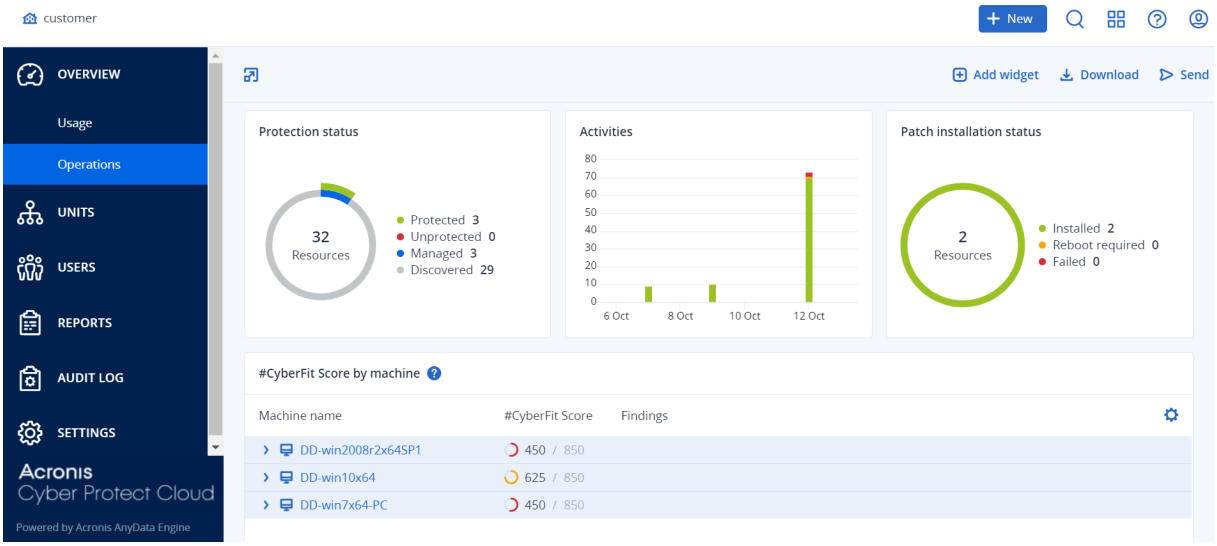
Operasi

Dasbor **Operasi** menyediakan sejumlah widget kustom yang memberikan ikhtisar operasi terkait dengan layanan Cyber Protection. Widget untuk layanan lain akan tersedia di rilis mendatang.

Secara default, data ditampilkan untuk penyewa tempat Anda beroperasi. Anda dapat mengubah penyewa yang ditampilkan secara individual untuk setiap widget dengan mengeditnya. Informasi teragregasi tentang penyewa pelanggan turunan langsung dari penyewa yang dipilih juga ditampilkan, termasuk yang berada di dalam folder. Dasbor *tidak* menampilkan informasi tentang mitra turunan dan penyewa turunan mereka; Anda harus menjelajahi mitra spesifik untuk melihat dasbornya. Namun, jika Anda mengonversikan penyewa mitra turunan ke penyewa folder, informasi tentang pelanggan turunan penyewa ini akan muncul di dasbor penyewa induk.

Widget diperbarui setiap dua menit. Widget memiliki elemen yang dapat diklik sehingga memungkinkan Anda untuk menyelidiki dan menyelesaikan masalah. Anda dapat mengunduh status dasbor saat ini dalam format .pdf atau/dan .xlsx, atau mengirimnya melalui email ke alamat mana pun, termasuk penerima eksternal.

Anda dapat memilih dari berbagai macam widget, yang disajikan sebagai tabel, diagram lingkaran, diagram batang, daftar, dan peta pohon. Anda dapat menambahkan beberapa widget dengan jenis yang sama untuk penyewa yang berbeda atau dengan filter yang berbeda.



Untuk mengatur ulang widget di dasbor

Seret dan lepaskan widget dengan mengklik namanya.

Untuk mengedit widget

Klik ikon pensil di sebelah nama widget. Pengeditan widget memungkinkan Anda untuk mengganti nama, mengubah periode waktu, memilih penyewa yang untuknya data ditampilkan, dan mengatur filter.

Untuk menambahkan widget

Klik **Tambah widget**, lalu lakukan salah satu cara berikut:

- Klik widget yang ingin Anda tambahkan. Widget akan ditambahkan dengan pengaturan default.
- Untuk mengedit widget sebelum menambahkannya, klik ikon roda gigi saat widget dipilih. Setelah mengedit widget, klik **Selesai**.

Untuk menghapus widget

Klik ikon tanda X di sebelah nama widget.

Status proteksi

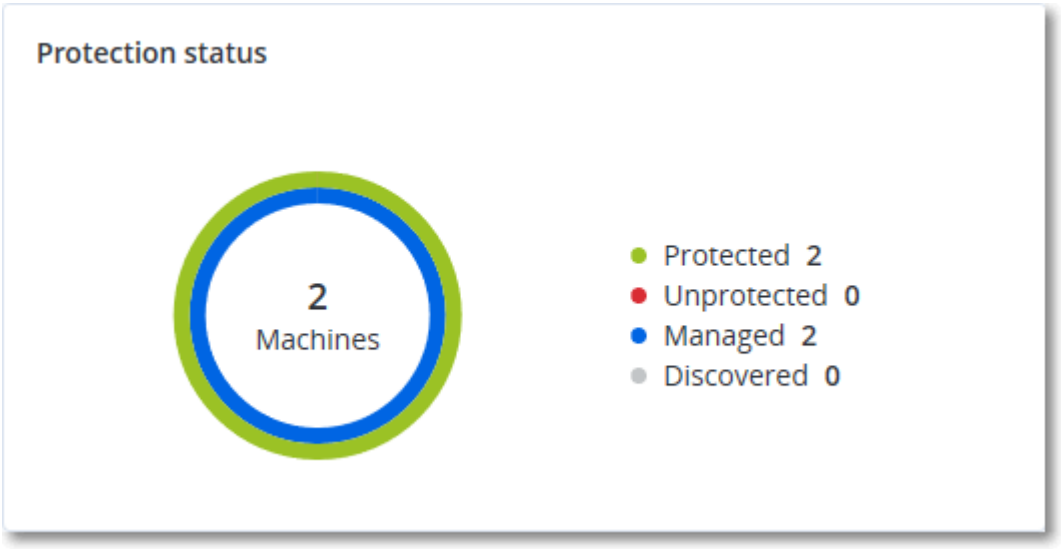
Status proteksi

Widget ini menampilkan status perlindungan saat ini untuk semua mesin.

Suatu mesin dapat memiliki salah satu status berikut:

- **Terlindungi** – mesin dengan rencana proteksi yang diterapkan.
- **Tak terlindungi** – mesin tanpa rencana proteksi yang diterapkan. Ini mencakup mesin yang terdeteksi dan mesin yang dikelola tanpa ada rencana proteksi yang diterapkan.
- **Dikelola** – mesin dengan agen perlindungan yang sudah diinstal.
- **Ditemukan** – mesin tanpa agen perlindungan yang sudah diinstal.

Jika mengeklik status mesin, Anda akan diarahkan ke daftar mesin dengan status ini untuk keterangan lebih lanjut.



Mesin yang ditemukan

Widget ini menampilkan daftar mesin yang ditemukan selama rentang waktu tertentu.

Discovered machines

Device name	IP address	OS	Organizational unit	Discovery type
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network
Windows 10 Enterprise 2016 LTSB				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Local Network
device2	-	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Manual, Loc...
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Local Network
device5	-	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Manual
-				
-	10.250.41.189	-	-	Manual
-	10.248.44.199	-	-	Manual

Skor #CyberFit berdasarkan mesin

Widget ini menunjukkan total Skor #CyberFit untuk setiap mesin, skor gabungannya, dan temuan untuk setiap metrik yang dinilai:

- Antimalware
- Cadangan
- Firewall
- VPN
- Enkripsi
- NTLM traffic

Untuk meningkatkan skor setiap metrik, Anda dapat melihat rekomendasi yang tersedia dalam laporan.

Untuk detail selengkapnya tentang Skor #CyberFit, lihat "Skor #CyberFit untuk mesin".

#CyberFit Score by machine

Metric	#CyberFit Score	Findings
DESKTOP-2N2TRE8	625 / 850	
Anti-malware	275 / 275	You have anti-malware protection enabled
Backup	175 / 175	You have a backup solution protecting your data
Firewall	175 / 175	You have a firewall enabled for public and private networks
VPN	0 / 75	No VPN solution was found, your connection to public and shared networks is n...
Encryption	0 / 125	No disk encryption was found, your device is at risk from physical tampering
NTLM traffic	0 / 25	Outgoing NTLM traffic to remote servers is not denied, your credentials may be ...

Widget Deteksi dan Tanggapan Titik Akhir (Endpoint Detection and Response/EDR)

Penting
Ini adalah versi Akses Awal dari dokumentasi EDR. Beberapa fitur dan deskripsi mungkin belum lengkap.

Deteksi dan Tanggapan Titik Akhir (Endpoint Detection and Response/EDR) termasuk sejumlah widget yang dapat diakses melalui dasbor **Operasi**.

Widget yang tersedia diantaranya:

- Distribusi insiden teratas per beban kerja
- MTTR insiden
- Burndown insiden keamanan
- Status jaringan beban kerja

Distribusi Insiden Teratas per beban kerja

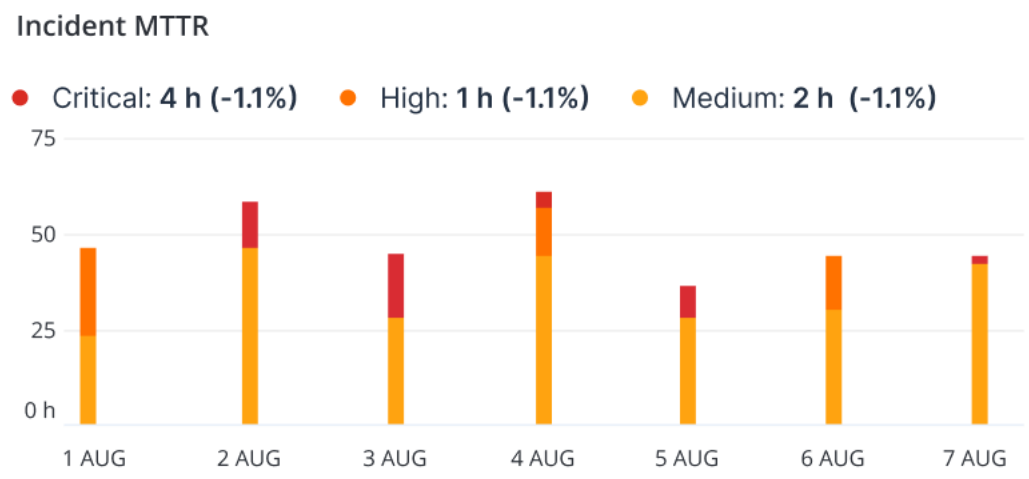
Widget ini menampilkan lima beban kerja teratas dengan insiden paling banyak (klik **Tampilkan semua** untuk mengarahkan langsung ke daftar insiden, yang difilter berdasarkan pengaturan widget).

Arahkan pointer mouse disekitar baris beban kerja untuk menampilkan rincian status investigasi saat ini untuk insiden tersebut; status investigasi adalah **Belum mulai**, **Menginvestigasi**, **Tertutup**, dan **Positif salah**. Lalu klik beban kerja yang ingin dianalisa lebih jauh, dan pilih pelanggan yang relevan dalam jendela popup yang ditampilkan; daftar insiden direfresh berdasarkan pengaturan widget.

MTTR insiden

Widget ini menampilkan waktu resolusi rata-rata untuk insiden keamanan. Ini menandakan seberapa cepat insiden teridentifikasi dan terpecahkan.

Klik pada kolom untuk menampilkan rincian insiden berdasarkan keparahannya (**Kritis**, **Tinggi**, dan **Menengah**), dan indikasi yang menjelaskan seberapa lama insiden yang berdasarkan perbedaan tingkat keparahan tersebut dapat diselesaikan. Nilai dalam % yang ditampilkan dalam tanda kurung menandakan peningkatan atau penurunan dibandingkan periode waktu sebelumnya.

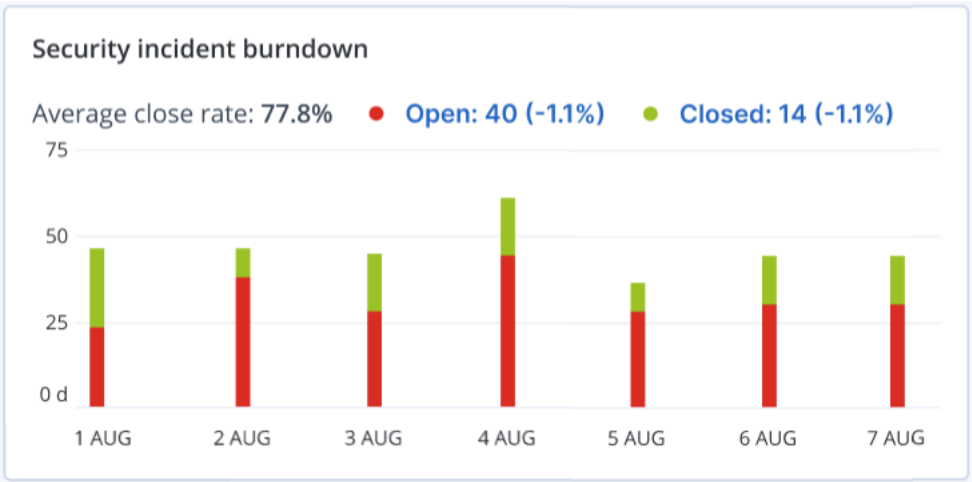


Burndown insiden keamanan

Widget ini menampilkan rentang efisiensi dalam penutupan insiden; jumlah insiden terbuka yang diukur berlawanan dengan jumlah insiden tertutup selama periode waktu tertentu.

Arahkan pointer mouse terhadap sebuah kolom untuk menampilkan uraian insiden tertutup dan terbuka untuk tanggal terpilih. Jika Anda mengeklik nilai Terbuka, sebuah popup ditampilkan sesuai dengan penyewa relevan yang Anda pilih; daftar insiden tersaring untuk penyewa terpilih ditampilkan, untuk menampilkan insiden yang saat ini terbuka (dalam status **Menginvestigasi** atau **Belum Mulai**). Jika Anda mengeklik nilai Tertutup, daftar insiden menampilkan penyewa terpilih, dan disaring untuk menampilkan insiden yang tidak lagi terbuka (dalam status **Tertutup** atau **Positif salah**).

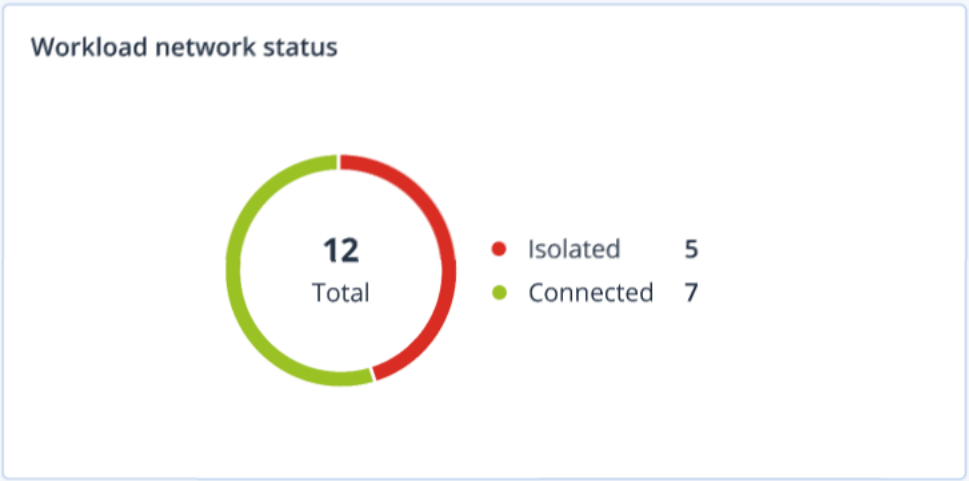
Nilai dalam % yang ditampilkan dalam tanda kurung menandakan peningkatan atau penurunan dibandingkan periode waktu sebelumnya.



Status jaringan beban kerja

Widget ini menampilkan status jaringan saat ini dari beban kerja Anda, dan mengindikasikan jumlah beban kerja yang terisolasi dan jumlah beban kerja yang terhubung.

Klik nilai Terisolasi, sebuah popup ditampilkan sesuai dengan penyewa relevan yang Anda pilih. Tampilan beban kerja yang ditampilkan akan disaring untuk menampilkan beban kerja terisolasi. Klik nilai Terhubung untuk menampilkan Beban Kerja dengan daftar agen yang disaring untuk menampilkan beban kerja terhubung (untuk penyewa terpilih).



Pemantauan kesehatan disk

Pemantauan kesehatan disk menyediakan informasi status kesehatan disk saat ini dan prakiraannya sehingga Anda dapat mencegah kehilangan data yang mungkin berhubungan dengan kegagalan disk. Tipe disk HDD dan SSD didukung.

Pembatasan

- Prakiraan kesehatan disk hanya didukung untuk mesin yang menjalankan Windows.
- Hanya disk mesin fisik yang dapat dipantau. Disk mesin virtual tidak dapat dipantau dan ditampilkan dalam widget kesehatan disk.
- Konfigurasi RAID tidak didukung.
- Di drive NVMe, pemantauan kesehatan disk hanya didukung untuk drive yang mengomunikasikan data SMART via API Windows. Pemantauan kesehatan disk tidak didukung untuk drive NVMe yang perlu membaca data SMART langsung dari drive.

Kesehatan disk diwakili salah satu status berikut:

- **OK**
  Kesehatan disk di antara 70% dan 100%.
- **Peringatan**
  Kesehatan disk di antara 30% dan 70%.
- **Kritis**
  Kesehatan disk di antara 0% dan 30%.
- **Menghitung data disk**
  Status terkini dan prakiraan disk sedang dihitung.

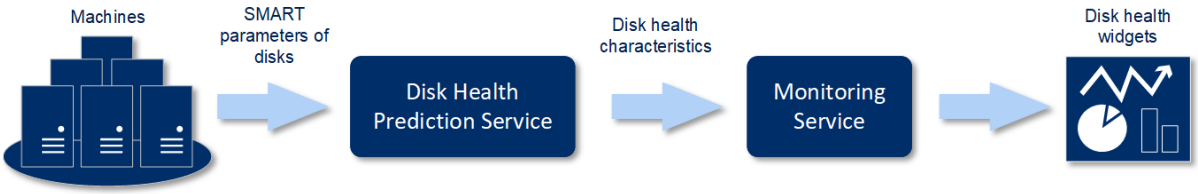
Cara kerjanya

Layanan Prediksi Kesehatan Disk menggunakan model prediksi berbasis AI.

1. Agen proteksi mengumpulkan parameter SMART dari disk dan meneruskan data ini ke Layanan Prediksi Kesehatan Disk:
   - SMART 5 – Hitungan sektor yang dialokasikan ulang.
   - SMART 9 – Jam menyala.
   - SMART 187 – Laporan kesalahan yang tidak dapat dikoreksi.
   - SMART 188 – Batas waktu perintah.
   - SMART 197 – Hitungan sektor tertunda terkini.
   - SMART 198 – Hitungan sektor offline yang tidak dapat dikoreksi.
   - SMART 200 – Laju kesalahan tulis.
2. Layanan Prediksi Kesehatan Disk memproses parameter SMART yang diterima, membuat prakiraan, dan memberikan karakteristik kesehatan disk berikut:
   - Status terkini kesehatan disk: OK, peringatan, kritis.
   - Prakiraan kesehatan disk: negatif, stabil, positif.
   - Persentase kemungkinan prakiraan kesehatan disk.

   Periode prediksinya satu bulan.

3. Layanan Pemantauan menerima karakteristik ini, lalu menunjukkan informasi relevan di widget kesehatan disk di konsol layanan.



Widget kesehatan disk

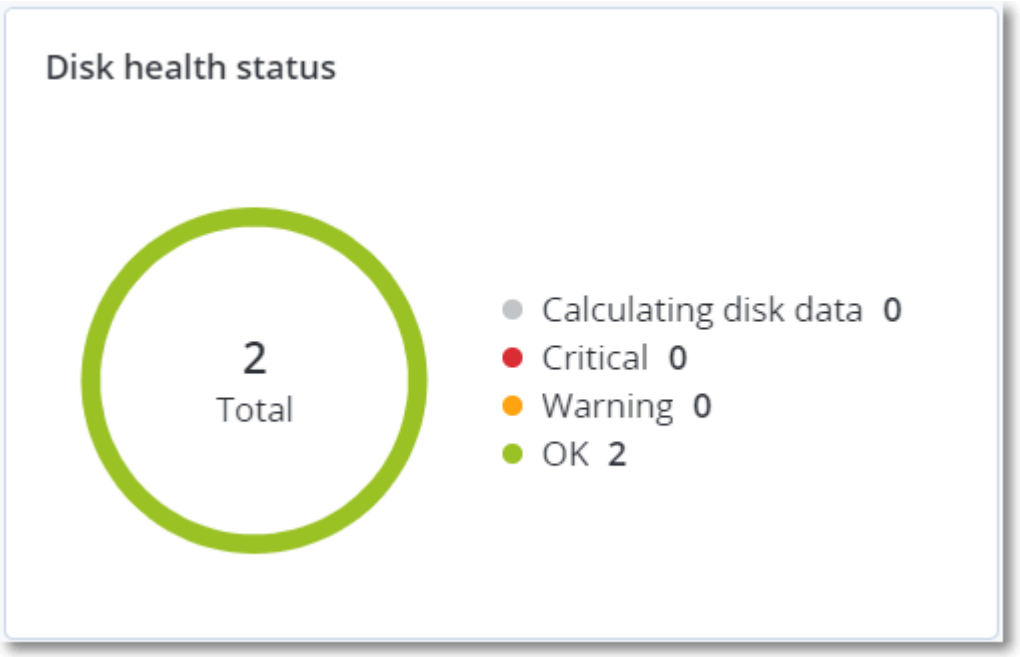
Hasil pemantauan kesehatan disk disajikan di widget berikut yang tersedia di konsol layanan.

- **Gambaran kesehatan disk** adalah widget peta hierarki dengan dua tingkat detail yang dapat diaktifkan dengan diperinci.
  - Tingkat mesin
    Menunjukkan informasi ringkas tentang status kesehatan disk per mesin pelanggan yang dipilih. Hanya status disk paling kritis yang ditunjukkan. Status lainnya ditampilkan di tooltip saat Anda mengarahkan pointer mouse ke blok tertentu. Ukuran blok mesin bergantung pada ukuran total semua disk mesin ini. Warna blok mesin bergantung pada status disk paling kritis yang ditemukan.

- Tingkat disk
  Menunjukkan status disk terkini dari semua disk untuk mesin yang dipilih. Setiap blok disk menunjukkan salah satu prakiraan kesehatan disk berikut dan persentase peluangnya.
  - Akan didegradasi
  - Akan tetap stabil

- Akan membaik

- **Status kesehatan disk** adalah widget diagram lingkaran yang menunjukkan jumlah disk untuk setiap status.



Peringatan status kesehatan disk

Pemeriksaan kesehatan disk berjalan setiap 30 menit, sedangkan peringatan terkait dihasilkan satu kali sehari. Saat kesehatan disk berubah dari **Peringatan** ke **Kritis**, peringatan akan muncul.

Nama peringatan	Tingkat keparahan	Status kesehatan disk	Deskripsi
Kegagalan disk mungkin terjadi	Peringatan	(30 – 70)	Disk <disk name> pada mesin ini mungkin akan gagal di masa mendatang. Jalankan pencadangan profil penuh pada disk ini sesegera mungkin, ganti lalu pulihkan profil ke disk baru.
Kegagalan disk akan terjadi	Kritis	(0 – 30)	Disk <disk name> pada mesin ini berada dalam status kritis dan kemungkinan besar akan gagal dalam waktu dekat. Pencadangan profil disk ini tidak disarankan pada titik ini karena tambahan tekanan dapat menyebabkan disk gagal. Segera cadangkan semua file terpenting pada disk ini lalu ganti disk.

Peta perlindungan data

Peta perlindungan data memungkinkan Anda untuk memeriksa semua data yang penting bagi Anda dan mendapatkan informasi terperinci tentang jumlah, ukuran, lokasi, status proteksi semua file penting dalam tampilan peta pohon terukur.

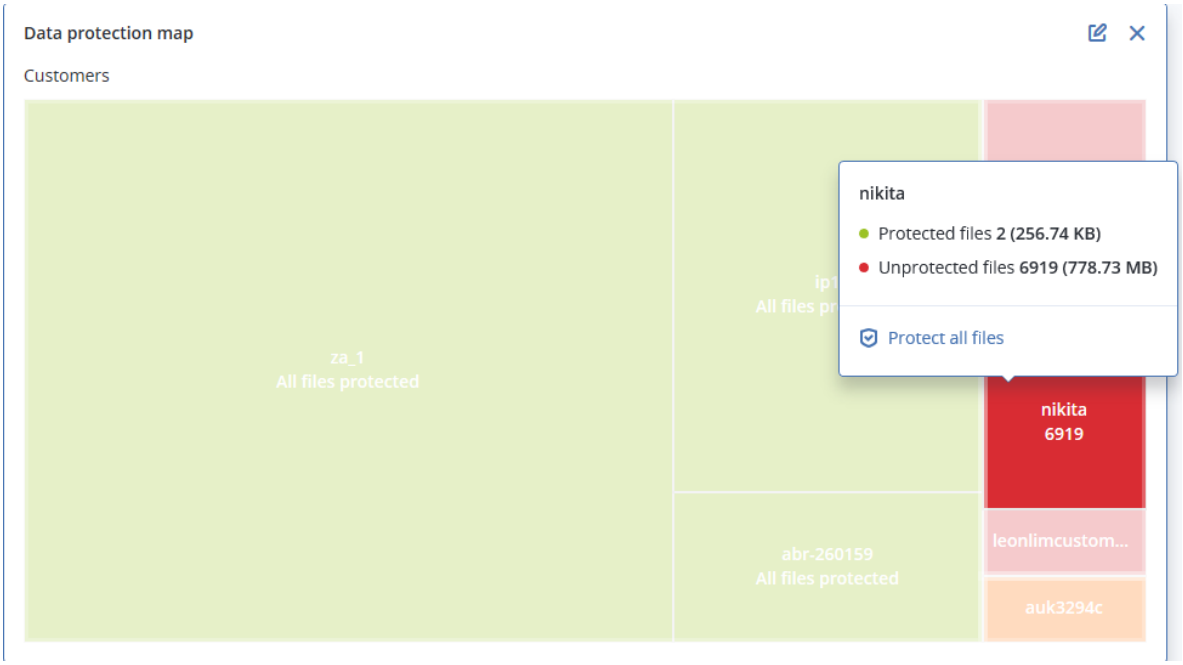
Setiap ukuran blok bergantung pada jumlah/ukuran total semua file penting yang dimiliki pelanggan/mesin.

File dapat berada dalam salah satu status perlindungan berikut:

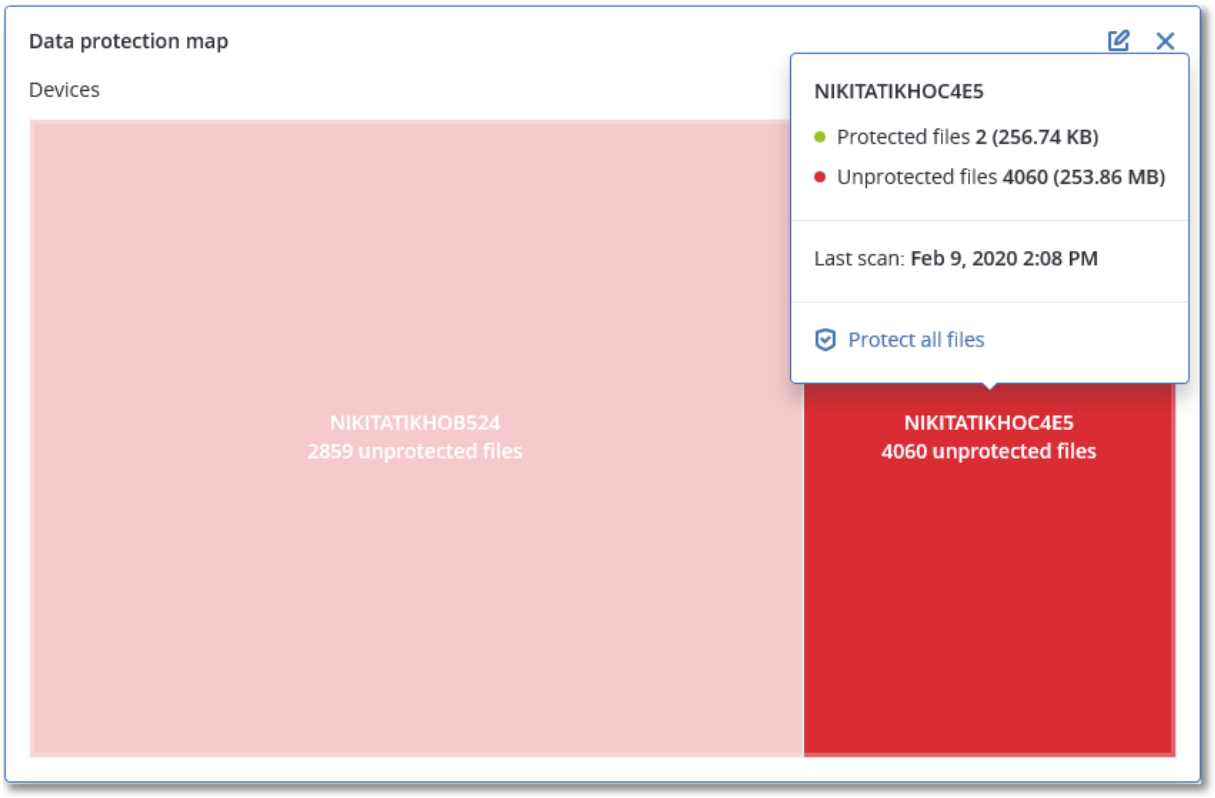
- **Kritis** – terdapat 51-100% file tidak terlindungi dengan ekstensi yang Anda tetapkan yang tidak dicadangkan dan tidak akan dicadangkan untuk penyewa pelanggan/mesin/lokasi yang dipilih.
- **Rendah** – terdapat 21-50% file tidak terlindungi dengan ekstensi yang Anda tetapkan yang tidak dicadangkan untuk penyewa pelanggan/mesin/lokasi yang dipilih.
- **Sedang** – terdapat 1-20% file tidak terlindungi dengan ekstensi yang Anda tetapkan yang tidak dicadangkan untuk penyewa pelanggan/mesin/lokasi yang dipilih.
- **Tinggi** – semua file dengan ekstensi yang Anda tetapkan yang dilindungi (dicadangkan) untuk penyewa pelanggan/mesin/lokasi yang dipilih.

Hasil pemeriksaan perlindungan data dapat ditemukan di dasbor widget Peta Perlindungan Data, suatu widget peta pohon yang memiliki dua tingkat detail yang dapat diaktifkan dengan diperinci:

- Tingkat penyewa pelanggan – menunjukkan informasi ringkas tentang status proteksi file-file penting per pelanggan yang telah Anda pilih.



- Tingkat mesin – menampilkan informasi tentang status proteksi file-file penting per mesin milik pelanggan yang dipilih.



Untuk melindungi file yang tidak dilindungi, beralihlah ke blok dan klik **Lindungi semua file**. Di jendela dialog, Anda dapat menemukan informasi tentang jumlah file yang tidak terlindungi dan lokasinya. Untuk melindungi file-file tersebut, klik **Lindungi semua file**.

Anda juga dapat mengunduh laporan terperinci dalam format CSV.

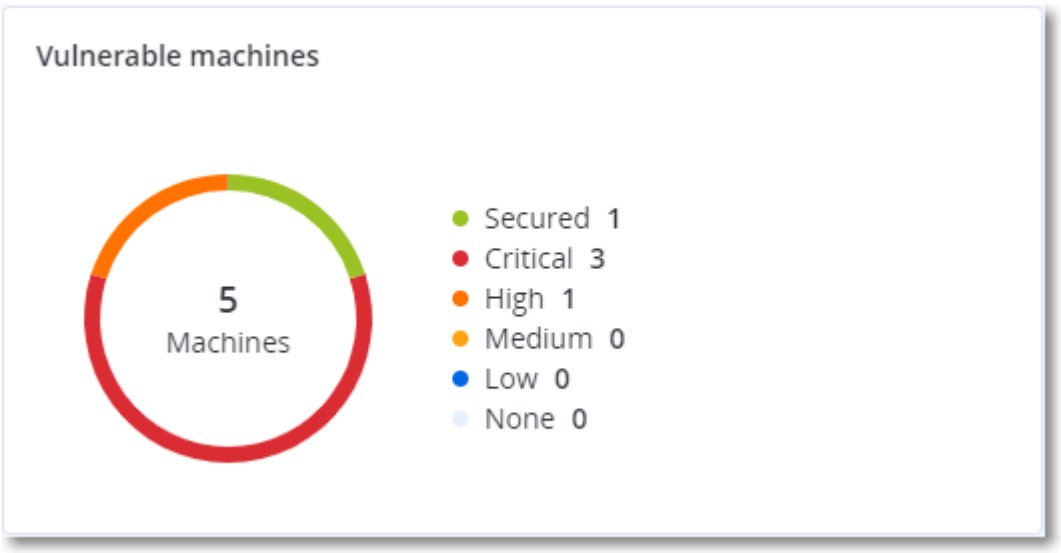
Widget penilaian kerentanan

Mesin yang rentan

Widget ini menampilkan mesin yang rentan dengan tingkat kerentanan.

Kerentanan yang ditemukan dapat memiliki salah satu tingkat keparahan berikut berdasarkan Sistem Penilaian Kerentanan Umum (CVSS) v3.0:

- Aman: tidak ada kerentanan yang ditemukan
- Kritis: 9,0 - 10,0 CVSS
- Tinggi: 7,0 - 8,9 CVSS
- Sedang: 4,0 - 6,9 CVSS
- Rendah: 0,1 - 3,9 CVSS
- Tidak ada: 0,0 CVSS



Kerentanan yang ada

Widget ini menampilkan kerentanan yang ada saat ini pada mesin. Di widget **Kerentanan yang ada**, terdapat dua kolom yang menunjukkan stempel waktu:

- **Terdeteksi pertama** – tanggal dan waktu saat kerentanan terdeteksi pertama kali pada mesin.
- **Terdeteksi terakhir** – tanggal dan waktu saat kerentanan terdeteksi terakhir kali pada mesin.

Existing vulnerabilities

Machine name	Vendor	Product	Vulnerability name/ID	Severity	Last detected	First detected
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM

More

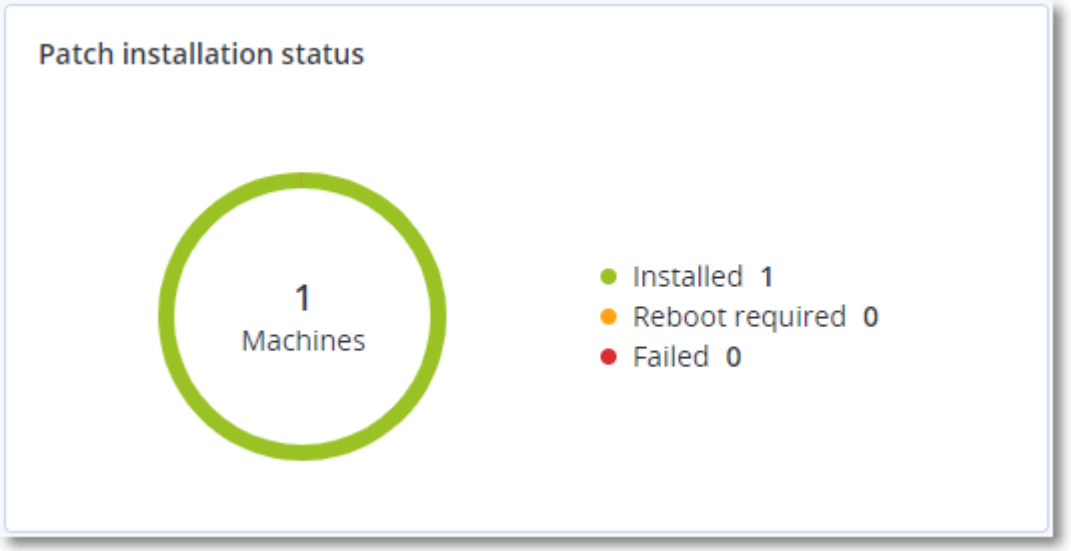
Widget instalasi patch

Ada empat widget terkait dengan fungsi pengelolaan patch.

Status instalasi patch

Widget ini menampilkan jumlah mesin yang dikelompokkan berdasarkan status instalasi patch.

- **Diinstal** – semua patch yang tersedia sudah diinstal pada mesin
- **Boot ulang diperlukan** – setelah instalasi patch, boot ulang diperlukan untuk mesin
- **Gagal** – instalasi patch gagal pada mesin



Ringkasan instalasi patch

Widget ini menampilkan ringkasan patch pada mesin berdasarkan status instalasi patch.

Patch installation summary

Installation status	Total number of machines	Total number of updates	Microsoft updates	Application updates	Critical severity	High severity	Medium severity
Installed	1	2	1	1	2	0	0

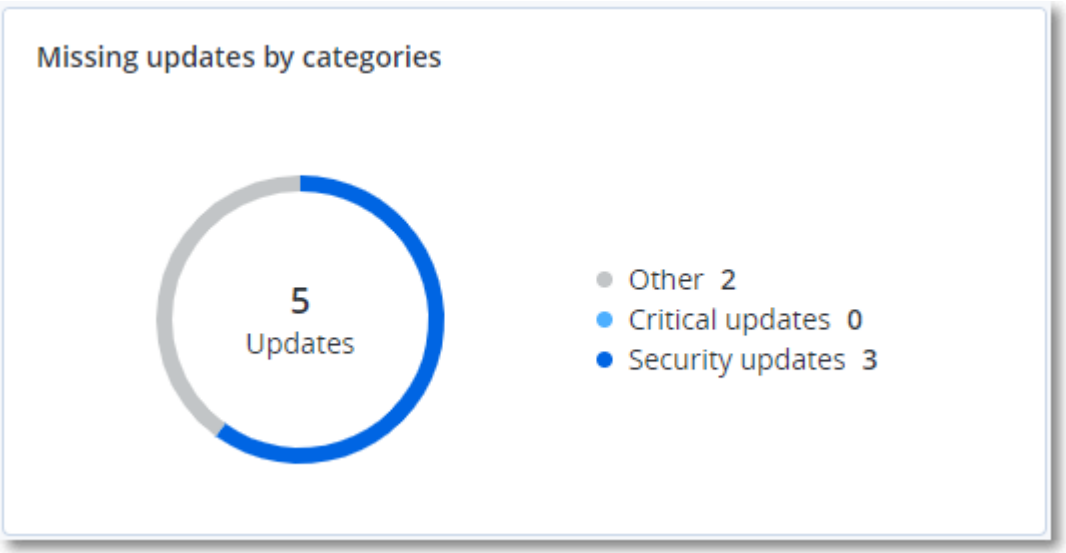
Riwayat instalasi patch

Widget ini menampilkan informasi terperinci tentang patch pada mesin.

Pembaruan yang tidak ada berdasarkan kategori

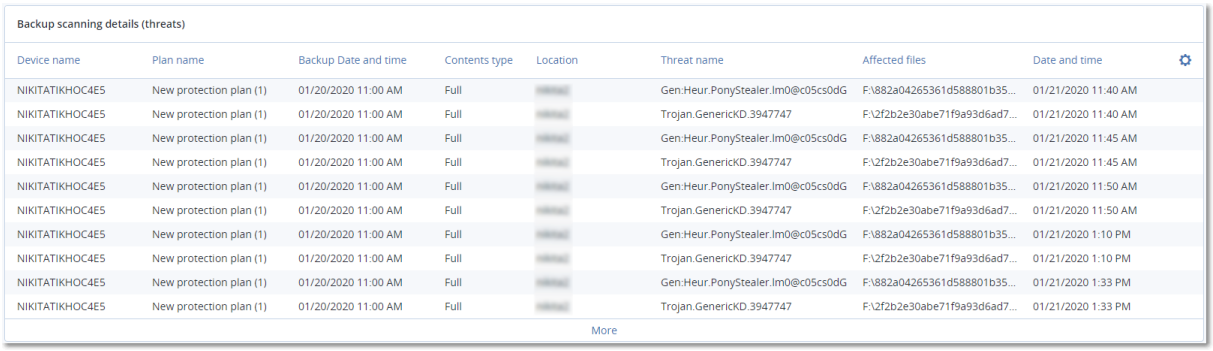
Widget ini menampilkan jumlah pembaruan yang tidak ada per kategori. Kategori berikut ini ditampilkan:

- Pembaruan keamanan
- Pembaruan penting
- Lain



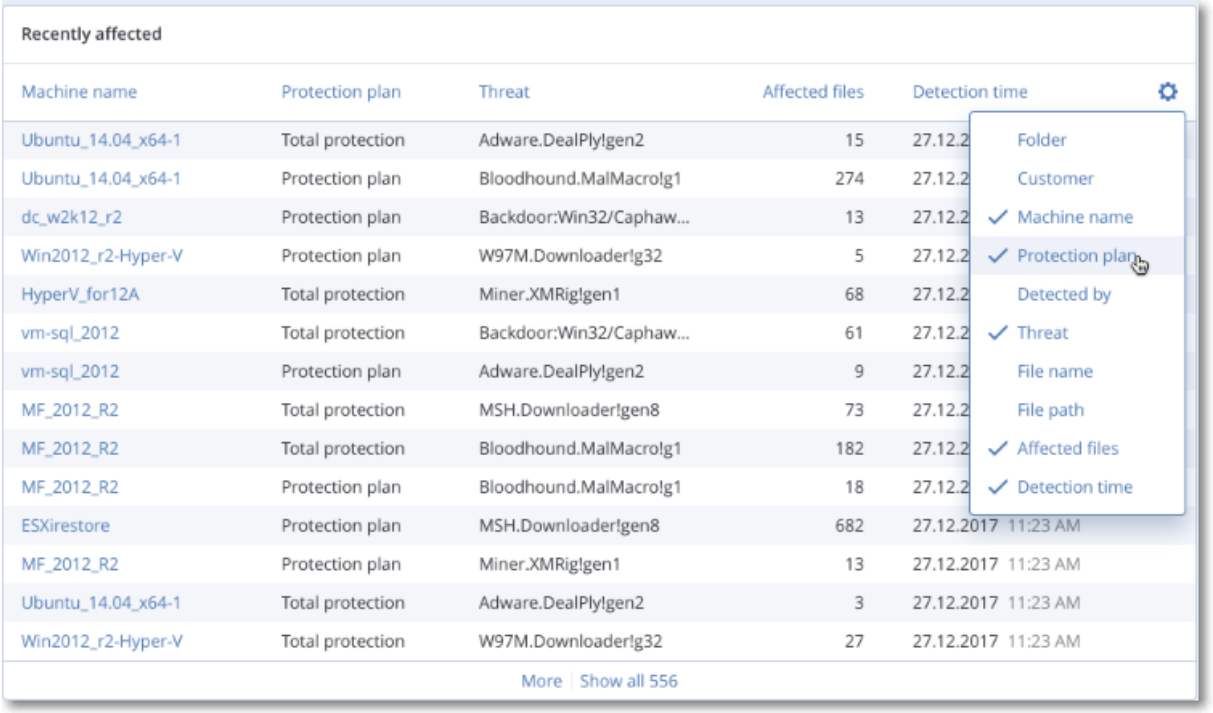
Detail pemindaian cadangan

Widget ini menampilkan informasi terperinci tentang ancaman yang terdeteksi pada cadangan.



Baru-baru ini terdampak

Widget ini menampilkan informasi mendetail tentang beban kerja yang terpengaruh oleh ancaman, seperti virus, malware, dan ramsomeware. Anda dapat menemukan informasi tentang ancaman yang terdeteksi, waktu ketika ancaman terdeteksi, dan berapa banyak file yang terpengaruh.



Mengunduh data untuk beban kerja yang terpengaruh baru-baru ini

Anda dapat mengunduh data untuk beban kerja yang terpengaruh baru-baru ini, membuat file CSV, dan mengirimkannya ke penerima yang Anda tentukan.

Cara mengunduh data untuk beban kerja yang terpengaruh baru-baru ini

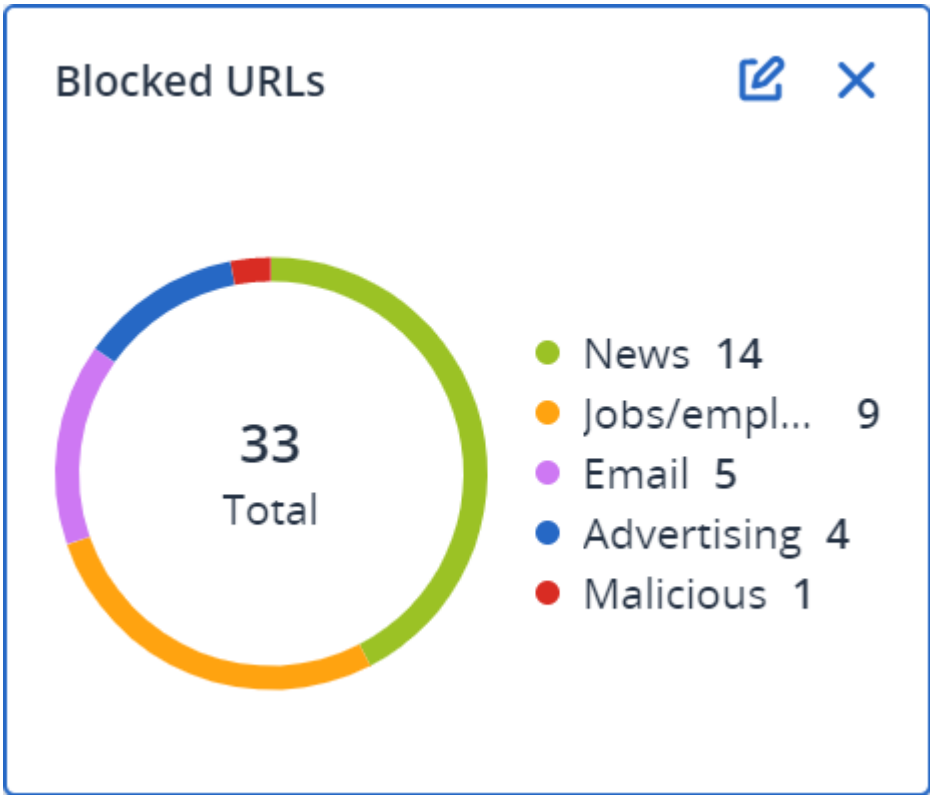
1. Di widget **Terpengaruh baru-baru ini**, klik **Unduh data**.
2. Di bidang **Periode waktu**, masukkan jumlah hari yang Anda inginkan untuk mengunduh data. Jumlah hari maksimum yang dapat Anda masukkan adalah 200 hari.
3. Di bidang **Penerima**, masukkan alamat email semua orang yang akan menerima email dengan tautan untuk mengunduh file CSV.

4. Klik **Unduh**.

   Sistem mulai membuat file CSV dengan data untuk beban kerja yang terpengaruh dalam jangka waktu yang Anda tentukan. Ketika file CSV selesai, sistem mengirim email ke penerima. Setiap penerima kemudian dapat mengunduh file CSV.

URL yang diblokir

Widget menunjukkan statistik URL yang diblokir berdasarkan kategori. Untuk informasi lebih lanjut tentang pemfilteran dan kategorisasi URL, lihat panduan pengguna Perlindungan Cyber.



Widget inventaris perangkat lunak

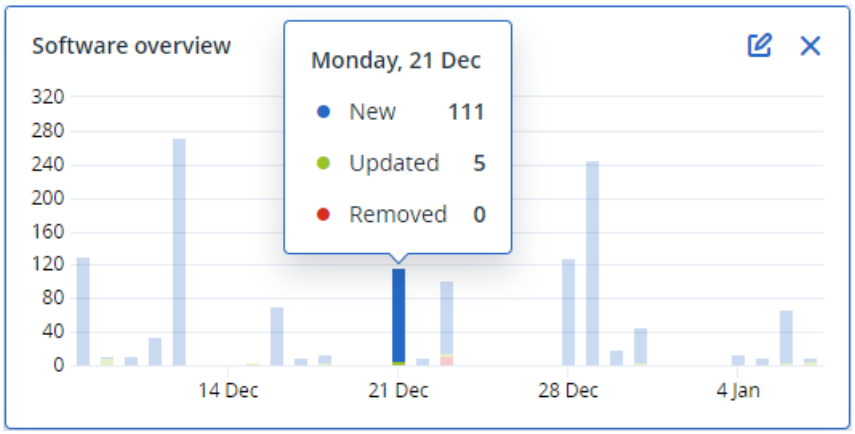
Widget tabel **Inventaris perangkat lunak** menampilkan informasi terperinci tentang semua perangkat lunak yang diinstal pada perangkat Windows dan macOS di organisasi klien Anda.

Software inventory

Folder name	Customer name	Machine name	Software name	Software version	Vendor name	Status	Date installed	Last run	Scan time	Location	User	System type
ACP-QAZ03-A01												
ACP-QAZ03-A01												
ACP-QAZ03-A03												
folder1	rbarf4	ACP-QAZ03-A03	Microsoft Visual C...	9.0.30729.6161	Microsoft Corpora...	New	-	-	11/28/2020, 11:39 ...	-	System	X86
folder1	rbarf4	ACP-QAZ03-A03	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 11:39 ...	-	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\B...	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Mozilla Firefox	45.0.1	Mozilla	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\...	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Mozilla Maintenan...	45.0.1	Mozilla	New	-	-	11/28/2020, 11:39 ...	-	System	X86
folder1	rbarf4	ACP-QAZ03-A03	VMware Tools	10.0.6.3560309	VMware, Inc.	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\V...	System	X64
ACP-QAZ03-A04												
folder1	rbarf4	ACP-QAZ03-A04	Google Chrome	79.0.3945.130	Google LLC	New	-	-	11/28/2020, 2:49 PM	C:\Program Files (x...	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Google Update He...	1.3.36.31	Google LLC	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft Visual C...	9.0.30729.6161	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 2:49 PM	-	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\B...	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Notepad++	6.7.4	Notepad++ Team	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft OneDrive	20.201.1005.0009	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Mozilla Firefox	45.0.1	Mozilla	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\...	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Mozilla Maintenan...	45.0.1	Mozilla	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft Update ...	2.68.0.0	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X64
folder1	rbarf4	ACP-QAZ03-A04	VMware Tools	10.0.6.3560309	VMware, Inc.	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\V...	System	X64

More | Less | Show 1000+

Widget **Ikhtisar perangkat lunak** menampilkan jumlah aplikasi baru, yang diperbarui, dan dihapus pada perangkat Windows dan macOS di organisasi klien Anda dalam kurun waktu tertentu (7 hari, 30 hari, atau bulan ini).



Saat Anda mengarahkan pointer mouse di atas bilah tertentu pada diagram, sebuah tooltip dengan informasi berikut menampilkan:

Baru - jumlah aplikasi yang baru diinstal.

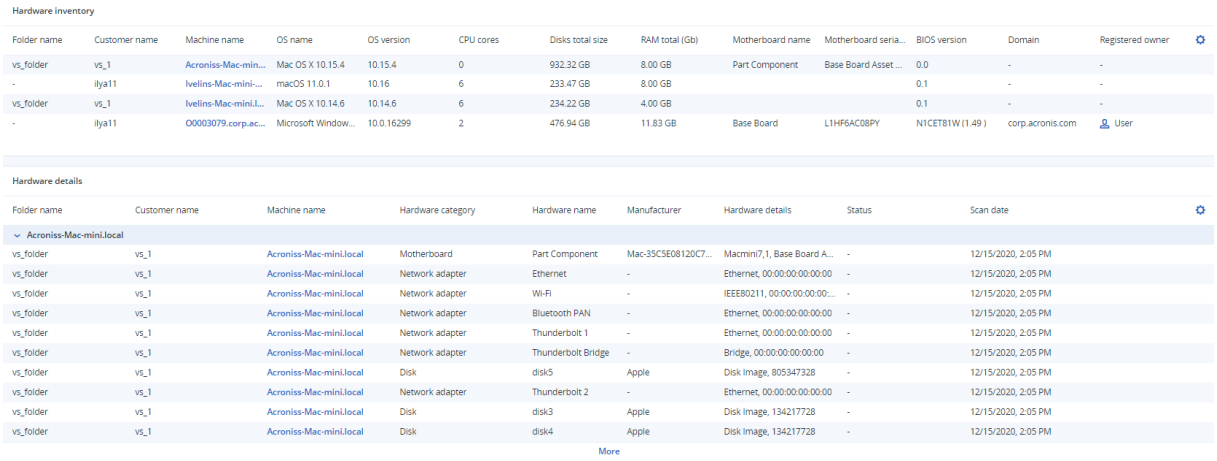
Diperbarui - jumlah aplikasi yang diperbarui.

Dihapus - jumlah aplikasi yang dihapus.

Saat Anda mengeklik bagian bilah yang sesuai dengan status tertentu, jendela pop-up akan dimuat. Jendela tersebut mencantumkan semua pelanggan yang memiliki perangkat dengan aplikasi dalam status yang dipilih pada tanggal terpilih. Anda dapat memilih pelanggan dari daftar, klik **Buka pelanggan**, dan Anda akan dialihkan ke halaman **Manajemen Perangkat Lunak** -> **Inventaris Perangkat Lunak** dalam konsol layanan pelanggan. Informasi di halaman difilter untuk tanggal dan status yang sesuai.

Widget inventaris perangkat keras

Widget tabel **Inventaris perangkat keras** dan **Detail perangkat keras** menampilkan informasi tentang semua perangkat keras yang diinstal pada perangkat fisik dan virtual Windows dan macOS di organisasi klien Anda.



Hardware inventory

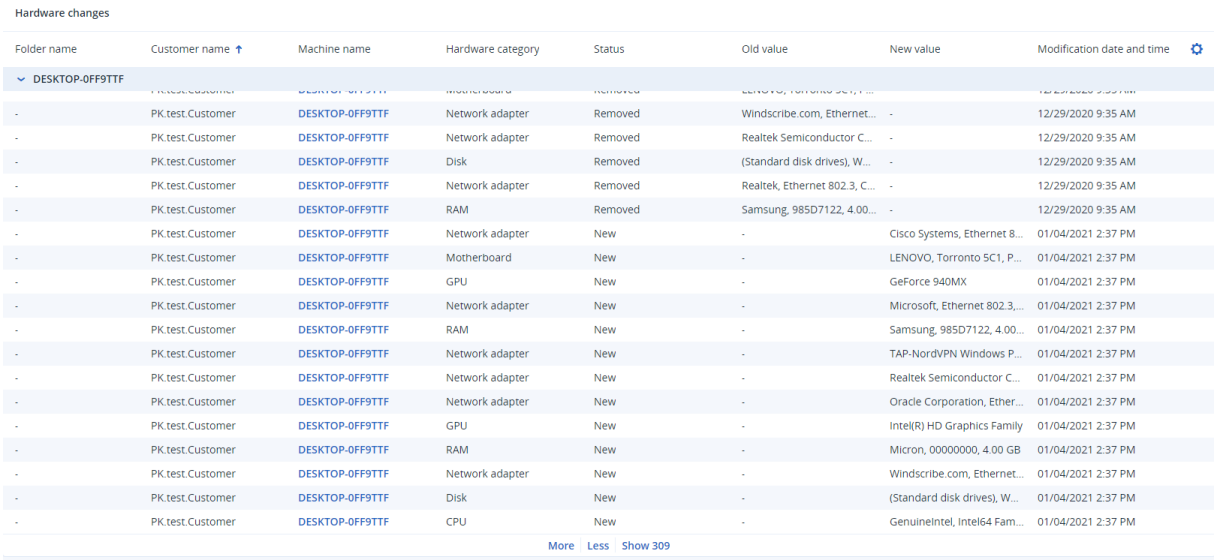
Folder name	Customer name	Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner
vs_folder	vs_1	Acroniss-Mac-min...	Mac OS X 10.15.4	10.15.4	0	932.32 GB	8.00 GB	Part Component	Base Board Asset ...	0.0	-	-
-	ilya11	ivelins-Mac-mini-...	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-
vs_folder	vs_1	ivelins-Mac-mini.l...	Mac OS X 10.14.6	10.14.6	6	234.22 GB	4.00 GB			0.1	-	-
-	ilya11	O0003079.corp.ac...	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	N1CET81W (1.49)	corp.acronis.com	User

Hardware details

Folder name	Customer name	Machine name	Hardware category	Hardware name	Manufacturer	Hardware details	Status	Scan date
Acroniss-Mac-mini.local								
vs_folder	vs_1	Acroniss-Mac-mini.local	Motherboard	Part Component	Mac-35C5E08120C7...	Macmini7,1, Base Board A...	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Ethernet	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Wi-Fi	-	IEEE80211, 00:00:00:00:00:...	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Bluetooth PAN	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt 1	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt Bridge	-	Bridge, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk5	Apple	Disk Image, 805347328	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt 2	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk3	Apple	Disk Image, 134217728	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk4	Apple	Disk Image, 134217728	-	12/15/2020, 2:05 PM

More

Widget tabel **Perubahan perangkat keras** menampilkan informasi tentang perangkat keras yang ditambahkan, dihapus, dan diubah pada perangkat fisik dan virtual Windows dan macOS di organisasi klien Anda untuk jangka waktu tertentu (7 hari, 30 hari, atau bulan saat ini).



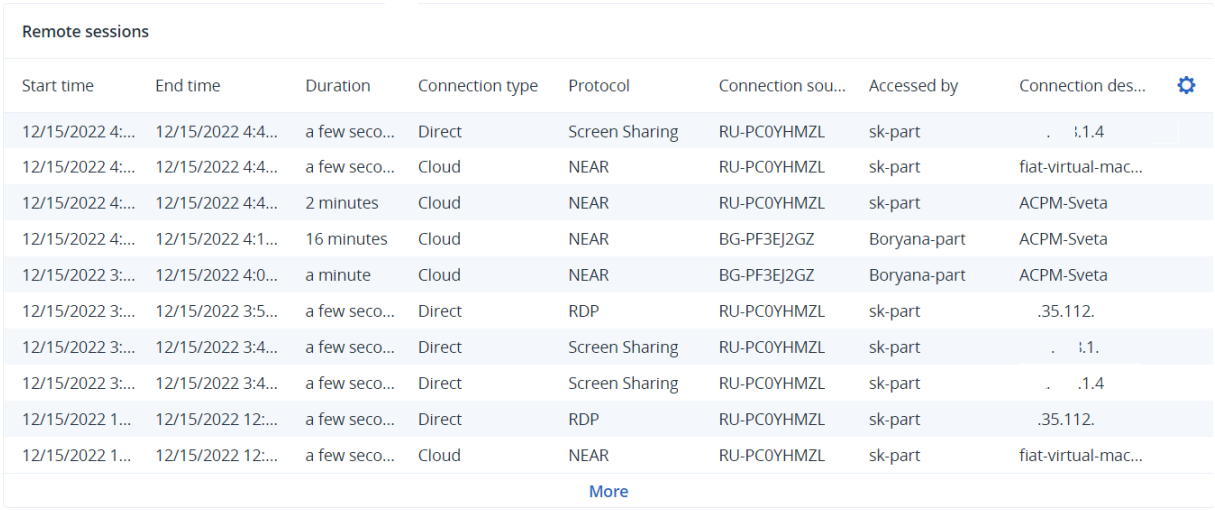
Hardware changes

Folder name	Customer name	Machine name	Hardware category	Status	Old value	New value	Modification date and time
DESKTOP-0FF9TTF							
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Windscribe.com, Ethernet...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Realtek Semiconductor C...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Disk	Removed	(Standard disk drives), W...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Realtek, Ethernet 802.3, C...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	Removed	Samsung, 985D7122, 4.00...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 8...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Torronto 5C1, P...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	GPU	New	-	GeForce 940MX	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Microsoft, Ethernet 802.3,...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows P...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor C...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ether...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Windscribe.com, Ethernet...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), W...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	CPU	New	-	GenuineIntel, Intel64 Fam...	01/04/2021 2:37 PM

More | Less | Show 309

Riwayat sesi

Widget menampilkan detail informasi tentang sesi desktop jarak jauh dan transfer file yang dilakukan di organisasi klien Anda selama periode waktu tertentu.



Pelaporan

Untuk membuat laporan tentang penggunaan dan operasi layanan, klik **Laporan**.

Penggunaan

Laporan penggunaan menyediakan data historis tentang penggunaan layanan. Laporan penggunaan tersedia dalam format CSV dan HTML.

Tipe laporan

Anda dapat memilih salah satu dari jenis laporan berikut:

- **Penggunaan saat ini**

  Laporan mencakup metrik penggunaan layanan saat ini.

  Metrik penggunaan dihitung dalam setiap periode penagihan penyewa turunan. Jika penyewa yang dimasukkan dalam laporan memiliki periode penagihan yang berbeda, penggunaan penyewa induk dapat berbeda dari jumlah penggunaan penyewa turunan.
- **Distribusi penggunaan saat ini**

  Laporan ini hanya tersedia untuk penyewa mitra yang dikelola oleh sistem penyediaan eksternal. Laporan ini berguna ketika periode penagihan penyewa turunan tidak sesuai dengan periode penagihan penyewa utama. Laporan mencakup metriks penggunaan layanan bagi penyewa turunan yang dikalkulasikan dalam periode penagihan penyewa utama yang sedang berjalan. Penggunaan penyewa induk dijamin berada pada jumlah yang sama dengan penggunaan penyewa turunan.
- **Ringkasan untuk periode**

  Laporan mencakup metriks penggunaan layanan di akhir periode yang telah ditentukan dan perbedaan yang timbul antara metrik di awal dan akhir periode yang telah ditentukan.
- **Hari ke hari untuk periode**

  Laporan mencakup metrik penggunaan layanan dan perubahan yang ada setiap harinya dalam periode yang telah ditentukan.

Lingkup laporan

Anda dapat memilih lingkup laporan dari nilai berikut:

- **Pelanggan dan mitra langsung**
  Laporan akan mencakup metrik penggunaan layanan hanya untuk penyewa turunan langsung dari penyewa tempat Anda beroperasi.
- **Semua pelanggan dan mitra**
  Laporan ini akan mencakup metrik penggunaan layanan untuk semua penyewa turunan dari penyewa tempat Anda beroperasi.
- **Semua pelanggan dan mitra (termasuk rincian pengguna)**
  Laporan ini akan mencakup metrik penggunaan layanan untuk semua penyewa turunan dari penyewa tempat Anda beroperasi dan untuk semua pengguna di dalam penyewa.

Metrik dengan penggunaan nol

Anda dapat mengurangi jumlah baris dalam laporan dengan menampilkan informasi tentang metrik yang memiliki penggunaan bukan nol, dan menyembunyikan informasi tentang metrik yang memiliki penggunaan nol.

Mengonfigurasi laporan penggunaan terjadwal

Laporan terjadwal mencakup metrik penggunaan layanan untuk bulan kalender penuh terakhir. Laporan dibuat pada pukul 23:59:59 UTC di hari pertama setiap bulan dan dikirim pada hari kedua bulan tersebut. Laporan dikirim ke semua administrator penyewa Anda yang memiliki kotak centang **Laporan penggunaan terjadwal** yang dipilih dalam pengaturan pengguna.

Untuk mengaktifkan atau menonaktifkan laporan terjadwal

1. Masuk ke portal manajemen.
2. Pastikan Anda beroperasi di penyewa teratas yang tersedia untuk Anda.
3. Klik **Laporan** > **Penggunaan**.
4. Klik **Terjadwal**.
5. Pilih atau kosongkan kotak centang **Kirim ringkasan bulanan** laporan.
6. Dalam **Tingkat detail**, pilih cakupan laporan.
7. [Opsional] Pilih **Sembunyikan metrik dengan penggunaan nol** jika Anda tidak ingin menyertakan metrik dengan penggunaan nol dari laporan.

Mengonfigurasi laporan penggunaan kustom

Jenis laporan ini dapat dibuat sesuai permintaan dan tidak dapat dijadwalkan. Laporan akan dikirim ke alamat email Anda.

Untuk membuat laporan kustom

1. Masuk ke portal manajemen.
2. Navigasikan ke penyewa yang untuknya Anda ingin membuat penyewa.
3. Klik **Laporan** > **Penggunaan**.
4. Pilih tab **Kustom**.
5. Di **Jenis**, pilih jenis laporan seperti yang dijelaskan di atas.
6. [Tidak tersedia untuk jenis laporan **Penggunaan saat ini**] Di **Periode**, pilih periode pelaporan:
   - **Bulan kalender saat ini**
   - **Bulan kalender sebelumnya**
   - **Kustom**
7. [Tidak tersedia untuk jenis laporan **Penggunaan saat ini**] Jika Anda ingin menentukan periode pelaporan kustom, pilih tanggal mulai dan tanggal akhir. Jika tidak, lewati langkah ini.
8. Di **Tingkat detail**, pilih lingkup laporan seperti yang dijelaskan di atas.
9. [Opsional] Pilih **Sembunyikan metrik dengan penggunaan nol** jika Anda tidak ingin menyertakan metrik dengan penggunaan nol dari laporan.
10. Untuk menghasilkan laporan, klik **Hasilkan lalu kirim**.

Laporan operasi

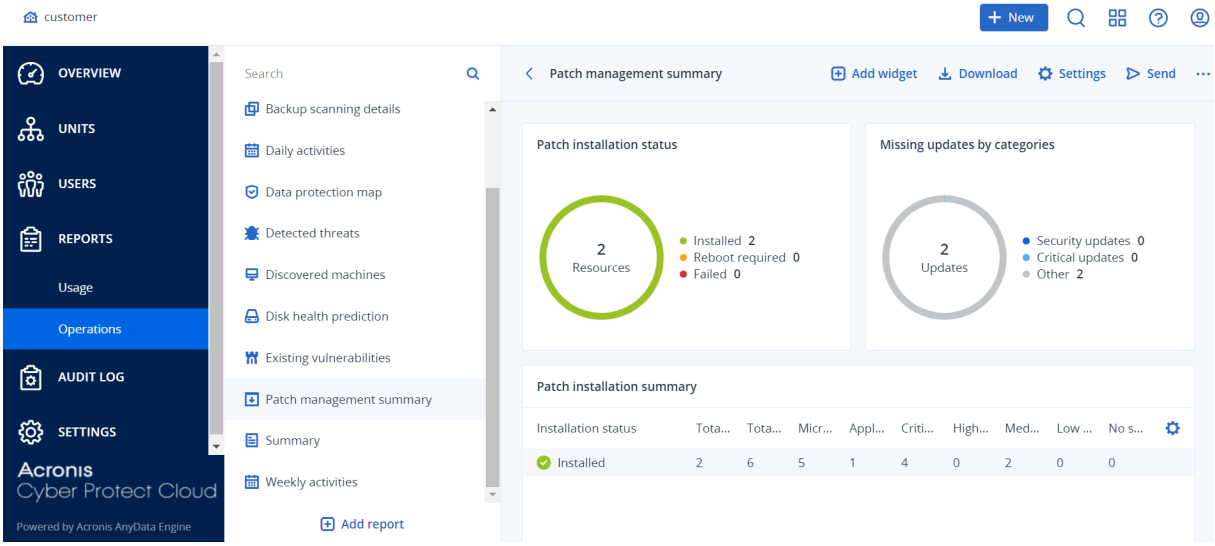
Laporan tentang operasi dapat menyertakan set widget dasbor **Operasi**. Secara default, semua widget menampilkan informasi ringkasan untuk penyewa tempat Anda beroperasi. Anda dapat mengubah ini secara individual untuk setiap widget dengan mengeditnya, atau untuk semua widget dalam pengaturan laporan.

Bergantung pada tipe widget, laporan tersebut mencakup data untuk suatu rentang waktu atau untuk saat penjelajahan atau pembuatan laporan. Lihat "Data yang dilaporkan berdasarkan tipe widget" (hlm. 117).

Semua widget historis menampilkan data untuk rentang waktu yang sama. Anda dapat mengubah rentang ini di pengaturan laporan.

Anda dapat menggunakan laporan default atau membuat laporan kustom.

Anda dapat mengunduh laporan tentang operasi atau mengirimnya melalui email dalam format Excel (XLSX) atau PDF.



Laporan default tercantum di bawah ini:

Nama laporan	Deskripsi
Skor #CyberFit berdasarkan mesin	Menampilkan Skor #CyberFit, berdasarkan evaluasi metrik kemanan dan konfigurasi untuk setiap mesin, serta rekomendasi untuk penyempurnaan.
Peringatan	Menampilkan peringatan yang terjadi selama periode waktu tertentu.
Detail pemindaian cadangan	Menampilkan informasi terperinci tentang ancaman yang terdeteksi dalam cadangan.
Aktivitas sehari-hari	Menampilkan informasi ringkasan tentang aktivitas yang dilakukan selama periode waktu tertentu.
Peta perlindungan data	Menampilkan informasi terperinci tentang jumlah, ukuran, lokasi, status proteksi semua file penting dalam mesin.
Ancaman terdeteksi	Menampilkan perincian mesin yang terdampak melalui jumlah ancaman yang diblokir serta mesin yang sehat dan rentan.
Mesin yang ditemukan	Menampilkan semua mesin yang ditemukan dalam jaringan organisasi.
Prediksi kesehatan disk	Menampilkan prediksi ketika HDD/SSD Anda akan rusak dan status disk saat ini.
Kerentanan yang ada	Menampilkan kerentanan yang ada untuk OS dan aplikasi dalam organisasi Anda. Laporan juga menampilkan rincian mesin yang terdampak dalam jaringan Anda untuk setiap produk yang tercantum.

Rangkuman manajemen patch	Menampilkan jumlah patch yang tidak ada, patch yang diinstal, dan patch yang diterapkan. Anda dapat memperinci laporan untuk mendapatkan informasi patch yang hilang/terinstal serta perincian semua sistem.
Ringkasan	Menampilkan informasi ringkasan tentang perangkat terlindungi untuk periode waktu tertentu.
Aktivitas mingguan	Menampilkan informasi ringkasan tentang aktivitas yang dilakukan selama periode waktu tertentu.
Inventaris perangkat lunak	Menampilkan informasi terperinci tentang semua perangkat lunak yang diinstal pada mesin Windows dan macOS di organisasi klien Anda.
Inventaris Perangkat Keras	Menampilkan informasi terperinci tentang semua perangkat lunak yang tersedia pada mesin Windows dan macOS fisik dan virtual di organisasi klien Anda.
Sesi jarak jauh	Menampilkan detail informasi tentang sesi desktop jarak jauh dan transfer file yang dilakukan di organisasi klien Anda selama periode waktu tertentu.

Untuk menampilkan laporan, klik namanya.

Untuk mengakses operasi disertai laporan, klik ikon elipsis vertikal pada baris laporan. Operasi yang sama tersedia dari dalam laporan.

Menambahkan laporan

1. Klik **Tambah laporan**.
2. Lakukan salah satu langkah berikut:
   - Untuk menambahkan laporan yang telah ditetapkan, klik namanya.
   - Untuk menambahkan laporan kustom, klik **Kustom**, klik nama laporan (nama yang ditetapkan secara default seperti **Kustom (1)**), lalu tambahkan widget ke laporan.
3. [Opsional] Seret dan lepas widget untuk menyusunnya kembali.
4. [Opsional] Edit laporan seperti yang dijelaskan di bawah ini.

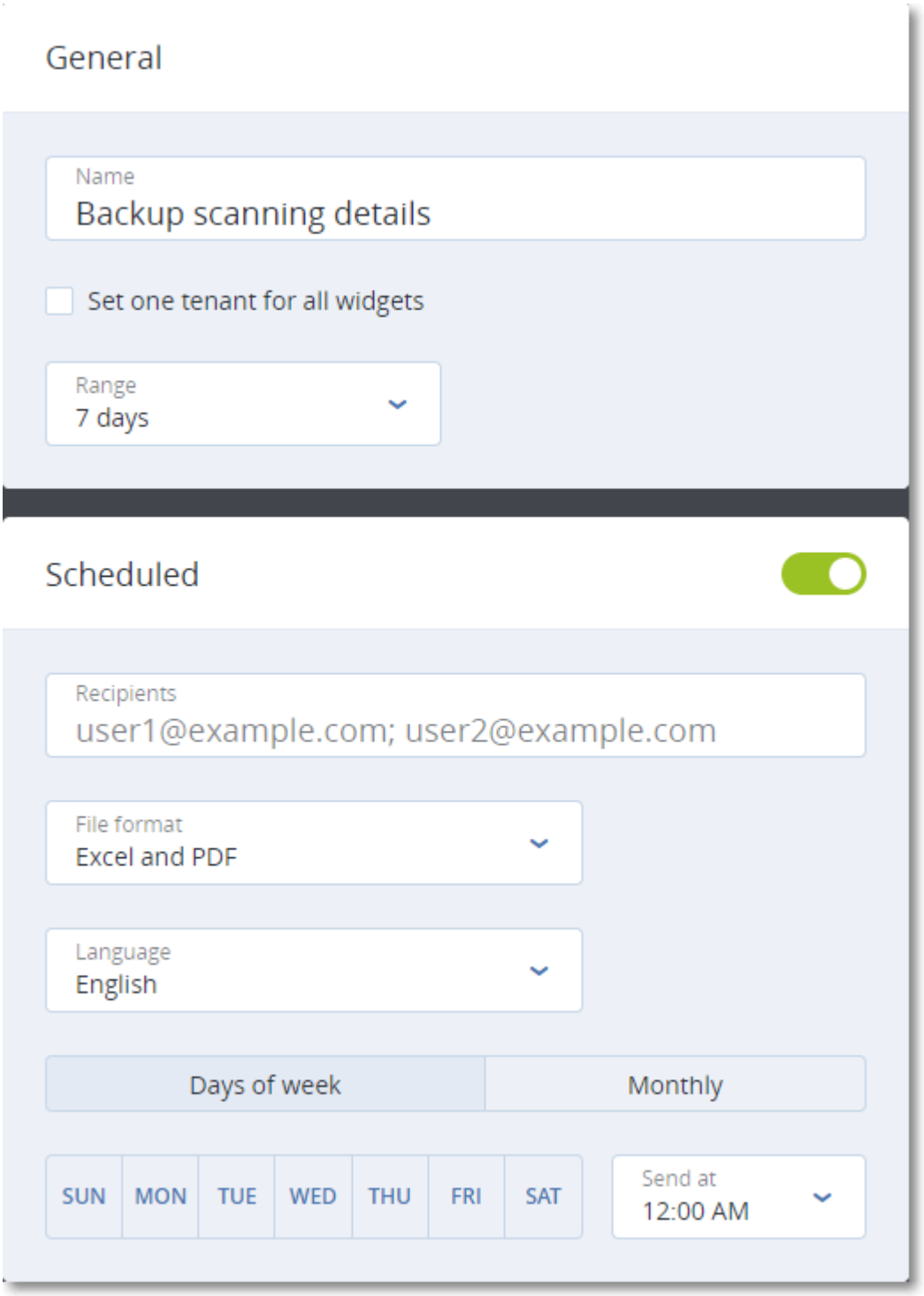
Mengedit pengaturan laporan

Untuk mengedit laporan, klik namanya, lalu klik **Pengaturan**. Saat mengedit laporan, Anda dapat:

- Mengganti nama laporan
- Mengubah penyewa yang ditampilkan untuk semua widget yang disertakan dalam laporan
  Jika Anda memiliki penyewa anak, maka opsi **Atur satu penyewa untuk semua widget** tersedia untuk Anda. Opsi ini memungkinkan Anda memfilter data di semua widget laporan dari penyewa

yang dipilih. Jika opsi ini tidak dipilih, widget akan menampilkan data untuk semua penyewa anak dari penyewa saat ini.

- Mengubah rentang waktu untuk semua widget yang disertakan dalam laporan
- Menjadwalkan pengiriman laporan melalui email dalam format PDF atau/dan Excel.



Menjadwalkan laporan

1. Klik nama laporan, lalu klik **Pengaturan**.
2. Aktifkan switch **Terjadwal**.
3. Tentukan alamat email penerima.
4. Pilih format laporan: PDF, Excel, atau keduanya.
5. Pilih hari dan waktu kapan laporan akan dikirim.
6. Klik **Simpan** di sudut kanan atas.

Mengekspor dan mengimpor struktur laporan

Anda dapat mengekspor dan mengimpor struktur laporan (set widget dan pengaturan laporan) ke file JSON. Menyalin struktur laporan dari satu penyewa ke penyewa lainnya mungkin akan berguna.

Untuk mengekspor struktur laporan, klik nama laporan, klik ikon elipsis vertikal di sudut kanan atas, lalu klik **Ekspor**.

Untuk mengimpor struktur laporan, klik **Tambah laporan**, lalu klik **Impor**.

Mengunduh laporan

Anda dapat mengunduh laporan, klik **Unduh** dan pilih format yang diperlukan:

- Excel dan PDF
- Excel
- PDF

Membuang data laporan

Anda dapat mengirim sampah data laporan dalam file CSV melalui email. Buangan mencakup semua data laporan (tanpa pemfilteran) untuk rentang waktu kustom. Stempel waktu dalam laporan CSV dalam format UTC sedangkan dalam laporan Excel dan PDF stempel waktu berada dalam zona waktu sistem saat ini.

Perangkat lunak menghasilkan buangan data pada saat memproses. Jika Anda menetapkan jangka waktu yang lama, tindakan ini mungkin memerlukan waktu lama.

Untuk membuang data laporan

1. Klik nama laporan.
2. Klik ikon elipsis vertikal di sudut kanan atas, lalu klik **Buang data**.
3. Tentukan alamat email penerima.
4. Di **Rentang waktu**, tentukan rentang waktunya.
5. Klik **Kirim**.

Ringkasan eksekutif

Rangkuman laporan Eksekutif memberikan ikhtisar tentang status proteksi lingkungan pelanggan Anda dan perangkat terproteksinya selama rentang waktu tertentu.

Rangkuman laporan Eksekutif mencakup bagian dengan widget dinamis yang menunjukkan metrik kinerja utama yang terkait dengan penggunaan layanan awan berikut oleh klien: Cadangan, Proteksi antimalware, Penilaian kerentanan, Manajemen patch, Pencegahan Kehilangan Data, Notaris, Pemulihan Bencana, dan Files Sync & Share.

Ada beberapa cara agar Anda dapat menyesuaikan laporan.

- Tambah atau hapus bagian.
- Ubah urutan bagian.
- Ganti nama bagian.
- Pindah widget dari satu bagian ke bagian lainnya.
- Ubah urutan widget di setiap bagian.
- Tambah atau hapus widget.
- Sesuaikan widget.

Anda dapat membuat rangkuman laporan Eksekutif dalam format PDF dan Excel, lalu mengirimkannya ke pemangku kepentingan atau pemilik organisasi pelanggan Anda, agar mereka dapat melihat dengan mudah nilai bisnis dan teknis dari layanan yang diberikan.

Administrator mitra hanya dapat membuat dan mengirimkan rangkuman laporan Eksekutif ke pelanggan langsung. Dalam hal hierarki penyewa yang lebih kompleks yang memiliki submitra, submitra tersebut harus membuat laporan.

Widget ringkasan eksekutif

Anda dapat menambah atau menghapus bagian dan widget dari rangkuman laporan Eksekutif, sehingga mengontrol informasi apa yang akan dimasukkan ke dalamnya.

Widget ikhtisar beban kerja

Tabel berikut ini memberikan informasi lebih lanjut tentang widget dalam bagian **Ikhtisar beban kerja**.

Widget	Deskripsi
Status proteksi beban kerja awan	Widget ini menampilkan jumlah beban kerja awan yang terproteksi dan tidak terproteksi berdasarkan jenisnya pada saat laporan dibuat. Beban kerja awan yang dilindungi adalah beban kerja awan di mana setidaknya satu rencana pencadangan diterapkan. Beban kerja awan yang tidak dilindungi adalah beban kerja awan di mana tidak ada rencana pencadangan yang diterapkan. Tipe beban kerja awan berikut ditampilkan

Widget	Deskripsi
	dalam diagram (dalam urutan alfabetis dari A sampai Z): • Google Workspace Drive • Google Workspace Gmail • Google Workspace Shared Drive • Kotak surat Exchange yang Dihosting • Kotak surat Microsoft 365 • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • Situs web Untuk beberapa tipe beban kerja, digunakan grup beban kerja berikut: • Microsoft 365: Pengguna, Grup, Folder Umum, Tim, dan Koleksi Situs • Google Workspace: Pengguna dan Drive Bersama • Exchange yang Dihosting: Pengguna Jika dalam satu grup beban kerja terdapat lebih dari 10.000 beban kerja, widget tidak menampilkan data apa pun untuk beban kerja terkait. Misalnya, jika pelanggan memiliki akun Microsoft 365 dengan 10.000 kotak surat dan layanan OneDrive untuk 500 pengguna, semuanya termasuk dalam sumber daya Pengguna. Jumlah beban kerja ini adalah 10.500, yang melampaui batas 10.000 dalam grup sumber daya. Maka, widget akan menyembunyikan tipe beban kerja terkait: Kotak Surat Microsoft 365, dan Microsoft 365 OneDrive.
Ringkasan perlindungan cyber	Widget menunjukkan metrik utama Kinerja perlindungan cyber selama rentang waktu tertentu. **Data dicadangkan** - ukuran total arsip yang dibuat di penyimpanan awan dan lokal. **Ancaman yang dimitigasi** - jumlah total malware yang diblokir di semua perangkat. **URL berbahaya yang diblokir** - jumlah total URL yang diblokir pada semua perangkat. **Kerentanan yang di-patch** - jumlah total kerentanan yang diperbaiki melalui pemasangan patch perangkat lunak di semua perangkat. **Patch yang diinstal** - jumlah total patch yang diinstal pada semua perangkat. **Server yang dilindungi oleh DR** - jumlah total server yang dilindungi oleh Pemulihan Bencana. **Pengguna File Sync & Share** - jumlah total pengguna akhir dan pengguna tamu yang menggunakan Cyber Files.

Widget	Deskripsi
	File yang sudah dinotarisasikan - jumlah total file yang dinotarisasikan. **Dokumen yang dibubuhi eSign** - jumlah total dokumen yang dibubuhi eSign. **Perangkat periferal yang diblokir** - jumlah total perangkat periferal yang diblokir.
Status jaringan beban kerja	Widget ini menampilkan jumlah beban kerja yang terisolasi dan jumlah beban kerja yang terhubung (status normal beban kerja). Pilih pelanggan yang relevan; Tampilan beban kerja yang ditampilkan disaring untuk menampilkan beban kerja terisolasi. Klik nilai Terhubung untuk menampilkan Beban Kerja dengan daftar agen yang disaring untuk menampilkan beban kerja terhubung (untuk pelanggan terpilih).
Status proteksi beban kerja	Widget menampilkan beban kerja yang dilindungi dan tidak dilindungi berdasarkan tipe pada saat pembuatan laporan. Beban kerja yang dilindungi adalah beban kerja di mana setidaknya satu rencana proteksi atau pencadangan diterapkan. Beban kerja yang tidak dilindungi adalah beban kerja di mana tidak ada rencana proteksi atau pencadangan yang diterapkan. Beban kerja berikut dihitung: **Server** - server fisik, dan server Pengontrol Domain. **Stasiun kerja** - stasiun kerja fisik. **Mesin virtual** - mesin virtual berbasis agen dan tanpa agen. **Server hosting web** - server virtual atau fisik dengan cPanel atau Plesk yang terinstal. **Perangkat seluler** - perangkat seluler fisik. Satu beban kerja dapat termasuk dalam lebih dari satu kategori. Misalnya, suatu server hosting web termasuk dalam dua kategori - **Server**, dan **Server hosting web**.
Status proteksi beban kerja awan	**Status proteksi beban kerja awan** Widget menampilkan jumlah beban kerja awan yang dilindungi dan tidak dilindungi berdasarkan tipe pada saat pembuatan laporan. Beban kerja awan yang dilindungi adalah beban kerja awan di mana setidaknya satu rencana pencadangan diterapkan. Beban kerja awan yang tidak dilindungi adalah beban kerja awan di mana tidak ada rencana pencadangan yang diterapkan. Tipe beban kerja awan berikut ditampilkan dalam diagram (dalam urutan alfabetis dari A sampai Z): • Google Workspace Drive • Google Workspace Gmail • Google Workspace Shared Drive • Kotak surat Exchange yang Dihosting • Kotak surat Microsoft 365

Widget	Deskripsi
	• Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • Situs web Untuk beberapa tipe beban kerja, digunakan grup beban kerja berikut: • Microsoft 365: Pengguna, Grup, Folder Umum, Tim, dan Koleksi Situs • Google Workspace: Pengguna dan Drive Bersama • Exchange yang Dihosting: Pengguna Jika dalam satu grup beban kerja terdapat lebih dari 10.000 beban kerja, widget tidak menampilkan data apa pun untuk beban kerja terkait. Misalnya, jika pelanggan memiliki akun Microsoft 365 dengan 10.000 kotak surat dan layanan OneDrive untuk 500 pengguna, semuanya termasuk dalam sumber daya Pengguna. Jumlah beban kerja ini adalah 10.500, yang melampaui batas 10.000 dalam grup sumber daya. Maka, widget akan menyembunyikan tipe beban kerja terkait: Kotak Surat Microsoft 365, dan Microsoft 365 OneDrive.

Widget proteksi antimalware

Tabel berikut ini memberikan informasi lebih lanjut tentang widget dalam bagian **Perlindungan ancaman**.

Widget	Deskripsi
Pemindaian antimalware pada file	Widget menampilkan hasil pemindaian antimalware sesuai permintaan pada perangkat selama rentang waktu tertentu. **File** - jumlah total file yang dipindai **Bersih** - jumlah total file bersih **Terdeteksi, dikarantina** - jumlah total file terinfeksi yang dikarantina **Terdeteksi, tidak dikarantina** - jumlah total file terinfeksi yang tidak dikarantina **Perangkat terlindungi** - Jumlah total perangkat dengan kebijakan proteksi antimalware yang diterapkan **Jumlah total perangkat terdaftar** - Jumlah total perangkat terdaftar pada waktu pembuatan laporan
Pemindaian antimalware cadangan	Widget menunjukkan hasil pemindaian antimalware pada cadangan untuk rentang tanggal tertentu, menggunakan metrik berikut: • Jumlah total titik pemulihan yang dipindai • Jumlah titik pemulihan bersih • Jumlah titik pemulihan bersih dengan partisi yang tidak didukung

Widget	Deskripsi
	• Jumlah titik pemulihan yang terinfeksi. Metrik ini mencakup jumlah titik pemulihan yang terinfeksi dengan partisi yang tidak didukung.
URL yang diblokir	Selama rentang waktu tertentu, widget menampilkan jumlah URL yang diblokir yang dikelompokkan berdasarkan kategori situs web. Widget tersebut mencantumkan tujuh kategori situs web yang memiliki jumlah URL diblokir terbesar, dan menggabungkan kategori situs web lain dalam **Lainnya**. Untuk informasi lebih lanjut tentang kategori situs web, lihat topik filter URL dalam Cyber Protection.
Burndown insiden keamanan	Widget ini menampilkan rentang efisiensi dalam menutup insiden untuk perusahaan terpilih; jumlah insiden terbuka yang dibandingkan dengan jumlah insiden tertutup selama periode waktu tertentu. Arahkan pointer mouse terhadap sebuah kolom untuk menampilkan uraian insiden tertutup dan terbuka untuk tanggal terpilih. Nilai dalam % yang ditampilkan dalam tanda kurung menandakan peningkatan atau penurunan dibandingkan periode waktu sebelumnya.
MTTR Insiden	Widget ini menampilkan waktu resolusi rata-rata untuk insiden keamanan. Ini menandakan seberapa cepat insiden teridentifikasi dan terpecahkan. Klik pada kolom untuk menampilkan rincian insiden berdasarkan keparahannya (**Kritis**, **Tinggi**, dan **Menengah**), dan indikasi yang menjelaskan seberapa lama insiden yang berdasarkan perbedaan tingkat keparahan tersebut dapat diselesaikan. Nilai dalam % yang ditampilkan dalam tanda kurung menandakan peningkatan atau penurunan dibandingkan periode waktu sebelumnya.
Status ancaman	Widget ini menampilkan status ancaman terkini untuk beban kerja perusahaan (dengan mengesampingkan jumlah beban kerja), menyoroti jumlah insiden terkini yang belum dimitigasi dan yang perlu untuk diinvestigasi. Widget ini juga mengindikasikan jumlah insiden yang sudah dimitigasi (secara manual dan/atau secara otomatis oleh sistem).
Ancaman terdeteksi oleh teknologi proteksi	Selama rentang waktu tertentu, widget menampilkan jumlah ancaman terdeteksi yang dikelompokkan berdasarkan teknologi proteksi berikut: • Pemindaian antimalware • Mesin perilaku • Perlindungan cryptomining • Pencegahan eksploit • Perlindungan aktif ransomware • Perlindungan waktu nyata • Pemfilteran URL

Widget pencadangan

Tabel berikut ini memberikan informasi lebih lanjut tentang widget dalam bagian **Cadangan**.

Widget	Deskripsi
Beban kerja dicadangkan	Widget menampilkan jumlah total beban kerja terdaftar berdasarkan status cadangan. **Dicadangkan** - jumlah beban kerja yang dicadangkan (sekurangnya ada satu pencadangan yang berhasil dilakukan) selama rentang tanggal laporan. **Tidak dicadangkan** - jumlah beban kerja yang tidak dicadangkan (tidak ada pencadangan yang berhasil dilakukan) selama rentang tanggal laporan.
Status kesehatan disk berdasarkan perangkat fisik	Widget menampilkan kumpulan status kesehatan perangkat fisik berdasarkan status kesehatan disk-nya. **OK** - Status kesehatan disk ini bernilai [70-100]. Status perangkat adalah **OK** ketika semua disk-nya dalam status **OK**. **Peringatan** - Status kesehatan disk ini bernilai [30-70]. Suatu perangkat berstatus **Peringatan** ketika status sekurangnya salah satu disknya adalah **Peringatan**, dan ketika tidak ada disk dalam status **Kesalahan**. **Kesalahan** - Status kesehatan disk ini bernilai [0-30]. Suatu perangkat berstatus **Kesalahan** ketika status sekurangnya salah satu disknya adalah **Kesalahan**. **Menghitung data disk** - Status perangkat adalah **Menghitung data disk** jika status disk tersebut belum dihitung.
Penggunaan penyimpanan cadangan	Selama rentang waktu tertentu, widget menampilkan jumlah total dan ukuran total cadangan di penyimpanan awan dan lokal.

Widget penilaian kerentanan dan manajemen patch

Tabel berikut ini memberikan informasi lebih lanjut tentang widget dalam bagian **Penilaian kerentanan dan manajemen patch**.

Widget	Deskripsi
Kerentanan yang di-patch	Widget menampilkan hasil kinerja penilaian kerentanan selama rentang waktu tertentu. **Total**- jumlah total kerentanan yang di-patch. **Kerentanan perangkat lunak Microsoft**- jumlah total kerentanan Microsoft yang diperbaiki pada semua perangkat Windows.

Widget	Deskripsi
	Kerentanan perangkat lunak pihak ketiga Windows- jumlah total kerentanan pihak ketiga Windows yang diperbaiki pada semua perangkat Windows. **Beban kerja yang dipindai** - jumlah total perangkat yang berhasil dipindai untuk menemukan kerentanan sekurangnya satu kali dalam rentang waktu tertentu.
Patch yang diinstal	Widget menampilkan hasil kinerja manajemen patch selama rentang waktu tertentu. **Diinstal** - jumlah total patch yang berhasil diinstal pada semua perangkat. **Patch perangkat lunak Microsoft** - jumlah total patch perangkat lunak Microsoft yang diinstal pada semua perangkat Windows. **Patch perangkat lunak pihak ketiga Windows** - jumlah total patch perangkat lunak pihak ketiga Windows yang diinstal pada semua perangkat Windows. **Beban kerja yang di-patch** - jumlah total perangkat yang berhasil di-patch (sekurangnya satu patch berhasil dipasang selama rentang waktu tertentu).

Widget Pemulihan Bencana

Tabel berikut menyediakan informasi tentang widget dalam bagian **Pemulihan bencana**.

Widget	Deskripsi
Statistik Pemulihan Bencana	Widget menampilkan metrik kinerja utama Pemulihan Bencana selama rentang waktu tertentu. **Failover produksi** - jumlah operasi failover produksi selama rentang waktu tertentu. **Failover uji** - jumlah total operasi failover uji yang dilakukan selama rentang waktu tertentu. **Server utama** - jumlah total server utama pada saat pembuatan laporan. **Server pemulihan** - jumlah total server pemulihan pada saat pembuatan laporan. **IP Publik** - jumlah total alamat IP publik (pada saat pembuatan laporan). **Total titik komputasi yang dipakai** - jumlah total titik komputasi yang dipakai selama rentang waktu tertentu.
Server Pemulihan Bencana sudah diuji	Widget menunjukkan informasi tentang server yang dilindungi oleh Pemulihan Bencana dan diuji dengan failover uji. Widget menunjukkan metrik berikut:

Widget	Deskripsi
	Server terlindungi - jumlah server yang dilindungi oleh Pemulihan Bencana (server yang memiliki sekurangnya satu server pemulihan) pada saat pembuatan laporan. **Teruji** - jumlah server yang dilindungi oleh Pemulihan Bencana yang diuji menggunakan failover uji selama rentang waktu yang dipilih, di antara semua server yang dilindungi oleh Pemulihan Bencana. **Belum diuji** - jumlah server yang dilindungi oleh Pemulihan Bencana yang belum diuji menggunakan failover uji selama rentang waktu yang dipilih, di antara semua server yang dilindungi oleh Pemulihan Bencana. Widget juga menunjukkan ukuran penyimpanan Pemulihan Bencana (dalam GB) pada saat pembuatan laporan. Itu adalah jumlah ukuran cadangan di server awan.
Server yang dilindungi oleh Pemulihan Bencana	Widget menunjukkan informasi tentang server yang dilindungi oleh Pemulihan Bencana dan server yang tidak dilindungi. Widget menunjukkan metrik berikut: Jumlah total server yang terdaftar dalam penyewa pelanggan pada saat pembuatan laporan. **Terlindungi** - jumlah server yang dilindungi oleh Pemulihan Bencana (memiliki sekurangnya satu server pemulihan dan keseluruhan cadangan server) di antara semua server terdaftar pada saat pembuatan laporan. **Tidak terlindungi** - jumlah total server yang tidak terlindungi di antara semua server terdaftar pada saat pembuatan laporan.

Widget Pencegahan Kehilangan Data

Topik berikut memberi informasi lebih banyak tentang Perangkat periferal yang diblokir di bagian **Pencegahan Kehilangan Data**.

Widget menampilkan jumlah total perangkat yang diblokir dan jumlah total perangkat diblokir berdasarkan tipe perangkat selama rentang waktu tertentu.

- Penyimpanan yang dapat dilepas
- Dapat dilepas yang terenkripsi
- Printer
- Papan klip - mencakup tipe perangkat Papan klip and Tangkapan layar.
- Perangkat seluler
- Bluetooth
- Drive optik
- Drive flopi

- USB - mencakup tipe perangkat port USB dan Port USB yang dialihkan.
- FireWire
- Drive yang dipetakan
- Papan Klip yang dialihkan - termasuk tipe perangkat Papan Klip dialihkan yang masuk dan Papan klip dialihkan yang keluar.

Widget menampilkan tujuh tipe perangkat pertama yang memiliki jumlah perangkat diblokir tertinggi, dan menggabungkan tipe perangkat lain dalam tipe perangkat **Lainnya**.

Widget File Sync & Share

Tabel berikut ini memberikan informasi lebih lanjut tentang widget dalam bagian **File Sync & Share**.

Widget	Deskripsi
Statistik File Sync & Share	Widget menunjukkan metrik berikut: **Total penyimpanan awan yang digunakan** - Total penggunaan penyimpanan semua pengguna. **Pengguna akhir** - jumlah total pengguna akhir. **Rata-rata penyimpanan yang digunakan per pengguna akhir** - rata-rata penggunaan penyimpanan per pengguna akhir. **Pengguna tamu** - jumlah total pengguna tamu.
Penggunaan penyimpanan File Sync & Share oleh pengguna akhir	Widget tersebut menunjukkan jumlah total pengguna akhir File Sync & Share yang memiliki penggunaan penyimpanan dalam rentang berikut: • 0 - 1 GB • 1 - 5 GB • 5 - 10 GB • 10 - 50 GB • 50 - 100 GB • 100 - 500 GB • 500 - 1 TB • 1+ TB

Widget Notaris

Tabel berikut ini memberikan informasi lebih lanjut tentang widget dalam bagian **Notaris**.

Widget	Deskripsi
Statistik Notaris cyber	Widget menunjukkan metrik Notaris berikut:

Widget	Deskripsi
	Penyimpanan awan Notaris yang digunakan - ukuran total penyimpanan yang digunakan untuk layanan Notaris. **File yang sudah dinotarisasikan** - jumlah total file yang dinotarisasikan. **Dokumen yang dibubuhi eSign** - jumlah total dokumen dan file yang dibubuhi eSign.
File yang sudah dinotarisasikan para pengguna akhir	Menunjukkan jumlah total file yang dinotarisasikan untuk semua pengguna akhir. Pengguna dikelompokkan berdasarkan jumlah file yang dinotarisasikan yang mereka miliki. • Hingga 10 file • 11 - 100 file • 101 - 500 file • 501 - 1000 file • 1000+ file
Dokumen yang dibubuhi eSign pada pengguna akhir	Widget tersebut menunjukkan jumlah total dokumen dan file yang dibubuhi eSign untuk semua pengguna akhir. Pengguna dikelompokkan berdasarkan jumlah file dan dokumen yang sudah dibubuhi eSign yang mereka miliki. • Hingga 10 file • 11 - 100 file • 101 - 500 file • 501 - 1000 file • 1000+ file

Mengonfigurasi pengaturan rangkuman laporan Eksekutif

Anda dapat memperbarui pengaturan laporan yang dikonfigurasi ketika rangkuman laporan Eksekutif dibuat.

Untuk memperbarui pengaturan rangkuman laporan eksekutif

1. Dalam konsol manajemen, buka **Laporan**>**Rangkuman eksekutif**.
2. Klik nama rangkuman laporan Eksekutif yang ingin Anda perbarui.
3. Klik **Pengaturan**.
4. Ubah nilai bidang sesuai keperluan.
5. Klik **Simpan**.

Membuat rangkuman laporan Eksekutif

Anda dapat membuat rangkuman laporan Eksekutif, mempratinjau isinya, mengonfigurasi penerima laporan, dan menjadwalkan waktu untuk mengirimkannya secara otomatis.

Untuk membuat rangkuman laporan Eksekutif

1. Dalam konsol manajemen, buka **Laporan**>**Rangkuman eksekutif**.
2. Klik **Buat rangkuman laporan eksekutif**.
3. Pada **Nama laporan**, tulis nama laporan.
4. Pilih Penerima laporan.
   - Jika Anda ingin mengirim laporan ke semua pelanggan langsung, pilih **Kirim ke semua pelanggan langsung**.
   - Jika Anda ingin mengirim laporan ke pelanggan tertentu
     a. Hapus **Kirim ke semua pelanggan langsung**.
     b. Klik **Pilih kontak**.
     c. Pilih pelanggan tertentu. Anda dapat menggunakan Cari untuk menemukan kontak tertentu dengan mudah.
     d. Klik **Pilih**.
5. Pilih Rentang: **30 hari** atau **Bulan ini**
6. Pilih format file: **PDF**, **Excel**, atau **Excel dan PDF**.
7. Konfigurasi pengaturan penjadwalan.
   - Jika Anda ingin mengirim laporan ke penerima pada tanggal dan waktu tertentu:
     a. Aktifkan opsi **Terjadwal**.
     b. Klik bidang **Hari setiap bulan**, hapus bidang Hari terakhir, dan klik tanggal yang ingin Anda atur.
     c. Di bidang **Waktu**, masukkan jam yang ingin Anda tentukan.
     d. Klik **Terapkan**.
   - Jika Anda ingin membuat laporan tanpa mengirimkannya ke penerima, nonaktifkan opsi **Terjadwal**.
8. Klik **Simpan**.

Menyesuaikan Rangkuman laporan eksekutif

Anda dapat menentukan informasi apa yang akan dimasukkan dalam laporan ringkasan Eksekutif. Anda dapat menambah atau menghapus bagian, menambah atau menghapus widget, mengganti

nama bagian, menyesuaikan widget, serta menyeret dan menjatuhkan widget dan bagian untuk mengubah urutan munculnya informasi dalam laporan.

Untuk menambahkan bagian

1. Klik **Tambah item** > **Tambah bagian**.
2. Di jendela **Tambah bagian**, ketik nama bagian, atau gunakan nama bagian default.
3. Klik **Tambahkan ke laporan**.

Untuk mengganti nama bagian

1. Di bagian yang ingin Anda ganti namanya, klik **Edit**.
2. Di jendela **Edit bagian**, ketikkan nama baru.
3. Klik **Simpan**.

Untuk menghapus bagian

1. Di bagian yang ingin Anda hapus, klik **Hapus bagian**.
2. Di jendela konfirmasi **Hapus bagian**, klik **Hapus**.

Untuk menambahkan widget dengan pengaturan default ke suatu bagian

1. Di bagian yang ingin Anda tambahkan widget, klik **Tambah widget**.
2. Dalam jendela **Tambah widget**, klik widget yang ingin Anda tambahkan.

Untuk menambahkan widget yang disesuaikan ke suatu bagian

1. Di bagian yang ingin Anda tambahkan widget, klik **Tambah widget**.
2. Dalam jendela **Tambah widget**, temukan widget yang ingin Anda tambahkan, dan klik **Sesuaikan**.
3. Konfigurasi bidang sesuai keperluan.
4. Klik **Tambah widget**.

Untuk menambahkan widget dengan pengaturan default ke laporan

1. Klik **Tambah item** > **Tambah widget**.
2. Dalam jendela **Tambah widget**, klik widget yang ingin Anda tambahkan.

Untuk menambahkan widget yang disesuaikan ke laporan

1. Klik **Tambah widget**.
2. Dalam jendela **Tambah widget**, temukan widget yang ingin Anda tambahkan, dan klik **Sesuaikan**.
3. Konfigurasi bidang sesuai keperluan.
4. Klik **Tambah widget**.

Untuk mengatur ulang pengaturan default widget

1. Dalam widget yang ingin Anda sesuaikan, klik **Edit**.
2. Klik **Atur ulang ke default**.
3. Klik **Selesai**.

Untuk menyesuaikan widget

1. Dalam widget yang ingin Anda sesuaikan, klik **Edit**.
2. Edit bidang sesuai keperluan.
3. Klik **Selesai**.

Mengirim rangkuman laporan Eksekutif

Anda dapat mengirim rangkuman laporan Eksekutif sesuai permintaan. Dalam kasus ini, pengaturan **Terjadwal** diabaikan, laporan akan segera dikirim. Saat mengirim laporan, sistem menggunakan nilai Penerima, Rentang, dan Format file yang dikonfigurasi dalam **Pengaturan**. Anda dapat mengubah pengaturan ini secara manual sebelum mengirimkan laporan. Untuk informasi lebih lanjut, lihat "Mengonfigurasi pengaturan rangkuman laporan Eksekutif" (hlm. 113).

Untuk mengirim rangkuman laporan Eksekutif

1. Di portal manajemen, buka **Laporan**>**Rangkuman eksekutif**.
2. Klik nama rangkuman laporan Eksekutif yang ingin Anda kirim.
3. Klik **Kirim sekarang**.
   Sistem mengirimkan rangkuman laporan Eksekutif ke penerima yang dipilih.

Zona waktu dalam laporan

Zona waktu yang digunakan dalam laporan bervariasi tergantung pada jenis laporan. Tabel berikut berisi informasi untuk referensi Anda.

Lokasi dan jenis laporan	Zona waktu yang digunakan dalam laporan
Portal manajemen> Gambaran Umum> Operasi (widget)	Waktu pembuatan laporan berada di zona waktu mesin tempat browser berjalan.
Portal manajemen> Gambaran Umum> Operasi (diekspor ke PDF atau xlsx)	• Stempel waktu laporan yang diekspor berada di zona waktu mesin yang digunakan untuk mengekspor laporan. • Zona waktu aktivitas yang ditampilkan dalam laporan adalah UTC.
Manajemen portal> Laporan > Penggunaan > Laporan terjadwal	• Laporan ini dibuat pada pukul 23:59:59 UTC pada hari pertama bulan itu. • Laporan dikirim pada hari kedua bulan itu.
Manajemen portal> Laporan >	Zona waktu dan tanggal laporan adalah UTC.

Penggunaan > Laporan kustom	
Portal manajemen> Laporan > Operasi (widget)	• Waktu pembuatan laporan berada di zona waktu mesin tempat browser berjalan. • Zona waktu aktivitas yang ditampilkan dalam laporan adalah UTC.
Portal manajemen> Laporan > Operasi (diekspor ke PDF atau xlsx)	• Stempel waktu laporan yang diekspor berada di zona waktu mesin yang digunakan untuk mengekspor laporan. • Zona waktu aktivitas yang ditampilkan dalam laporan adalah UTC.
Portal manajemen> Laporan > Operasi (pengiriman terjadwal)	• Zona waktu pengiriman laporan adalah UTC. • Zona waktu aktivitas yang ditampilkan dalam laporan adalah UTC.
Portal manajemen> Pengguna > Rekap harian tentang peringatan aktif	• Laporan ini dikirim sekali sehari antara pukul 10:00 dan 23:59 UTC. Waktu ketika laporan dikirim tergantung pada beban kerja di pusat data. • Zona waktu aktivitas yang ditampilkan dalam laporan adalah UTC.
Portal manajemen> Pengguna > Pemberitahuan status Perlindungan Cyber	• Laporan ini dikirim ketika aktivitas selesai. **Catatan** Tergantung pada beban kerja di pusat data, beberapa laporan mungkin dikirim dengan penundaan. • Zona waktu aktivitas dalam laporan adalah UTC.

Data yang dilaporkan berdasarkan tipe widget

Berdasarkan rentang data yang ditampilkannya, widget pada dasbor terdiri dari dua tipe:

- Widget yang menampilkan data aktual pada saat penjelajahan atau pembuatan laporan.
- Widget yang menampilkan data historis.

Saat Anda mengonfigurasi rentang tanggal dalam pengaturan laporan untuk menghapus data untuk periode tertentu, rentang waktu yang dipilih akan berlaku hanya untuk widget yang menampilkan data historis. Untuk widget yang menampilkan data aktual pada saat penjelajahan, parameter rentang waktu tidak berlaku.

Tabel berikut mencantumkan widget yang tersedia dan rentang datanya.

Nama widget	Data yang ditampilkan di widget dan laporan
Skor #CyberFit berdasarkan mesin	Aktual

5 peringatan terbaru	Aktual
Detail peringatan aktif	Aktual
Ringkasan peringatan aktif	Aktual
Aktivitas	Historis
Daftar aktivitas	Historis
Riwayat peringatan	Historis
Pemindaian antimalware pada cadangan	Historis
Pemindaian antimalware pada file	Historis
Detail pemindaian cadangan (ancaman)	Historis
Status cadangan	Historis - dalam kolom **Total berjalan** dan **Jumlah berhasil berjalan** Aktual - di semua kolom lainnya
Penggunaan penyimpanan cadangan	Historis
Perangkat periferal diblokir	Historis
URL yang diblokir	Aktual
Aplikasi awan	Aktual
Status proteksi beban kerja awan	Aktual
Cyber protection	Aktual
Ringkasan perlindungan cyber	Historis
Peta perlindungan data	Historis
Perangkat	Aktual
Server pemulihan bencana sudah diuji	Historis
Statistik pemulihan bencana	Historis
Mesin yang ditemukan	Aktual
Gambaran umum kesehatan disk	Aktual
Status kesehatan disk	Aktual
Status kesehatan disk berdasarkan perangkat fisik	Aktual
Dokumen yang dibubuhi eSign pada pengguna akhir	Aktual
Kerentanan yang ada	Historis

Statistik File Sync & Share	Aktual
Penggunaan penyimpanan File Sync & Share Cyber oleh pengguna akhir	Aktual
Perubahan perangkat keras	Historis
Detail perangkat keras	Aktual
Inventaris perangkat keras	Aktual
Rangkuman peringatan riwayat	Historis
Ringkasan lokasi	Aktual
Pembaruan yang tidak ada berdasarkan kategori	Aktual
Tidak terlindungi	Aktual
File yang sudah dinotarisasikan para pengguna akhir	Aktual
Statistik notaris	Aktual
Riwayat instalasi patch	Historis
Status instalasi patch	Historis
Ringkasan instalasi patch	Historis
Kerentanan yang di-patch	Historis
Patch yang diinstal	Historis
Status proteksi	Aktual
Baru-baru ini terdampak	Historis
Sesi jarak jauh	Historis
Burndown insiden keamanan	Historis
MTTR insiden keamanan	Historis
Server yang dilindungi oleh pemulihan bencana	Aktual
Inventaris perangkat lunak	Aktual
Ikhtisar perangkat lunak	Historis
Status ancaman	Aktual
Ancaman terdeteksi oleh teknologi proteksi	Historis
Distribusi insiden teratas per beban kerja	Aktual
Mesin yang rentan	Aktual

Status jaringan beban kerja	Aktual
Beban kerja dicadangkan	Historis
Status proteksi beban kerja	Aktual

Log audit

Untuk melihat log audit, klik **Log audit**.

Log audit menyajikan catatan kronologis event berikut:

- Operasi yang dilakukan pengguna dalam portal manajemen
- Operasi dengan sumber daya awan-ke-awan yang dijalankan pengguna dalam konsol layanan Cyber Protection
- Operasi Skrip Cyber yang dilakukan pengguna dalam konsol layanan Cyber Protection
- Pesan sistem tentang kuota yang telah tercapai dan penggunaan kuota

Log menampilkan event pada penyewa yang sedang Anda operasikan dan penyewa turunannya. Anda dapat mengklik suatu event untuk melihat lebih banyak informasi tentangnya.

Log audit disimpan di pusat data dan ketersediaannya tidak dapat dipengaruhi oleh masalah pada mesin pengguna akhir.

Log dihapus setiap hari. Event dihapus setelah 180 hari.

Bidang log audit

Untuk setiap event, log akan menampilkan:

- **Event**
  Deskripsi singkat event. Misalnya, **Penyewa dibuat**, **Penyewa telah dihapus**, **Pengguna dibuat**, **Pengguna telah dihapus**, **Kuota telah tercapai**, **Konten cadangan ditelusuri**, **Skrip telah diubah**.
- **Tingkat keparahan**
  Dapat merupakan salah satu dari hal-hal berikut:
  - **Eror**
    Menunjukkan eror.
  - **Peringatan**
    Menunjukkan potensi tindakan negatif. Misalnya, **Penyewa telah dihapus**, **Pengguna telah dihapus**, **Kuota telah tercapai**.
  - **Pemberitahuan**
    Menunjukkan event yang mungkin perlu diperhatikan. Misalnya, **Penyewa telah diperbarui**, **Pengguna diperbarui**.
  - **Informasi**

Menunjukkan perubahan atau tindakan informatif yang netral. Misalnya, **Penyewa telah dibuat**, **Pengguna dibuat**, **Kuota telah diperbarui**, **Rencana skrip telah dihapus**.

- **Tanggal**

  Tanggal dan waktu ketika event terjadi.
- **Nama objek**

  Objek yang dengannya operasi dilakukan. Misalnya, objek event **Pengguna diperbarui** adalah pengguna yang propertinya diubah. Untuk event yang berhubungan dengan kuota, kuota adalah objeknya.
- **Penyewa**

  Nama penyewa di mana objek berada.
- **Inisiator**

  Log masuk pengguna yang menginisiasi event. Untuk pesan sistem dan event yang diinisiasi oleh administrator tingkat yang lebih tinggi, inisiator ditampilkan sebagai **Sistem**.
- **Penyewa inisiator**

  Nama penyewa milik inisiator. Untuk pesan sistem dan event yang diinisiasi oleh administrator tingkat yang lebih tinggi, bidang ini kosong.
- **Metode**

  Menampilkan apakah event diinisiasi melalui antarmuka web atau melalui API.
- **IP**

  Alamat IP mesin asal event diinisiasi.

Filter dan pencarian

Anda dapat memfilter peristiwa berdasarkan jenis, keparahan, atau tanggal. Anda juga dapat mencari peristiwa berdasarkan nama, objek, penyewa, inisiator, dan penyewa inisiator.

Paket Perlindungan Tingkat Lanjut

Paket perlindungan tingkat lanjut dapat diaktifkan sebagai tambahan fitur layanan Perlindungan dan dikenakan biaya tambahan. Paket perlindungan tingkat lanjut memberikan fungsi unik yang tidak tumpang-tindih dengan set fitur standar dan paket tingkat lanjut lainnya. Klien dapat melindungi beban kerja dengan satu, beberapa, atau semua paket tingkat lanjut. Paket perlindungan tingkat lanjut packs tersedia untuk kedua mode penagihan layanan Perlindungan - Per beban kerja and Per gigabyte.

Fitur File Sync & Share Tingkat Lanjut dapat diaktifkan dengan layanan File Sync & Share. Fitur tersebut tersedia dalam kedua mode penagihan - Per pengguna dan Per gigabyte.

Anda dapat mengaktifkan paket perlindungan tingkat lanjut berikut:

- Cadangan Tingkat Lanjut
- Manajemen Tingkat Lanjut
- Keamanan Tingkat Lanjut
- Keamanan Tingkat Lanjut + EDR
- Pencegahan Hilangnya Data Tingkat Lanjut
- Pemulihan Bencana Tingkat Lanjut
- Keamanan Email Tingkat Lanjut
- File Sync & Share Tingkat Lanjut

Catatan
Paket tingkat lanjut hanya dapat digunakan jika fitur yang diperluas diaktifkan. Pengguna tidak dapat menggunakan fitur tingkat lanjut jika fitur layanan standar dinonaktifkan. Misalnya, pengguna tidak dapat menggunakan fitur paket Cadangan Tingkat Lanjut jika fitur Perlindungan dinonaktifkan.

Jika paket perlindungan tingkat lanjut diaktifkan, fiturnya akan muncul dalam rencana proteksi dan ditandai dengan ikon fitur Tingkat Lanjut  . Jika pengguna mencoba mengaktifkan fitur tersebut, Anda akan diberi tahu bahwa biaya tambahan berlaku.

Jika paket fitur perlindungan tingkat lanjut tidak diaktifkan, tetapi upsell diaktifkan, fitur perlindungan tingkat lanjut akan muncul dalam rencana proteksi, tetapi tidak dapat diakses untuk digunakan. Ikon berikut ditampilkan di samping nama fitur  . Akan muncul pesan yang meminta pengguna menghubungi administrator untuk mengaktifkan set fitur tingkat lanjut yang diperlukan.

Jika paket perlindungan tingkat lanjut tidak diaktifkan dan upsell dinonaktifkan, pelanggan tidak akan melihat fitur tingkat lanjut fitur dalam rencana proteksi mereka.

Fitur dan paket lanjutan yang disertakan dalam layanan Cyber Protect

Jika Anda mengaktifkan set layanan atau fitur di Cyber Protect, Anda mengaktifkan sejumlah fitur yang disertakan dan tersedia secara default. Selain itu, Anda dapat mengaktifkan paket perlindungan tingkat lanjut.

Bagian berikut berisi ikhtisar tingkat tinggi tentang paket tingkat lanjut dan fitur layanan Cyber Protect. Untuk daftar lengkap penawaran, lihat Cyber Protect Panduan Pelisensian.

Fitur tingkat lanjut dan yang disertakan dalam layanan Proteksi

Fitur tingkat lanjut dan yang disertakan dalam layanan Proteksi

Grup fitur	Fitur standar yang disertakan	Fitur tingkat lanjut
Keamanan	• Skor #CyberFit • Penilaian kerentanan • Perlindungan anti-ransomware: Active protection • Perlindungan Antivirus dan Antimalware: Deteksi file berbasis tanda tangan awan (tanpa perlindungan waktu nyata, hanya pemindaian terjadwal)* • Perlindungan Antivirus dan Antimalware: Pra-eksekusi penganalisis file berbasis AI, Cyber Engine berbasis perilaku • Manajemen Microsoft Defender *Untuk mendeteksi serangan zero day, Cyber Protect menggunakan aturan dan algoritme pemindaian heuristik untuk mencari perintah berbahaya.	Ada dua paket perlindungan lanjutan yang tersedia: **Keamanan Tingkat Lanjut** dan **Keamanan Tingkat Lanjut + EDR**. Paket Keamanan Tingkat Lanjut termasuk: • Perlindungan antivirus dan antimalware dengan deteksi berbasis tanda tangan lokal (dengan perlindungan waktu nyata) • Pencegahan eksploit • Pemfilteran URL • Manajemen firewall titik akhir • Cadangan forensik, cadangan pemindaian untuk malware, pemulihan aman, daftar izin perusahaan • Rencana proteksi cerdas (integrasi dengan peringatan CPPOC) • Pemindaian cadangan terpusat untuk malware • Penghapusan jarak jauh Paket perlindungan Keamanan Lanjutan + EDR mencakup semua fitur di atas serta kemampuan Deteksi dan Tanggapan Titik Akhir berikut untuk mengidentifikasi ancaman tingkat lanjut atau serangan yang sedang berlangsung:

Grup fitur	Fitur standar yang disertakan	Fitur tingkat lanjut
		• Mengelola insiden di halaman Insiden terpusat • Visualisasikan cakupan dan dampak insiden • Rekomendasi dan langkah remediasi • Periksa serangan yang diungkapkan secara publik pada beban kerja Anda menggunakan umpan Ancaman • Simpan peristiwa keamanan selama 180 hari Untuk informasi tentang cara mengaktifkan Keamanan Lanjutan + EDR, lihat "Mengaktifkan Keamanan Tingkat Lanjut + EDR" (hlm. 128).
Pencegahan Kehilangan Data	• Kontrol perangkat	• Pencegahan sadar-konten kehilangan data dari beban kerja melalui perangkat periferal dan komunikasi jaringan • Deteksi otomatis bawaan untuk informasi pengenal pribadi (PII), informasi kesehatan yang dilindungi (PHI), dan data Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS), serta dokumen dalam kategori “Ditandai sebagai Informasi Rahasia” • Pembuatan kebijakan pencegahan kehilangan data otomatis dengan bantuan pengguna akhir opsional • Penegakan pencegahan kehilangan data adaptif dengan penyesuaian kebijakan berbasis pembelajaran otomatis • Logging audit terpusat berbasis awan, peringatan, dan pemberitahuan pengguna akhir
Manajemen	• Manajemen grup beban kerja • Manajemen rencana proteksi terpusat • Inventaris perangkat keras • Kontrol jarak jauh • Tindakan jarak jauh • Koneksi bersamaan per teknisi	• Manajemen patch • Kesehatan disk • Inventaris perangkat lunak • Patching yang aman untuk file • Pembuatan Skrip Cyber • Bantuan jarak jauh • Transfer dan berbagi file

Grup fitur	Fitur standar yang disertakan	Fitur tingkat lanjut
	• Protokol koneksi jarak jauh: RDP	• Memilih sesi untuk dihubungkan • Mengamati beban kerja dalam beberapa tampilan • Mode koneksi: kontrol, amati, dan tutup • Koneksi melalui aplikasi Bantuan Cepat • Protokol koneksi jarak jauh: NEAR dan Berbagi Layar • Sesi perekaman untuk koneksi NEAR • Transmisi tangkapan layar • Laporan riwayat sesi
Keamanan email	Tidak ada	Perlindungan waktu nyata untuk Microsoft 365 dan kotak surat Gmail Anda: • Antispam Antimalware • Pindaian URL dalam email • Analisis DMARC • Antiphishing • Perlindungan penyamaran • Pindaian lampiran • Pelucutan dan rekonstruksi konten • Grafik kepercayaan Lihat panduan konfigurasi.
Cyber Disaster Recovery Cloud	Anda dapat menggunakan fitur standar Pemulihan Bencana untuk menguji skenario Pemulihan Bencana untuk beban kerja Anda. Perhatikan fitur standar Pemulihan Bencana yang tersedia dan batasannya: • Lakukan failover uji dalam lingkungan jaringan yang terisolasi. Terbatas untuk 32 titik komputasi per bulan, dan maksimal 5 operasi failover uji di waktu yang sama. • Konfigurasi server pemulihan: 1 CPU dan RAM 2 GB, 1 CPU dan RAM 4 GB, dan 2 CPU dan RAM 8 GB. • Jumlah titik pemulihan yang tersedia untuk failover: hanya titik pemulihan	Anda dapat mengaktifkan paket Pemulihan Bencana Tingkat Lanjut, dan melindungi beban kerja Anda menggunakan funsionalitas Pemulihan Bencana lengkap. Perhatikan fitur tingkat lanjut Pemulihan Bencana yang tersedia: • Failover produksi • Lakukan failover uji dalam lingkungan jaringan yang terisolasi. • Jumlah titik pemulihan yang tersedia untuk failover: semua titik pemulihan yang tersedia setelah pembuatan server pemulihan. • Server utama • Konfigurasi server Pemulihan/Utama:

Grup fitur	Fitur standar yang disertakan	Fitur tingkat lanjut
	terakhir yang tersedia setelah pencadangan. • Mode konektivitas yang tersedia: Hanya-awan dan Titik-ke-situs. • Ketersediaan gateway VPN: Gateway VPN akan ditangguhkan sementara jika tidak aktif selama 4 jam setelah failover uji terakhir selesai, dan akan disebarkan lagi saat Anda memulai failover uji. • Jumlah jaringan awan: 1. • Akses internet • Operasi dengan runbook: buat dan edit.	Tidak ada pembatasan • Mode konektivitas yang tersedia: Hanya-awan, Titik-ke-situs, VPN Terbuka Situs-ke-situs, dan VPN IPsec multi-situs. • Ketersediaan gateway VPN: selalu tersedia. • Jumlah jaringan awan: 23. • Alamat IP publik • Akses internet • Operasi dengan runbook: buat, edit, dan eksekusi.

Fitur bayar sesuai pemakaian dan fitur tingkat lanjut dalam layanan Perlindungan

Fitur bayar-sesuai-pemakaian dan fitur tingkat lanjut dalam layanan Perlindungan

Grup fitur	Fitur bayar sesuai penggunaan	Fitur tingkat lanjut
Cadangan	• Cadangan file • Cadangan profil • Cadangan aplikasi • Pencadangan berbagi jaringan • Pencadangan ke penyimpanan awan • Pencadangan ke penyimpanan lokal **Catatan** Biaya untuk penggunaan penyimpanan awan berlaku.	• Microsoft SQL Server dan klaster Microsoft Exchange • Oracle DB • SAP HANA • Peta Perlindungan Data • Perlindungan Data Berkelanjutan • Rencana pemrosesan data off-host • Notarisasi cadangan • Kursi Microsoft 365 • Kursi Google Workspace
File Sync & Share	• Simpan konten berbasis file yang terenkripsi • Sinkronkan file di antara perangkat khusus • Bagikan folder dan file dengan orang dan sistem khusus	• Notarisasi dan tanda tangan elektronik • Templat dokumen* *Cadangan file sinkronisasi dan file yang dibagikan
Pengiriman Data Fisik	Fungsionalitas Pengiriman Data Fisik	N/A
Notaris	• Notarisasi file • Membubuhkan eSign pada file	N/A

Grup fitur	Fitur bayar sesuai penggunaan	Fitur tingkat lanjut
	• Templat dokumen	

Catatan
Anda tidak dapat mengaktifkan paket perlindungan tingkat lanjut tanpa mengaktifkan fitur perlindungan standar yang diperluas. Jika Anda menonaktifkan fitur, paket tingkat lanjut akan dinonaktifkan secara otomatis dan rencana proteksi yang menggunakannya akan dibatalkan secara otomatis. Misalnya, jika Anda menonaktifkan fitur Perlindungan, paket tingkat lanjut akan dinonaktifkan secara otomatis dan semua paket yang menggunakannya akan dibatalkan.

Pengguna tidak dapat menggunakan paket perlindungan tingkat lanjut tanpa perlindungan standar, tetapi hanya dapat menggunakan fitur perlindungan standar yang disertakan bersama dengan paket tingkat lanjut pada beban kerja tertentu. Dalam hal ini, pelanggan hanya akan dikenakan biaya untuk paket tingkat lanjut yang mereka gunakan.

Untuk informasi tentang penagihan, lihat "Mode penagihan untuk Cyber Protect" (hlm. 7).

Pencegahan Hilangnya Data Tingkat Lanjut

Modul Pencegahan Kehilangan Data Tingkat Lanjut mencegah kebocoran informasi sensitif dari stasiun kerja, server, dan mesin virtual dengan memeriksa konten data yang ditransfer melalui saluran lokal dan jaringan serta menerapkan berbagai aturan kebijakan aliran data khusus organisasi.

Sebelum Anda mulai menggunakan modul Pencegahan Kehilangan Data Tingkat Lanjut, pastikan Anda telah membaca dan memahami konsep dasar dan logika dari manajemen Pencegahan Kehilangan Data Tingkat Lanjut yang dijelaskan di Panduan Fundamental.

Anda juga mungkin perlu meninjau dokumen Spesifikasi Teknis.

Mengaktifkan Pencegahan Kehilangan Data Tingkat Lanjut

Secara default, Pencegahan Kehilangan Data Tingkat Lanjut diaktifkan di konfigurasi untuk penyewa baru. Jika fungsionalitas dinonaktifkan saat proses pembuatan penyewa, Administrator Mitra dapat mengaktifkannya nanti.

Untuk mengaktifkan Pencegahan Kehilangan Data Tingkat Lanjut

1. Di konsol manajemen Cyber Protect Cloud, navigasi ke **Klien**.
2. Pilih penyewa untuk pengeditan.
3. Di bagian **Pilih layanan**, gulirkan ke **Perlindungan**, dan di mode penagihan yang Anda terapkan, pilih **Pencegahan Kehilangan Data Tingkat Lanjut**.
4. Di bagian Konfigurasi layanan, gulirkan ke **Pencegahan Kehilangan Data Tingkat Lanjut** dan konfigurasikan kuota.
   Secara default, kuota diatur ke tidak terbatas.

5. Simpan pengaturan Anda.

Keamanan Tingkat Lanjut + EDR

Deteksi dan tanggapan titik akhir (EDR) mendeteksi aktivitas mencurigakan pada beban kerja, termasuk serangan yang tidak terdeteksi dan menghasilkan insiden. Insiden ini memberikan ikhtisar langkah demi langkah dari setiap serangan, membantu Anda memahami bagaimana serangan terjadi dan cara mencegahnya terjadi lagi. Dengan interpretasi yang mudah dipahami dari setiap tahap serangan, waktu yang dihabiskan untuk menyelidiki serangan dapat dikurangi menjadi hitungan menit.

Mengaktifkan Keamanan Tingkat Lanjut + EDR

Sebagai administrator mitra, Anda dapat mengaktifkan paket perlindungan Keamanan Tingkat Lanjut + EDR untuk menyediakan fungsionalitas Deteksi dan Tanggapan Titik Akhir (EDR) dalam rencana proteksi klien.

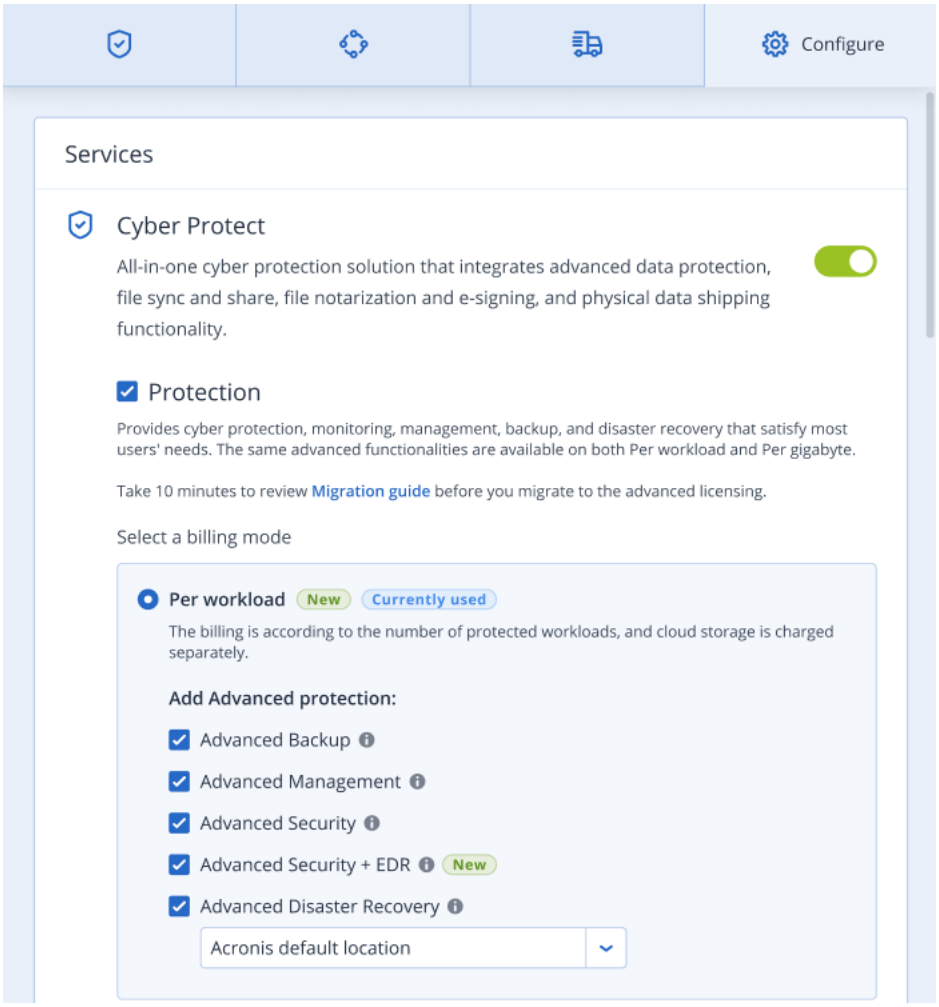
Untuk mengaktifkan paket Keamanan Tingkat Lanjut + EDR

1. Masuk ke portal manajemen.

   Catatan
   Jika diminta, pilih klien tempat Anda ingin menerapkan paket perlindungan Keamanan Tingkat Lanjut + EDR, dan klik **Aktifkan**.

2. Di panel navigasi kiri, klik **KLIEN**.
3. Di bawah Cyber Protect, klik tab **Perlindungan**.
   Daftar klien yang sudah berlangganan layanan Perlindungan ditampilkan.
4. Klik klien relevan yang ingin Anda tambahkan paket Keamanan Tingkat Lanjut + EDR.
   Di tab **Konfigurasi**, di bawah bagian Perlindungan, pastikan kotak centang **Keamanan Tingkat**

Lanjut + EDR dicentang.



Pemulihan Bencana Tingkat Lanjut

Anda dapat mengaktifkan paket Pemulihan Bencana Tingkat Lanjut, dan melindungi beban kerja Anda menggunakan funsionalitas Pemulihan Bencana lengkap.

Fitur Pemulihan Bencana tingkat lanjut berikut tersedia:

- Failover produksi
- Lakukan failover uji dalam lingkungan jaringan yang terisolasi.
- Jumlah titik pemulihan yang tersedia untuk failover: semua titik pemulihan yang tersedia setelah pembuatan server pemulihan.
- Server utama
- Konfigurasi server Pemulihan/Utama: Tidak ada pembatasan
- Mode konektivitas yang tersedia: Hanya-awan, Titik-ke-situs, VPN Terbuka Situs-ke-situs, dan VPN IPsec multi-situs.
- Ketersediaan gateway VPN: selalu tersedia.

- Jumlah jaringan awan: 23.
- Alamat IP publik
- Akses internet
- Operasi dengan runbook: buat, edit, dan eksekusi.

Keamanan Email Tingkat Lanjut

Paket Keamanan Surel Tingkat Lanjut memberikan perlindungan waktu nyata untuk kotak surat Microsoft 365, Google Workspace, atau Open-Xchange Anda:

- Antimalware dan anti-spam
- Pindaian URL dalam email
- Analisis DMARC
- Antiphishing
- Perlindungan penyamaran
- Pindaian lampiran
- Pelucutan dan rekonstruksi konten
- Grafik kepercayaan

Pelajari selengkapnya tentang Keamanan Surel Tingkat Lanjut di Lembar data Keamanan Surel Tingkat Lanjut.

Untuk instruksi konfigurasi, lihat Keamanan Surel Tingkat Lanjut dengan Titik Persepsi.

Integrasi

Integrasi dengan sistem pihak ketiga

Penyedia layanan dapat mengintegrasikan Cyber Protect Cloud dengan sistem pihak ketiga sebagai berikut:

- Dengan mengatur ekstensi platform di sistem ini.

  Halaman **Integrasi** dari portal manajemen mencantumkan ekstensi yang tersedia untuk sistem Otomasi Layanan Profesional (PSA) dan Pemantauan dan Manajemen Jarak Jauh (RMM) yang paling populer.

  Ini adalah cara yang disarankan untuk mengintegrasikan platform.
- Dengan membuat klien API untuk sistem dan dengan kemudian mengaktifkan sistem untuk mengakses antarmuka pemrograman aplikasi (API) platform dan layanannya. Klien API adalah bagian dari framework otorisasi OAuth 2.0 dari platform. Untuk informasi lebih lanjut tentang OAuth 2.0, lihat https://tools.ietf.org/html/rfc6749.

  Ini adalah cara tingkat rendah untuk mengintegrasikan platform yang memerlukan keterampilan pemrograman. Kami menyarankan untuk memilihnya ketika tidak ada ekstensi platform untuk sistem atau sistem disesuaikan untuk kasus-kasus seperti mengelola platform dan layanannya yang tidak tercakup oleh ekstensi yang tersedia.

Menyiapkan integrasi untuk Cyber Protect Cloud

1. Masuk ke portal manajemen.
2. Buka **Integrasi** di menu navigasi utama.
3. Klik nama sistem pihak ketiga yang ingin Anda aktifkan integrasinya.
4. Ikuti petunjuk di layar.

Temukan informasi selengkapnya tentang integrasi yang tersedia dengan sistem pihak ketiga, termasuk dokumentasi langkah demi langkah di https://solutions.acronis.com.

Mengelola klien API

Sistem pihak ketiga dapat diintegrasikan dengan Cyber Protect Cloud dengan menggunakan antarmuka pemrograman aplikasi (API). Akses ke API ini diaktifkan melalui klien API, bagian integral dari framework otorisasi OAuth 2.0 dari platform.

Apa itu klien API?

Klien API adalah akun platform khusus yang dimaksudkan untuk mewakili sistem pihak ketiga yang perlu mengautentikasi dan diotorisasi untuk mengakses data dalam API platform dan layanannya.

Akses klien dibatasi pada penyewa, di mana administrator membuat klien, dan subpenyewanya.

Saat dibuat, klien mewarisi peran layanan dari akun administrator dan peran ini tidak dapat diubah nanti. Mengubah peran akun administrator atau menonaktifkannya tidak memengaruhi klien.

Kredensial klien terdiri dari pengidentifikasi unik (ID) dan nilai rahasia. Kredensial tidak kedaluwarsa dan tidak dapat digunakan untuk masuk ke portal manajemen atau konsol layanan apa pun. Nilai rahasia dapat diatur ulang.

Tidak dimungkinkan untuk mengaktifkan otentikasi dua faktor untuk klien.

Prosedur integrasi yang umum

1. Administrator membuat klien API dalam penyewa yang akan dikelola oleh sistem pihak ketiga.
2. Administrator mengaktifkan alur kredensial klien OAuth 2.0 dalam sistem pihak ketiga.
   Menurut alur ini, sebelum mengakses penyewa dan layanannya melalui API, sistem harus terlebih dahulu mengirim kredensial klien yang dibuat ke platform dengan menggunakan API otorisasi. Platform membuat dan mengirim kembali token keamanan, string tersembunyi khusus yang ditugaskan untuk klien khusus ini. Kemudian, sistem harus menambahkan token ini ke semua permintaan API.
   Token keamanan menghilangkan kebutuhan untuk melewatkan kredensial klien dengan permintaan API. Untuk keamanan tambahan, token berakhir dalam dua jam. Setelah ini, semua permintaan API dengan token yang kedaluwarsa akan gagal dan sistem perlu meminta token baru dari platform.

Untuk informasi lebih lanjut tentang penggunaan API otorisasi dan platform, lihat panduan developer di https://developer.acronis.com/doc/account-management/v2/guide/index.

Membuat klien API

1. Masuk ke portal manajemen.
2. Klik **Pengaturan** > **klien API** > **Buat klien API**.
3. Masukkan nama untuk klien API.
4. Klik **Berikutnya**.
   Klien API dibuat dengan status **Aktif** secara default.
5. Salin dan simpan ID dan nilai rahasia klien dan URL pusat data. Anda akan membutuhkannya saat mengaktifkan alur kredensial klien OAuth 2.0 dalam sistem pihak ketiga.

   Penting
   Untuk alasan keamanan, nilai rahasia hanya ditampilkan satu kali. Tidak ada cara untuk mengembalikan nilai ini jika Anda kehilangannya - atur ulang saja.

6. Klik **Selesai**.

Mengatur ulang nilai rahasia klien API

1. Masuk ke portal manajemen.
2. Klik **Pengaturan** > **klien API**.
3. Temukan klien yang diperlukan dalam daftar.
4. Klik , lalu klik **Atur ulang rahasia**.
5. Konfirmasi keputusan Anda dengan mengklik **Berikutnya**.
   Nilai rahasia baru akan dibuat. ID klien dan URL pusat data tidak akan berubah.
   Semua token keamanan yang ditetapkan untuk klien ini akan segera kedaluwarsa dan permintaan API dengan token ini akan gagal.
6. Salin dan simpan nilai rahasia klien yang baru.

   Penting
   Untuk alasan keamanan, nilai rahasia hanya ditampilkan satu kali. Tidak ada cara untuk mengembalikan nilai ini jika Anda kehilangannya - atur ulang saja.

7. Klik **Selesai**.

Menonaktifkan klien API

1. Masuk ke portal manajemen.
2. Klik **Pengaturan** > **klien API**.
3. Temukan klien yang diperlukan dalam daftar.
4. Klik , dan kemudian klik **Nonaktifkan**.
5. Konfirmasi keputusan Anda.
   Status klien akan berubah menjadi **Dinonaktifkan**.
   Permintaan API dengan token keamanan yang ditetapkan untuk klien ini akan gagal tetapi token tidak akan segera kedaluwarsa. Menonaktifkan klien tidak memengaruhi waktu kedaluwarsa token.
   Pengaktifan kembali klien dapat dilakukan kapan saja.

Mengaktifkan klien API yang dinonaktifkan

1. Masuk ke portal manajemen.
2. Klik **Pengaturan** > **klien API**.
3. Temukan klien yang diperlukan dalam daftar.
4. Klik , dan kemudian klik **Aktifkan**.
   Status klien akan berubah menjadi **Aktif**.

Permintaan API dengan token keamanan yang ditetapkan untuk klien ini akan berhasil jika token ini belum kedaluwarsa.

Menghapus klien API

1. Masuk ke portal manajemen.
2. Klik **Pengaturan** > **klien API**.
3. Temukan klien yang diperlukan dalam daftar.
4. Klik , dan kemudian klik **Hapus**.
5. Konfirmasi keputusan Anda.
   Semua token keamanan yang ditetapkan untuk klien ini akan segera kedaluwarsa dan permintaan API dengan token ini akan gagal.

Penting
Tidak ada cara untuk memulihkan klien yang dihapus.

Referensi integrasi

Tabel berikut mencantumkan integrasi yang diimplementasikan dengan pihak ketiga dan menyediakan tautan ke dokumentasi terkait.

NAMA INTEGRASI	Lihat online	Buka PDF
Autotask PSA	https://www.acronis.com/support/documentation/AutotaskPSA/	https://dl.acronis.com/u/pdf/AutotaskPSA_Integration_quickstartguide_en-US.pdf
CloudBlue Commerce	https://www.acronis.com/support/documentation/CloudBlueCommerce/	https://dl.acronis.com/u/pdf/CloudBlue_Commerce_Integration_Guide_en-US.pdf
CloudBlue PSA	https://www.acronis.com/support/documentation/CloudBluePSA/	https://dl.acronis.com/u/pdf/CloudBluePSAIntegration_quickstartguide_en-US.pdf
ConnectWise Automate	https://www.acronis.com/support/documentation/ConnectWiseAutomate/	https://dl.acronis.com/u/pdf/AcronisConnectWiseAutomatePlugin_userguide_en-US.pdf
ConnectWise Command	https://www.acronis.com/support/documentation/ConnectWiseCommand/	https://dl.acronis.com/u/pdf/ConnectWiseCommandIntegration_quickstartguide_en-US.pdf
Connect	https://www.acronis.com/support/documentati	https://dl.acronis.com/u/pdf/ConnectWise

NAMA INTEGRASI	Lihat online	Buka PDF
Wise Control	on/ConnectWiseControl/	Control_integration_en-US.pdf
Connect Wise Manage	https://www.acronis.com/support/documentation/ConnectWiseManage/	https://dl.acronis.com/u/pdf/ConnectWiseManageIntegration_quickstartguide_en-US.pdf
Datto RMM	https://www.acronis.com/support/documentation/DattoRMM/	https://dl.acronis.com/u/pdf/DattoRMMIntegration_quickstartguide_en-US.pdf
Jamf Pro	https://www.acronis.com/support/documentation/JamfPro/	https://dl.acronis.com/u/pdf/JamfProIntegration_quickstartguide_en-US.pdf
Kaseya BMS	https://www.acronis.com/support/documentation/KaseyaBMS/	https://dl.acronis.com/u/pdf/AcronisKaseyaBMSPlugin_userguide_en-US.pdf
Kaseya VSA	https://www.acronis.com/support/documentation/KaseyaVSA/	https://download.acronis.com/pdf/AcronisKaseyaVSAPlugin_userguide_en-US.pdf
Matrix 42	https://www.acronis.com/support/documentation/Matrix42/	https://dl.acronis.com/u/pdf/Matrix42Integration_quickstartguide_en-US.pdf
Microsoft Intune	https://www.acronis.com/support/documentation/MicrosoftIntune/	https://dl.acronis.com/u/pdf/MicrosoftIntuneIntegration_quickstartguide_en-US.pdf
N-able N-central	https://www.acronis.com/support/documentation/NableNcentral/	https://dl.acronis.com/u/pdf/N-able_N-central_Integration_Guide_en-US.pdf
N-able N-sight RMM	https://www.acronis.com/en-us/support/documentation/NableNsightRMM/	https://dl.acronis.com/u/pdf/N-ableN-sightRMMIntegration_quickstartguide_en-US.pdf
Ninja One	https://www.acronis.com/support/documentation/NinjaOne/	https://dl.acronis.com/u/pdf/NinjaOneIntegration_quickstartguide_en-US.pdf
Omnivoice	https://www.acronis.com/support/documentation/Omnivoice/	https://dl.acronis.com/u/pdf/OmnivoiceIntegration_quickstartguide_en-US.pdf
Plesk	https://www.acronis.com/support/documentation/Plesk/	https://dl.acronis.com/u/pdf/Acronis_Backup_extension_for_Plesk_en-US.pdf
PRTG	https://www.acronis.com/support/documentation/PRTG/	https://dl.acronis.com/u/pdf/AcronisPRTGPlugin_userguide_en-US.pdf
Service Now	https://www.acronis.com/support/documentation/ServiceNow/	https://dl.acronis.com/u/pdf/ServiceNow_Integration_quickstartguide_en-US.pdf

NAMA INTEGRASI	Lihat online	Buka PDF
Splashtop	https://www.acronis.com/support/documentation/Splashtop/	https://dl.acronis.com/u/pdf/Splashtop_Integration_quickstartguide_en-US.pdf
Tigerpaw One	https://www.acronis.com/en-us/support/documentation/TigerpawOne/	https://dl.acronis.com/u/pdf/TigerpawOneIntegration_quickstartguide_en-US.pdf
WHM & cPanel	https://www.acronis.com/en-us/support/documentation/WHMCPanel/	https://www.acronis.com/en-us/support/documentation/WHMCPanel/
WHMCS	https://www.acronis.com/en-us/support/documentation/WHMCS/	https://dl.acronis.com/u/pdf/WHMCS_Integration_Manual_en-US.pdf

Integrasi dengan VMware Cloud Director

Penyedia layanan dapat mengintegrasikan VMware Cloud Director (sebelumnya VMware vCloud Director) dengan Cyber Protect Cloud dan menyediakan solusi pencadangan istimewa bagi pelanggannya untuk mesin virtual mereka.

Integrasi mencakup langkah-langkah berikut:

1. Mengonfigurasi perantara pesan RabbitMQ untuk lingkungan VMware Cloud Director.
   RabbitMQ memungkinkan sinkronisasi perubahan dalam lingkungan VMware Cloud Director menjadi Cyber Protect Cloud.
2. Menginstal plug-in untuk VMware Cloud Director.
   Plug-in ini menambah Cyber Protection ke antarmuka pengguna VMware Cloud Director.
3. Menyebarkan agen manajemen.
   Agen manajemen memetakan secara otomatis Organisasi VMware Cloud Director ke penyewa pelanggan di Cyber Protect Cloud, dan Administrator Organisasi ke administrator penyewa pelanggan. Untuk informasi lebih lanjut tentang Organisasi, lihat Membuat Organisasi di VMware Cloud Director di VMware Knowledge Base.
   Penyewa pelanggan dibuat di dalam penyewa mitra yang untuknya integrasi VMware Cloud Director dikonfigurasi. Penyewa pelanggan baru ini berada dalam mode **Terkunci** dan tidak dapat dikelola oleh administrator mitra dalam Cyber Protect Cloud.

   Catatan
   Hanya Administrator Organisasi dengan alamat email unik dalam VMware Cloud Director yang dipetakan ke Cyber Protect Cloud.

4. Menyebarkan satu atau beberapa agen pencadangan.
   Agen pencadangan menyediakan fungsi pencadangan dan pemulihan untuk mesin virtual di lingkungan VMware Cloud Director.

Untuk menonaktifkan integrasi antara VMware Cloud Director dan Cyber Protect Cloud, hubungi dukungan teknis.

Pembatasan

- Integrasi dengan VMware Cloud Director dimungkinkan hanya untuk penyewa mitra dalam mode manajemen yang **Dikelola oleh penyedia layanan**, yang penyewa induknya (jika ada) juga menggunakan mode manajemen yang **Dikelola oleh penyedia layanan**. Untuk informasi lebih lanjut tentang tipe penyewa dan mode manajemennya, lihat "Membuat penyewa" (hlm. 32).
  Semua mitra langsung yang ada dapat mengonfigurasi integrasi dengan VMware Cloud Director. Administrator mitra juga dapat mengaktifkan opsi ini untuk sub-penyewa dengan memilih kotak centang **Infrastruktur VMware Cloud Director milik mitra** saat membuat penyewa mitra anak.
- Autentikasi dua faktor harus dinonaktifkan untuk penyewa mitra yang integrasinya dengan VMware Cloud Director dikonfigurasi.
- Administrator yang memiliki peran Administrator Organisasi dalam beberapa Organisasi VMware Cloud Director dapat mengelola pencadangan dan pemulihan hanya untuk satu penyewa pelanggan di Cyber Protection.
- Cyber Protection konsol web terbuka di tab baru.

Persyaratan perangkat lunak

Versi VMware Cloud Director yang didukung

- VMware Cloud Director 10.0, 10.1, 10.2, 10.3, 10.4, 10.4.1

Browser web yang didukung

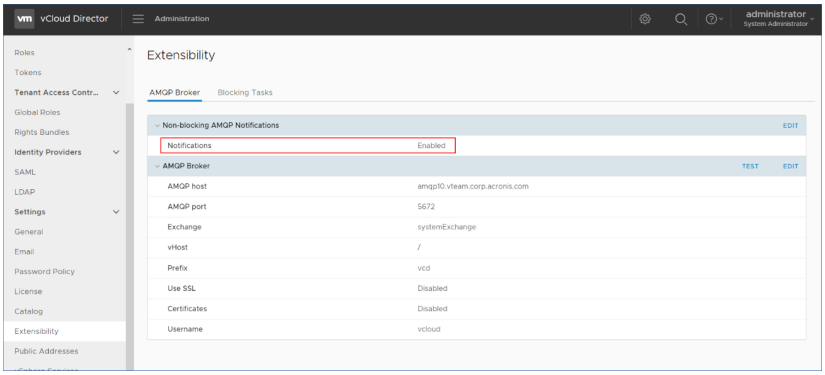
- Google Chrome 29 ke atas
- Mozilla Firefox 23 ke atas
- Opera 16 ke atas
- Microsoft Edge 25 ke atas
- Safari 8 ke atas yang berjalan di sistem operasi macOS dan iOS

Di browser web lain (termasuk browser Safari yang berjalan di sistem operasi lain), antarmuka pengguna mungkin akan ditampilkan dengan tidak tepat atau beberapa fungsi mungkin tidak tersedia.

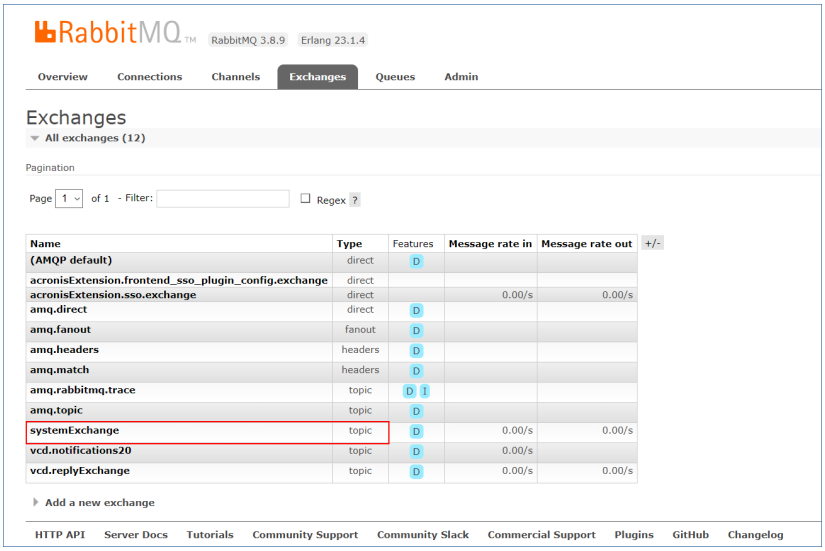
Mengonfigurasi perantara pesan RabbitMQ

1. Instal perantara RabbitMQ AMQP untuk lingkungan VMware Cloud Director Anda.
   Untuk informasi lebih lanjut tentang cara menginstall RabbitMQ, lihat dokumentasi VMware: Menginstal dan Mengonfigurasi Perantara RabbitMQ AMQP.

2. Masuk ke portal penyedia VMware Cloud Director sebagai Administrator Sistem.
3. Buka **Administrasi** > **Ekstensibilitas**, lalu verifikasi bahwa di bawah **Notifikasi AMQP Non-blokir**, **Notifikasi** diaktifkan.



4. Masuk ke konsol manajemen RabbitMQ sebagai administrator.
5. Pada tab **Pertukaran**, verifikasi bahwa pertukaran tersebut (secara default, dengan nama **SystemExchange**) dibuat, dan tipenya adalah **topik**.



Menginstal plug-in untuk VMware Cloud Director

1. Klik tautan berikut untuk mengunduh file **vCDPlugin.zip**: https://dl.managed-protection.com/u/vCD/vCDPlugin.zip.
2. Masuk ke portal penyedia VMware Cloud Director sebagai administrator sistem.
3. Dari menu navigasi, pilih **Sesuaikan Portal**.
4. Pada tab **Kelola Plugin**, klik **Unggah**.
   Wizard **Unggah Plugin** terbuka.
5. Klik **Pilih File Plugin**, lalu pilih file **vCDPlugin.zip**.
6. Klik **Berikutnya**.

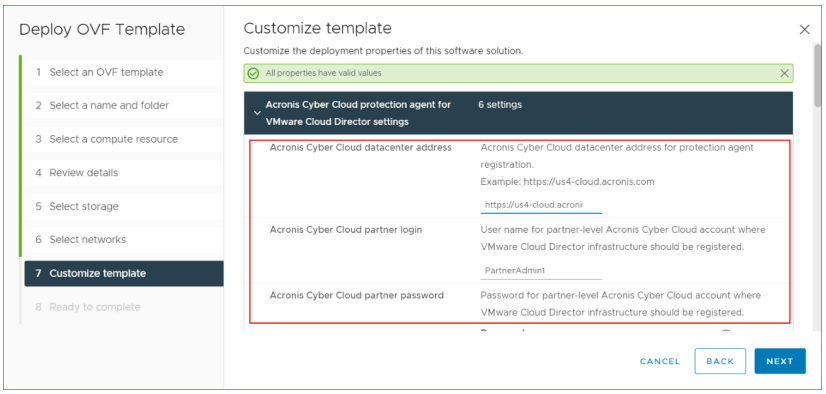
7. Konfigurasi cakupan dan publikasi:
   a. Di bagian **Cakupan untuk**, pilih hanya kotak centang **Penyewa**.
   b. Di bagian **Publikasi ke**, pilih **Semua penyewa** untuk mengaktifkan plug-in untuk semua penyewa yang ada dan berikutnya, atau pilih penyewa individual yang padanya Anda ingin mengaktifkan plug-in.
8. Klik **Berikutnya**.
9. Tinjau pengaturan Anda, lalu klik **Selesai**.

Menginstal agen manajemen

1. Masuk ke portal manajemen Cyber Protect Cloud sebagai administrator mitra.
2. Buka **Pengaturan** > **Lokasi**, lalu klik **Tambahkan VMware Cloud Director**.
3. Klik tautan **Agen Manajemen** dan unduh file ZIP tersebut.
4. Ekstraksi file templat agen manajemen `vCDManagementAgent.ovf` dan file hard disk virtual `vCDManagementAgent-disk1.vmdk`.
5. Dalam vSphere Client, sebarkan templat OVF agen manajemen ke host ESXi di bawah instans vCenter yang dikelola oleh VMware Cloud Director.

   Penting
   Instal hanya satu agen manajemen per lingkungan VMware Cloud Director.

6. Dalam wizard **Sebarkan Templat OVF**, konfigurasi agen manajemen dengan mengatur yang berikut:



   a. URL pusat data Cyber Protect Cloud. Contohnya, `https://us5-cloud.example.com`.
   b. Login dan kata sandi administrator mitra.
   c. ID penyimpanan cadangan untuk mesin virtual di lingkungan VMware Cloud Director. Penyimpanan cadangan ini hanya dapat dimiliki oleh mitra. Untuk detail lebih lanjut tentang penyimpanan, lihat "Mengelola lokasi dan penyimpanan" (hlm. 65).
      Untuk memeriksa ID, di portal manajemen, buka **Pengaturan** > **Lokasi**, lalu pilih penyimpanan yang diinginkan. Anda dapat melihat ID-nya setelah bagian **uuid=** part in the URL.

d. Mode penagihan Cyber Protect Cloud: **Per gigabyte** atau **Per beban kerja**.

> **Catatan**
> Mode penagihan yang dipilih berlaku untuk semua penyewa pelanggan yang akan dibuat.

e. Parameter VMware Cloud Director: alamat infrastruktur, masuk administrator sistem, dan kata sandi.

f. Parameter RabbitMQ: alamat server, port, nama host virtual, login administrator, dan kata sandi.

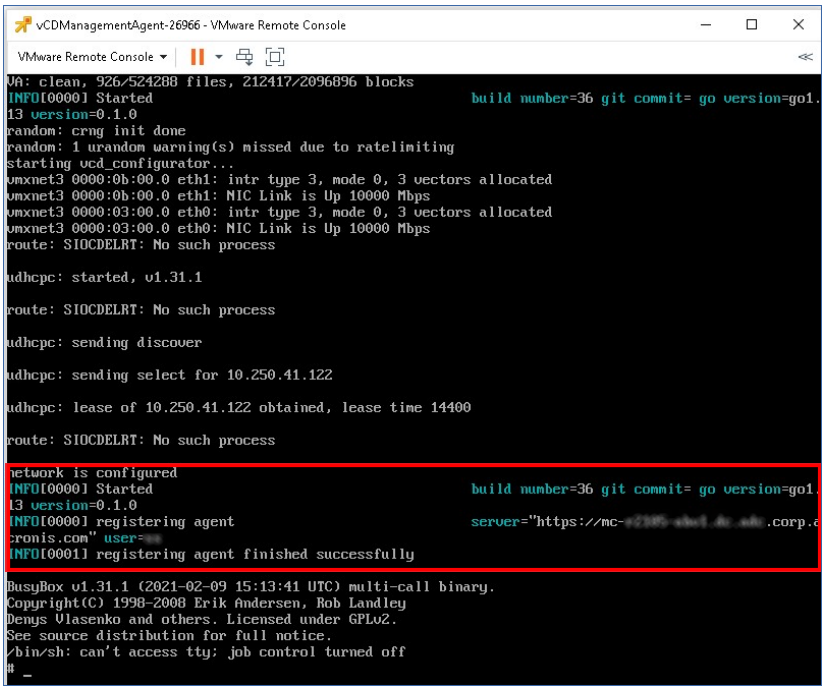
g. Parameter jaringan: Alamat IP, subnet mask, gateway default, DNS, akhiran DNS.

Secara default, hanya satu antarmuka jaringan yang diaktifkan. Untuk mengaktifkan antarmuka jaringan kedua, pilih kotak centang di samping **Aktifkan eth1**.

> **Catatan**
> Pastikan pengaturan jaringan Anda mengizinkan agen manajemen untuk mengakses lingkungan VMware Cloud Director dan pusat data Cyber Protect Cloud Anda.

Anda juga dapat mengonfigurasi pengaturan agen manajemen setelah penyebaran awal. Dalam vSphere Client, matikan mesin virtual dengan agen manajemen, lalu klik **Konfigurasi** > **Pengaturan** > **Opsi vApp**. Terapkan pengaturan yang diinginkan, lalu nyalakan mesin virtual dengan agen manajemen.

7. [Opsional] Dalam vSphere Client, buka konsol mesin virtual dengan agen manajemen, lalu verifikasi pengaturan Anda.

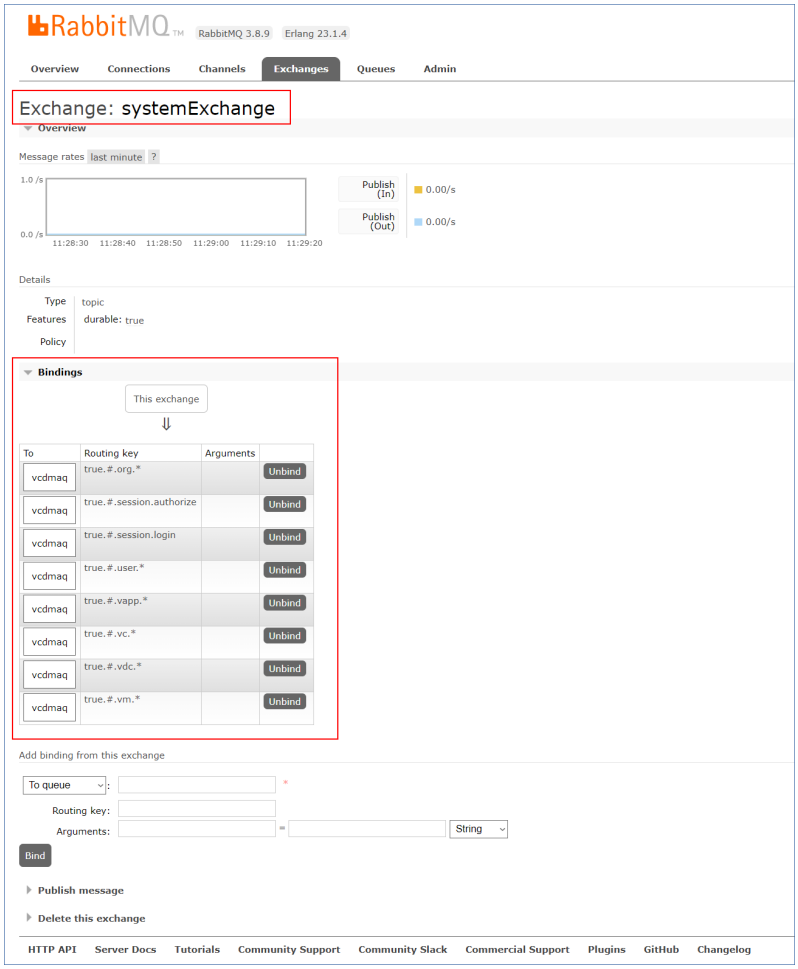


8. Verifikasi koneksi RabbitMQ.

a. Masuk ke konsol manajemen RabbitMQ sebagai administrator.

b. Dalam tab **Pertukaran**, pilih pertukaran yang Anda tentukan selama instalasi RabbitMQ. Secara default, namanya adalah **systemExchange**.

c. Verifikasi pengikatan ke antrean **vcdmaq**.



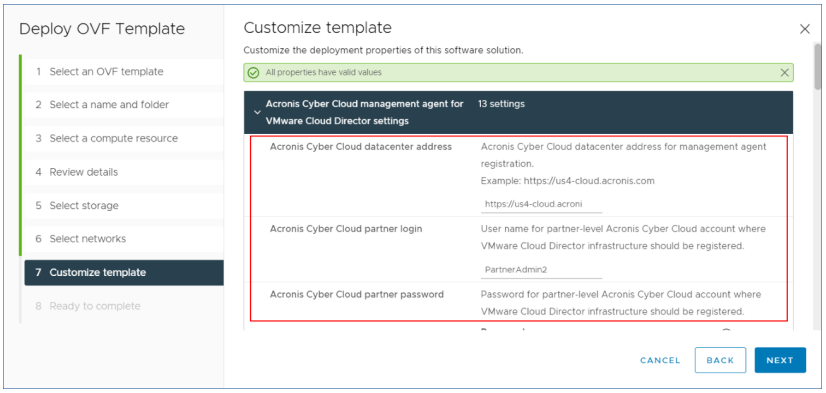
Menginstal agen pencadangan

1. Masuk ke portal manajemen sebagai administrator mitra.
2. Buka **Pengaturan** > **Lokasi**, lalu klik **Tambahkan VMware Cloud Director**.
3. Klik tautan **Agen Pencadangan** dan unduh file ZIP tersebut.
4. Ekstraksi file templat agen pencadangan `vCDCyberProtectAgent.ovf` dan file hard disk virtual `vCDCyberProtectAgent-disk1.vmdk`.
5. Dalam vSphere Client, sebarkan templat agen pencadangan ke host ESXi yang diinginkan.

   Anda membutuhkan setidaknya satu agen pencadangan per host. Secara default, agen pencadangan diberi 8 GB RAM dan 2 CPU, dan dapat memproses hingga 10 tugas pencadangan atau pemulihan secara serentak. Untuk memproses lebih banyak tugas atau mendistribusikan lalu lintas pencadangan dan pemulihan, sebarkan agen tambahan ke host yang sama.

Catatan
Cadangan mesin virtual pada host ESXi yang tidak memiliki agen pencadangan yang diinstal akan gagal dengan kesalahan "Waktu tunggu tugas habis".

6. Dalam wizard **Sebarkan Templat OVF**, konfigurasi agen pencadangan dengan mengatur yang berikut:



a. URL pusat data Cyber Protect Cloud. Contohnya, `https://us5-cloud.example.com`.

b. Login dan kata sandi administrator mitra.

c. Parameter VMware vCenter: alamat server, login, dan kata sandi.

   Agen akan menggunakan kredensial ini untuk terhubung ke vCenter Server. Kami sarankan Anda untuk menggunakan akun dengan peran **Administrator**. Atau, sediakan akun dengan privilese yang diperlukan pada vCenter Server.

d. Parameter jaringan: Alamat IP, subnet mask, gateway default, DNS, akhiran DNS.

   Secara default, hanya satu antarmuka jaringan yang diaktifkan. Untuk mengaktifkan antarmuka jaringan kedua, pilih kotak centang di samping **Aktifkan eth1**.

   Catatan
   Pastikan pengaturan jaringan Anda akan mengizinkan agen pencadangan untuk mengakses Pusat vCenter dan pusat data Cyber Protect Cloud Anda.

e. Batas pengunduhan: kecepatan pengunduhan maksimum (dalam Kbps), yang menentukan kecepatan baca arsip cadangan selama operasi pemulihan. Nilai defaultnya adalah 0 - tidak terbatas.

f. Batas pengunggahan: kecepatan pengunggahan maksimum (dalam Kbps), yang menentukan kecepatan tulis arsip cadangan selama operasi pemulihan. Nilai defaultnya adalah 0 - tidak terbatas.

Anda juga dapat mengonfigurasi parameter pengaturan agen pencadangan setelah penyebaran awal. Dalam vSphere Client, matikan mesin virtual dengan agen pencadangan, lalu klik **Konfigurasi** > **Pengaturan** > **Opsi vApp**. Terapkan pengaturan yang diinginkan, lalu nyalakan mesin virtual dengan agen pencadangan.

7. Dalam vSphere Client, pastikan bahwa **Host** dan **Storage vMotion** dinonaktifkan untuk mesin virtual dengan agen pencadangan.

Memperbarui agen

Untuk memperbarui agen manajemen

1. Masuk ke portal manajemen Cyber Protect Cloud sebagai administrator mitra.
2. Buka **Pengaturan** > **Lokasi**, lalu klik **Tambahkan VMware Cloud Director**.
3. Klik tautan **Agen Manajemen**, lalu unduh file ZIP dengan agen terbaru.
4. Ekstraksi file templat agen manajemen `vCDManagementAgent.ovf` dan file hard disk virtual `vCDManagementAgent-disk1.vmdk`.
5. Dalam vSphere Client, matikan mesin virtual dengan agen manajemen terkini.
6. Sebarkan mesin virtual dengan agen manajemen baru menggunakan file `vCDManagementAgent.ovf` dan `vCDManagementAgent-disk1.vmdk` terbaru.
7. Konfigurasi agen manajemen menggunakan pengaturan yang sama dengan yang lama.
8. [Opsional] Hapus mesin virtual dengan agen manajemen lama.

Penting
Anda harus memiliki hanya satu agen manajemen aktif per lingkungan VMware Cloud Director.

Untuk memperbarui agen pencadangan

1. Masuk ke portal manajemen Cyber Protect Cloud sebagai administrator mitra.
2. Buka **Pengaturan** > **Lokasi**, lalu klik **Tambahkan VMware Cloud Director**.
3. Klik tautan **Agen Pencadangan** dan unduh file ZIP dengan agen terbaru.
4. Ekstraksi file templat agen manajemen `vCDCyberProtectAgent.ovf` dan file hard disk virtual `vCDCyberProtectAgent-disk1.vmdk`.
5. Dalam vSphere Client, matikan mesin virtual dengan agen pencadangan terkini.
   Semua tugas pemulihan dan pencadangan yang sedang berjalan mungkin akan gagal. Untuk memeriksa apakah ada tugas yang sedang berjalan, dalam vSphere Client, buka konsol mesin virtual dengan agen pencadangan, lalu jalankan perintah `ps | grep esx_worker`. Pastikan bahwa tidak ada proses `esx_worker` yang aktif.
6. Terapkan mesin virtual dengan agen manajemen baru menggunakan file `vCDCyberProtectAgent.ovf` dan `vCDCyberProtectAgent-disk1.vmdk` terbaru.
7. Konfigurasi agen pencadangan menggunakan pengaturan yang sama dengan yang lama.
8. [Opsional] Hapus mesin virtual dengan agen pencadangan lama.

Mengakses konsol web Cyber Protection

Administrator berikut dapat mengelola cadangan mesin virtual di Organisasi VMware Cloud Director:

- Administrator Organisasi
- Administrator pencadangan yang ditetapkan secara khusus
  Untuk informasi lebih lanjut tentang cara membuat administrator tersebut, lihat "Membuat administrator pencadangan" (hlm. 144).

Administrator dapat mengakses konsol web Cyber Protection kustom dengan mengeklik **Perlindungan Cyber** di menu navigasi pada portal penyewa VMware Cloud Director.

Catatan
Sign-on tunggal tersedia hanya untuk Administrator Organisasi dan tidak didukung untuk Administrator Sistem yang menggunakan portal penyewa VMware Cloud Director.

Di konsol web Cyber Protection, administrator dapat mengakses elemen Organisasi VMware Cloud Director miliknya sendiri: pusat data virtual, vApp, dan mesin virtual individual. Mereka dapat mengelola cadangan dan pemulihan sumber daya Organisasi VMware Cloud Director.

Administrator mitra dapat mengakses konsol web Cyber Protection milik penyewa pelanggan mereka dan dapat mengelola cadangan dan pemulihan atas nama mereka.

Pembatasan

Daftar batasan akan berubah dalam rilis Cyber Protect Cloud yang akan datang.

Cadangan

- Hanya pencadangan keseluruhan mesin yang didukung. Filter file, atau memilih disk atau volume, tidak tersedia.
- Hanya penyimpanan awan yang didukung sebagai lokasi pencadangan. Penyimpanan dikonfigurasi du pengaturan agen manajemen dan pengguna tidak dapat mengubahnya di rencana proteksi.
- Grup dinamis tidak didukung.
- Skema pencadangan berikut didukung: **Selalu inkremental (file tunggal)**, **Selalu penuh**, dan **Mingguan penuh, Inkremental harian**.
- Pembersihan didukung hanya setelah pencadangan.

Pemulihan

- Pemulihan yang didukung hanya ke mesin virtual asli. Mesin virtual asli harus ada di lingkungan VMware Cloud Director.
- Pemulihan tingkat file tidak didukung.

Membuat administrator pencadangan

Administrator Organisasi dapat menugaskan manajemen cadangan kepada administrator pencadangan yang ditetapkan secara khusus.

Untuk membuat administrator pencadangan

1. Di portal penyewa VMware Cloud Director, klik **Administrasi** > **Peran** > **Baru**.
2. Di jendela **Tambah Peran**, tentukan nama dan deskripsi untuk peran baru.
3. Gulir ke bawah daftar izin, lalu, di bagian **Lainnya**, pilih **Operator pencadangan VM layanan mandiri**.

   Catatan
   Izin **Operator pencadangan VM layanan mandiri** menjadi tersedia setelah Anda menginstal plug-in untuk VMware Cloud Director. Untuk informasi lebih lanjut tentang cara melakukan ini, lihat "Menginstal plug-in untuk VMware Cloud Director" (hlm. 138).

4. Di portal penyewa VMware Cloud Director, klik **Pengguna**.
5. Pilih pengguna, lalu klik **Edit**.
6. Tetapkan pengguna ini untuk peran baru yang Anda buat.

Hasilnya, pengguna yang dipilih akan dapat mengelola cadangan untuk mesin virtual dalam Organisasi ini.

Catatan
Administrator Sistem lingkungan VMware Cloud Director dapat menentukan peran global dengan izin **Operator pencadangan VM layanan mandiri** yang diaktifkan, lalu memublikasikan peran ini untuk penyewa. Maka, Administrator Organisasi hanya perlu menetapkan peran untuk seorang pengguna.

Laporan sistem, file log, dan file konfigurasi

Untuk tujuan pemecahan masalah, Anda mungkin perlu membuat laporan sistem menggunakan alat `sysinfo`, atau memeriksa log dan file konfigurasi pada mesin virtual dengan agen.

Anda dapat mengakses mesin virtual secara langsung dengan membuka konsolnya di vSphere Client, atau dari jarak jauh − melalui klien SSH. Untuk mengakses mesin virtual melalui klien SSH, Anda harus mengaktifkan terlebih dahulu koneksi SSH ke mesin ini.

Untuk mengaktifkan koneksi SSH ke mesin virtual

1. Dalam vSphere Client, buka konsol mesin virtual dengan agen.
2. Pada command prompt, jalankan perintah berikut: `/bin/sshd` untuk memulai daemon SSH.

Hasilnya, Anda dapat terhubung ke mesin virtual ini menggunakan klien SSH, seperti WinSCP.

Untuk menjalankan alat `sysinfo`

1. Akses mesin virtual dengan agen.
   - Untuk mengaksesnya secara langsung, dalam vSphere Client, buka konsol mesin virtual.
   - Untuk mengakses dari jarak jauh, hubungkan ke mesin virtual melalui klien SSH.
     Gunakan kombinasi login:kata sandi default berikut ini: `root`:`root`.
2. Navigasi ke direktori `/bin`, lalu jalankan alat `sysinfo`.

```
# cd /bin/
# ./sysinfo
```

Hasilnya, file laporan sistem akan disimpan ke direktori default: `/var/lib/Acronis/sysinfo`.

Anda dapat menentukan direktori lain dengan menjalankan alat `sysinfo` dengan opsi `--target_dir`.

```
./sysinfo --target_dir path/to/report/dir
```

3. Menggunakan klien SSH, unduh laporan sistem yang sudah dibuat.

Untuk mengakses log atau file konfigurasi

1. Hubungkan ke mesin virtual melalui klien SSH.
   Gunakan kombinasi login:kata sandi default berikut ini: `root`:`root`.
2. Unduh file yang diinginkan.
   Anda dapat menemukan file log di lokasi berikut:
   - Agen pencadangan: `/opt/acronis/var/log/vmware-cloud-director-backup-service/log.log`
   - Agen manajemen: `/opt/acronis/var/log/vmware-cloud-director-management-agent/log.log`

   Anda dapat menemukan file konfigurasi di lokasi berikut:
   - Agen pencadangan: `/opt/acronis/etc/vmware-cloud-director-backup-service/config.yml`
   - Agen manajemen: `/opt/acronis/etc/vmware-cloud-director-management-agent/config.yaml`

Menghapus integrasi dengan VMware Cloud Director

Mengembalikan konfigurasi dan membatalkan pendaftaran instans VMware Cloud Director dari Cyber Protect Cloud adalah prosedur yang rumit. Silakan hubungi perwakilan dukungan Anda untuk mendapatkan bantuan.

Pengaturan privasi

Pengaturan privasi membantu Anda menunjukkan apakah Anda memberikan izin pengumpulan, penggunaan, dan pengungkapan informasi pribadi atau tidak.

Bergantung pada negara tempat Anda menggunakan pusat data Cyber Protect dan Cyber Protect Cloud yang memberikan layanan untuk Anda, pada peluncuran awal Cyber Protect, Anda mungkin diminta mengonfirmasi apakah Anda setuju menggunakan Google Analytics di Cyber Protect.

Google Analytics membantu kami memahami perilaku pengguna dengan lebih baik dan meningkatkan pengalaman pengguna di Cyber Protect dengan mengumpulkan data pseudonim.

Jika Anda tidak melihat izin dan menu Google Analytics di antarmuka Cyber Protect, artinya Google Analytics tidak digunakan di negara Anda.

Jika Anda mengaktifkan atau menolak mengaktifkan Google Analytics di peluncuran awal Cyber Protect, Anda dapat mengubah keputusan kapan saja.

Untuk mengaktifkan atau menonaktifkan Google Analytics

1. Di konsol Cyber Protect, klik ikon akun di sudut kanan atas.
2. Pilih **Pengaturan privasi saya**.
3. Di bagian **Pengumpulan data Google Analytics**, klik salah satu tombol berikut:
   - **Aktif** untuk mengaktifkan Google Analytics
   - **Nonaktif** untuk menonaktifkan Google Analytics

Indeks

L

M