

Portal Manajemen

24.02

Daftar isi

Tentang dokumen ini	5
Tentang portal manajemen	6
Akun dan unit	6
Manajemen kuota	7
Melihat kuota untuk organisasi Anda	8
Menentukan kuota untuk pengguna Anda	13
Browser web yang didukung	15
Petunjuk langkah demi langkah	17
Mengaktifkan akun administrator	17
Persyaratan kata sandi	17
Mengakses portal manajemen dan layanan	17
Untuk beralih antara portal manajemen dan konsol layanan	18
Navigasi di portal manajemen	18
Membuat unit	18
Membuat akun pengguna	19
Peran pengguna yang tersedia untuk setiap layanan	21
Peran administrator hanya baca	23
Pulihkan peran operator	24
Mengubah pengaturan pemberitahuan untuk pengguna	24
Pemberitahuan yang diterima oleh peran pengguna	26
Menonaktifkan dan mengaktifkan akun pengguna	26
Menghapus akun pengguna	26
Mentransfer kepemilikan akun pengguna	27
Mengatur autentikasi dua faktor	28
Cara kerjanya	28
Propagasi pengaturan dua faktor lintas level penyewa	30
Mengatur autentikasi dua faktor untuk penyewa Anda	31
Mengelola autentikasi dua faktor untuk pengguna	31
Mengatur ulang autentikasi dua faktor jika perangkat faktor kedua hilang	33
Perlindungan brute-force	33
Memperbarui agen secara otomatis	34
Untuk memperbarui agen secara otomatis	34
Untuk memantau pembaruan agen	36
Mengonfigurasi penyimpanan yang tidak dapat diubah	36
Penyimpanan dan agen yang didukung	38

Pemantauan	39
Penggunaan	39
Dasbor operasi	39
Status proteksi	40
Skor #CyberFit berdasarkan mesin	41
Widget Deteksi dan Tanggapan Titik Akhir (EDR)	42
Pemantauan kesehatan disk	45
Peta perlindungan data	49
Widget penilaian kerentanan	50
Widget instalasi patch	51
Detail pemindaian cadangan	53
Baru-baru ini terdampak	53
URL yang diblokir	54
Widget inventaris perangkat lunak	55
Widget inventaris perangkat keras	56
Riwayat sesi	57
Log audit	57
Bidang log audit	58
Filter dan pencarian	59
Pelaporan	60
Laporan penggunaan	60
Tipe laporan	60
Lingkup laporan	60
Metrik dengan penggunaan nol	60
Mengonfigurasi Laporan penggunaan terjadwal	61
Mengonfigurasi Laporan penggunaan kustom	61
Data dalam Laporan penggunaan	62
Laporan operasi	62
Tindakan dengan laporan	63
Ringkasan eksekutif	65
Widget ringkasan eksekutif	66
Mengonfigurasi pengaturan rangkuman laporan Eksekutif	74
Membuat rangkuman laporan Eksekutif	75
Menyesuaikan Rangkuman laporan eksekutif	75
Mengirim rangkuman laporan Eksekutif	77
Zona waktu dalam laporan	77
Data yang dilaporkan berdasarkan tipe widget	78

Integrasi	82
Katalog integrasi	82
Semua integrasi	82
Integrasi dalam penggunaan	83
Membatasi akses ke antarmuka web	83
Membatasi akses ke perusahaan Anda	84
Mengelola klien API	84
Apa itu klien API?	84
Prosedur integrasi yang umum	85
Membuat klien API	85
Mengatur ulang nilai rahasia klien API	85
Menonaktifkan klien API	86
Mengaktifkan klien API yang dinonaktifkan	86
Menghapus klien API	87
Indeks	88

Tentang dokumen ini

Dokumen ini ditujukan untuk administrator pelanggan yang ingin menggunakan portal manajemen awan untuk membuat dan mengelola akun, unit, dan kuota pelanggan guna mengonfigurasi dan mengontrol akses, serta memantau penggunaan dan operasi organisasi awan mereka.

Tentang portal manajemen

Portal manajemen adalah antarmuka web platform web yang menyediakan layanan perlindungan data.

Sementara tiap layanan memiliki antarmuka webnya sendiri, yang disebut konsol layanan, portal manajemen memungkinkan administrator untuk mengendalikan penggunaan layanan, membuat akun pengguna dan unit penyimpanan, membuat laporan, dan masih banyak lagi.

Akun dan unit

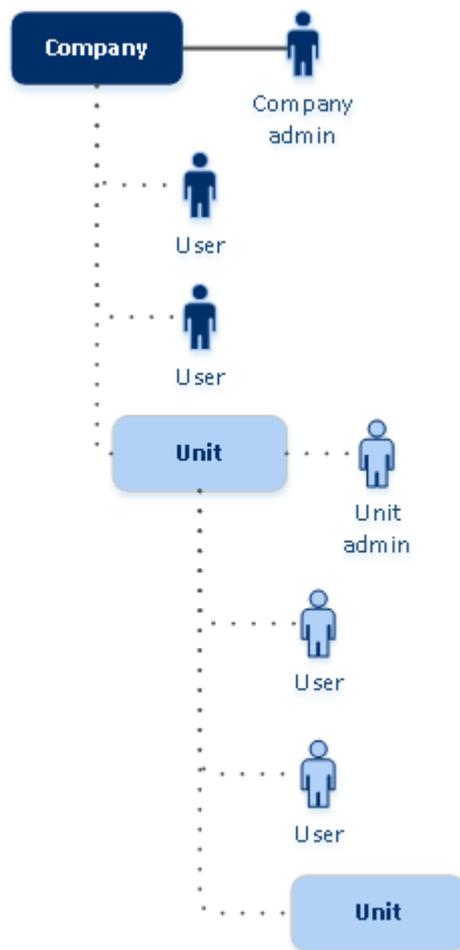
Terdapat dua jenis akun pengguna: akun administrator dan akun pengguna.

- **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.

Administrator dapat membuat unit penyimpanan, yang biasanya berhubungan dengan unit atau departemen sebuah organisasi. Setiap akun ada pada tingkat perusahaan atau dalam unit.

Administrator dapat mengelola unit penyimpanan, akun administrator, dan akun pengguna pada tingkat atau di bawah tingkat mereka dalam hierarki.

Diagram berikut menggambarkan tiga tingkat hierarki – satu perusahaan dan dua unit. Unit opsional dan akun ditunjukkan dengan garis putus-putus.



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

Operasi	Pengguna	Administrator
Buat unit	Tidak	Iya
Buat akun	Tidak	Iya
Unduh dan instal perangkat lunak	Iya	Iya
Gunakan layanan	Iya	Iya
Buat laporan tentang penggunaan layanan	Tidak	Iya

Manajemen kuota

Kuota membatasi kemampuan penyewa untuk menggunakan layanan.

Di portal manajemen, Anda dapat melihat kuota layanan yang dialokasikan untuk organisasi Anda oleh penyedia layanan tapi Anda tidak dapat mengelolanya.

Anda dapat mengelola kuota layanan untuk pengguna Anda.

Melihat kuota untuk organisasi Anda

Di portal manajemen, buka **Ikhtisar > Penggunaan**. Anda akan melihat dasbor yang menampilkan kuota yang dialokasikan untuk organisasi Anda. Kuota untuk setiap layanan ditampilkan di tab terpisah.

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.

Penting

Agen lokal dan agen cloud menggunakan kuota terpisah. Jika Anda mencadangkan beban kerja yang sama dengan menggunakan kedua agen tersebut, Anda akan dikenakan biaya dua kali.

Misalnya:

- Jika Anda mencadangkan kotak surat 120 pengguna dengan menggunakan agen lokal, dan Anda mencadangkan file OneDrive pengguna yang sama dengan menggunakan agen cloud, Anda akan dikenakan biaya untuk 240 kursi Microsoft 365.
 - Jika Anda mencadangkan kotak surat 120 pengguna dengan menggunakan agen lokal, dan Anda juga mencadangkan kotak surat yang sama dengan menggunakan agen cloud, Anda akan dikenakan biaya untuk 240 kursi Microsoft 365.
-

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. Untuk mempelajari cara memblokir semua pengguna tanpa lisensi di organisasi Microsoft 365, lihat "Mencegah pengguna Microsoft 365 tanpa lisensi untuk masuk" (hlm. 11).

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.

- **Google Workspace Shared Drive**

Kuota ini diterapkan oleh penyedia layanan ke seluruh perusahaan. Kuota ini mengaktifkan atau menonaktifkan kemampuan untuk melindungi Google Workspace Shared Drive. 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 Google Workspace Shared Drive 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**

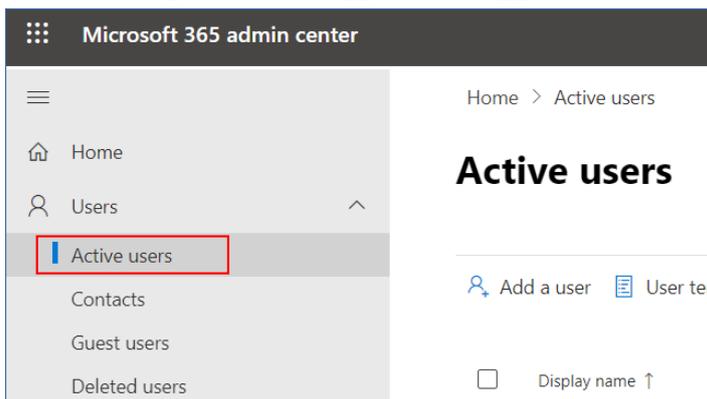
Kuota **Sumber daya awan** menggabungkan kuota untuk penyimpanan cadangan dan kuota untuk pemulihan bencana. Kuota penyimpanan cadangan membatasi ukuran total cadangan yang terletak di penyimpanan awan. Saat kelebihan kuota penyimpanan cadangan terlampaui, pencadangan akan gagal.

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

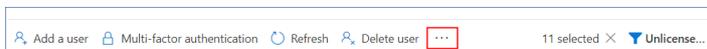
1. Masuk ke pusat admin Microsoft 365 (<https://admin.microsoft.com>) sebagai administrator global.
2. Di menu navigasi, buka **Pengguna > Pengguna Aktif**.



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 cadangan server yang dilindungi dengan pemulihan bencana. Penggunaan penyimpanan pemulihan Bencana sama dengan penggunaan penyimpanan cadangan beban kerja yang dilindungi dengan server pemulihan bencana. Penyimpanan ini dihitung mulai dari saat server pemulihan dibuat, terlepas dari apakah server sedang berjalan. 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 akan 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.

Saat kuota dinonaktifkan, server akan terlihat di konsol Cyber Protect, tetapi 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

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

- **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.

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.

- **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

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

- **Penyimpanan notaris**

Menentukan ruang penyimpanan awan maksimum untuk file yang diaktakan, file yang ditandatangani, dan file yang notarisasi atau penandatanganannya sedang berlangsung.

Untuk mengurangi penggunaan kuota ini, Anda dapat menghapus file yang sudah dinotariskan atau ditandatangani dari penyimpanan notaris.

- **Notarisasi**

Menentukan jumlah maksimum file yang dapat dinotariskan menggunakan layanan notaris.

File dianggap telah diaktakan segera setelah diunggah ke penyimpanan notaris, dan status akta berubah menjadi **Dalam proses**.

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

- **eSignature**

Menentukan jumlah maksimum eSignature.

Menentukan kuota untuk pengguna Anda

Kuota memungkinkan Anda untuk membatasi kemampuan pengguna dalam menggunakan layanan. Untuk menetapkan kuota bagi pengguna, pilih pengguna pada tab **Pengguna** di **Manajemen Perusahaan**, lalu klik ikon pensil pada bagian **Kuota**.

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 pengguna mencapai 20, pengguna akan menerima pemberitahuan melalui email, tapi layanan Cyber Protection akan tetap tersedia.

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

Kuota Backup

Anda dapat menentukan kuota penyimpanan cadangan dan jumlah maksimum mesin/perangkat/situs web yang dapat dilindungi oleh pengguna. 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 penyimpanan

- **Penyimpanan cadangan**

Kuota penyimpanan cadangan membatasi ukuran total cadangan yang terletak di penyimpanan awan. Jika kelebihan kuota penyimpanan cadangan terlampaui, pencadangan akan gagal.

Penting

Agen lokal dan agen cloud menggunakan kuota terpisah. Jika Anda mencadangkan beban kerja yang sama dengan menggunakan kedua agen tersebut, Anda akan dikenakan biaya dua kali.

Misalnya:

- Jika Anda mencadangkan kotak surat 120 pengguna dengan menggunakan agen lokal, dan Anda mencadangkan file OneDrive pengguna yang sama dengan menggunakan agen cloud, Anda akan dikenakan biaya untuk 240 kursi Microsoft 365.
 - Jika Anda mencadangkan kotak surat 120 pengguna dengan menggunakan agen lokal, dan Anda juga mencadangkan kotak surat yang sama dengan menggunakan agen cloud, Anda akan dikenakan biaya untuk 240 kursi Microsoft 365.
-

Kuota File Sync & Share

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

- **Ruang penyimpanan pribadi**
Menentukan ruang penyimpanan awan yang dialokasikan untuk file pengguna.

Kuota Notary

Anda dapat menentukan kuota Notary berikut untuk pengguna:

- **Penyimpanan notaris**
Menentukan ruang penyimpanan awan maksimum untuk file yang diaktakan, file yang ditandatangani, dan file yang notarisasi atau penandatanganannya sedang berlangsung. Untuk mengurangi penggunaan kuota ini, Anda dapat menghapus file yang sudah dinotariskan atau ditandatangani dari penyimpanan notaris.
- **Notarisasi**
Menentukan jumlah maksimum file yang dapat dinotariskan menggunakan layanan notaris. File dianggap telah diaktakan segera setelah diunggah ke penyimpanan notaris, dan status akta berubah menjadi **Dalam proses**.
Jika file yang sama diaktakan berkali-kali, setiap notarisasi dihitung sebagai yang baru.
- **eSignature**
Menentukan jumlah maksimum eSignature.

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.

Petunjuk langkah demi langkah

Langkah berikut akan memandu Anda melalui penggunaan dasar portal manajemen. Langkah tersebut menjelaskan cara untuk:

- Mengaktifkan akun administrator Anda
- Mengakses portal manajemen dan layanan
- Membuat unit
- Membuat akun pengguna

Mengaktifkan akun administrator

Setelah mendaftar layanan, 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. 17).

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 dan layanan

1. Buka halaman masuk konsol layanan.
2. Ketik login, lalu klik **Lanjutkan.**
3. Ketik kata sandi, lalu klik **Lanjutkan.**
4. Lakukan salah satu langkah berikut:

- Untuk masuk ke portal manajemen, klik **Portal Manajemen**.
- Untuk masuk ke layanan, klik nama layanan.

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

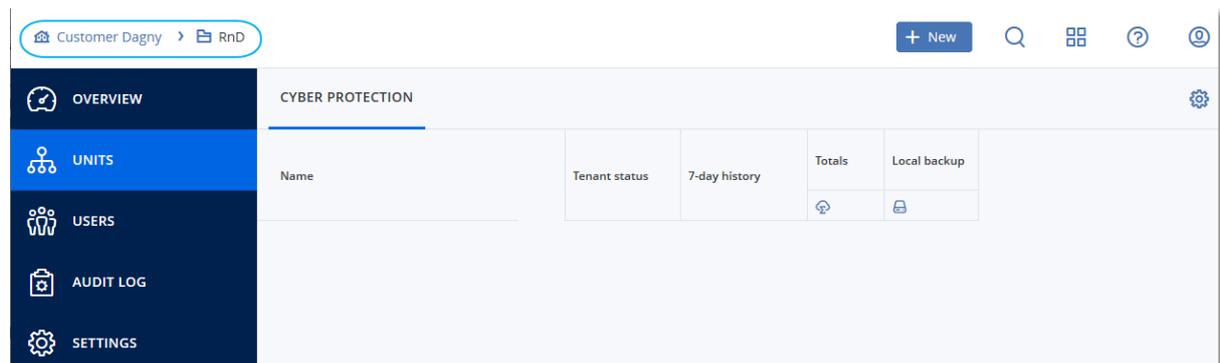
Untuk beralih antara portal manajemen dan konsol layanan

Untuk beralih antara portal manajemen dan konsol layanan, klik ikon  di sudut kanan atas, lalu pilih **Portal manajemen** atau layanan yang ingin Anda akses.

Navigasi di portal manajemen

Ketika menggunakan portal manajemen, pada waktu tertentu Anda beroperasi di dalam perusahaan atau di dalam unit. Ini ditunjukkan di sudut kiri atas.

Secara default, tingkat hierarki paling atas yang tersedia untuk Anda dipilih. Klik nama unit untuk menelusuri hierarki. Untuk menavigasi kembali ke tingkat atas, klik namanya di sudut kiri atas.



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

- Dengan menggunakan tombol **Baru**, Anda dapat membuat unit atau akun pengguna hanya di perusahaan atau unit ini.
- Tab **Unit-unit** hanya menampilkan unit yang merupakan turunan langsung dari perusahaan atau unit ini.
- Tab **Pengguna** hanya menampilkan akun pengguna yang ada di perusahaan atau unit ini.

Membuat unit

Lewati langkah ini jika Anda tidak ingin mengelola akun ke dalam unit.

Jika Anda berencana membuat unit di lain waktu, perlu diketahui bahwa akun yang ada tidak dapat dipindahkan antar unit atau antara perusahaan dan unit. Pertama, Anda perlu membuat unit, lalu mengisinya dengan akun.

Untuk membuat unit

1. Masuk ke portal manajemen.
2. Navigasikan ke unit di mana Anda ingin membuat unit baru.
3. Di sudut kanan atas, klik **Baru > Unit**.
4. Di bagian **Nama**, tentukan nama unit baru.
5. [Opsional] Di bidang **Bahasa**, ubah bahasa default pemberitahuan, laporan, dan perangkat lunak yang akan digunakan dalam unit ini.
6. Lakukan salah satu langkah berikut:
 - Untuk membuat administrator unit, klik **Berikutnya**, lalu ikuti langkah yang dijelaskan dalam "[Membuat akun pengguna](#)", mulai dari langkah 4.
 - Untuk membuat unit tanpa administrator, klik **Simpan dan tutup**. Anda dapat menambahkan administrator dan pengguna ke unit nanti.

Unit yang baru dibuat akan muncul di tab **Unit-unit**.

Jika Anda ingin mengedit pengaturan unit atau menentukan informasi kontak, pilih unit di tab **Unit-unit**, lalu klik ikon pensil di bagian yang ingin Anda edit.

Membuat akun pengguna

Lewati langkah ini jika Anda tidak ingin membuat akun pengguna tambahan.

Anda mungkin ingin membuat akun tambahan dalam kasus berikut:

- Akun administrator perusahaan — untuk membagikan tugas manajemen dengan orang lain.
- Akun administrator unit — untuk mendelegasikan manajemen kepada orang lain yang izin aksesnya akan dibatasi pada unit yang sesuai.
- Akun pengguna — untuk memungkinkan pengguna mengakses hanya subset layanan.

Untuk membuat akun pengguna

1. Masuk ke portal manajemen.
2. Navigasikan ke unit di mana Anda ingin membuat akun pengguna baru.
3. Di sudut kanan atas, klik **Baru > Pengguna**.
4. Tentukan informasi 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.

- [Opsional] **Nama depan**
 - [Opsional] **Nama belakang**
 - Di bagian **Bahasa**, ubah bahasa default pemberitahuan, laporan, dan perangkat lunak yang akan digunakan untuk akun ini.
5. Pilih layanan yang akses dan perannya di tiap layanan akan diberikan kepada pengguna.
- Jika Anda memilih kotak centang **Administrator perusahaan**, pengguna akan memiliki akses ke portal manajemen dan peran administrator di semua layanan.
 - Jika Anda memilih kotak centang **Administrator unit**, pengguna akan memiliki akses ke portal manajemen, tapi akan atau tidak akan memiliki peran administrator, bergantung pada layanan.
 - Jika tidak, pengguna akan memiliki [peran yang Anda tentukan di layanan yang Anda pilih](#).
6. Klik **Buat**.

Unit yang baru dibuat akan muncul di tab **Pengguna**.

Jika Anda ingin mengedit pengaturan pengguna atau menentukan pengaturan pemberitahuan dan kuota 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 akunya 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 fitur Pemulihan Bencana layanan Perlindungan 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. Misalnya, peran ini memberikan izin penuh untuk layar Deteksi dan Tanggapan Titik Akhir, termasuk widget.
	Administrator hanya baca Level mitra	Peran ini memberikan akses hanya baca ke semua objek di portal manajemen mitra dan portal manajemen semua pelanggan dari mitra ini. Pengguna seperti ini dapat mengakses data dari pengguna lain dari organisasi dalam mode hanya baca. Mereka dapat mengedit rencana proteksi, tetapi mereka tidak dapat menyimpan perubahan apa pun pada rencana scripting, rencana monitoring, atau rencana agen.
	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.
Perlindungan	Administrator cyber	Selain hak peran Administrator, peran ini memungkinkan mengonfigurasi dan mengelola layanan

		<p>Cyber Protection, serta menyetujui tindakan dalam Pembuatan Skrip Cyber.</p> <p>Peran administrator Cyber hanya tersedia untuk penyewa dengan paket Manajemen Tingkat Lanjut yang diaktifkan.</p>
	Administrator	<p>Peran ini memungkinkan untuk mengonfigurasi dan mengelola Perlindungan bagi pelanggan Anda.</p> <p>Misalnya, peran ini diperlukan untuk mengonfigurasi dan mengelola fungsionalitas Pemulihan Bencana, fungsionalitas Deteksi dan Tanggapan Titik Akhir, dan daftar izin perusahaan.</p>
	Administrator hanya baca	<p>Peran ini memberikan akses hanya baca untuk semua objek pada layanan Perlindungan. Pengguna tersebut dapat mengakses data pengguna lain pada organisasi dalam mode hanya baca.</p> <p>Administrator hanya baca tidak dapat mengonfigurasi dan mengelola fungsi Pemulihan Bencana, fungsi Deteksi dan Tanggapan Titik Akhir, atau daftar izin perusahaan.</p>
	Pulihkan operator	<p>Peran tersebut memberi akses ke cadangan organisasi Microsoft 365 dan Google Workspace, serta memungkinkan pemulihan cadangan tersebut sekaligus membatasi akses ke konten sensitif.</p>
	Pengguna	<p>Peran ini mengaktifkan menggunakan layanan Perlindungan namun tanpa hak istimewa administratif. Akses disediakan untuk fungsi seperti Deteksi dan Tanggapan Titik Akhir, tapi pengguna yang ditugaskan peran ini tidak dapat mengakses data pengguna lain dalam organisasi.</p>
File Sync & Share	Administrator	<p>Peran ini memungkinkan konfigurasi dan pengelolaan File Sync & Share bagi pengguna Anda. Akun dengan peran ini tidak dihitung sebagai bagian dari kuota Pengguna karena akun ini tidak menyediakan akses ke fungsi File Sync & Share.</p>
	Pengguna	<p>Peran ini memungkinkan penggunaan layanan File Sync & Share. Pengguna hanya dapat mengakses data mereka sendiri dan data yang dibagikan dengan mereka.</p>
	Tamu	<p>Akun dengan peran ini dibuat ketika pengguna File Sync & Share membagikan konten dengan pengguna Cyber Protect Cloud yang tidak diaktifkan untuk menggunakan</p>

		<p>layanan File Sync & Share, atau dengan orang yang bukan pengguna Cyber Protect Cloud.</p> <p>Peran Tamu tidak memiliki folder sinkronisasi, tidak dapat menggunakan penyimpanan awan, dan tidak dihitung sebagai bagian dari kuota Pengguna karena tidak memberikan akses ke fungsionalitas File Sync & Share. Tamu dapat 'dipromosikan' ke peran Pengguna atau Administrator.</p>
Notary	Administrator	Peran ini memungkinkan untuk mengonfigurasi dan mengelola Notary bagi pengguna Anda.
	Pengguna	Peran ini mengaktifkan menggunakan layanan Notary namun tanpa hak istimewa administratif. Pengguna tersebut tidak dapat mengakses data pengguna lain pada organisasi.

Peran administrator hanya baca

Akun dengan peran ini memiliki akses hanya baca ke konsol Cyber Protect 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.

Mengubah pengaturan pemberitahuan untuk pengguna

Untuk mengubah pengaturan pemberitahuan bagi pengguna, buka **Manajemen Perusahaan > Pengguna**. Pilih pengguna yang ingin Anda konfigurasi 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 Cyber Protect 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 perifer 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 (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

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](#).

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:

- Semua notifikasi yang dikonfigurasi untuk akun ini akan dinonaktifkan.
- Semua data milik akun pengguna ini akan dihapus.
- Administrator tidak dapat mengakses portal manajemen.
- Semua pencadangan beban kerja yang berkaitan dengan pengguna ini akan dihapus.
- Semua mesin yang berkaitan dengan akun pengguna ini akan menjadi tidak terdaftar.
- Semua rencana proteksi akan dicabut dari semua beban kerja yang berkaitan dengan pengguna ini.
- Semua data File Sync & Share milik pengguna ini (misalnya, file dan folder) akan dihapus.
- Data notaris milik pengguna ini (misalnya, berkas yang dinotariskan, berkas yang ditandatangani secara elektronik) akan dihapus.
- Anda akan melihat **Status** pengguna sebagai **Dihapus**. Ketika Anda mengarahkan pointer mouse ke status **Dihapus**, Anda akan melihat tanggal ketika pengguna dihapus dan catatan bahwa Anda masih dapat memulihkan semua data dan pengaturan pengguna yang relevan dalam waktu 30 hari sejak tanggal penghapusan ini.

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 **Iya**.

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 32 digit yang ditunjukkan di bawah kode QR dan menambahkannya secara manual di aplikasi autentikasi.

Penting

Sangat disarankan untuk menyimpannya (cetak kode QR, tuliskan rahasia kata sandi satu kali sementara (TOTP), gunakan aplikasi yang mendukung pencadangan kode di cloud). Anda memerlukan kata sandi satu kali (TOTP) sementara untuk mengatur ulang autentikasi dua faktor jika perangkat faktor kedua hilang.

6. Kode kata sandi satu kali (TOTP) sementara akan dihasilkan dalam aplikasi autentikasi. Kode tersebut dihasilkan secara otomatis setiap 30 detik.
7. Pengguna harus memasukkan kode TOTP pada jendela **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.

Untuk memulihkan autentikasi dua faktor pada perangkat baru

Jika Anda memiliki akses ke aplikasi autentikasi seluler yang disiapkan sebelumnya:

1. Instal aplikasi autentikator di perangkat baru Anda.
2. Gunakan file PDF yang Anda simpan saat mengatur 2FA di perangkat Anda. File ini berisi kode 32 digit yang harus dimasukkan di aplikasi autentikator untuk menautkan kembali aplikasi autentikator ke akun Acronis Anda.

Penting

Jika kode sudah benar tetapi tidak berfungsi, pastikan untuk menyinkronkan waktu di aplikasi seluler autentikator.

3. Jika Anda melewatkan menyimpan file PDF selama penyiapan:
 - a. **Klik *Atur ulang 2FA*** dan masukkan kata sandi sekali pakai yang ditampilkan di aplikasi autentikator seluler yang telah diatur sebelumnya.

b. Ikuti petunjuk di layar.

Jika Anda tidak memiliki akses ke aplikasi autentikator seluler yang disiapkan sebelumnya:

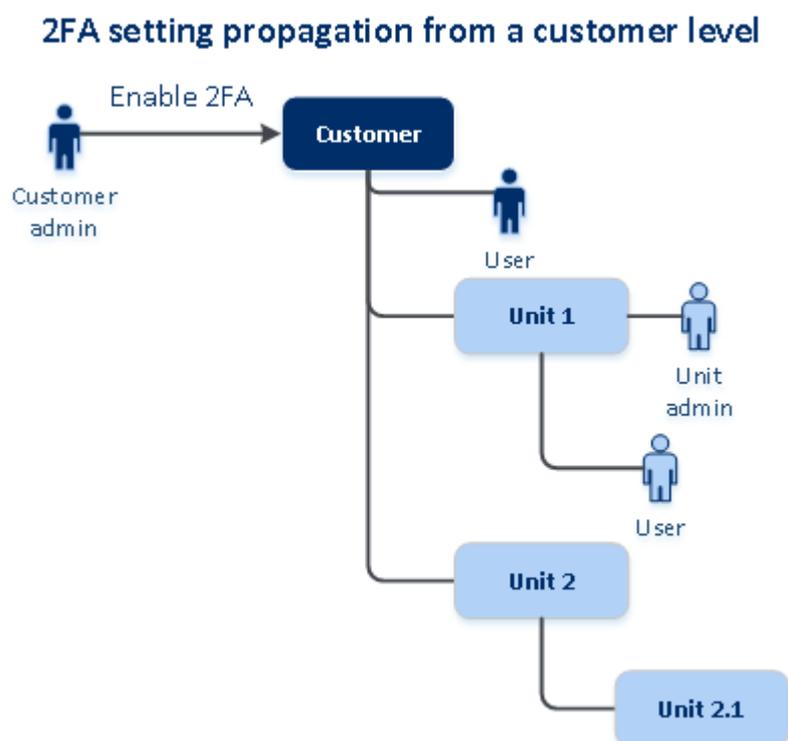
1. Ambil perangkat seluler baru.
2. Gunakan file PDF yang disimpan untuk menautkan perangkat baru (nama default file tersebut adalah `cyberprotect-2fa-backupcode.pdf`).
3. Pulihkan akses ke akun Anda dari cadangan. Pastikan pencadangan didukung oleh aplikasi seluler Anda.
4. Buka aplikasi dengan akun yang sama dari perangkat seluler lain jika didukung oleh aplikasi.

Propagasi pengaturan dua faktor lintas level penyewa

Autentikasi dua faktor diatur pada level **organisasi**. Anda dapat mengatur autentikasi dua faktor hanya untuk organisasi Anda.

Pengaturan autentikasi dua faktor dipropagasi lintas level pengguna sebagai berikut:

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



Catatan

1. Mengatur autentikasi dua faktor pada level unit tidak dimungkinkan.
 2. Anda dapat mengelola pengaturan autentikasi dua faktor untuk pengguna organisasi anak (unit).
-

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 mengonfigurasi 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 tepercaya 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 memkonfirmasi 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.

Memperbarui agen secara otomatis

Penting

Saat ini, Anda akan mendapatkan akses ke fungsionalitas manajemen pembaruan agen hanya jika mengaktifkan Perlindungan.

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.

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 dari Penyedia Layanan jika Anda tidak mengaktifkan Proteksi.

Untuk mengatur pembaruan agen otomatis dari halaman awal Portal Manajemen

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

Update channel

Current
The most up-to-date version of agents.

Previous release
The latest version of the agents from the previous release.

Automatically update agents
Agents will be automatically updated during the specified maintenance window.

Maintenance window
New versions will be installed only in the set timeframe.

From 23:00 To 08:00

Mon Tue Wed Thu Fri Sat Sun

Save Cancel [Reset to default settings](#)

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 jika Anda mengaktifkan modul Proteksi.

Untuk memantau pembaruan agen, lihat bagian Peringatan dan Aktivitas [Panduan Pengguna Cyber Protect](#).

Mengonfigurasi penyimpanan yang tidak dapat diubah

Dengan penyimpanan yang tidak dapat diubah, Anda dapat mengakses cadangan yang dihapus selama periode retensi tertentu. Anda dapat memulihkan konten dari cadangan ini, tetapi Anda tidak dapat mengubah, memindahkan, atau menghapusnya. Ketika periode retensi berakhir, cadangan yang dihapus akan dihapus secara permanen.

Penyimpanan yang tidak dapat diubah berisi cadangan berikut:

- Cadangan yang dihapus secara manual.
- Cadangan yang dihapus secara otomatis, sesuai dengan pengaturan di bagian **Berapa lama akan disimpan** dalam rencana proteksi atau bagian **Aturan retensi** dalam rencana pembersihan.

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

Penyewa yang dihapus tidak dikenakan biaya untuk penyimpanan apa pun, termasuk penyimpanan yang tidak dapat diubah.

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

- **Mode tata kelola**
Anda dapat menonaktifkan dan mengaktifkan kembali penyimpanan yang tidak dapat diubah. Anda dapat mengubah periode retensi atau beralih ke mode Kepatuhan.
- **Mode kepatuhan**

Peringatan!

Memilih mode Kepatuhan tidak dapat dibatalkan.

Anda tidak dapat menonaktifkan penyimpanan yang tidak dapat diubah. Anda tidak dapat mengubah periode retensi dan tidak dapat kembali ke mode Tata Kelola.

Mengonfigurasi pengaturan penyimpanan yang tidak dapat diubah memerlukan autentikasi dua faktor dalam penyewa yang memiliki akun administrator.

Catatan

Untuk memberi akses ke cadangan yang telah dihapus, port 40440 pada penyimpanan cadangan harus diaktifkan untuk koneksi masuk.

Cara mengaktifkan penyimpanan yang tidak dapat diubah

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 3650 hari.
Periode retensi default adalah 14 hari. Periode retensi yang lebih lama akan menyebabkan peningkatan penggunaan penyimpanan.
4. Pilih mode penyimpanan yang tidak dapat diubah, lalu konfirmasi pilihan Anda jika diminta.
5. Klik **Simpan**.

Peringatan!

Pemilihan **Mode kepatuhan** tidak dapat dibatalkan. Setelah memilih mode ini, Anda tidak akan diizinkan untuk menonaktifkan penyimpanan yang tidak dapat diubah, atau mengubah mode atau periode retensinya.

6. Untuk membuat arsip yang ada mendukung penyimpanan yang tidak dapat diubah, buat cadangan baru di arsip tersebut.
Untuk membuat cadangan baru, jalankan rencana proteksi secara manual atau sesuai jadwal.

Peringatan!

Jika Anda menghapus cadangan sebelum membuat arsip mendukung penyimpanan yang tidak dapat diubah, cadangan tersebut akan dihapus secara permanen.

Cara menonaktifkan penyimpanan yang tidak dapat diubah

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

Catatan

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

Peringatan!

Penonaktifan penyimpanan yang tidak dapat diubah tidak segera berlaku. Selama masa tenggang 14 hari, penyimpanan yang tidak dapat diubah masih aktif dan Anda dapat mengakses cadangan yang dihapus sesuai dengan periode penyimpanan aslinya. Ketika masa tenggang berakhir, semua cadangan di penyimpanan yang tidak dapat diubah akan dihapus secara permanen.

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

Penyimpanan dan agen yang didukung

- Penyimpanan yang tidak dapat diubah hanya didukung pada penyimpanan cloud.
Penyimpanan yang tidak dapat diubah tersedia untuk penyimpanan cloud yang dihosting Acronis dan yang dihosting mitra yang menggunakan Cyber Infrastructure versi 4.7.1 atau lebih baru.
Semua penyimpanan yang dapat digunakan dengan Cyber Infrastructure Gateway Cadangan didukung. Misalnya, penyimpanan Cyber Infrastructure, penyimpanan Amazon S3 dan EC2, dan penyimpanan Microsoft Azure.
Penyimpanan yang tidak dapat diubah memerlukan Port TCP 40440 dibuka untuk layanan Gateway cadangan di Cyber Infrastructure. Dalam versi 4.7.1 dan seterusnya, Port TCP 40440 secara otomatis dibuka dengan jenis lalu lintas **Cadangan (ABGW) publik**. Untuk informasi lebih lanjut tentang jenis lalu lintas, lihat [dokumen Infrastruktur Cyber Acronis](#).
- 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.

Pemantauan

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

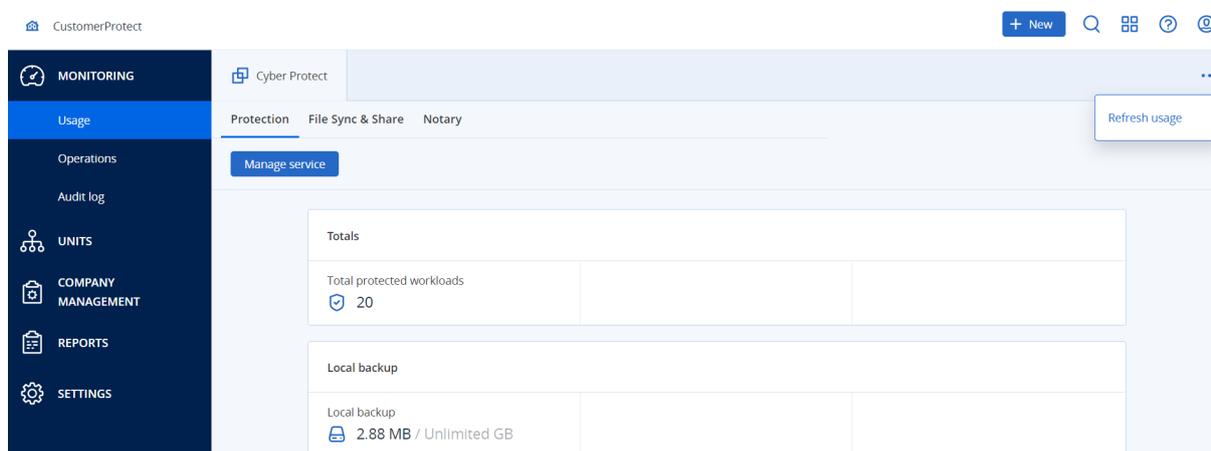
Penggunaan

Tab **Penggunaan** memberikan ikhtisar tentang penggunaan layanan (termasuk kuota, jika ada) dan memungkinkan Anda untuk mengakses konsol layanan.

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.



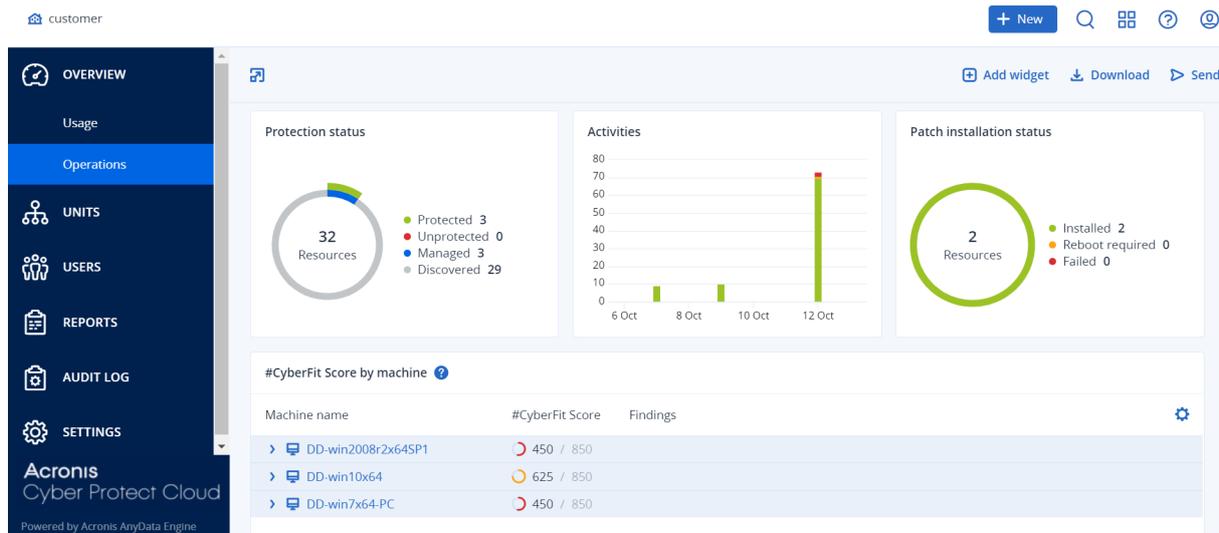
Dasbor operasi

Dasbor **Operasi** hanya tersedia untuk administrator perusahaan ketika beroperasi di tingkat perusahaan.

Dasbor **Operasi** menyediakan sejumlah widget kustom yang memberikan ikhtisar operasi terkait dengan layanan Cyber Protection.

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 atau mengirimnya melalui email dalam format .pdf atau/dan .xlsx.

Anda dapat memilih dari berbagai macam widget, yang disajikan sebagai tabel, diagram lingkaran, diagram batang, daftar, dan peta pohon. Anda dapat menambahkan beberapa widget yang jenisnya sama 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 rentang waktu, 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 menemukannya, klik ikon pensil saat widget dipilih. Setelah mengedit widget, klik **Selesai**.

Untuk menghapus widget

Klik ikon tanda X di sebelah nama widget.

Status proteksi

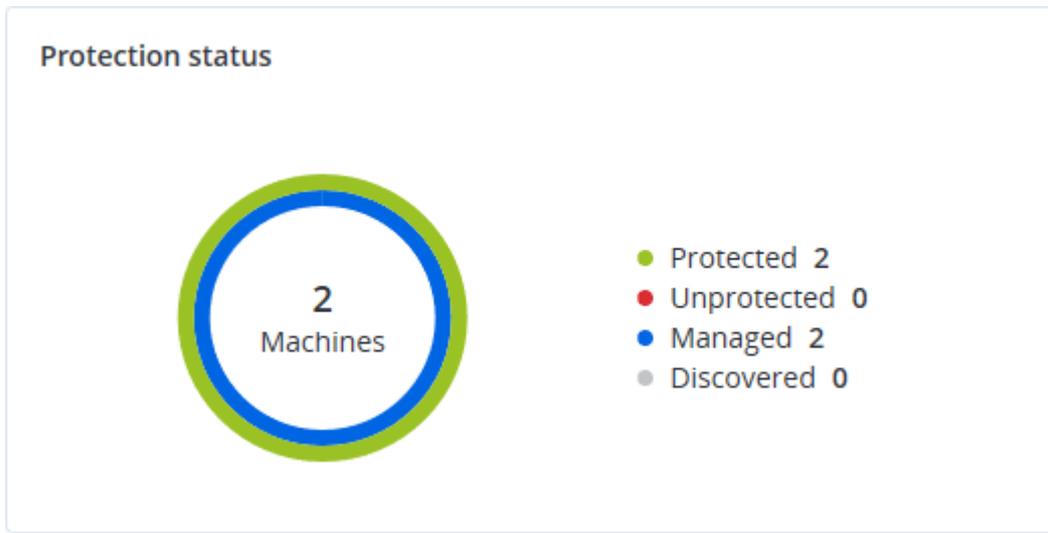
Status proteksi

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 mengklik 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 (EDR)

Penting

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

Deteksi dan Tanggapan Titik Akhir (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.

Top Incident distribution per workload		
SCRANTON		123
qa-gw3t68hh		41
RG_345		32
Georgy_Win_64		11
w_35jf_4		12

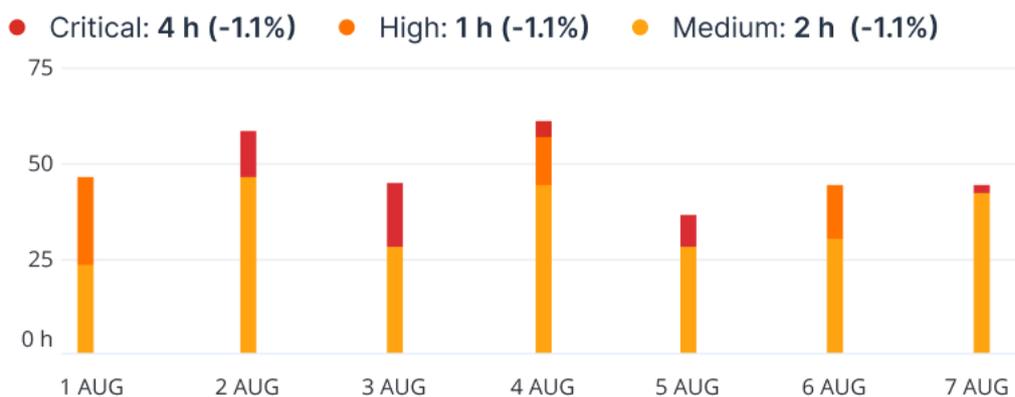
[Show all](#)

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 **Sedang**), 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.

Incident MTTR



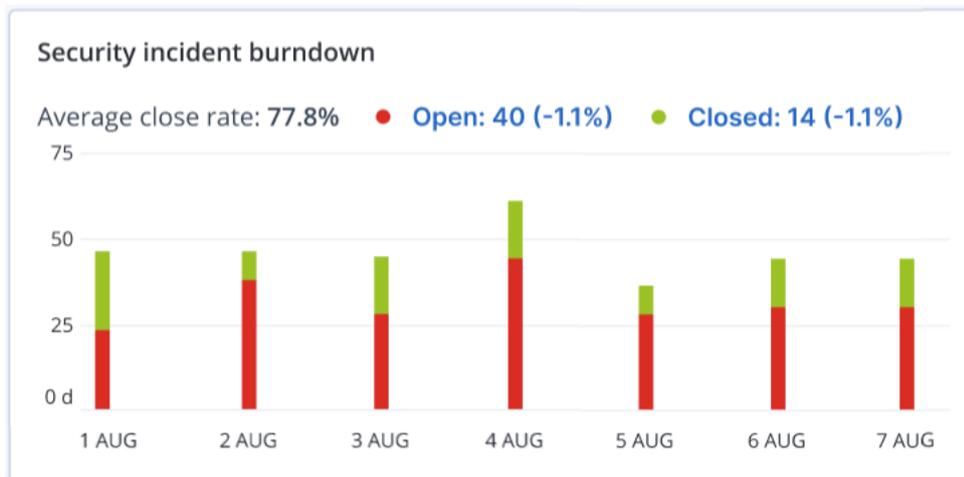
Burndown insiden keamanan

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 mengklik 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 mengklik nilai Tertutup, daftar insiden menampilkan penyewa terpilih, dan disaring untuk menampilkan insiden yang tidak lagi terbuka (dalam status **Tertutup** atau **Positif salah**).

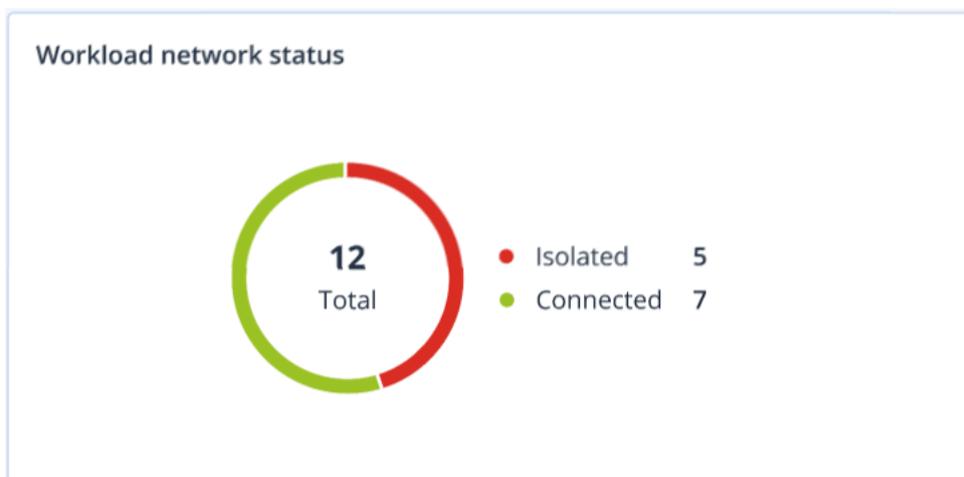
Nilai dalam % yang ditampilkan dalam tanda kurung menandakan peningkatan atau penurunan dibandingkan periode waktu sebelumnya.



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. Widget kesehatan disk tidak menyertakan informasi apa pun tentang mesin dengan implementasi RAID.
- SSD NVMe tidak didukung.

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

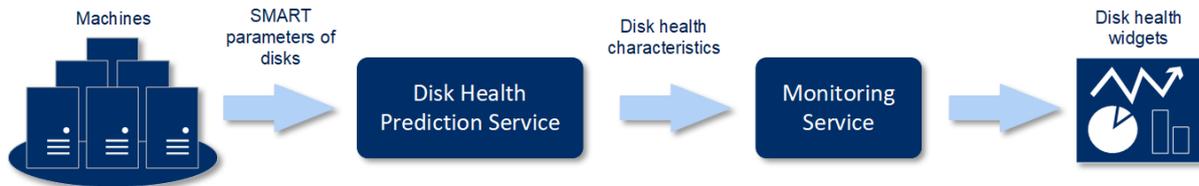
Layanan Prediksi Kesehatan Disk menggunakan model prediksi berbasis AI.

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 menampilkan informasi yang relevan di widget kesehatan disk di konsol Cyber Protect.



Widget kesehatan disk

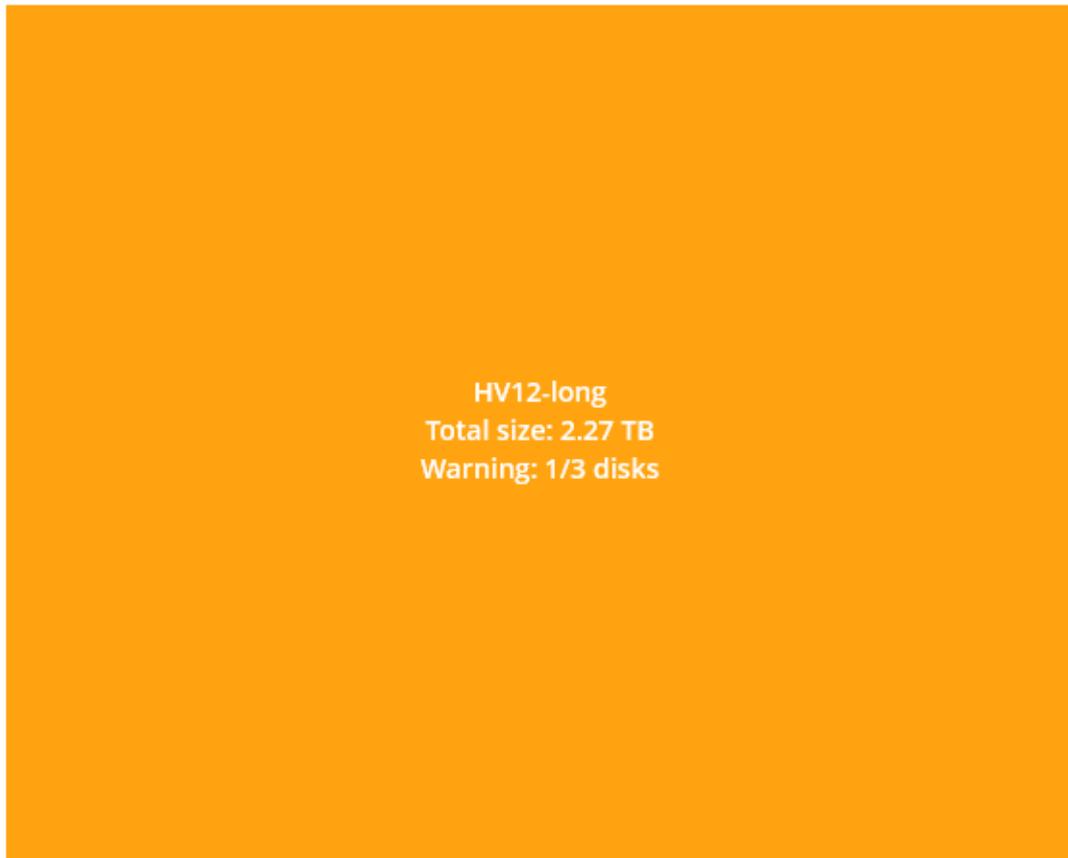
Hasil pemantauan kesehatan disk disajikan dalam widget berikut yang tersedia di konsol Cyber Protect.

- **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.

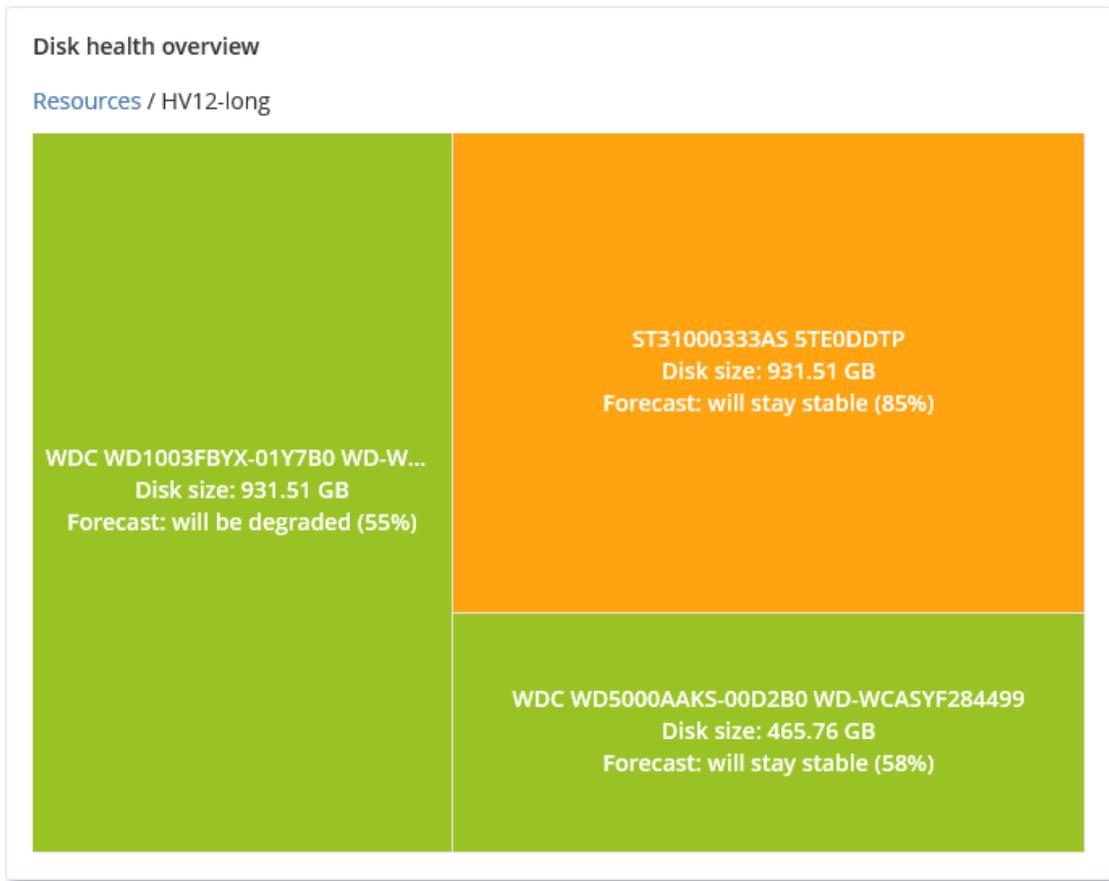
Disk health overview

Resources

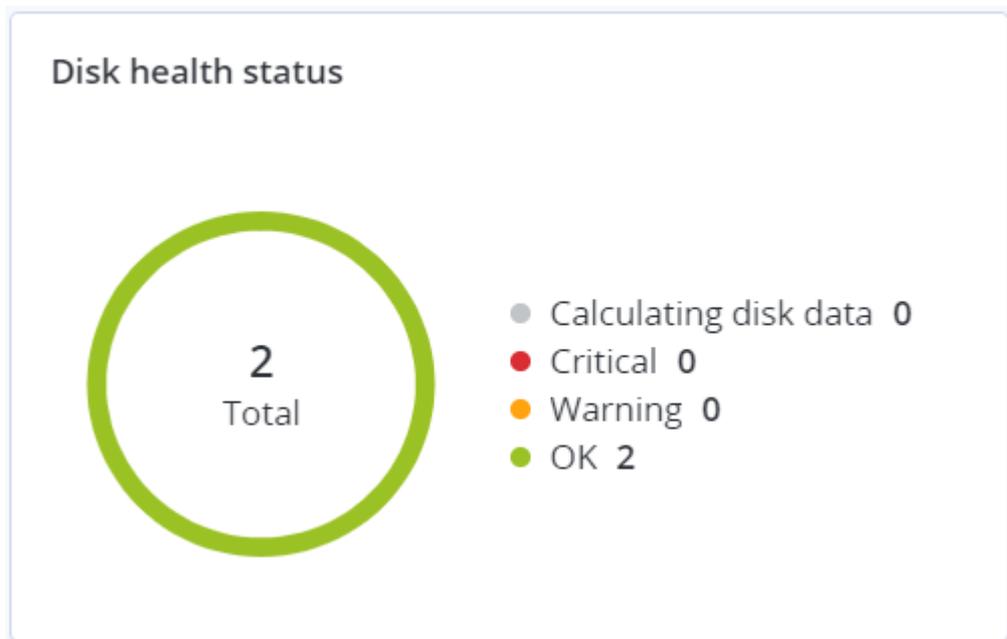


- Tingkat disk
 - Menunjukkan status disk terkini dari semua disk untuk mesin yang dipilih. Setiap blok disk menunjukkan salah satu prakiraan kesehatan disk berikut dan persentase peluangnya.
 - Akan didegradasi
 - Akan tetap stabil

- 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 <nama disk> pada mesin ini berada dalam kondisi kritis, dan kemungkinan besar akan segera gagal. Kami tidak menyarankan pencadangan image disk ini pada saat ini, karena tekanan tambahan dapat menyebabkan kegagalan disk. Segera cadangkan semua file terpenting pada disk ini lalu ganti disk.

Peta perlindungan data

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

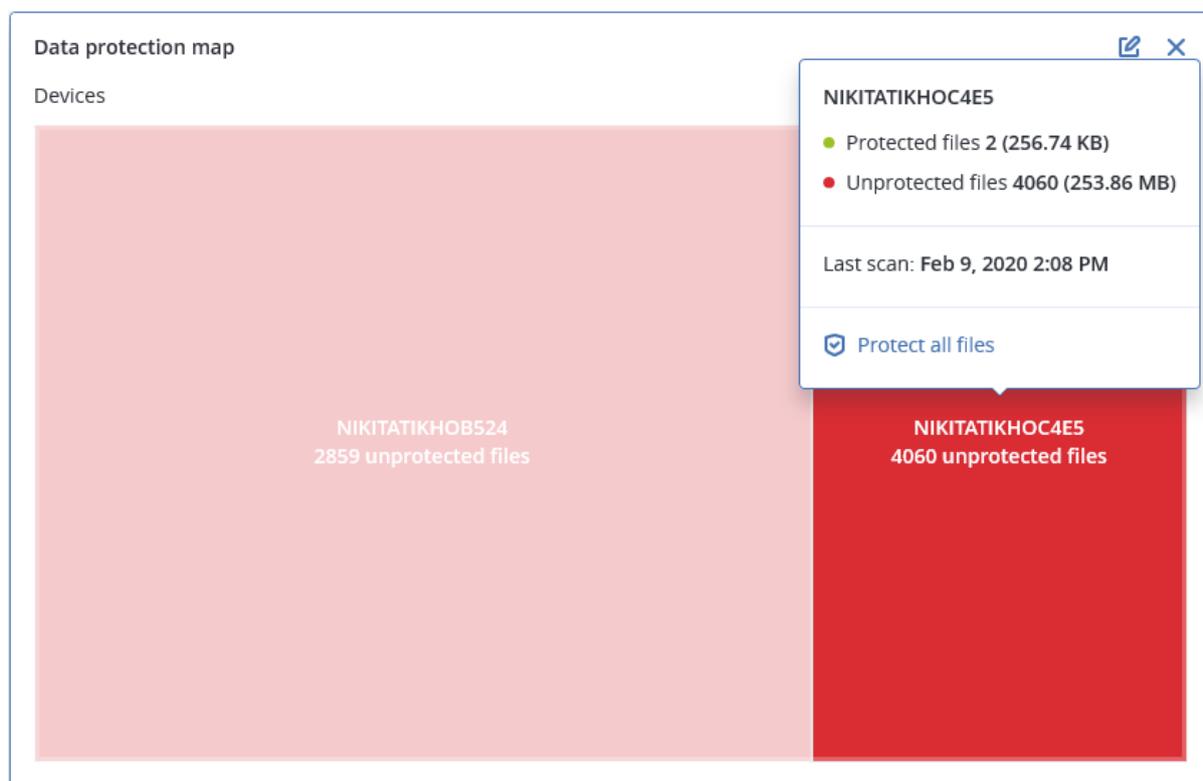
Setiap ukuran blok bergantung pada jumlah/ukuran total semua file penting yang dimiliki pelanggan/mesin.

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

Hasil pemeriksaan perlindungan data dapat ditemukan di dasbor widget Peta Perlindungan Data, suatu widget peta pohon yang menunjukkan detail pada tingkat mesin:

- 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-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
More							

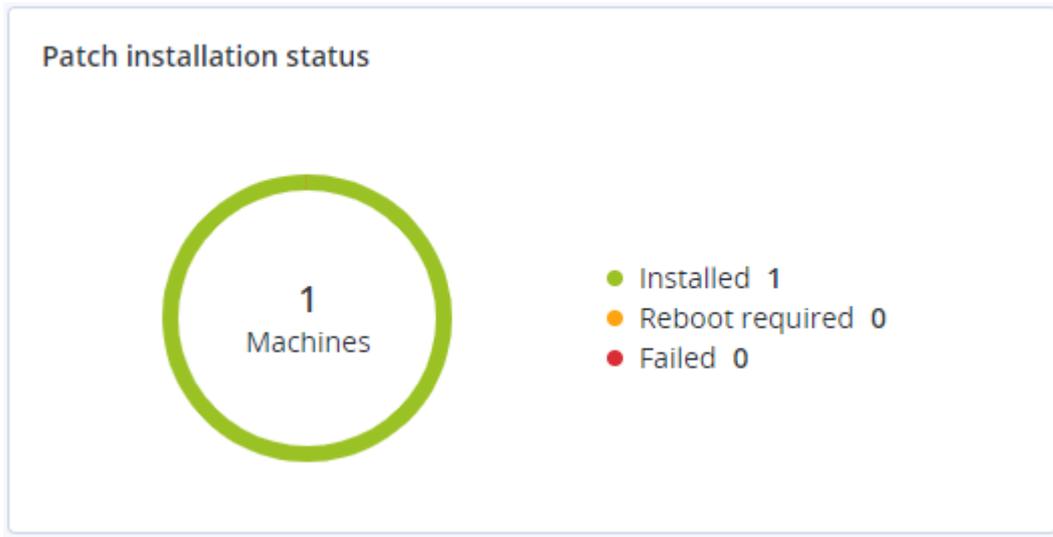
Widget instalasi patch

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

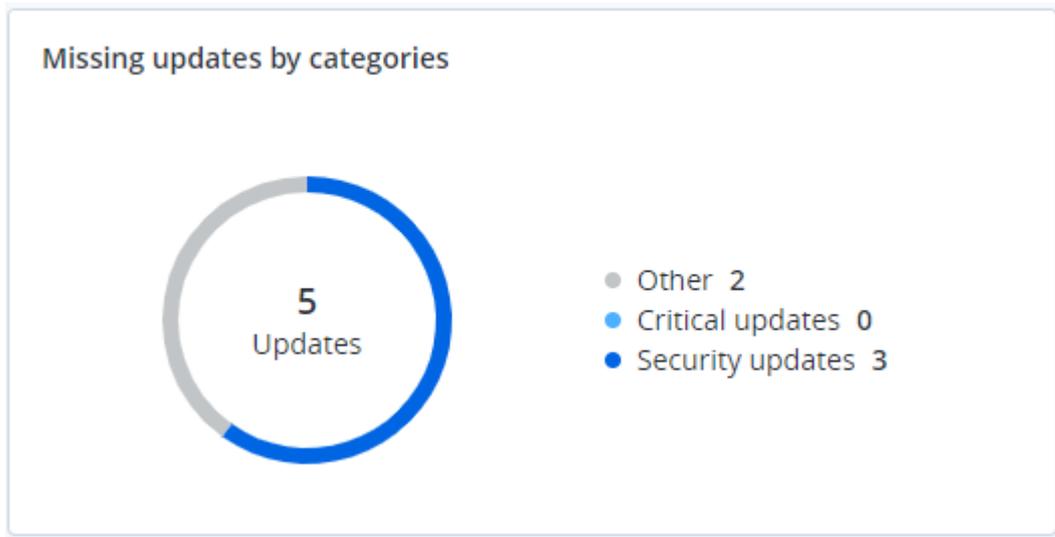
Widget ini menampilkan informasi terperinci tentang patch pada mesin.

Patch installation history						
Machine name	Update name	Version	Severity	Approval status	Installation status	Installation date ↓
NIKITATIKHOC4E5	FastStone Soft FastStone I...	5.9	Medium	New	● Installed	02/05/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	● Failed	02/04/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	● Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	● Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	● Installed	02/04/2020
NIKITATIKHOC4E5	Oracle Java Runtime Envir...	8.0.2410.7	High	New	● Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	● Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	● Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	● Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	● Failed	02/04/2020

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.

Backup scanning details (threats)							
Device name	Plan name	Backup Date and time	Contents type	Location	Threat name	Affected files	Date and time
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	██████████	Gen.Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	██████████	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	██████████	Gen.Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	██████████	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	██████████	Gen.Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	██████████	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	██████████	Gen.Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	██████████	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	██████████	Gen.Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:33 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	██████████	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:33 PM

Baru-baru ini terdampak

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

Recently affected					
Machine name	Protection plan	Threat	Affected files	Detection time	
Ubuntu_14.04_x64-1	Total protection	Adware.DealPlyIgen2	15	27.12.2017 11:23 AM	Folder
Ubuntu_14.04_x64-1	Protection plan	Bloodhound.MalMacroIg1	274	27.12.2017 11:23 AM	Customer
dc_w2k12_r2	Protection plan	Backdoor:Win32/Caphaw...	13	27.12.2017 11:23 AM	✓ Machine name
Win2012_r2-Hyper-V	Protection plan	W97M.DownloaderIg32	5	27.12.2017 11:23 AM	✓ Protection plan
HyperV_for12A	Total protection	Miner.XMRigIgen1	68	27.12.2017 11:23 AM	Detected by
vm-sql_2012	Total protection	Backdoor:Win32/Caphaw...	61	27.12.2017 11:23 AM	✓ Threat
vm-sql_2012	Protection plan	Adware.DealPlyIgen2	9	27.12.2017 11:23 AM	File name
MF_2012_R2	Total protection	MSH.DownloaderIgen8	73	27.12.2017 11:23 AM	File path
MF_2012_R2	Total protection	Bloodhound.MalMacroIg1	182	27.12.2017 11:23 AM	✓ Affected files
MF_2012_R2	Protection plan	Bloodhound.MalMacroIg1	18	27.12.2017 11:23 AM	✓ Detection time
ESXirestore	Protection plan	MSH.DownloaderIgen8	682	27.12.2017 11:23 AM	
MF_2012_R2	Protection plan	Miner.XMRigIgen1	13	27.12.2017 11:23 AM	
Ubuntu_14.04_x64-1	Total protection	Adware.DealPlyIgen2	3	27.12.2017 11:23 AM	
Win2012_r2-Hyper-V	Total protection	W97M.DownloaderIg32	27	27.12.2017 11:23 AM	

[More](#) | [Show all 556](#)

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.

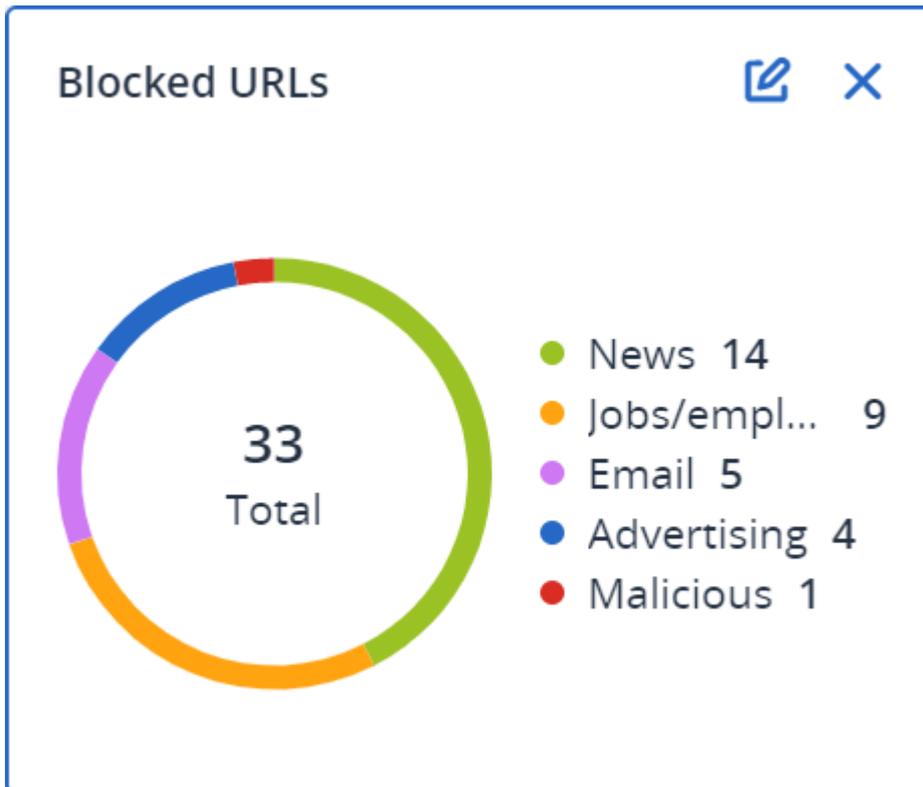
Cara mengunduh data untuk beban kerja yang terpengaruh baru-baru ini

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

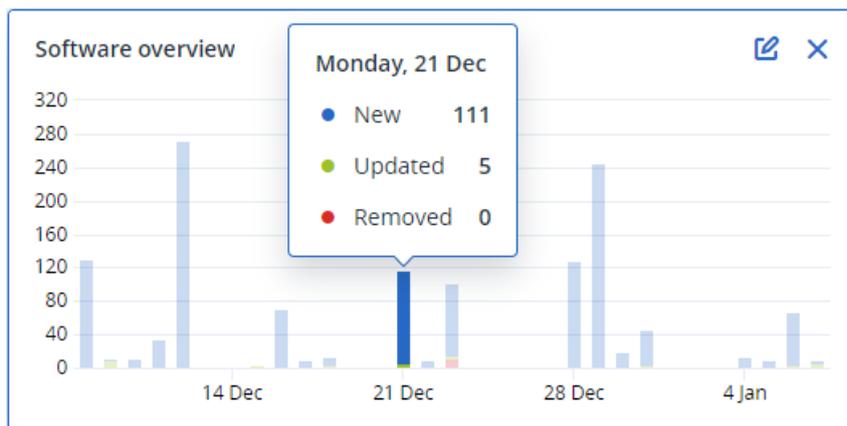
Widget tabel **Inventaris perangkat lunak** menampilkan informasi terperinci tentang semua perangkat lunak yang diinstal pada perangkat Windows dan macOS di organisasi Anda.

Software inventory

Machine name	Software name	Software version	Vendor name	Status	Date installed	Last run	Scan time	Location	User
~ 00003079									
00003079	Microsoft Policy Platform	68.1.1010.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft PowerPoint MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
00003079	Microsoft PowerPoint MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Publisher MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
00003079	Microsoft Publisher MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Silverlight	5.1.50918.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	c:\Program Files\Microsof...	System
00003079	Microsoft Skype for Busin...	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Skype for Busin...	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
00003079	Microsoft VC++ redistribu...	12.0.0.0	Intel Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Visual C++ 200...	8.0.61000	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Visual C++ 200...	9.0.30729	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Visual C++ 2010	10.0.40219	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Visual C++ 201...	11.0.61030.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System

More Less Show 248

Widget tabel **Perubahan 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, Anda akan dialihkan ke halaman **Manajemen Perangkat Lunak** -> **Inventaris Perangkat Lunak**. 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 Anda.

Hardware inventory												
Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner	Registered organiz...	Scan date and time
Ivelins-Mac-mini...	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-	-	12/14/2020 10:23 ...
00003079.corp...	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	NICET81W(1.49)	corp.acronis.com	User	Acronis Inc.	12/13/2020 8:18 PM

Hardware details						
Machine name	Hardware category	Hardware name	Hardware details	Manufacturer	Status	Scan date
Ivelins-Mac-mini-2.local	CPU	To Be Filled By O.E.M.	Core i5, 3000, 6	Intel(R) Core(TM) i5-8500B CPU @ 3.00GHz	OK	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	RAM	4ATF51264HZ-2G6E3	9876543210, 4294...	1FACDD62	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	RAM	4ATF51264HZ-2G6E3	9876543210, 4294...	1FB057DA	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Ethernet	Ethernet, 00:00:00...	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Wi-Fi	IEEE80211, 00:00:00...	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Bluetooth PAN	Ethernet, 00:00:00...	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 1	Ethernet, 00:00:00...	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 2	Ethernet, 00:00:00...	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 3	Ethernet, 00:00:00...	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 4	Ethernet, 00:00:00...	-	-	12/14/2020, 10:23 AM

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 Anda untuk jangka waktu tertentu (7 hari, 30 hari, atau bulan saat ini).

Hardware changes						
Machine name	Hardware category	Status	Old value	New value	Modification date and time	
DESKTOP-0FF9TTF						
DESKTOP-0FF9TTF	Network adapter	Changed	Oracle Corporation, Ethernet 802.3, ...	Oracle Corporation, Ethernet 802.3, ...	01/11/2021 9:28 AM	
DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor Corp., Ether...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Toronto 5C1, PF0PJB10	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), WDC WD10JP...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 802.3, 00:0...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ethernet 802.3, ...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00 GB	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows Provider V9...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM	

[More](#)

Riwayat sesi

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

Remote sessions							
Start time	End time	Duration	Connection type	Protocol	Connection sou...	Accessed by	Connection des...
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. 1.1.4
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...
12/15/2022 4:...	12/15/2022 4:4...	2 minutes	Cloud	NEAR	RU-PC0YHMZL	sk-part	ACPM-Sveta
12/15/2022 4:...	12/15/2022 4:1...	16 minutes	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 4:0...	a minute	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 3:5...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. 1.1.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. 1.4
12/15/2022 1:...	12/15/2022 12:...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 1:...	12/15/2022 12:...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...

[More](#)

Log audit

Untuk melihat log audit, buka **Pemantauan > 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 Cyber Protect
- Operasi Cyber Scripting yang dilakukan oleh pengguna di konsol Cyber Protect
- Pesan sistem tentang kuota yang telah tercapai dan penggunaan kuota

Log menampilkan event pada organisasi atau unit yang Anda operasikan dan unit 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 telah 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 unit milik objek. Misalnya, penyewa event **Pengguna diperbarui** adalah unit di mana pengguna berada. Penyewa event **Kuota telah tercapai** adalah pengguna yang kuotanya telah tercapai.

- **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 unit 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.

Pelaporan

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

Catatan

Fungsi ini tidak tersedia di edisi Standard pada layanan Cyber Protection.

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.
- **Ringkasan untuk periode**
Laporan mencakup metrik 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 unit turunan langsung perusahaan atau unit tempat Anda beroperasi.
- **Semua pelanggan dan mitra**
Laporan akan mencakup metrik penggunaan layanan untuk semua unit turunan perusahaan atau unit tempat Anda beroperasi.
- **Semua pelanggan dan mitra (termasuk rincian pengguna)**
Laporan akan mencakup metrik penggunaan layanan untuk semua unit turunan perusahaan atau unit tempat Anda beroperasi, dan untuk semua pengguna di dalam unit.

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 perusahaan Anda atau unit 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 perusahaan atau unit 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

Laporan kustom 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 unit](#) yang untuknya Anda ingin membuat laporan.
3. Klik **Laporan > Penggunaan**.
4. Klik **Kustom**.
5. Dalam **Tipe**, pilih tipe laporan.
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. Dalam **Tingkat detail**, pilih cakupan laporan.
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**.

Data dalam Laporan penggunaan

Laporan tentang penggunaan layanan Cyber Protection mencakup data berikut tentang perusahaan atau unit:

- Ukuran cadangan berdasarkan unit, pengguna, dan jenis perangkat.
- Jumlah perangkat yang terlindungi berdasarkan unit, pengguna, jenis perangkat.
- Nilai harga berdasarkan unit, pengguna, jenis perangkat.
- Ukuran total cadangan.
- Jumlah total perangkat yang dilindungi.
- Total nilai harga.

Catatan

Jika layanan Cyber Protection tidak dapat mendeteksi jenis perangkat, perangkat tersebut muncul sebagai **tidak bertipe** di dalam laporan.

Laporan operasi

Laporan **Operasi** hanya tersedia untuk administrator perusahaan ketika beroperasi di tingkat perusahaan.

Laporan tentang operasi dapat menyertakan set [widget dasbor Operasi](#). Semua widget menunjukkan informasi ringkasan untuk seluruh perusahaan.

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. 78).

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 atau mengirimnya melalui email dalam format XLSX (Excel) atau PDF.

Laporan default tercantum di bawah ini:

Nama laporan	Deskripsi
Skor #CyberFit berdasarkan mesin	Menampilkan Skor #CyberFit, berdasarkan evaluasi metrik keamanan 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 Anda.
Inventaris Perangkat Keras	Menampilkan informasi terperinci tentang semua perangkat lunak yang tersedia pada mesin Windows dan macOS fisik dan virtual di organisasi Anda.
Sesi jarak jauh	Menampilkan detail informasi tentang sesi desktop jarak jauh dan transfer file yang dilakukan di organisasi Anda selama periode waktu tertentu.

Tindakan dengan laporan

Untuk menampilkan laporan, klik namanya.

Untuk menambahkan laporan baru

1. Di konsol Cyber Protect, buka **Laporan**.
2. Pada daftar laporan yang tersedia, klik **Tambah laporan**.
3. [Untuk menambahkan laporan yang telah ditetapkan] Klik nama laporan yang telah ditetapkan.
4. [Untuk menambahkan laporan kustom] Klik **Kustom**, lalu tambahkan widget ke laporan.
5. [Opsional] Seret dan lepas widget untuk menyusunnya kembali.

Untuk mengedit laporan

1. Di konsol Cyber Protect, buka **Laporan**.
2. Di daftar laporan, pilih laporan yang ingin Anda edit.
Anda dapat melakukan hal berikut:
 - Mengganti nama laporan.
 - Mengubah rentang waktu untuk semua widget dalam laporan.
 - Menentukan penerima laporan dan kapan laporan akan dikirim ke mereka. Format yang tersedia adalah PDF dan XLSX.

Untuk menghapus laporan

1. Di konsol Cyber Protect, buka **Laporan**.
2. Di daftar laporan, pilih laporan yang ingin Anda hapus.
3. Klik ikon elipsis (...), lalu klik **Hapus**.
4. Konfirmasikan pilihan Anda dengan mengeklik **Hapus**.

Untuk menjadwalkan laporan

1. Di konsol Cyber Protect, buka **Laporan**.
2. Di daftar laporan, pilih laporan yang ingin Anda jadwalkan, lalu klik **Pengaturan**.
3. Aktifkan switch **Terjadwal**.
 - Tentukan alamat email penerima.
 - Pilih format laporan.

Catatan

Anda dapat mengekspor hingga 1000 item dalam file PDF dan hingga 10.000 item dalam file XLSX. Tanda waktu di file PDF dan XLSX menggunakan waktu lokal mesin Anda.

- Pilih bahasa laporan.
 - Konfigurasi jadwal.
4. Klik **Simpan**.

Untuk mengunduh laporan

1. Di konsol Cyber Protect, buka **Laporan**.
2. Di daftar laporan, pilih laporan, lalu klik **Unduh**.

3. Pilih format laporan.

Untuk mengirim laporan

1. Di konsol Cyber Protect, buka **Laporan**.
2. Di daftar laporan, pilih laporan, lalu klik **Kirim**.
3. Tentukan alamat email penerima.
4. Pilih format laporan.
5. Klik **Kirim**.

Untuk mengekspor struktur laporan

1. Di konsol Cyber Protect, buka **Laporan**.
2. Di daftar laporan, pilih laporan.
3. Klik ikon elipsis (...), lalu klik **Ekspor**.

Hasilnya, struktur laporan disimpan di mesin Anda sebagai file JSON.

Untuk membuang data laporan

Dengan menggunakan opsi ini, Anda dapat mengekspor semua data selama periode kustom, tanpa filter, ke file CSV dan mengirim file CSV ke penerima email.

Catatan

Anda dapat mengekspor hingga 150.000 item dalam file CSV. Tanda waktu di file CSV menggunakan Waktu Universal Terkoordinasi (UTC).

1. Di konsol Cyber Protect, buka **Laporan**.
2. Di daftar laporan, pilih laporan yang datanya ingin Anda buang.
3. Klik ikon elipsis (...), lalu klik **Buang data**.
4. Tentukan alamat email penerima.
5. Di **Rentang waktu**, tentukan periode kustom kapan Anda ingin membuang data.

Catatan

Menyiapkan file CSV untuk periode lebih lama memakan waktu lebih lama.

6. Klik **Kirim**.

Ringkasan eksekutif

Rangkuman laporan Eksekutif memberikan ikhtisar tentang status proteksi lingkungan organisasi Anda dan perangkat yang terproteksi selama rentang waktu tertentu.

Rangkuman laporan Eksekutif mencakup bagian yang dapat disesuaikan dengan widget dinamis yang menunjukkan metrik kinerja utama yang terkait dengan penggunaan layanan awan berikut:

Cadangan, Proteksi antimalware, Penilaian kerentanan, Manajemen patch, Notaris, Pemulihan Bencana, dan Files Sync & Share.

Anda dapat menyesuaikan laporan dalam beberapa cara.

- 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 Anda, agar mereka dapat melihat dengan mudah nilai bisnis dan teknis dari layanan yang diberikan.

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	<p>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 dalam diagram (dalam urutan alfabetis dari A sampai Z):</p> <ul style="list-style-type: none">• 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

Widget	Deskripsi
	<p>Untuk beberapa tipe beban kerja, digunakan grup beban kerja berikut:</p> <ul style="list-style-type: none"> • Microsoft 365: Pengguna, Grup, Folder Umum, Tim, dan Koleksi Situs • Google Workspace: Pengguna dan Drive Bersama • Exchange yang Dihosting: Pengguna <p>Jika dalam satu grup beban kerja terdapat lebih dari 10.000 beban kerja, widget tidak menampilkan data apa pun untuk beban kerja terkait.</p> <p>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.</p>
<p>Ringkasan perlindungan cyber</p>	<p>Widget menunjukkan metrik utama Kinerja perlindungan cyber selama rentang waktu tertentu.</p> <p>Data dicadangkan - ukuran total arsip yang dibuat di penyimpanan awan dan lokal.</p> <p>Ancaman yang dimitigasi - jumlah total malware yang diblokir di semua perangkat.</p> <p>URL berbahaya yang diblokir - jumlah total URL yang diblokir pada semua perangkat.</p> <p>Kerentanan yang di-patch - jumlah total kerentanan yang diperbaiki melalui pemasangan patch perangkat lunak di semua perangkat.</p> <p>Patch yang diinstal - jumlah total patch yang diinstal pada semua perangkat.</p> <p>Server yang dilindungi oleh DR - jumlah total server yang dilindungi oleh Pemulihan Bencana.</p> <p>Pengguna File Sync & Share - jumlah total pengguna akhir dan pengguna tamu yang menggunakan Cyber Files.</p> <p>File yang sudah dinotarisasikan - jumlah total file yang dinotarisasikan.</p> <p>Dokumen yang dibubuhi eSign - jumlah total dokumen yang dibubuhi eSign.</p> <p>Perangkat periferal yang diblokir - jumlah total perangkat periferal yang diblokir.</p>
<p>Status jaringan beban kerja</p>	<p>Widget ini menampilkan jumlah beban kerja yang terisolasi dan jumlah beban kerja yang terhubung (status normal beban kerja).</p> <p>Pilih pelanggan yang relevan; Tampilan beban kerja yang ditampilkan disaring untuk menampilkan beban kerja terisolasi. Klik nilai Terhubung</p>

Widget	Deskripsi
	untuk menampilkan Beban Kerja dengan daftar agen yang disaring untuk menampilkan beban kerja terhubung (untuk pelanggan terpilih).
Status proteksi beban kerja	<p>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:</p> <p>Server - server fisik, dan server Pengontrol Domain.</p> <p>Stasiun kerja - stasiun kerja fisik.</p> <p>Mesin virtual - mesin virtual berbasis agen dan tanpa agen.</p> <p>Server hosting web - server virtual atau fisik dengan cPanel atau Plesk yang terinstal.</p> <p>Perangkat seluler - perangkat seluler fisik.</p> <p>Satu beban kerja dapat termasuk dalam lebih dari satu kategori. Misalnya, suatu server hosting web termasuk dalam dua kategori - Server, dan Server hosting web.</p>

Widget proteksi antimalware

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

Widget	Deskripsi
Pemindaian antimalware pada file	<p>Widget menampilkan hasil pemindaian antimalware sesuai permintaan pada perangkat selama rentang waktu tertentu.</p> <p>File - jumlah total file yang dipindai</p> <p>Bersih - jumlah total file bersih</p> <p>Terdeteksi, dikarantina - jumlah total file terinfeksi yang dikarantina</p> <p>Terdeteksi, tidak dikarantina - jumlah total file terinfeksi yang tidak dikarantina</p> <p>Perangkat terlindungi - Jumlah total perangkat dengan kebijakan proteksi antimalware yang diterapkan</p> <p>Jumlah total perangkat terdaftar - Jumlah total perangkat terdaftar pada waktu pembuatan laporan</p>
Pemindaian antimalware pada cadangan	<p>Widget menunjukkan hasil pemindaian antimalware pada cadangan untuk rentang tanggal tertentu, menggunakan metrik berikut:</p> <ul style="list-style-type: none"> Jumlah total titik pemulihan yang dipindai Jumlah titik pemulihan bersih

Widget	Deskripsi
	<ul style="list-style-type: none"> • Jumlah titik pemulihan bersih dengan partisi yang tidak didukung • Jumlah titik pemulihan yang terinfeksi. Metrik ini mencakup jumlah titik pemulihan yang terinfeksi dengan partisi yang tidak didukung.
URL yang diblokir	<p>Selama rentang waktu tertentu, widget menampilkan jumlah URL yang diblokir yang dikelompokkan berdasarkan kategori situs web.</p> <p>Widget tersebut mencantumkan tujuh kategori situs web yang memiliki jumlah URL diblokir terbesar, dan menggabungkan kategori situs web lain dalam Lainnya.</p> <p>Untuk informasi lebih lanjut tentang kategori situs web, lihat topik filter URL dalam Cyber Protection.</p>
Burndown insiden keamanan	<p>Widget ini menampilkan rentang efisiensi dalam menutup insiden untuk perusahaan terpilih; jumlah insiden terbuka yang dibandingkan dengan jumlah insiden tertutup selama periode waktu tertentu.</p> <p>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.</p>
MTRR Insiden	<p>Widget ini menampilkan waktu resolusi rata-rata untuk insiden keamanan. Ini menandakan seberapa cepat insiden teridentifikasi dan terpecahkan.</p> <p>Klik pada kolom untuk menampilkan rincian insiden berdasarkan keparahannya (Kritis, Tinggi, dan Sedang), 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.</p>
Status ancaman	<p>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).</p>
Ancaman terdeteksi oleh teknologi proteksi	<p>Selama rentang waktu tertentu, widget menampilkan jumlah ancaman terdeteksi yang dikelompokkan berdasarkan teknologi proteksi berikut:</p> <ul style="list-style-type: none"> • Pemindaian antimalware • Mesin perilaku • Perlindungan cryptomining • Pencegahan exploit • 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	<p>Widget menampilkan jumlah total beban kerja terdaftar berdasarkan status cadangan.</p> <p>Dicadangkan - jumlah beban kerja yang dicadangkan (sekurangnya ada satu pencadangan yang berhasil dilakukan) selama rentang tanggal laporan.</p> <p>Tidak dicadangkan - jumlah beban kerja yang tidak dicadangkan (tidak ada pencadangan yang berhasil dilakukan) selama rentang tanggal laporan.</p>
Status kesehatan disk berdasarkan perangkat fisik	<p>Widget menampilkan kumpulan status kesehatan perangkat fisik berdasarkan status kesehatan disk-nya.</p> <p>OK - Status kesehatan disk ini bernilai [70-100]. Status perangkat adalah OK ketika semua disk-nya dalam status OK.</p> <p>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.</p> <p>Kesalahan - Status kesehatan disk ini bernilai [0-30]. Suatu perangkat berstatus Kesalahan ketika status sekurangnya salah satu disknya adalah Kesalahan.</p> <p>Menghitung data disk - Status perangkat adalah Menghitung data disk jika status disk tersebut belum dihitung.</p>
Penggunaan penyimpanan cadangan	<p>Selama rentang waktu tertentu, widget menampilkan jumlah total dan ukuran total cadangan di penyimpanan awan dan lokal.</p>

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

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

Widget Pemulihan Bencana

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

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

Widget	Deskripsi
	<p>Server terlindungi - jumlah server yang dilindungi oleh Pemulihan Bencana (server yang memiliki sekurangnya satu server pemulihan) pada saat pembuatan laporan.</p> <p>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.</p> <p>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.</p> <p>Widget juga menunjukkan ukuran penyimpanan Pemulihan Bencana (dalam GB) pada saat pembuatan laporan. Itu adalah jumlah ukuran cadangan di server awan.</p>
<p>Server yang dilindungi oleh Pemulihan Bencana</p>	<p>Widget menunjukkan informasi tentang server yang dilindungi oleh Pemulihan Bencana dan server yang tidak dilindungi.</p> <p>Widget menunjukkan metrik berikut:</p> <p>Jumlah total server yang terdaftar dalam penyewa pelanggan pada saat pembuatan laporan.</p> <p>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.</p> <p>Tidak terlindungi - jumlah total server yang tidak terlindungi di antara semua server terdaftar pada saat pembuatan laporan.</p>

Widget Pencegahan Kehilangan Data

Topik berikut memberi informasi lebih banyak tentang Perangkat periferai 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	<p>Widget menunjukkan metrik berikut:</p> <p>Total penyimpanan awan yang digunakan - Total penggunaan penyimpanan semua pengguna.</p> <p>Pengguna akhir - jumlah total pengguna akhir.</p> <p>Rata-rata penyimpanan yang digunakan per pengguna akhir - rata-rata penggunaan penyimpanan per pengguna akhir.</p> <p>Pengguna tamu - jumlah total pengguna tamu.</p>
Penggunaan penyimpanan File Sync & Share oleh pengguna akhir	<p>Widget tersebut menunjukkan jumlah total pengguna akhir File Sync & Share yang memiliki penggunaan penyimpanan dalam rentang berikut:</p> <ul style="list-style-type: none"> • 0 - 1 GB • 1 - 5 GB • 5 - 10 GB • 10 - 50 GB • 50 - 100 GB • 100 - 500 GB • 500 - 1 TB • 1+ TB

Widget Notary

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

Widget	Deskripsi
Statistik Notaris	Widget menunjukkan metrik Notaris berikut:

Widget	Deskripsi
cyber	<p>Penyimpanan awan Notaris yang digunakan - ukuran total penyimpanan yang digunakan untuk layanan Notaris.</p> <p>File yang sudah dinotarisasikan - jumlah total file yang dinotarisasikan.</p> <p>Dokumen yang dibubuhi eSign - jumlah total dokumen dan file yang dibubuhi eSign.</p>
File yang sudah dinotarisasikan para pengguna akhir	<p>Menunjukkan jumlah total file yang dinotarisasikan untuk semua pengguna akhir. Pengguna dikelompokkan berdasarkan jumlah file yang dinotarisasikan yang mereka miliki.</p> <ul style="list-style-type: none"> • Hingga 10 file • 11 - 100 file • 101 - 500 file • 501 - 1000 file • 1000+ file
Dokumen yang dibubuhi eSign pada pengguna akhir	<p>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.</p> <ul style="list-style-type: none"> • 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 kontak dan pengguna, pilih **Kirim ke semua kontak dan pengguna**.
 - Jika Anda ingin mengirim laporan ke kontak dan pengguna tertentu
 - a. Hapus **Kirim ke semua kontak dan pengguna**.
 - b. Klik **Pilih kontak**.
 - c. Pilih kontak and pengguna 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. 74).

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)	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> Zona waktu pengiriman laporan adalah UTC. Zona waktu aktivitas yang ditampilkan dalam laporan adalah UTC.
Portal manajemen> Pengguna > Rekap harian tentang peringatan aktif	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Laporan ini dikirim ketika aktivitas selesai. <hr/> <p>Catatan Tergantung pada beban kerja di pusat data, beberapa laporan mungkin dikirim dengan penundaan.</p> <hr/> <ul style="list-style-type: none"> 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

Integrasi

Katalog integrasi

Halaman ini bertindak sebagai tempat global di mana semua aplikasi integrasi terdaftar dan diperbarui.

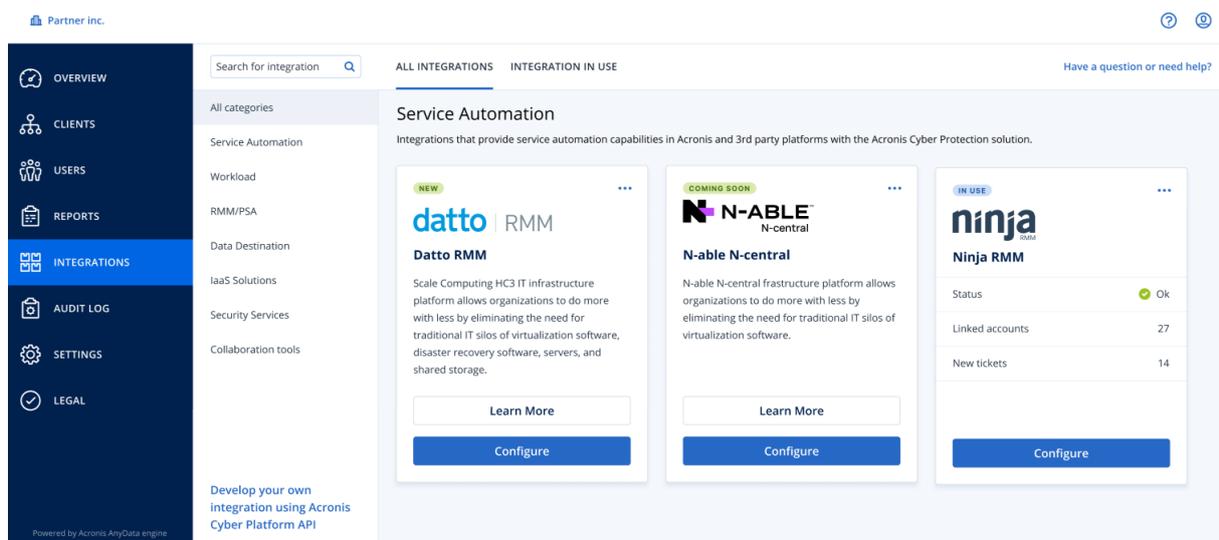
Menambahkan integrasi baru atau memodifikasi integrasi yang ada dapat dilakukan di sini.

Catatan

Hanya pengguna dengan peran **Administrator perusahaan** yang diizinkan untuk mengubah konfigurasi integrasi.

Semua integrasi

Tab **Semua integrasi** menampilkan daftar integrasi yang tersedia saat ini, disusun sebagai petak yang berurutan.



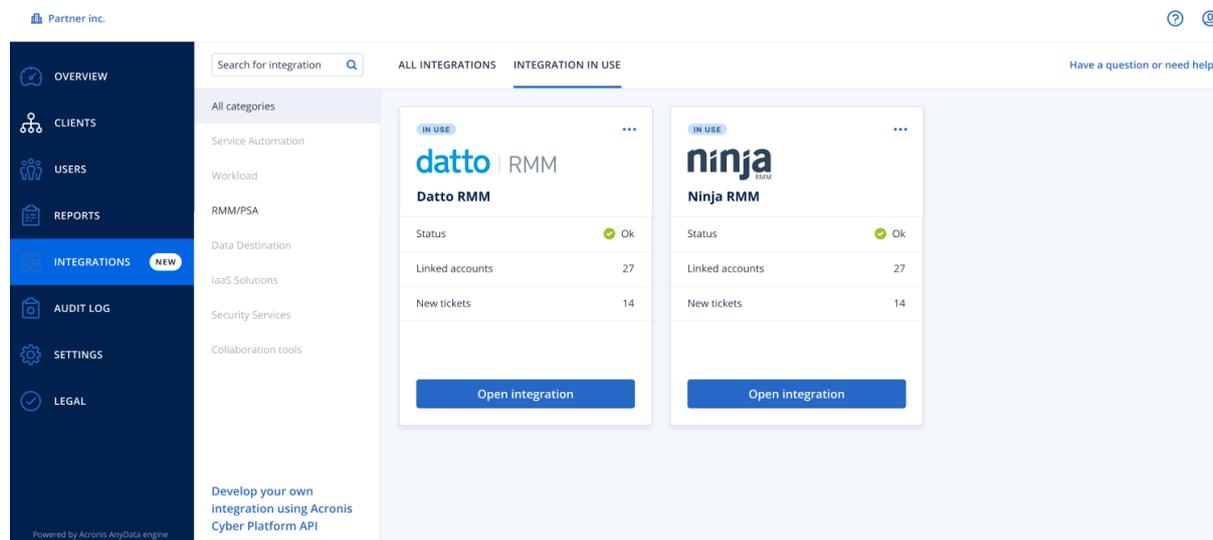
Setiap petak menampilkan deskripsi produk dan dua opsi tambahan:

- **Pelajari selengkapnya**—klik tombol ini untuk melihat detail selengkapnya tentang integrasi tertentu:
 - **Fitur integrasi**
 - **Tautan dokumentasi**
 - **Kontak dukungan**
- **Konfigurasi**—gunakan opsi ini untuk mengedit beberapa pengaturan integrasi.

Petak yang mewakili integrasi tidak aktif akan berwarna abu-abu dan dinonaktifkan, dan mungkin berlabel "**segera hadir**".

Integrasi dalam penggunaan

Tab **Integrasi sedang digunakan** menunjukkan daftar semua integrasi yang sedang digunakan secara aktif, masing-masing disertai beberapa informasi umum.



Klik **Buka integrasi** untuk secara langsung mengakses aplikasi terkait.

Di sebelah kiri, ada daftar kategori integrasi, tempat semua aplikasi yang ada diklasifikasikan ke dalam beberapa grup seperti otomatisasi layanan, beban kerja, RMM/PSA, dll. Mengeklik kategori masing-masing akan menampilkan integrasi yang ada di grup tertentu ini. Kategori yang Anda lihat saat ini akan disorot.

Gunakan opsi **Pencarian** untuk membuat kueri dan mencari integrasi pilihan Anda.

Anda dapat memfilter daftar integrasi berdasarkan kategori dan label. Label diurutkan secara alfabetis. Jika tidak ditemukan hasil, perluas pencarian Anda untuk mencakup lebih banyak kategori.

Untuk menonaktifkan aplikasi, klik ikon elipsis (...) di sudut kanan atas petak, dan pilih **Nonaktifkan**.

Tautan ke [dokumentasi API Acronis](#) juga tersedia, jika Anda tertarik mengembangkan integrasi sendiri.

Membatasi akses ke antarmuka web

Anda dapat membatasi akses ke antarmuka web dengan menentukan daftar alamat IP dari pengguna 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 unit turunan.

Untuk membatasi akses ke antarmuka web

1. Masuk ke portal manajemen.
2. [Navigasikan ke unit](#) yang ingin Anda batasi aksesnya.
3. Klik **Pengaturan > Keamanan**.
4. Pilih kotak centang **Aktifkan kontrol logon**.
5. Pada **Alamat IP yang diizinkan**, tentukan alamat IP yang diizinkan. Anda dapat memasukkan 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**.

Membatasi akses ke perusahaan Anda

Administrator perusahaan dapat membatasi akses ke perusahaan untuk administrator tingkat yang lebih tinggi.

Jika akses ke perusahaan dibatasi, administrator tingkat yang lebih tinggi hanya dapat memodifikasi properti perusahaan. Mereka sama sekali tidak dapat melihat akun pengguna dan unit turunan.

Untuk membatasi akses ke perusahaan

1. Masuk ke portal manajemen.
2. Klik **Pengaturan > Keamanan**.
3. Nonaktifkan opsi **Akses dukungan**.
4. Klik **Simpan**.

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 melewati 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 **Diaktifkan** 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 **Diaktifkan**.
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.

Indeks

A

Akun dan unit 6

Apa itu klien API? 84

B

Baru-baru ini terdampak 53

Bidang log audit 58

Browser web yang didukung 15

Burndown insiden keamanan 43

C

Cara kerjanya 28, 45

D

Dasbor operasi 39

Data dalam Laporan penggunaan 62

Data yang dilaporkan berdasarkan tipe widget 78

Detail pemindaian cadangan 53

Distribusi Insiden Teratas per beban kerja 42

F

Filter dan pencarian 59

I

Integrasi 82

Integrasi dalam penggunaan 83

K

Katalog integrasi 82

Kerentanan yang ada 51

Kuota Backup 8, 14

Kuota Disaster Recovery 11

Kuota File Sync & Share 12, 15

Kuota Notary 13, 15

Kuota Pengiriman Data Fisik 13

Kuota untuk penyimpanan 10, 14

Kuota untuk sumber data awan 8

L

Laporan operasi 62

Laporan penggunaan 60

Lingkup laporan 60

Log audit 57

M

Manajemen kuota 7

Melihat kuota untuk organisasi Anda 8

Membatasi akses ke antarmuka web 83

Membatasi akses ke perusahaan Anda 84

Membuat akun pengguna 19

Membuat klien API 85

Membuat rangkuman laporan Eksekutif 75

Membuat unit 18

Memperbarui agen secara otomatis 34

Mencegah pengguna Microsoft 365 tanpa lisensi untuk masuk 11

Menentukan kuota untuk pengguna Anda 13

Mengakses portal manajemen dan layanan 17

Mengaktifkan akun administrator 17

Mengaktifkan klien API yang dinonaktifkan 86

Mengatur autentikasi dua faktor 28

Mengatur autentikasi dua faktor untuk penyewa Anda 31

Mengatur ulang autentikasi dua faktor jika perangkat faktor kedua hilang 33

Mengatur ulang nilai rahasia klien API 85

Mengelola autentikasi dua faktor untuk pengguna 31

Mengelola klien API 84

Menghapus akun pengguna 26

Menghapus klien API 87

Mengirim rangkuman laporan Eksekutif 77

Mengonfigurasi Laporan penggunaan kustom 61

Mengonfigurasi Laporan penggunaan terjadwal 61

Mengonfigurasi pengaturan rangkuman laporan Eksekutif 74

Mengonfigurasi penyimpanan yang tidak dapat diubah 36

Mengubah pengaturan pemberitahuan untuk pengguna 24

Mengunduh data untuk beban kerja yang terpengaruh baru-baru ini 54

Menonaktifkan dan mengaktifkan akun pengguna 26

Menonaktifkan klien API 86

Mentransfer kepemilikan akun pengguna 27

Menyesuaikan Rangkuman laporan eksekutif 75

Mesin yang ditemukan 41

Mesin yang rentan 50

Metrik dengan penggunaan nol 60

MTTR insiden 43

N

Navigasi di portal manajemen 18

P

Pelaporan 60

Pemantauan 31, 39

Pemantauan kesehatan disk 45

Pembaruan yang tidak ada berdasarkan kategori 52

Pembatasan 45

Pemberitahuan yang diterima oleh peran pengguna 26

Penggunaan 39

Peran pengguna yang tersedia untuk setiap layanan 21

Peringatan status kesehatan disk 49

Perlindungan brute-force 33

Persyaratan kata sandi 17

Peta perlindungan data 49

Petunjuk langkah demi langkah 17

Propagasi pengaturan dua faktor lintas level penyewa 30

Prosedur integrasi yang umum 85

R

Ringkasan eksekutif 65

Ringkasan instalasi patch 52

Riwayat instalasi patch 52

Riwayat sesi 57

S

Semua integrasi 82

Skor #CyberFit berdasarkan mesin 41

Status instalasi patch 51

Status jaringan beban kerja 44

Status proteksi 40

T

Tentang dokumen ini 5

Tentang portal manajemen 6

Tipe laporan 60

U

Untuk beralih antara portal manajemen dan konsol layanan 18

Untuk memantau pembaruan agen 36

Untuk memperbarui agen secara otomatis 34

Untuk mengaktifkan autentikasi dua faktor bagi pengguna 33

Untuk mengaktifkan autentikasi dua faktor bagi penyewa Anda 31

Untuk mengatur ulang autentikasi dua faktor bagi pengguna 32

Untuk mengatur ulang browser tepercaya bagi pengguna 32

Untuk menonaktifkan autentikasi dua faktor bagi pengguna 32

Untuk menonaktifkan autentikasi dua faktor bagi penyewa Anda 31

URL yang diblokir 54

W

Widget Deteksi dan Tanggapan Titik Akhir (EDR) 42

Widget File Sync & Share 73

Widget ikhtisar beban kerja 66

Widget instalasi patch 51

Widget inventaris perangkat keras 56

Widget inventaris perangkat lunak 55

Widget kesehatan disk 46

Widget Notary 73

Widget Pemulihan Bencana 71

Widget pencadangan 70

Widget Pencegahan Kehilangan Data 72

Widget penilaian kerentanan 50

Widget penilaian kerentanan dan manajemen patch 70

Widget proteksi antimalware 68

Widget ringkasan eksekutif 66

Z

Zona waktu dalam laporan 77