Management-Portal

24.03

Anleitung für Firmenadministratoren

REVISION: 11.04.2024

Inhaltsverzeichnis

Über dieses Dokument **5**
Über das Management-Portal **6**
Konten und Abteilungen 6
Quota-Verwaltung 7
Quotas für Ihr Unternehmen einsehen 8
Quotas für Ihre Benutzer definieren 14
Unterstützte Webbrowser 16
Schritt-für-Schritt-Anleitungen **17**
Ein Administratorkonto aktivieren 17
Anforderungen an das Kennwort 17
Auf das Management-Portal und die Services zugreifen 18
Zwischen dem Management-Portal und den Service-Konsolen umschalten 18
Im Management-Portal navigieren 18
Eine Abteilung erstellen 19
Ein Benutzerkonto erstellen 19
Für jeden Service verfügbare Benutzerrollen 21
Nur-Lesen-Administrator-Rolle 24
Rolle 'Restore Operator' 24
Die Benachrichtigungseinstellungen für einen Benutzer ändern 25
Je nach Benutzerrolle empfangene Benachrichtigungen 27
Ein Benutzerkonto deaktivieren und aktivieren 27
Ein Benutzerkonto löschen 27
Die Eigentümerschaft eines Benutzerkontos übertragen 28
Zwei-Faktor-Authentifizierung einrichten 29
Und so funktioniert es 29
Die Zwei-Faktoren-Einrichtung zwischen Mandantenebenen weitergeben 31
Die Zwei-Faktor-Authentifizierung für Ihren Mandanten einrichten 32
Die Zwei-Faktor-Authentifizierung für Benutzer verwalten 33
Die Zwei-Faktor-Authentifizierung bei Verlust des Zweit-Faktor-Gerätes zurücksetzen 35
Schutz vor Brute-Force-Angriffen 35
Agenten automatisch aktualisieren 36
So können Sie Agenten automatisch aktualisieren lassen 37
So können Sie die Agenten-Updates überwachen 38
Unveränderlichen Storage konfigurieren 38
Unterstützte Storages und Agenten 40

Task-Verwaltung **41**
Service Desk-Tickets einsehen 41
Ein Service Desk-Ticket erstellen 42
Service Desk-Tickets aktualisieren 43
Monitoring **45**
Nutzung 45
Aktionen-Dashboard 45
Schutzstatus 46
#CyberFit-Score pro Maschine 48
Endpoint Detection & Response (EDR)-Widgets 48
Überwachung der Laufwerksintegrität 51
Data Protection-Karte 56
Widget für Schwachstellenbewertung 57
Widgets für Patch-Installation 58
Backup-Scanning-Details 60
Kürzlich betroffen 60
Blockierte URLs 61
Widgets für Software-Inventarisierung 62
Widgets für Hardware-Inventarisierung 63
Sitzungsverlauf 64
Überwachungsprotokoll 64
Felder im Überwachungsprotokoll 65
Filter und Suche 66
Berichte **67**
Nutzungsberichte 67
Berichtstyp 67
Berichtsumfang 67
Metriken mit einer Nutzung von Null 67
Geplante Nutzungsberichte konfigurieren 68
Benutzerdefinierte Nutzungsberichte konfigurieren 68
Daten in Nutzungsberichten 69
Aktionen-Berichte 69
Aktionen mit Berichten 71
Kurzübersicht 73
Kurzübersicht-Widgets 73
Die Einstellungen des Kurzübersichtsberichts konfigurieren 82
Einen Kurzübersichtsbericht erstellen 83

Den Kurzübersichtsbericht anpassen ... 83
Kurzübersichtsberichte senden ... 85
Zeitzonen in Berichten ... 85
Berichtsdaten je nach Widget-Typ ... 86
Integrationen ... **90**
Katalog der Integrationen ... 90
Alle Integrationen ... 90
Verwendete Integrationen ... 91
Zugriff auf die Weboberfläche beschränken ... 91
Den Zugriff auf Ihre Firma beschränken ... 92
API-Clients verwalten ... 92
Was ist ein API-Client? ... 93
Eine typische Integrationsprozedur ... 93
Einen API-Client erstellen ... 93
Den geheimen Wert eines API-Clients zurücksetzen ... 94
Einen API-Client deaktivieren ... 94
Einen deaktivierten API-Client wieder aktivieren ... 95
Einen API-Client löschen ... 95
Index ... **96**

Über dieses Dokument

Dieses Dokument richtet sich an Kunden-Administratoren, die das Cloud-Management-Portal verwenden wollen, um Benutzerkonten, Abteilungen und Quotas zu erstellen und zu verwalten, den Zugriff darauf zu konfigurieren und zu kontrollieren sowie die Nutzung und Operationen in ihrem Cloud-Unternehmen zu überwachen.

Über das Management-Portal

Das Management-Portal ist eine Weboberfläche für die Cloud-Plattform, die Data Protection-Services bereitstellt.

Während jeder Service seine eigene Weboberfläche hat, die Service-Konsole genannt wird, können Administratoren über das Management-Portal die Nutzung der Services kontrollieren, Benutzerkonten und Abteilungen erstellen, Berichte generieren und vieles mehr.

Konten und Abteilungen

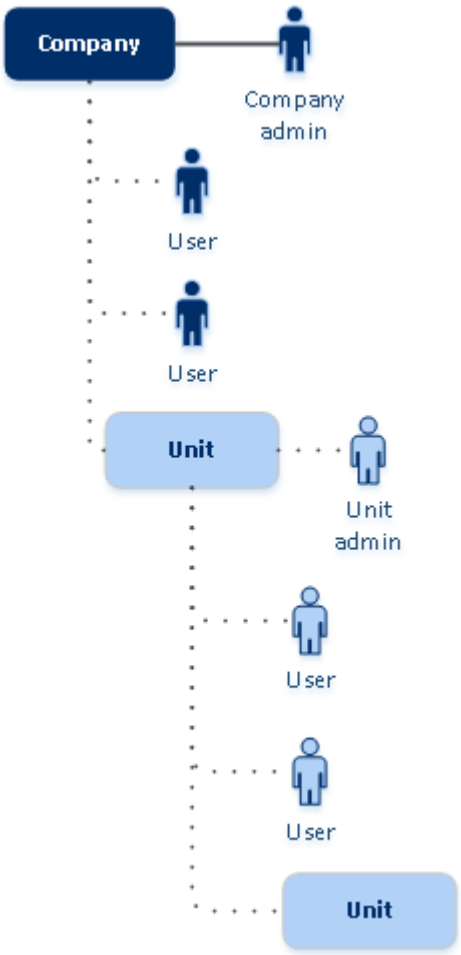
Es gibt zwei Arten von Benutzerkonten: Administrator- und Benutzerkonten.

- **Administratoren** haben Zugriff auf das Management-Portal. Sie verfügen in allen Services über die Administratoren-Rolle.
- **Benutzer** haben keinen Zugriff auf das Management-Portal. Wie sie auf die Services zugreifen können und welche Rollen sie in den Services haben, wird von einem Administrator definiert.

Administratoren können Abteilungen erstellen, die typischerweise mit bestimmten Abteilungen oder Bereichen eines Unternehmens korrespondieren. Jedes Konto existiert entweder auf der Firmenebene oder in einer Abteilung.

Ein Administrator kann Abteilungen, Administrator-Konten und Benutzerkonten innerhalb oder unterhalb seiner jeweiligen Ebene in der Hierarchie verwalten.

Die folgende Abbildung verdeutlicht drei Hierarchie-Ebenen – eine Firma- und zwei Abteilungen. Optionale Abteilungen und Konten sind als gepunktete Linie dargestellt.



Die nachfolgende Tabelle fasst die Aktionen zusammen, die von Administratoren und Benutzern durchgeführt werden können.

Aktion	Benutzer	Administratoren
Abteilungen erstellen	Nein	Ja
Konten erstellen	Nein	Ja
Die Software herunterladen und installieren	Ja	Ja
Services verwenden	Ja	Ja
Berichte über die Service-Nutzung erstellen	Nein	Ja

Quota-Verwaltung

Quotas beschränken die Möglichkeit eines Mandanten, den Service zu verwenden.

Im Management-Portal können Sie die Service-Quotas einsehen, die Ihr Service-Provider Ihrem Unternehmen zugewiesen hat, die Sie aber nicht verwalten können.

Sie können die Service-Quotas für Ihre Benutzer verwalten.

Quotas für Ihr Unternehmen einsehen

Gehen Sie im Management-Portal zu **Überblick** –> **Nutzung**. Sie sehen ein Dashboard, das die zugewiesenen Quotas für Ihr Unternehmen anzeigt. Die Quotas für jeden Service werden auf einer separaten Registerkarte angezeigt.

Backup-Quotas

Sie können die Cloud Storage-Quota, die Quota für lokale Backups und die maximale Anzahl an Maschinen/Geräten/Websites spezifizieren, die ein Benutzer sichern darf. Folgende Quotas sind verfügbar.

Quotas für Geräte

- **Workstations**
- **Server**
- **Virtuelle Maschinen**
- **Mobilgeräte**
- **Webhosting-Server** (Linux-basierte physische oder virtuelle Server, die Plesk, cPanel-, DirectAdmin-, VirtualMin- oder ISPManager-Control-Panels ausführen)
- **Websites**

Ein(e) Maschine/Gerät/Website wird als 'geschützt' betrachtet, wenn auf diese(s) mindestens ein Schutzplan angewendet wurde. Ein Mobilgerät wird nach Durchführung des ersten Backups als 'geschützt' betrachtet.

Wenn die Überschreitungsgrenze für eine bestimmte Anzahl von Geräten erreicht ist, kann der Benutzer keinen weiteren Geräten mehr einen Schutzplan zuweisen.

Quotas für Cloud-Datenquellen

- **Microsoft 365-Arbeitsplätze**

  Diese Quota wird vom Service-Provider auf die komplette Firma angewendet. Firmenadministratoren können die Quota und Nutzungsinformationen im Management-Portal einsehen.

  Die Lizenzierung der Microsoft 365-Arbeitsplätze ist abhängig vom Abrechnungsmodus, der für Cyber Protection ausgewählt wurde.

Wichtig
Der lokale Agent und der Cloud Agent verbrauchen separate Quotas. Wenn Sie dieselben Workloads mit beiden Agenten sichern, werden Ihnen zwei Gebühren berechnet. Beispiel:

- Wenn Sie die Postfächer von 120 Benutzern mit dem lokalen Agenten und die OneDrive-Dateien derselben Benutzer mit dem Cloud Agenten sichern, werden Ihnen 240 Microsoft 365-Arbeitsplätze berechnet.
- Wenn Sie die Postfächer von 120 Benutzern mit dem lokalen Agenten sichern und dieselben Postfächer zudem mit dem Cloud Agenten sichern, werden Ihnen 240 Microsoft 365-Arbeitsplätze berechnet.

Im **pro Workload**-Abrechnungsmodus wird die Quota **Microsoft 365-Arbeitsplätze** für jeden Nutzer einzeln berechnet. Ein eindeutiger Benutzer ist ein Anwender, der mindestens eine der folgenden Eigenschaften aufweist:

- Geschütztes Postfach
- Geschütztes OneDrive
- Zugriff auf mindestens eine geschützte Firmenebenen-Ressource: eine Microsoft 365 SharePoint Online-Website oder Microsoft 365 Teams.
  Wie Sie die Anzahl der Mitglieder einer Microsoft 365 SharePoint- oder Teams-Website überprüfen können, erfahren Sie in diesem Knowledge Base-Artikel.

Hinweis
Gesperrte Microsoft 365-Benutzer, die kein geschütztes persönliches Postfach oder OneDrive haben und nur auf gemeinsame Ressourcen (gemeinsame Postfächer, SharePoint-Websites und Microsoft Teams) zugreifen können, werden nicht berechnet.
Gesperrte Benutzer sind solche, die über keine gültige Anmeldung verfügen und keinen Zugriff auf die Microsoft 365-Services haben. Wie Sie alle nicht lizenzierten Benutzer in einer Microsoft 365-Organisation blockieren können, erfahren Sie unter '"Verhindern, dass sich nicht lizenzierte Microsoft 365-Benutzer anmelden können" (S. 11)'.

Die folgenden Microsoft 365-Arbeitsplätze sind nicht kostenpflichtig und erfordern keine Pro-Arbeitsplatz-Lizenz:

- Freigegebene Postfächer
- Räume und Geräte
- Externe Benutzer mit Zugriff auf gesicherte SharePoint-Websites und/oder Microsoft Teams

Weitere Informationen zu den Lizenzierungsoptionen mit dem 'pro Gigabyte'-Abrechnungsmodus finden Sie im folgenden Dokument: Cyber Protect Cloud: 'pro Gigabyte'-Abrechnungsmodus für Microsoft 365.
Weitere Informationen zu den Lizenzierungsoptionen mit dem 'pro Workload'-Abrechnungsmodus finden Sie im folgenden Dokument: Cyber Protect Cloud: Microsoft 365-Lizenzierung und Preisänderungen.

- **Microsoft 365-Teams**

Diese Quota wird vom Service-Provider auf die komplette Firma angewendet. Diese Quota aktiviert oder deaktiviert die Möglichkeit, Microsoft 365-Teams zu schützen, und legt die maximale Anzahl von Teams fest, die geschützt werden können. Zum Schutz eines Teams ist, unabhängig von der Anzahl seiner Mitglieder oder Kanäle, nur eine Quota erforderlich. Firmenadministratoren können die Quota und Nutzungsinformationen im Management-Portal einsehen.

- **Microsoft 365 SharePoint Online**

  Diese Quota wird vom Service-Provider auf die komplette Firma angewendet. Diese Quota aktiviert oder deaktiviert die Möglichkeit, SharePoint Online-Websites zu schützen, und legt die maximale Anzahl von Website-Sammlungen und Gruppen-Websites fest, die geschützt werden können.

  Firmenadministratoren können die Quota im Management-Portal einsehen. Sie können außerdem die Quota und den Speicherplatz, der von den SharePoint Online-Backups belegt wird, in den Nutzungsberichten einsehen.
- **Google Workspace-Arbeitsplätze**

  Diese Quota wird vom Service-Provider auf die komplette Firma angewendet. Der Firma kann es erlaubt werden, **Gmail**-Postfächer (inkl. Kalender und Kontakte), **Google Drive**-Dateien oder beides zu sichern. Firmenadministratoren können die Quota und Nutzungsinformationen im Management-Portal einsehen.
- **Google Workspace Shared Drive**

  Diese Quota wird vom Service-Provider auf die komplette Firma angewendet. Diese Quota (de)aktiviert die Möglichkeit, Google Workspace Shared Drives zu sichern. Wenn diese Quota aktiviert ist, können beliebig viele Shared Drives gesichert werden. Firmenadministratoren können zwar nicht die Quota im Management-Portal einsehen, aber den Speicherplatz in den Nutzungsberichten einsehen, der von den Shared Drive-Backups belegt wird.

  Backups von Google Workspace Shared Drives sind nur für Kunden verfügbar, die mindestens eine Quota für Google Workspace-Arbeitsplätze zusätzlich haben. Diese Quota wird nur überprüft und nicht in Anspruch genommen.

Ein Microsoft 365-Arbeitsplatz gilt als geschützt, solange mindestens ein Schutzplan auf das Postfach oder OneDrive-Laufwerk des Benutzers oder angewendet wird. Ein Google Workspace-Arbeitsplatz gilt als geschützt, solange mindestens ein Schutzplan auf das Postfach oder das Google Drive-Laufwerk des Benutzers angewendet wird.

Wenn die Überschreitungsgrenze für eine bestimmte Anzahl von Arbeitsplätzen erreicht ist, kann ein Firmenadministrator keinen weiteren Arbeitsplätzen mehr einen Schutzplan zuweisen.

Quotas für Storage

- **Lokales Backup**

  Die Quota '**Lokales Backup**' beschränkt die Gesamtgröße der lokalen Backups, die mithilfe der Cloud-Infrastruktur erstellt werden können. Für diese Quota kann keine Überschreitung festgelegt werden.
- **Cloud-Ressourcen**

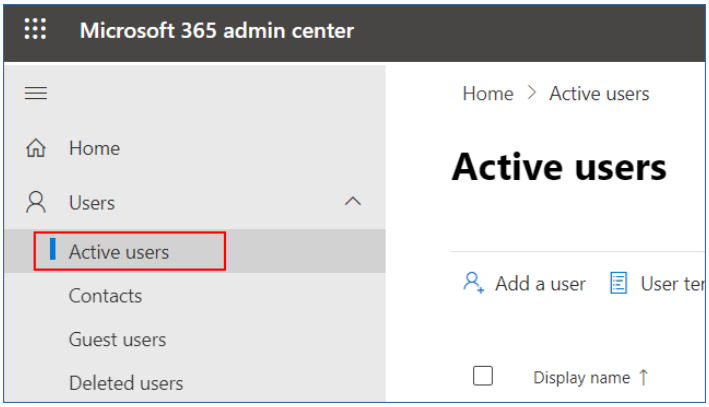
Die Quota **Cloud-Ressourcen** kombiniert die Quota für Backup Storage und die Quotas für Disaster Recovery. Die Backup Storage-Quota begrenzt die Gesamtgröße der Backups, die im Cloud Storage gespeichert sind. Wird die Backup Storage-Quota-Überschreitungsgrenze erreicht, werden weitere Backups fehlschlagen.

Verhindern, dass sich nicht lizenzierte Microsoft 365-Benutzer anmelden können

Sie können alle nicht lizenzierten Benutzer in Ihrer Microsoft 365-Organisation daran hindern, sich anzumelden, indem Sie deren Anmeldestatus bearbeiten.

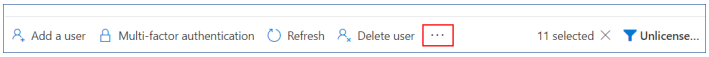
So können Sie verhindern, dass sich nicht lizenzierte Benutzer anmelden

1. Melden Sie sich im Microsoft 365 Admin Center (https://admin.microsoft.com) als globaler Administrator an.
2. Gehen Sie im Navigationsmenü zu **Benutzer** –> **Aktive Benutzer**.



3. Klicken Sie auf **Filter** und wählen Sie **Nicht lizenzierte Benutzer**.

4. vieren Sie die Kontrollkästchen neben den Benutzernamen und klicken Sie anschließend auf das Drei-Punkte-Symbol (...).



5. Wählen Sie aus dem Menü den Befehl **Anmeldestatus bearbeiten** aus.
6. Aktivieren Sie das Kontrollkästchen **Benutzer an der Anmeldung hindern** und klicken Sie anschließend auf **Speichern**.

Disaster Recovery-Quotas

Hinweis
Die Disaster Recovery-Angebotselemente sind nur mit dem Disaster Recovery-Add-on verfügbar.

Diese Quotas werden vom Service-Provider auf die komplette Firma angewendet. Firmenadministratoren können die Quotas und Nutzungsinformationen im Management-Portal einsehen, jedoch keine Quotas für bestimmte Benutzer festlegen.

- **Disaster Recovery Storage**

  Der Disaster Recovery Storage zeigt die Backup Storage-Größe für diejenigen Server an, die per Disaster Recovery geschützt werden. Die Nutzung des Disaster Recovery Storage entspricht der Nutzung des Backup Storage derjenigen Workloads, die über Disaster Recovery-Server geschützt werden. Dieser Storage wird ab dem Zeitpunkt berechnet, an dem ein Recovery-Server erstellt wird – unabhängig davon, ob der Server gerade läuft. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, können keine primären Server und Recovery-Server erstellt oder Laufwerke zu vorhandenen primären Servern hinzugefügt/erweitert werden. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, kann kein Failover initiiert oder ein gestoppter Server gestartet werden. Die Ausführung laufender Server wird aber fortgesetzt.
- **Berechnungspunkte**

  Diese Quota begrenzt die CPU- und RAM-Ressourcen, die die primären Server und Recovery-Server während eines Abrechnungszeitraums verbrauchen dürfen. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, werden alle primären Server und Recovery-Server heruntergefahren. Diese Server können erst wieder verwendet werden, wenn der nächste Abrechnungszeitraum beginnt. Der vorgegebene Abrechnungszeitraum ist ein voller Kalendermonat.

  Wenn die Quota deaktiviert ist, können die Server überhaupt nicht verwendet werden (unabhängig vom Abrechnungszeitraum).
- **Öffentliche IP-Adressen**

  Mit dieser Quota wird die Anzahl der öffentlichen IP-Adressen beschränkt, die primären Servern und Recovery-Servern zugewiesen werden können. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, können keine öffentlichen IP-Adressen mehr für weitere Server aktiviert werden. Sie können einem Server die Verwendung öffentlicher IP-Adressen verbieten, wenn Sie in den Server-Einstellungen das Kontrollkästchen **Öffentliche IP-Adresse** deaktivieren. Anschließend können Sie einem anderen Server die Verwendung einer öffentlichen IP-Adresse (die normalerweise nicht dieselbe ist) erlauben.

  Wenn die Quota deaktiviert wird, hören alle Server auf, öffentliche IP-Adressen zu verwenden, und sind anschließend nicht mehr über das Internet erreichbar.
- **Cloud Server**

  Diese Quota ermöglicht es, die Gesamtzahl der primären Server und Recovery-Server zu beschränken. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, können keine primären Server oder Recovery-Server erstellt werden.

  Wenn die Quota deaktiviert wird, sind die Server zwar noch in der Cyber Protect-Konsole sichtbar, aber die einzige auf sie anwendbare Aktion ist **Löschen**.
- **Internetzugriff**

  Diese Quota (de)aktiviert den Internetzugriff für die primären Server und Recovery-Server.

  Wenn die Quota deaktiviert wird, werden die primären und Recovery-Server keine Verbindungen mit dem Internet herstellen können.

File Sync & Share-Quotas

Diese Quotas werden vom Service-Provider auf die komplette Firma angewendet. Firmenadministratoren können die Quotas und Nutzungsinformationen im Management-Portal einsehen.

- **Benutzer**
  Diese Quota definiert eine Anzahl von Benutzern, die auf diesen Service zugreifen dürfen. Administratorkonten werden nicht als Teil dieser Quota mitgezählt.
- **Cloud Storage**
  Dies ist ein Cloud Storage zum Speichern von Benutzerdateien. Die Quota definiert, wie viel Speicherplatz einem Mandanten im Cloud Storage zugewiesen ist.

Physischer Datenversand-Quotas

Die Quotas für den Service 'Physische Datenversand' (Physical Data Shipping) werden auf einer Pro-Laufwerk-Basis verbraucht. Sie können auf einem entsprechenden Laufwerk die anfänglichen Backups mehrerer Maschinen speichern.

Diese Quotas werden vom Service-Provider auf die komplette Firma angewendet. Firmenadministratoren können die Quotas und Nutzungsinformationen im Management-Portal einsehen, jedoch keine Quotas für bestimmte Benutzer festlegen.

- **In die Cloud**
  Ermöglicht es, ein anfängliches Backup per Festplattenlaufwerk an das Cloud Datacenter Ihrer Wahl zu senden. Diese Quota definiert die maximale Anzahl von Laufwerken, die zum Cloud Datacenter gesendet werden können.

Notary-Quotas

Diese Quotas werden vom Service-Provider auf die komplette Firma angewendet. Firmenadministratoren können die Quotas und Nutzungsinformationen im Management-Portal einsehen.

- **Notary Storage**
  Definiert den maximalen Speicherplatz im Cloud Storage für beglaubigte Dateien, signierte Dateien und Dateien, deren Beglaubigung oder Signierung gerade durchgeführt wird.
  Wenn Sie die Nutzung dieser Quota verringern wollen, können Sie bereits beglaubigte oder signierte Dateien aus dem Notary Storage löschen.
- **Beglaubigungen**
  Definiert die maximale Anzahl von Dateien, die mithilfe des Notary Service beglaubigt werden können.
  Eine Datei gilt als beglaubigt, sobald sie zum Notary Storage hochgeladen wurde und ihr Beglaubigungsstatus auf **Wird bearbeitet** geändert wurde.
  Wenn dieselbe Datei mehrfach beglaubigt wird, gilt jede Beglaubigung wie eine neue gezählt.

- **eSignaturen**
  Definiert die maximale Anzahl von digitalen eSignaturen.

Quotas für Ihre Benutzer definieren

Mit **Quotas** können Sie einschränken, ob und wie ein Benutzer den Service verwenden kann. Um Quotas für einen Benutzer festlegen zu können, müssen Sie in der Registerkarte **Benutzer** (unter under **Unternehmensverwaltung**) den gewünschten Anwender auswählen und anschließend im Bereich **Quotas** auf das Stiftsymbol klicken.

Wenn eine Quota überschritten wird, wird an den Benutzer (bzw. seine E-Mail-Adresse) eine entsprechende Benachrichtigung gesendet. Wenn Sie keine Quota-Überschreitung festlegen, wird die Quota als '**weich**' angesehen. Das bedeutet, dass keine Beschränkungen für die Nutzung des Cyber Protection Service gelten.

Wenn Sie eine Quota-Überschreitung spezifizieren, wird die Quota als '**hart**' angesehen. Eine **Überschreitung** erlaubt es dem Benutzer, die Quota um den spezifizierten Wert zu überschreiten. Wird die Überschreitung überschritten, werden Nutzungsbeschränkungen auf den Service angewendet.

Beispiel

Weiche Quota: Sie haben die Quota für Workstations auf 20 festgelegt. Wenn die Anzahl der geschützten Workstations des Benutzers den Wert 20 erreicht, erhält der Benutzer zwar eine E-Mail-Benachrichtigung, aber der Cyber Protection Service ist weiterhin verfügbar.

Harte Quota: Wenn Sie die Quota für Workstations auf 20 und die Überschreitung auf 5 festgelegt haben, erhält der Benutzer eine E-Mail-Benachrichtigung, wenn die Anzahl der geschützten Workstations 20 erreicht. Wenn die Anzahl 25 erreicht ist, wird der Cyber Protection Service für den Benutzer deaktiviert.

Backup-Quotas

Sie können die Backup Storage-Quota und die maximale Anzahl an Maschinen/Geräte/Websites spezifizieren, die ein Benutzer schützen darf. Folgende Quotas sind verfügbar.

Quotas für Geräte

- **Workstations**
- **Server**
- **Virtuelle Maschinen**
- **Mobilgeräte**
- **Webhosting-Server** (Linux-basierte physische oder virtuelle Server, die Plesk, cPanel-, DirectAdmin-, VirtualMin- oder ISPManager-Control-Panels ausführen)
- **Websites**

Ein(e) Maschine/Gerät/Website wird als 'geschützt' betrachtet, wenn auf diese(s) mindestens ein Schutzplan angewendet wurde. Ein Mobilgerät wird nach Durchführung des ersten Backups als 'geschützt' betrachtet.

Wenn die Überschreitungsgrenze für eine bestimmte Anzahl von Geräten erreicht ist, kann der Benutzer keinen weiteren Geräten mehr einen Schutzplan zuweisen.

Quota für Storage

- **Backup Storage**

Die Backup Storage-Quota begrenzt die Gesamtgröße der Backups, die im Cloud Storage gespeichert sind. Wird die Backup Storage-Quota-Überschreitungsgrenze erreicht, werden weitere Backups fehlschlagen.

Wichtig
Der lokale Agent und der Cloud Agent verbrauchen separate Quotas. Wenn Sie dieselben Workloads mit beiden Agenten sichern, werden Ihnen zwei Gebühren berechnet. Beispiel:

- Wenn Sie die Postfächer von 120 Benutzern mit dem lokalen Agenten und die OneDrive-Dateien derselben Benutzer mit dem Cloud Agenten sichern, werden Ihnen 240 Microsoft 365-Arbeitsplätze berechnet.
- Wenn Sie die Postfächer von 120 Benutzern mit dem lokalen Agenten sichern und dieselben Postfächer zudem mit dem Cloud Agenten sichern, werden Ihnen 240 Microsoft 365-Arbeitsplätze berechnet.

File Sync & Share-Quotas

Sie können folgende File Sync & Share-Quotas für einen Benutzer definieren:

- **Persönlicher Speicherplatz**
  Definiert, wie viel Speicherplatz im Cloud Storage für die Dateien eines Benutzers zugewiesen wird.

Notary-Quotas

Sie können folgende Notary-Quotas für einen Benutzer definieren:

- **Notary Storage**
  Definiert den maximalen Speicherplatz im Cloud Storage für beglaubigte Dateien, signierte Dateien und Dateien, deren Beglaubigung oder Signierung gerade durchgeführt wird.
  Wenn Sie die Nutzung dieser Quota verringern wollen, können Sie bereits beglaubigte oder signierte Dateien aus dem Notary Storage löschen.
- **Beglaubigungen**
  Definiert die maximale Anzahl von Dateien, die mithilfe des Notary Service beglaubigt werden können.

Eine Datei gilt als beglaubigt, sobald sie zum Notary Storage hochgeladen wurde und ihr Beglaubigungsstatus auf **Wird bearbeitet** geändert wurde.

Wenn dieselbe Datei mehrfach beglaubigt wird, gilt jede Beglaubigung wie eine neue gezählt.

- **eSignaturen**
  Definiert die maximale Anzahl von digitalen eSignaturen.

Unterstützte Webbrowser

Die Weboberfläche unterstützt folgende Webbrowser:

- Google Chrome 29 (oder höher)
- Mozilla Firefox 23 (oder höher)
- Opera 16 (oder höher)
- Microsoft Edge 25 (oder höher)
- Safari 8 (oder höher), unter den Betriebssystemen macOS oder iOS ausgeführt

In anderen Webbrowsern (inkl. Safari-Browser, die unter anderen Betriebssystem laufen) wird möglicherweise die Benutzeroberfläche nicht korrekt angezeigt oder stehen einige Funktionen nicht zur Verfügung.

Schritt-für-Schritt-Anleitungen

Die folgenden Schritte führen Sie durch die grundlegende Nutzung des Management-Portals. Sie erläutern, wie Sie Folgendes tun können:

- Ihr Administratorkonto aktivieren
- Auf das Management-Portal und die Services zugreifen
- Eine Abteilung erstellen
- Ein Benutzerkonto erstellen

Ein Administratorkonto aktivieren

Nachdem Sie sich an einem Service angemeldet haben, erhalten Sie eine E-Mail-Nachricht mit folgenden Informationen:

- **Ihr Anmeldename.** Dies ist der Benutzername, mit dem Sie sich anmelden. Ihr Anmeldename wird auch auf der Kontoaktivierungsseite angezeigt.
- **Konto aktivieren**-Schaltfläche. Klicken Sie auf die Schaltfläche und legen Sie das Kennwort für Ihr Konto fest. Stellen Sie sicher, dass Ihr Kennwort mindestens neun Zeichen lang ist. Weitere Informationen über Kennwörter finden Sie im Abschnitt '"Anforderungen an das Kennwort" (S. 17)'.

Anforderungen an das Kennwort

Das Kennwort für ein Benutzerkonto muss mindestens 9 Zeichen lang sein. Kennwörter werden zudem auf ihre Komplexität geprüft und dabei in eine der folgenden Kategorien eingeteilt:

- Schwach
- Mittel
- Stark

Ein schwaches Kennwort kann nicht gespeichert werden, auch wenn es 9 oder mehr Zeichen enthält. Kennwörter, die den Benutzernamen, den Anmeldenamen, die Benutzer-E-Mail-Adresse oder den Namen des Mandanten, zu dem ein Benutzerkonto gehört, enthalten, gelten immer als schwach. Auch Kennwörter, die besonders gängig sind, werden als schwach eingestuft.

Wenn Sie ein Kennwort stärker machen wollen, fügen Sie ihm mehr Zeichen hinzu. Es ist nicht zwingend notwendig, unterschiedliche Zeichentypen (wie Zahlen, Groß- und Kleinbuchstaben oder Sonderzeichen) zu verwenden. Aber damit können stärkere oder kürzere Kennwörter erzeugt werden.

Auf das Management-Portal und die Services zugreifen

1. Gehen Sie zur Anmeldeseite der Service-Konsole.
2. Geben Sie den Anmeldenamen ein und klicken Sie dann auf **Weiter**.
3. Geben Sie das Kennwort ein und klicken Sie dann auf **Weiter**.
4. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Klicken Sie auf **Management-Portal**, um sich am Management-Portal anzumelden.
   - Klicken Sie auf den Namen eines Services, um sich an diesem Service anzumelden.

Das Zeitlimit für das Management-Portal beträgt 24 Stunden für aktive Sitzungen und 1 Stunde für inaktive Sitzungen.

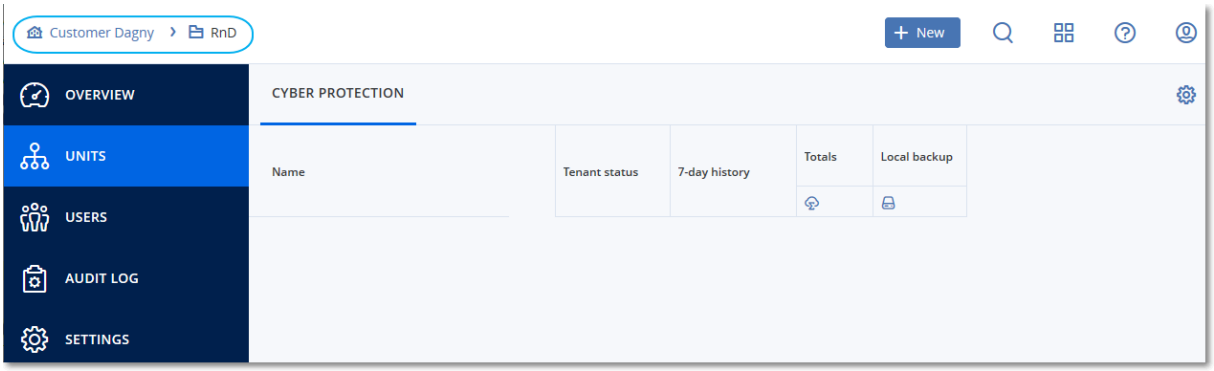
Zwischen dem Management-Portal und den Service-Konsolen umschalten

Wenn Sie zwischen dem Management-Portal und den Service-Konsolen umschalten wollen, klicken Sie auf das -Symbol in der rechten oberen Ecke und wählen Sie dann das **Management-Portal** oder den Service, zu dem Sie wechseln wollen.

Im Management-Portal navigieren

Wenn Sie das Management-Portal verwenden, arbeiten Sie jederzeit innerhalb der Firma oder einer Abteilung. Dies wird auch in der linken oberen Ecke angezeigt.

Standardmäßig ist die oberste Hierarchie-Ebene ausgewählt, die für Sie verfügbar ist. Klicken Sie auf den Abteilungsnamen, um durch die Hierarchie zu blättern. Wenn Sie zu einer höheren Ebene zurück wollen, klicken Sie in der linken oberen Ecke auf den entsprechenden Namen.



Alle Teile der Benutzeroberfläche betreffen und beeinflussen nur die Firma oder eine Abteilung, in welcher Sie gerade arbeiten. Beispiel:

- Mithilfe der Schaltfläche **Neu** können Sie eine Abteilung oder ein Benutzerkonto nur in dieser Firma oder Unit erstellen.

- In der Registerkarte **Abteilungen** werden nur solche Abteilungen angezeigt, die dieser Firma oder Abteilung in der Hierarchie untergeordnet sind.
- In der Registerkarte **Benutzer** werden nur solche Benutzerkonten angezeigt, die in dieser Firma oder Abteilung vorhanden sind.

Eine Abteilung erstellen

Überspringen Sie diesen Schritt, wenn Sie keine Konten innerhalb von Abteilungen organisieren wollen.

Wenn Sie erst später Abteilungen erstellen wollen, sollten Sie beachten, dass existierende Konten weder zwischen Abteilungen noch zwischen der Firma und Abteilungen verschoben werden können. Sie müssen zuerst eine Abteilung erstellen und können diesen erst danach mit Konten „befüllen“.

So erstellen Sie eine Abteilung

1. Melden Sie sich am Management-Portal an.
2. Gehen Sie zu der Abteilung, in der Sie eine neue Abteilung erstellen wollen.
3. Klicken Sie in der rechten oberen Ecke auf **Neu** –> **Abteilung**.
4. Spezifizieren Sie bei **Name** eine Bezeichnung für die neue Abteilung.
5. [Optional] Ändern Sie bei **Sprache** die Standardsprache für die in dieser Abteilung verwendete(n) Benachrichtigungen, Berichte und Software.
6. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie einen Abteilungsadministrator erstellen wollen, klicken Sie zuerst auf **Weiter** und befolgen Sie dann die im Abschnitt 'Ein Benutzerkonto erstellen' beschriebenen Schritte (beginnend mit Schritt 4).
   - Wenn Sie eine Abteilung ohne einen Administrator erstellen wollen, klicken Sie auf **Speichern und schließen**. Sie können der Abteilung auch später noch Administratoren und Benutzer hinzufügen.

Die neu erstellte Abteilung wird in der Registerkarte **Abteilungen** angezeigt.

Wenn Sie die Abteilungseinstellungen bearbeiten oder Kontaktinformationen spezifizieren wollen, müssen Sie die Abteilung zuerst in der Registerkarte **Abteilungen** auswählen und dann auf das Stiftsymbol in dem Bereich klicken, den Sie bearbeiten wollen.

Ein Benutzerkonto erstellen

Überspringen Sie diesen Schritt, falls Sie keine weiteren Benutzerkonten erstellen wollen.

Die Erstellung zusätzlicher Konten kann in folgenden Fällen angebracht sein:

- Firmenadministrator-Konten – um die Verwaltungsaufgaben mit anderen Personen zu teilen.
- Kunden-Administrator-Konten – um die Verwaltung an andere Personen zu delegieren, deren Zugriffsberechtigungen auf die entsprechenden Abteilungen begrenzt werden.

- Benutzerkonten – um es zu ermöglichen, dass Benutzer nur auf eine Teilmenge der Services zugreifen können.

So erstellen Sie ein Benutzerkonto

1. Melden Sie sich am Management-Portal an.
2. Gehen Sie zu der Abteilung, in der Sie ein neues Benutzerkonto erstellen wollen.
3. Klicken Sie in der rechten oberen Ecke auf **Neu** –> **Benutzer**.
4. Spezifizieren Sie die nachfolgenden Informationen für das Konto:
   - **Anmeldename**

     Wichtig
     Jedes Konto benötigt einen eindeutigen Anmeldenamen.

   - **E-Mail**

     Wichtig
     Wenn der Benutzer im File Sync & Share Service registriert ist, geben Sie bitte die E-Mail an, die für die File Sync & Share-Registrierung verwendet wurde.
     Bitte beachten Sie, dass jedes Kunden-Benutzerkonto eine eindeutige E-Mail-Adresse haben muss.

   - [Optional] **Vorname**
   - [Optional] **Nachname**
   - Ändern Sie bei **Sprache** die Standardsprache für die in diesem Konto verwendete(n) Benachrichtigungen, Berichte und Software.
5. Bestimmen Sie, auf welche Services die Benutzer zugreifen können und welche Rollen diese in jedem Service haben.
   - Wenn Sie das Kontrollkästchen **Firmenadministrator** auswählen, erhält der Benutzer Zugriff auf das Management-Portal und die Administrator-Rolle in allen Services.
   - Wenn Sie das Kontrollkästchen **Abteilungsadministrator** aktivieren, erhält der Benutzer Zugriff auf das Management-Portal. Ob er die Service-Administrator-Rolle (nicht) erhält, hängt vom Service ab.
   - Ansonsten erhält der Benutzer die Rollen, die Sie in den von Ihnen ausgewählten Services bestimmen.
6. Klicken Sie auf **Erstellen**.

Das neu erstellte Benutzerkonto wird in der Registerkarte **Benutzer** angezeigt.

Wenn Sie die Benutzereinstellungen bearbeiten oder Benachrichtigungseinstellungen und Quotas für den Benutzer spezifizieren wollen, müssen Sie den Benutzer zuerst in der Registerkarte **Benutzer** auswählen und dann auf das Stiftsymbol in dem Bereich klicken, den Sie bearbeiten wollen.

So können Sie das Kennwort eines Benutzers zurücksetzen

1. Gehen Sie im Management-Portal zu **Unternehmensverwaltung** –> **Benutzer**.
2. Wählen Sie den Benutzer aus, dessen Kennwort Sie zurücksetzen wollen, und klicken Sie dann auf das Drei-Punkte-Symbol > **Kennwort zurücksetzen**.
3. Bestätigen Sie die Aktion durch Klicken auf **Zurücksetzen**.

Der Benutzer kann nun den Zurücksetzungsprozess abschließen, indem er die Anweisungen in der ihm zugesendeten E-Mail befolgt.

Für Services, die keine Zwei-Faktor-Authentifizierung unterstützen (z.B. die Registrierung in Cyber Infrastructure), müssen Sie möglicherweise ein Benutzerkonto in ein *Service-Konto* umwandeln – also ein Konto, das keine Zwei-Faktor-Authentifizierung erfordert.

So können Sie ein Benutzerkonto in ein Service-Konto umwandeln

1. Gehen Sie im Management-Portal zu **Unternehmensverwaltung** –> **Benutzer**.
2. Wählen Sie denjenigen Benutzer aus, dessen Konto Sie in ein Service-Konto umwandeln wollen, und klicken Sie anschließend auf das Drei-Punkte-Symbol > **Als Service-Konto kennzeichnen**.
3. Geben Sie im Bestätigungsfenster den Zwei-Faktor-Authentifizierungscode ein und bestätigen Sie Ihre Aktion.

Das Konto kann jetzt auch für Services verwendet werden, die keine Zwei-Faktor-Authentifizierung unterstützen.

Für jeden Service verfügbare Benutzerrollen

Ein Benutzer kann mehrere Rollen haben, aber nur eine Rolle je Service.

Sie können für jeden Service festlegen, welche Rolle einem Benutzer zugewiesen wird.

Service	Rolle	Beschreibung
n/a	Firmenadministrator	Diese Rolle gewährt dem Administrator vollständige Rechte für alle Services. Diese Rolle gewährt Zugriff auf die Positivliste für Unternehmensapplikationen. Wenn die Disaster Recovery-Funktion des Schutz Service für die Firma aktiviert ist, gewährt die Rolle außerdem Zugriff auf die Disaster Recovery-Funktionalität.
Management-Portal	Administrator	Diese Rolle gewährt Zugriff auf das Management-Portal, wo der Administrator Benutzer innerhalb der kompletten Organisation verwalten kann. Diese Rolle gewährt beispielsweise volle Berechtigungen für die Endpoint Detection & Response-

		Anzeigen (einschließlich der Widgets).
	Nur-Lesen-Administrator Partnerebene	Diese Rolle ermöglicht einen schreibgeschützten Zugriff auf alle Objekte im Management-Portal des Partners und auf die Management-Portale aller Kunden dieses Partners. Solche Benutzer können auf Daten anderer Benutzer der Organisation im Nur-Lesen-Modus zugreifen. Sie können Schutzpläne bearbeiten, aber keine Änderungen an Skripting-, Monitoring- oder Agenten-Plänen speichern.
	Nur-Lesen-Administrator Kundenebene	Diese Rolle ermöglicht einen Nur-Lesen-Zugriff auf alle Objekte im Management-Portal des gesamten Unternehmens. Solche Benutzer können auf Daten anderer Benutzer der Organisation im Nur-Lesen-Modus zugreifen.
	Nur-Lesen-Administrator Abteilungsebene	Diese Rolle ermöglicht einen Nur-Lesen-Zugriff auf alle Objekte im Management-Portal der Firmenabteilung und deren Unterabteilungen. Solche Benutzer können auf Daten anderer Benutzer der Organisation im Nur-Lesen-Modus zugreifen.
Schutz	Cyber-Administrator	Zusätzlich zu den Rechten der Administrator-Rolle ermöglicht diese Rolle, den Cyber Protection Service zu konfigurieren und zu verwalten sowie Aktionen beim Cyber-Skripting zu genehmigen. Die Rolle des Cyber-Administrators ist nur für Mandanten mit aktiviertem Advanced Management-Paket verfügbar.
	Administrator	Diese Rolle ermöglicht es, die Schutz-Funktionalität für Ihre Kunden zu konfigurieren und zu verwalten. Die Rolle ist beispielsweise zur Konfiguration und Verwaltung der Disaster Recovery-Funktionalität, der Endpoint Detection & Response-Funktionalität sowie der Positivliste für Unternehmensapplikationen erforderlich.
	Nur-Lesen-Administrator	Die Rolle ermöglicht nur Lesezugriff auf alle Objekte im Schutz Service. Solche Benutzer können auf Daten anderer Benutzer der Organisation im Nur-Lesen-Modus zugreifen. Der Nur-Lesen-Administrator kann weder die Disaster Recovery-Funktionalität, noch die Endpoint Detection & Response-Funktionalität, noch die Positivliste für Unternehmensapplikationen konfigurieren bzw. verwalten.

	Operator wiederherstellen	Die Rolle ermöglicht den Zugriff auf Backups von Microsoft 365- und Google Workspace- Organisationen und erlaubt deren Wiederherstellung, während der Zugriff auf sensible Inhalte eingeschränkt wird.
	Benutzer	Diese Rolle ermöglicht die Verwendung des Schutz Service, jedoch ohne administrative Berechtigungen. Es wird Zugriff auf bestimmte Funktionalitäten (wie Endpoint Detection & Response) gewährt, aber Benutzer, denen diese Rolle zugewiesen wird, können nicht auf die Daten anderer Benutzer in der Organisation zugreifen.
File Sync & Share	Administrator	Diese Rolle ermöglicht es, die File Sync & Share-Funktionalität für Ihre Benutzer zu konfigurieren und zu verwalten. Ein Konto mit dieser Rolle wird nicht als Teil der Quota **Benutzer** mitgezählt, weil es keinen Zugriff auf die File Sync & Share-Funktionalität bietet.
	Benutzer	Diese Rolle ermöglicht es, den File Sync & Share Service zu verwenden. Die Benutzer haben nur Zugriff auf ihre eigenen Daten sowie auf die Daten, die mit ihnen geteilt werden.
	Gast	Ein Konto mit dieser Rolle wird erstellt, wenn ein File Sync & Share-Benutzer Inhalte entweder mit einem Cyber Protect Cloud-Benutzer teilt, für den die Nutzung des File Sync & Share Service nicht freigeschaltet wurde, oder wenn er Inhalte mit einer Person teilt, die kein Cyber Protect Cloud-Benutzer ist. Eine Gastrolle hat keinen Sync-Ordner, kann keinen Cloud Storage nutzen und wird nicht als Teil der Quota **Benutzer** gezählt, weil sie keinen Zugriff auf die File Sync & Share-Funktionalität ermöglicht. Ein Gast kann auf eine Benutzer- oder Administratorrolle 'hochgestuft' werden.
Notary	Administrator	Diese Rolle ermöglicht es, die Beglaubigungsfunktionalität für Ihre Kunden zu konfigurieren und zu verwalten.
	Benutzer	Diese Rolle ermöglicht die Verwendung des Notary Service, jedoch ohne administrative Berechtigungen. Solche Benutzer können nicht auf die Daten anderer Benutzer der Organisation zugreifen.

Nur-Lesen-Administrator-Rolle

Ein Konto mit dieser Rolle hat nur einen Lesezugriff auf die Cyber Protect-Konsole und kann Folgendes tun:

- Diagnoseinformationen sammeln (wie z.B. Systemberichte).
- Die Recovery-Punkte eines Backups anzeigen lassen, aber keine Backup-Inhalte und keine Dateien, Ordner oder E-Mails einsehen.

Ein Nur-Lesen-Administrator kann Folgendes tun:

- Irgendwelche Tasks starten oder stoppen.
  Ein Nur-Lesen-Administrator kann beispielsweise keine Wiederherstellung starten oder ein laufendes Backup stoppen.
- Auf das Dateisystem von Quell- oder Zielmaschinen zugreifen.
  Ein Nur-Lesen-Administrator kann beispielsweise keine Dateien, Ordner oder E-Mails auf einer gesicherten Maschine einsehen.
- Irgendwelche Einstellungen ändern.
  Ein Nur-Lesen-Administrator kann beispielsweise keinen Schutzplan erstellen oder dessen Einstellungen ändern.
- Irgendwelche Daten erstellen, aktualisieren oder löschen.
  Ein Nur-Lesen-Administrator kann beispielsweise keine Backups löschen.

Alle Benutzeroberflächenobjekte, auf die ein Nur-Lesen-Administrator keinen Zugriff hat, werden ausgeblendet – mit Ausnahme der Standardeinstellungen des Schutzplans. Diese Einstellungen werden zwar angezeigt, aber die Schaltfläche **Speichern** ist nicht aktiv.

Alle Änderungen, die sich auf Konten und Rollen beziehen, werden auf der Registerkarte **Aktivitäten** mit folgenden Informationen angezeigt:

- Was geändert wurde
- Wer die Änderungen durchgeführt hat
- Datum und Uhrzeit der Änderungen

Rolle 'Restore Operator'

Diese Rolle ist nur im Cyber Protection Service verfügbar und auf Microsoft 365- sowie Google Workspace-Backups beschränkt.

Ein Restore Operator kann Folgendes tun:

- Alarmmeldungen und Aktivitäten anzeigen.
- Die Liste der Backups durchsuchen und aktualisieren.
- Backups durchsuchen, ohne auf deren Inhalte zuzugreifen. Der Restore Operator kann die Namen der gesicherten Dateien sowie die Betreffs und Absender der gesicherten E-Mails sehen.

- Backups durchsuchen (Volltextsuche wird nicht unterstützt).
- Cloud-zu-Cloud-Backups an ihrem ursprünglichen Speicherort innerhalb der ursprünglichen Microsoft 365- oder Google Workspace-Organisation wiederherstellen.

Ein Restore Operator kann Folgendes nicht tun:

- Alarmmeldungen löschen.
- Microsoft 365- oder Google Workspace-Organisationen hinzufügen oder löschen.
- Backup-Speicherorte hinzufügen, löschen oder umbenennen.
- Backups löschen oder umbenennen.
- Ordner erstellen, löschen oder umbenennen, wenn ein Backup zu einem benutzerdefinierten Speicherort wiederhergestellt wird.
- Einen Backup-Plan anwenden oder ein Backup ausführen.
- Auf gesicherte Dateien oder die Inhalte von gesicherten E-Mails zugreifen.
- Gesicherte Dateien oder E-Mail-Anhänge herunterladen.
- Gesicherte Cloud-Ressourcen (wie E-Mails oder Kalenderelemente) per E-Mail versenden.
- Microsoft 365 Teams-Unterhaltungen einsehen oder wiederherstellen.
- Cloud-zu-Cloud Backups an nicht ursprünglichen Speicherorten wiederherstellen, z.B. in einem anderen Postfach, in OneDrive, Google Drive oder Microsoft 365 Team.

Die Benachrichtigungseinstellungen für einen Benutzer ändern

Wenn Sie die Benachrichtigungseinstellungen für einen Benutzer ändern wollen, gehen Sie zu **Unternehmensverwaltung** –> **Benutzer**. Wählen Sie den Benutzer, dessen Benachrichtigungen Sie konfigurieren wollen, und klicken Sie anschließend auf das Stiftsymbol im Bereich **Einstellungen**. Die folgenden Benachrichtigungseinstellungen sind verfügbar, wenn der Cyber Protection Service für den Mandanten aktiviert ist, in dem der Benutzer erstellt wird:

- **Benachrichtigungen über Quota-Überbenutzung** (standardmäßig aktiviert)
  Benachrichtigungen zu überschrittenen Quotas.
- **Geplante Nutzungsberichte** (standardmäßig aktiviert)
  Nutzungsberichte, die am ersten Tag eines jeden Monats gesendet werden.
- **URL-Branding-Benachrichtigungen** (standardmäßig deaktiviert)
  Benachrichtigungen über einen bevorstehenden Ablauf des Zertifikats, das für die benutzerdefinierte URL der Cyber Protect Cloud Services verwendet wird. Die Benachrichtigungen werden an alle Administratoren des ausgewählten Mandanten gesendet – 30 Tage, 15 Tage, 7 Tage, 3 Tage sowie 1 Tag vor Ablauf des Zertifikats.
- **Benachrichtigungen über Fehler**, **Benachrichtigungen über Warnungen** und **Benachrichtigungen über erfolgreiche Aktionen** (standardmäßig deaktiviert)

Benachrichtigungen über die Ausführungsergebnisse von Schutzplänen und die Ergebnisse von Disaster Recovery-Aktionen für jedes Gerät.

- **Tägliche Zusammenfassung über aktive Alarmmeldungen** (standardmäßig aktiviert)
  Die tägliche Zusammenfassung wird auf der Grundlage der Liste der aktiven Alarmmeldungen erstellt, die in dem Augenblick in der Cyber Protect-Konsole vorhanden sind, wenn die Zusammenfassung generiert wird. Die Zusammenfassung wird einmal täglich zwischen 10:00 und 23:59 Uhr (UTC) generiert und gesendet. Der genaue Zeitpunkt der Berichtsgenerierung und -übermittlung hängt vom Workload im Datacenter ab. Wenn zum betreffenden Zeitpunkt keine aktiven Alarmmeldungen vorliegen, wird auch keine Zusammenfassung gesendet. Die Zusammenfassung enthält keine Informationen über frühere Alarmmeldungen, die nicht mehr aktiv sind. Wenn z.B. ein Benutzer ein fehlgeschlagenes Backup findet und die Alarmmeldungen löscht oder wenn das Backup wiederholt und dann erfolgreich abgeschlossen wird, bevor die Zusammenfassung generiert wird, dann wird die Alarmmeldung nicht mehr vorhanden sein und die Zusammenfassung wird diese nicht mehr enthalten.
- **Gerätekontrolle-Benachrichtigungen** (standardmäßig deaktiviert)
  Benachrichtigungen über Versuche, Peripheriegeräte und Ports zu verwenden, die durch Schutzpläne mit aktiviertem Gerätekontrolle-Modul eingeschränkt werden.
- **Recovery-Benachrichtigungen** (standardmäßig deaktiviert)
  Benachrichtigungen über Wiederherstellungsaktionen auf folgenden Ressourcen: Benutzer-E-Mail-Nachrichten und das komplette Postfach, öffentliche Ordner, OneDrive / GoogleDrive: das komplette OneDrive sowie Dateien oder Ordner, SharePoint-Dateien, Teams: Kanäle, komplette Teams, E-Mail-Nachrichten und Team-Websites.
  Im Kontext dieser Benachrichtigungen werden folgende Aktionen als Wiederherstellungsaktionen betrachtet: als E-Mail senden, Herunterladen oder eine Wiederherstellung starten.
- **Data Loss Prevention-Benachrichtigungen** (standardmäßig deaktiviert)
  Benachrichtigungen über Data Loss Prevention Alarmmeldungen, die sich auf die Aktivitäten dieses Benutzers im Netzwerk beziehen.
- **Sicherheitsvorfall-Benachrichtigungen** (standardmäßig deaktiviert)
  Benachrichtigungen über Malware-Erkennungen bei On-Access-, On-Execution- oder On-Demand-Scans sowie über Erkennungen durch die Behavioral Engine oder die URL-Filter-Engine.
  Es stehen Ihnen zwei Optionen zur Verfügung: **Abgeschwächt** und **Nicht abgeschwächt**. Diese Optionen sind für Alarmmeldungen von Endpoint Detection & Response (EDR)-Vorfällen, EDR-Alarmmeldungen aus Bedrohungsfeeds sowie individuellen Alarmmeldungen (für Workloads, bei denen die EDR-Funktionalität nicht aktiviert ist) relevant.
  Wenn ein EDR-Alarm erstellt wird, wird eine E-Mail an den betreffenden Benutzer gesendet. Wenn sich der Bedrohungsstatus des Vorfalls ändert, wird eine neue E-Mail gesendet. Die E-Mails enthalten Aktionsschaltflächen, mit denen sich der Benutzer Details zu dem jeweiligen Vorfall anzeigen lassen kann (wenn dieser abgeschwächt wurde) oder den Vorfall untersuchen und beheben kann (wenn er nicht abgeschwächt wurde).
- **Infrastruktur-Benachrichtigungen** (standardmäßig deaktiviert)
  Benachrichtigungen über Probleme mit der Disaster Recovery-Infrastruktur: wenn die Disaster Recovery-Infrastruktur oder die VPN-Tunnel nicht verfügbar sind.

Alle Benachrichtigungen werden an die E-Mail-Adresse gesendet, die für den entsprechenden Benutzer spezifiziert wurde.

Je nach Benutzerrolle empfangene Benachrichtigungen

Die Benachrichtigungen, die Cyber Protection versendet, hängen von der Benutzerrolle ab.

Benachrichtigungstyp\Benutzerrolle	Benutzer	Kundenadministrator
Benachrichtigungen für eigene Geräte	Ja	Ja
Benachrichtigungen für alle Geräte in der Organisation	n/a	Ja (außer **Sicherheitsvorfall-Benachrichtigungen**)
Benachrichtigungen für Microsoft 365, Google Workspace und andere Cloud-basierte Backups	n/a	Ja

Ein Benutzerkonto deaktivieren und aktivieren

Unter bestimmten Umständen müssen Sie möglicherweise ein Benutzerkonto deaktivieren, um dessen Zugriff auf die Cloud-Plattform temporär sperren zu können.

So können Sie ein Benutzerkonto deaktivieren

1. Gehen Sie im Management-Portal zu **Benutzer**.
2. Wählen Sie das Benutzerkonto aus, welches Sie deaktivieren wollen, und klicken Sie dann auf das Drei-Punkte-Symbol > **Deaktivieren**.
3. Bestätigen Sie die Aktion durch Klicken auf **Deaktivieren**.

Als Ergebnis wird der Benutzer die Cloud-Plattform nicht mehr verwenden und keine Benachrichtungen empfangen können.

Wenn Sie ein deaktiviertes Benutzerkonto wieder aktivieren wollen, müssen Sie dieses zuerst in der Benutzerliste auswählen, dann auf das Drei-Punkte-Symbol > **Aktivieren** klicken.

Ein Benutzerkonto löschen

Möglicherweise wollen Sie ein Benutzerkonto dauerhaft löschen, um die von ihm verwendeten Ressourcen (z.B. den Speicherplatz oder die Lizenz) freizugeben. Die Nutzungsstatistiken werden innerhalb eines Tages nach dem Löschvorgang aktualisiert. Bei Konten mit vielen Daten kann es auch länger dauern.

Bevor Sie ein Benutzerkonto löschen können, müssen Sie es erst deaktivieren. Weitere Informationen über die entsprechende Durchführung finden Sie im Abschnitt 'Ein Benutzerkonto deaktivieren und aktivieren'.

So können Sie ein Benutzerkonto löschen

1. Gehen Sie im Management-Portal zu **Benutzer**.
2. Wählen Sie das deaktivierte Benutzerkonto aus, klicken Sie auf das Drei-Punkte-Symbol und anschließend auf **Löschen**.
3. Geben Sie zur Bestätigung der Aktion Ihren Anmeldenamen ein und klicken Sie dann auf **Löschen**.

Ergebnis:

- Alle für dieses Konto konfigurierten Benachrichtigungen werden deaktiviert.
- Alle Daten, die zu diesem Benutzerkonto gehören, werden gelöscht.
- Der Administrator wird nicht auf das Management-Portal zugreifen können.
- Alle Backups der Workloads, die mit diesem Benutzer assoziiert sind, werden gelöscht.
- Die Registrierung aller Maschinen, die mit diesem Benutzerkonto assoziiert sind, wird aufgehoben.
- Alle Schutzpläne werden von allen Workloads widerrufen, die mit diesem Benutzer assoziiert sind.
- Alle File Sync & Share-Daten, die zu diesem Benutzer gehören (z.B. Dateien und Ordner), werden gelöscht.
- Alle Notary-Daten, die zu diesem Benutzer gehören (z.B. beglaubigte Dateien, elektronisch signierte Dateien), werden gelöscht.
- Ihnen wird der **Mandantenstatus** als **Gelöscht** angezeigt. Wenn Sie mit dem Mauszeiger über den Status **Gelöscht** fahren, wird Ihnen das Datum angezeigt, zu dem der Benutzer gelöscht wurde – zusammen mit einem Hinweis, dass Sie alle relevanten Benutzerdaten und Einstellungen innerhalb von 30 Tagen nach diesem Löschdatum noch wiederherstellen können.

Die Eigentümerschaft eines Benutzerkontos übertragen

Möglicherweise müssen Sie die Eigentümerschaft eines Benutzerkontos übertragen, wenn Sie weiterhin auf die Daten eines gesperrten Benutzers zugreifen wollen.

Wichtig
Die Inhalte eines gelöschten Kontos können nicht neu zugewiesen werden.

So können Sie die Eigentümerschaft eines Benutzerkontos übertragen

1. Gehen Sie im Management-Portal zu **Benutzer**.
2. Wählen Sie das Benutzerkonto aus, dessen Eigentümerschaft Sie übertragen wollen, und klicken Sie denn im Bereich **Allgemeine Informationen** auf das Stiftsymbol.
3. Ersetzen Sie die vorliegende E-Mail-Adresse mit der E-Mail-Adresse des zukünftigen Kontobesitzers – und klicken Sie dann auf **Fertig**.
4. Bestätigen Sie die Aktion durch Klicken auf **Ja**.

5. Lassen Sie den zukünftigen Kontobesitzer seine E-Mail-Adresse verifizieren. Dazu muss er die ihm zugesendeten Anweisungen befolgen.
6. Wählen Sie das Benutzerkonto aus, dessen Eigentümerschaft Sie übertragen wollen, und klicken Sie dann auf das Drei-Punkte-Symbol > **Kennwort zurücksetzen**.
7. Bestätigen Sie die Aktion durch Klicken auf **Zurücksetzen**.
8. Lassen Sie den zukünftigen Kontobesitzer sein Kennwort zurücksetzen. Dazu muss er die Anweisungen befolgen, die ihm an seine E-Mail-Adresse zugesendet werden.

Der neue Besitzer kann jetzt auf das Konto zugreifen.

Zwei-Faktor-Authentifizierung einrichten

Die **Zwei-Faktor-Authentifizierung (2FA)** ist eine Variante der Multi-Faktor-Authentifizierung, bei der die Identität eines Benutzers anhand einer Kombination aus zwei verschiedenen Faktoren überprüft wird:

- Etwas, was der Benutzer weiß (eine PIN oder ein Kennwort)
- Etwas, was der Benutzer hat (ein Token)
- Etwas, was der Benutzer ist (Biometrik)

Die Zwei-Faktor-Authentifizierung bietet einen zusätzlichen Schutz gegen unbefugte Zugriffe auf Ihr Konto.

Die Plattform unterstützt die **TOTP (Time-based One-Time Password)**-Authentifizierung, die mit zeitlich limitierten Einmalkennwörtern arbeitet. Wenn die TOTP-Authentifizierung im System aktiviert ist, müssen Benutzer ihr herkömmlichs Kennwort sowie einen einmaligen TOTP-Code eingeben, um auf das System zugreifen zu können. Der Benutzer gibt sein Kennwort also als ersten Faktor und den TOTP-Code als zweiten Faktor ein. Der TOTP-Code wird von einer Authentifizierungsapplikation auf einem „Zweit-Faktor"-Gerät des Benutzers generiert – und zwar auf der Grundlage der aktuellen Uhrzeit und eines „Geheimnis" (auch Secret oder geheimer Schlüssel genannt, hier ein QR- oder alphanumerischen Code), welches von der Plattform bereitgestellt wird.

Und so funktioniert es

1. Sie aktivieren die Zwei-Faktor-Authentifizierung auf Ihrer Organisationsebene.
2. Die entsprechenden Anwender in Ihrem Unternehmens müssen eine Authentifizierungsapplikation auf einem ihrer Zweit-Faktor-Gerät (z.B. ein Mobiltelefon, Tablet, Laptop, Desktop-PC) installieren. Diese Applikation wird zum Generieren der einmaligen TOTP-Codes (also des Einmalkennwortes) verwendet. Diese Authentifikatoren werden empfohlen:
   - Google Authenticator
     iOS-App-Version (https://apps.apple.com/de/app/google-authenticator/id388497605)

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

- Microsoft Authenticator
  iOS-App-Version (https://apps.apple.com/de/app/microsoft-authenticator/id983156458)
  Android-Version (https://play.google.com/store/apps/details?id=com.azure.authenticator)

Wichtig
Die Benutzer müssen sicherstellen, dass die Uhrzeit auf dem Gerät, auf dem die Authentifizierungsapplikation installiert ist, korrekt eingestellt ist (also die aktuelle Uhrzeit widerspiegelt).

3. Die entsprechenden Benutzer Ihres Unternehmens müssen sich erneut am System anmelden.
4. Nach Eingabe ihrer Anmeldedaten (Benutzername, Kennwort) werden sie aufgefordert, eine Zwei-Faktor-Authentifizierung für ihr Benutzerkonto einzurichten.
5. Sie müssen einen angezeigten QR-Code mit ihrer Authentifizierungsapplikation scannen. Wenn es (aus welchem Grund auch immer) nicht möglich ist, den QR-Code zu scannen, kann der Benutzer alterantiv auch den 32-stelligen Code verwenden, der unter dem QR-Code angezeigt wird, und diesen dann manuell in die Authentifizierungsapplikation eingeben.

Wichtig
Es wird dringend empfohlen, diese Daten zu sichern (drucken Sie beispielsweise den QR-Code aus und notieren Sie sich das temporäre Einmalkennwort (den geheimen TOTP-Code). Verwenden Sie dabei eine Applikation, die die Sicherung von Codes per Cloud Backup unterstützt). Sie benötigen das temporäre Einmalkennwort (den TOTP-Code), um die Zwei-Faktor-Authentifizierung zurücksetzen zu können, falls das Zweit-Faktor-Gerät verloren gehen sollte.

6. Das temporäre Einmalkennwort (der TOTP-Code) wird in der Authentifizierungsapplikation generiert. Er wird alle 30 Sekunden automatisch neu generiert.
7. Der entsprechende Benutzer muss diesen einmaligen TOTP-Code dann im Fenster **Zwei-Faktor-Authentifizierung einrichten** eingeben, nachdem er zuvor sein eigenes Kennwort eingegeben hat.
8. Als Ergebnis dieser Prozedur ist dann die Zwei-Faktor-Authentifizierung für den Benutzer eingerichtet.

Wenn sich der Benutzer anschließend am System anmeldet, werden er jedes Mal aufgefordert, seine Anmeldedaten (Benutzername, Kennwort) sowie anschließend den einmaligen TOTP-Code anzugeben, der jedes Mal in der Authentifizierungsapplikation neu generiert wird. Ein Benutzer kann anschließend außerdem seinen Browser bei der Anmeldung am System als 'vertrauenswürdig' kennzeichnen. Das bewirkt, dass bei nachfolgenden Anmeldungen über diesen speziellen Browser kein einmaliger TOTP-Code mehr angefordert wird.

So können Sie die Zwei-Faktor-Authentifizierung auf einem neuen Gerät wiederherstellen

Wenn Sie Zugriff auf die zuvor eingerichtete Authentifizierungs-App für Mobilgeräte haben:

1. Installieren Sie eine Authenticator-App auf Ihrem neuen Gerät.
2. Verwenden Sie die PDF-Datei, die Sie beim Einrichten der Zwei-Faktor-Authentifizierung (2FA) auf Ihrem Gerät gesichert haben. Diese Datei enthält den 32-stelligen Code, der in der Authenticator-App eingegeben werden muss, um die Authenticator-App erneut mit Ihrem Acronis Konto verknüpfen zu können.

   Wichtig
   Wenn der Code korrekt ist, aber nicht funktioniert, stellen Sie sicher, dass die Uhrzeit in der Authenticator-App für Mobilgeräte synchronisiert wird.

3. Wenn Sie es beim Einrichten versäumt haben, die PDF-Datei zu sichern:

a. *Klicken Sie auf **2FA zurücksetzen** und geben Sie das Einmalkennwort ein, das in der zuvor eingerichteten Authenticator-App für Mobilgeräte angezeigt wird.*
b. Folgen Sie den Bildschirmanweisungen.

Wenn Sie keinen Zugriff auf die zuvor eingerichtete Authenticator-App für Mobilgeräte haben:

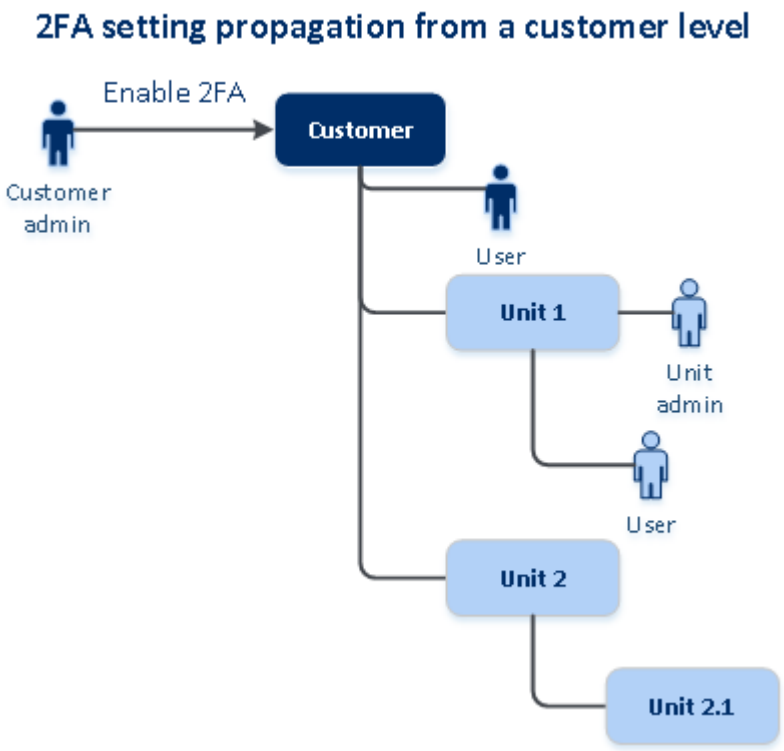
1. Nehmen Sie ein neues Mobilgerät.
2. Verwenden Sie die gespeicherte PDF-Datei, um ein neues Gerät zu verknüpfen (der Standardname der Datei ist `cyberprotect-2fa-backupcode.pdf`).
3. Stellen Sie den Zugriff auf Ihr Konto aus dem Backup wieder her. Stellen Sie sicher, dass Backups von Ihrer Mobilgeräte-App unterstützt werden.
4. Öffnen Sie die App unter dem gleichen Konto von einem anderen Mobilgerät aus, wenn dies von der App unterstützt wird.

Die Zwei-Faktoren-Einrichtung zwischen Mandantenebenen weitergeben

Die Zwei-Faktor-Authentifizierung wird auf der Ebene der **Organisation** (Unternehmensebene) eingerichtet. Sie können die Zwei-Faktor-Authentifizierung nur für Ihr eigenes Unternehmen einrichten.

Die Zwei-Faktor-Authentifizierungseinstellungen werden folgendermaßen zwischen Mandantenebenen weitergegeben:

- Abteilungen übernehmen automatisch die Zwei-Faktor-Authentifizierungseinstellungen von ihrer Kundenorganisation.



Hinweis

1. Es ist nicht möglich, die Zwei-Faktor-Authentifizierung auf der Abteilungsebene einzurichten.
2. Sie können die Einstellungen für die Zwei-Faktor-Authentifizierung für Benutzer der Unterorganisationen (Abteilungen) verwalten.

Die Zwei-Faktor-Authentifizierung für Ihren Mandanten einrichten

Als Administrator können Sie die Zwei-Faktor-Authentifizierung für Ihre Organisation aktivieren.

So können Sie die Zwei-Faktor-Authentifizierung für Ihren Mandanten aktivieren

1. Gehen Sie im Management-Portal zu **Einstellungen** –> **Sicherheit**.
2. Verschieben Sie den Schalter für die **Zwei-Faktor-Authentifizierung** und klicken Sie dann auf **Aktivieren**.

Jetzt müssen alle Benutzer Organisation die Zwei-Faktor-Authentifizierung für ihre Konten einrichten. Sie werden dazu aufgefordert, wenn sie sich das nächste Mal anmelden wollen oder wenn ihre aktuelle Sitzung abläuft.

Die Fortschrittsanzeige unter dem Schalter gibt an, wie viele Benutzer eine Zwei-Faktor-Authentifizierung für ihre Konten eingerichtet haben. Wenn Sie überprüfen wollen, welche Anwender ihre Konten bereits konfiguriert haben, müssen Sie zur Registerkarte **Unternehmensverwaltung** –> **Benutzer** wechseln und die Spalte **2FA-Status** überprüfen. Der 2FA-

Status von Benutzern, die noch keine Zwei-Faktor-Authentifizierung für ihre Konten konfiguriert haben, lautet **Setup erforderlich**.

Nachdem sie die Zwei-Faktor-Authentifizierung erfolgreich konfiguriert haben, müssen die Benutzer jedes Mal, wenn sie sich an der Service-Konsole anmelden, nicht nur ihren Anmeldenamen und ihr Kennwort eingeben, sondern auch einen TOTP-Code.

So können Sie die Zwei-Faktor-Authentifizierung für Ihren Mandanten deaktivieren

1. Gehen Sie im Management-Portal zu **Einstellungen** –> **Sicherheit**.
2. Wenn Sie die Zwei-Faktor-Authentifizierung deaktivieren wollen, müssen Sie erst den Schalter ausschalten und dann auf **Deaktivieren** klicken.
3. [Wenn mindestens ein Benutzer die Zwei-Faktor-Authentifizierung innerhalb der Organisation konfiguriert hat] Geben Sie den TOTP-Code ein, der in Ihrer Authentifizierungsapplikation auf dem jeweiligen Mobilgerät generiert wurde.

Als Ergebnis wird die Zwei-Faktor-Authentifizierung für Ihre Organisation deaktiviert, alle geheimen Schlüssel werden gelöscht und alle vertrauenswürdigen Browser werden verworfen. Alle Benutzer können sich wieder nur durch Eingabe ihrer Anmeldedaten (Benutzername, Kennwort) am System anmelden. In der Registerkarte **Unternehmensverwaltung** –> **Benutzer** wird die Spalte **2FA-Status** ausgeblendet.

Die Zwei-Faktor-Authentifizierung für Benutzer verwalten

Sie können die Einstellungen für die Zwei-Faktor-Authentifizierung für all Ihre Benutzer überwachen und zudem im Management-Portal die Einstellungen in der Registerkarte **Unternehmensverwaltung** –> **Benutzer** zurücksetzen.

Monitoring

Sie können im Management-Portal, unter **Unternehmensverwaltung** –> **Benutzer**, eine Liste aller Benutzer in Ihrer Organisation einsehen. Der **2FA-Status** gibt an, ob die Zwei-Faktor-Konfiguration für einen bestimmten Benutzer eingerichtet wurde.

So können Sie die Zwei-Faktor-Authentifizierung für einen Benutzer zurücksetzen

1. Gehen Sie im Management-Portal zu **Unternehmensverwaltung** –> **Benutzer**.
2. Suchen Sie in der Registerkarte **Benutzer** einen Benutzer, dessen Einstellungen Sie ändern möchten – und klicken Sie anschließend auf das Drei-Punkte-Symbol.
3. Klicken Sie auf **Zwei-Faktor-Authentifizierung zurücksetzen**.
4. Geben Sie den TOTP-Code ein, der in der Authentifizierungsapplikation auf Ihrem Zweit-Faktor-Gerät generiert wurde, und klicken Sie dann auf **Zurücksetzen**.

Anschließend kann der Benutzer die Zwei-Faktor-Authentifizierung wieder einrichten.

So können Sie die vertrauenswürdigen Browser eines Benutzers zurücksetzen

1. Gehen Sie im Management-Portal zu **Unternehmensverwaltung** –> **Benutzer**.
2. Suchen Sie in der Registerkarte **Benutzer** einen Benutzer, dessen Einstellungen Sie ändern möchten – und klicken Sie anschließend auf das Drei-Punkte-Symbol.
3. Klicken Sie auf **Alle vertrauenswürdigen Browser zurücksetzen**.
4. Geben Sie den TOTP-Code ein, der in der Authentifizierungsapplikation auf Ihrem Zweit-Faktor-Gerät generiert wurde, und klicken Sie dann auf **Zurücksetzen**.

Der Benutzer, dessen vertrauenswürdige Browser Sie zurückgesetzt haben, muss jetzt bei seiner nächsten Anmeldung den TOTP-Code eingeben.

Die Benutzer können alle vertrauenswürdigen Browser und die Einstellungen für die Zwei-Faktor-Authentifizierung selbst zurücksetzen. Dies kann bei der Anmeldung am System erfolgen, indem Sie auf den entsprechenden Link klicken und den TOTP-Code eingeben, um die Aktion zu bestätigen.

So können Sie die Zwei-Faktor-Authentifizierung für einen Benutzer deaktivieren

Wir raten davon ab, die Zwei-Faktor-Authentifizierung zu deaktivieren, weil die Mandanten damit einem erhöhten Sicherheitsrisiko ausgesetzt werden.

In Ausnahmefällen können Sie die Zwei-Faktor-Authentifizierung für einen bestimmten Benutzer deaktivieren, während Sie die Zwei-Faktor-Authentifizierung für alle anderen Benutzer des Mandanten beibehalten. Dies ist ein Workaround für solche Fälle, in denen die Zwei-Faktor-Authentifizierung in einem Mandanten aktiviert ist, bei dem eine Cloud-Integration konfiguriert ist – und diese Integration den Zugriff auf die Plattform über das Benutzerkonto (Anmelde-Kennwort) autorisiert. Um die Integration weiterhin verwenden zu können, kann der Benutzer als Übergangslösung in ein Service-Konto konvertiert werden, für das keine Zwei-Faktor-Authentifizierung erforderlich ist.

Wichtig
Es wird nicht empfohlen, reguläre Benutzer in Service-Benutzer umzuwandeln, um die Zwei-Faktor-Authentifizierung zu deaktivieren, weil dies ein Sicherheitsrisiko für den Mandanten darstellt.

Wenn Sie die Cloud-Integrationen verwenden wollen, ohne die Zwei-Faktor-Authentifizierung für die Mandanten zu deaktivieren, empfehlen wir als sichere Lösung, stattdessen API-Clients zu erstellen und Ihre Cloud-Integrationen so zu konfigurieren, dass sie mit diesen Clients funktionieren.

1. Gehen Sie im Management-Portal zu **Unternehmensverwaltung** –> **Benutzer**.
2. Suchen Sie in der Registerkarte **Benutzer** einen Benutzer, dessen Einstellungen Sie ändern möchten – und klicken Sie anschließend auf das Drei-Punkte-Symbol.

3. Klicken Sie auf **Als Service-Konto kennzeichnen**. Der Benutzer erhält anschließend einen speziellen Zwei-Faktor-Authentifizierungsstatus namens **Service-Konto**.
4. [Wenn für mindestens einen Benutzer innerhalb eines Mandanten die Zwei-Faktor-Authentifizierung konfiguriert ist] Geben Sie den TOTP-Code ein, der in der Authentifizierungsapplikation auf Ihrem Zweit-Faktor-Gerät generiert wurde, um die Deaktivierung zu bestätigen.

So können Sie die Zwei-Faktor-Authentifizierung für einen Benutzer aktivieren

Möglicherweise müssen Sie die Zwei-Faktor-Authentifizierung für einen bestimmten Benutzer wieder aktivieren, dessen Aktivierung Sie zuvor deaktiviert hatten.

1. Gehen Sie im Management-Portal zu **Unternehmensverwaltung** –> **Benutzer**.
2. Suchen Sie in der Registerkarte **Benutzer** einen Benutzer, dessen Einstellungen Sie ändern möchten – und klicken Sie anschließend auf das Drei-Punkte-Symbol.
3. Klicken Sie auf **Als Standard-Konto kennzeichnen**. Als Ergebnis dieser Prozedur muss der die Zwei-Faktor-Authentifizierung wieder einrichten oder den TOTP-Code bereitstellen, wenn er sich am System anmeldet.

Die Zwei-Faktor-Authentifizierung bei Verlust des Zweit-Faktor-Gerätes zurücksetzen

Befolgen Sie einen der nachfolgenden vorgeschlagenen Ansätze, um den Zugriff auf Ihr Konto zurückzusetzen, wenn das Zweit-Faktor-Gerät einmal verloren gehen sollte:

- Stellen Sie Ihren geheimen TOTP-Schlüssel (TOTP-„Geheimnis“ – ein QR-Code oder ein alphanumerischer Code) aus einem Backup wieder her.

  Verwenden Sie ein anderes Zweit-Faktor-Gerät und geben Sie den gespeicherte geheimen TOTP-Schlüssel in die Authentifizierungsapplikation ein, die auf diesem Alternativgerät installiert ist.
- Bitten Sie Ihren Administrator, die Zwei-Faktor-Authentifizierungseinstellungen für Sie zurückzusetzen.

Schutz vor Brute-Force-Angriffen

Bei einem Brute-Force-Angriff versucht ein Eindringling dadurch Zugang zum System zu erhalten, indem er viele Kennwörter an das System überträgt, um so das richtige Kennwort durch Ausprobieren zu erraten.

Der Brute-Force-Schutzmenachnismus der Plattform basiert auf Geräte-Cookies.

Die auf der Plattform verwendeten Einstellungen für den Brute-Force-Schutz sind vordefiniert:

Parameter	Das Kennwort eingeben	Den TOTP-Code eingeben

Versuchslimit	10	5
Versuchslimitzeitraum (das Limit wird nach dem Timeout zurückgesetzt)	15 min (900 s)	15 min (900 s)
Sperrung erfolgt bei	Versuchslimit + 1 (11. Versuch)	Versuchslimit
Sperrzeitraum	5 min (300 s)	5 min (300 s)

Wenn Sie die Zwei-Faktor-Authentifizierung aktiviert haben, wird ein Geräte-Cookie erst nach einer erfolgreichen Authentifizierung mit beiden Faktoren (Kennwort und TOTP-Code) an einen Client (Browser) ausgestellt.

Bei vertrauenswürdigen Browsern wird das Geräte-Cookie nach einer erfolgreichen Authentifizierung mit nur einem Faktor (Kennwort) ausgestellt.

Die Versuche zur Eingabe des TOTP-Codes werden pro Benutzer und nicht pro Gerät registriert. Das bedeutet, dass selbst wenn ein Benutzer versucht, den TOTP-Code mit verschiedenen Geräten einzugeben, diese (und damit er selbst) trotzdem blockiert werden.

Agenten automatisch aktualisieren

Wichtig
Derzeit können Sie nur auf die Verwaltungsfunktionen zur Aktualisierung der Agenten zugreifen, wenn Sie den Schutz aktiviert haben.

Cyber Protect hat drei Arten von Agenten, die auf geschützten Maschinen installiert werden können: den Agenten für Windows, den Agenten für Linux und den Agenten für Mac.

Cyber Files Cloud verfügt über eine Windows- und eine macOS-Version des Desktop-Agenten für File Sync & Share. Damit können Dateien und Ordner zwischen einer Maschine und dem File Sync & Share Cloud Storage eines Benutzers synchronisiert werden, um Offline-Arbeiten und andere moderne Arbeitskonzepte – wie Homeoffice-Arbeit oder die sichere berufliche Nutzung von privaten Geräten (BYOD-Konzepte) zu unterstützen.

Wenn Sie sich die Verwaltung mehrerer Workloads erleichtern wollen, können Sie konfigurieren (oder auch komplett deaktivieren), dass alle Agenten auf sämtlichen Maschinen automatisch und unbeaufsichtigt aktualisiert werden sollen.

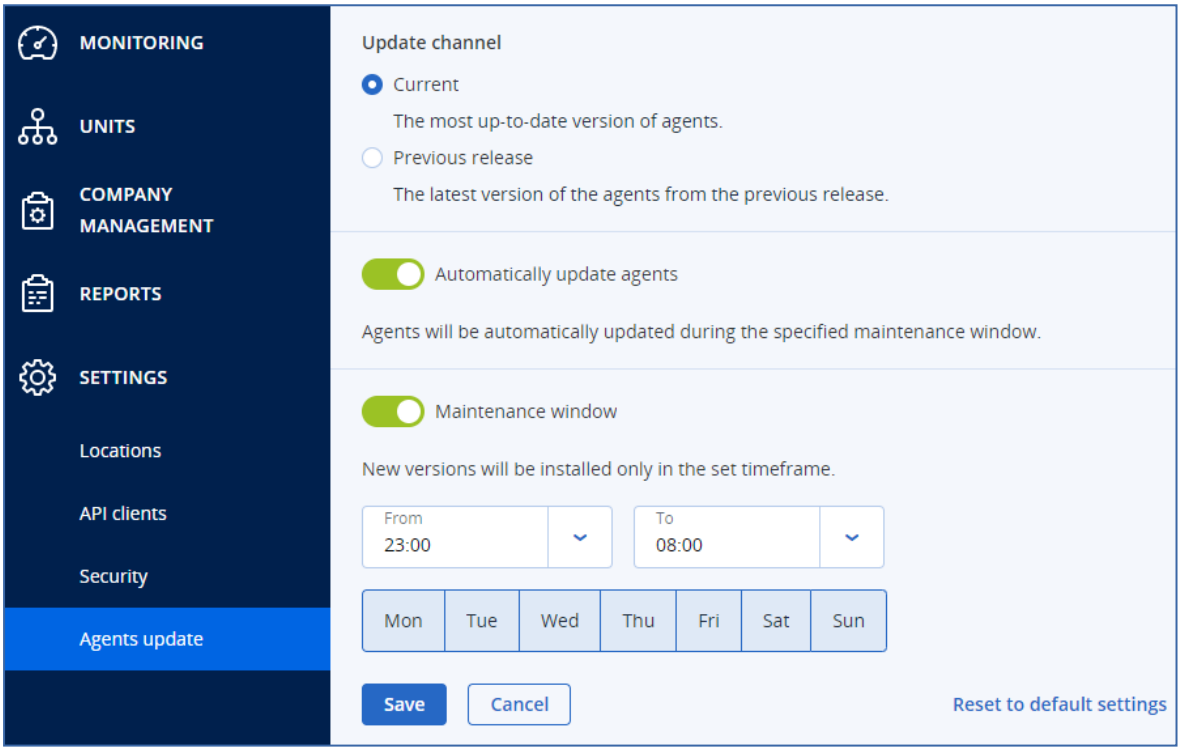
Hinweis
Wie Sie die Agenten auf einzelnen Maschinen verwalten und die Einstellungen für die automatische Aktualisierung der Agenten anpassen können, erfahren Sie im Abschnitt Update der Agenten in der Benutzeranleitung für Cyber Protect.

So können Sie Agenten automatisch aktualisieren lassen

Hinweis
Die Einstellungen für die automatische Aktualisierung des Agenten für File Sync & Share werden von Ihrem Service Provider übernommen, wenn Sie die Schutzfunktion nicht aktiviert haben.

So können Sie die automatische Aktualisierung der Agenten von der Einstiegsseite des Management-Portals aus festlegen

1. Wählen Sie **Einstellungen –> Agenten-Update**.



2. Wählen Sie aus, welche Version für die automatischen Updates erkannt werden soll: entweder **Aktuell** oder **Vorherige Version**.
   (Die Standardeinstellung ist **Aktuell**.)
3. Schalten Sie die Option **Agenten automatisch aktualisieren** ein.
   (Die Standardeinstellung ist **An**.)
4. Bestimmen Sie das Zeitfenster für den Wartungsvorgang.
   (Das Standardzeitfenster liegt zwischen 23:00 und 08:00.)

   Hinweis
   Obwohl die Prozesse zur Aktualisierung der Agenten so konzipiert wurden, dass sie schnell und reibungslos ablaufen, empfehlen wir einen Zeitrahmen zu wählen, der die Benutzer möglichst wenig stört. Denn die Benutzer selbst können die automatischen Updates weder verhindern noch aufschieben.

5. [Optional] Wählen Sie bestimmte Tage aus, an denen die automatischen Updates stattfinden sollen.
6. Wählen Sie den Befehl **Speichern** aus.

Hinweis
Die Möglichkeit für automatische Updates ist nur für folgende Agenten verfügbar:

- Die Agenten für Cyber Protect mit der Version 15.0.26986 (veröffentlicht im Mai 2021) und höher.
- Den Desktop Agenten für File Sync & Share mit der Version 15.0.30370 oder höher.

Ältere Agenten müssen zuerst noch manuell auf die neueste Version aktualisiert werden, bevor die automatische Update-Funktion genutzt werden kann.

So können Sie die Agenten-Updates überwachen

Wichtig
Die Agenten-Updates können nur überwacht werden, wenn Sie das Schutzmodul aktiviert haben.

Wie Sie die Aktualisierungen des Agenten überwachen können, ist in den Abschnitten für Alarmmeldungen und Aktivitäten in der Benutzeranleitung für Cyber Protect beschrieben.

Unveränderlichen Storage konfigurieren

Über den unveränderlichen Storage können Sie während einer spezifizierten Aufbewahrungsdauer auf gelöschte Backups zugreifen. Sie können die Inhalte dieser Backups wiederherstellen, aber Sie können diese nicht ändern, verschieben oder löschen. Wenn die Aufbewahrungsdauer endet, werden die gelöschten Backups dauerhaft gelöscht.

Der unveränderliche Storage enthält folgende Backups:

- Backups, die manuell gelöscht wurden.
- Backups, die – gemäß den Einstellungen im Bereich **Aufbewahrungsdauer** in einem Schutzplan oder im Bereich **Aufbewahrungsregeln** in einem Bereinigungsplan – automatisch gelöscht wurden.

Gelöschte Backups im unveränderlichen Storage belegen weiterhin Speicherplatz und werden entsprechend abgerechnet.

Gelöschten Mandanten wird keine Speicherplatz-Belegung (auch nicht im unveränderlichen Storage) in Rechnung gestellt.

Für Kunden-Mandanten ist der unveränderliche Storage in folgenden Modi verfügbar:

- **Governance-Modus**
  Sie können den unveränderlichen Storage erst deaktivieren und wieder aktivieren. Sie können die Aufbewahrungsdauer ändern oder auf den Compliance-Modus umschalten.
- **Compliance-Modus**

Warnung!
Die Auswahl des Compliance-Modus kann nicht rückgängig gemacht werden.

Sie können den unveränderlichen Storage nicht wieder deaktivieren. Sie können weder die Aufbewahrungsdauer ändern noch zurück in den Governance-Modus wechseln.

Zur Konfiguration der unveränderlichen Storage-Einstellungen ist eine Zwei-Faktor-Authentifizierung in dem Mandanten erforderlich, zu dem das Administratorkonto gehört.

Hinweis
Wenn Sie den Zugriff auf gelöschte Backups zulassen wollen, sollte der Port 40440 für eingehende Verbindungen auf dem Backup Storage aktiviert sein.

So können Sie den unveränderlichen Storage aktivieren

1. Melden Sie sich als Administrator am Management-Portal an und gehen Sie dann zu **Einstellungen** –> **Sicherheit**.
2. Aktivieren Sie den Schalter **Unveränderlicher Storage**.
3. Spezifizieren Sie eine Aufbewahrungsdauer in einem Bereich von 14 bis 3650 Tagen.
   Die standardmäßige Aufbewahrungsdauer beträgt 14 Tage. Eine längere Aufbewahrungsdauer führt zu einer erhöhten Speichernutzung.
4. Wählen Sie den Modus für den unveränderlichen Storage und bestätigen Sie bei entsprechender Aufforderung Ihre Wahl.
5. Klicken Sie auf **Speichern**.

   Warnung!
   Wenn Sie den **Compliance-Modus** auswählen, so kann dies nicht rückgängig gemacht werden. Wenn Sie diesen Modus ausgewählt haben, können Sie den unveränderlichen Storage nicht mehr deaktivieren und auch nicht mehr dessen Modus oder die Aufbewahrungsdauer ändern.

6. Wenn Sie erreichen wollen, dass ein vorhandenes Archiv den unveränderlichen Storage unterstützt, müssen Sie ein neues Backup in diesem Archiv erstellen.
   Führen Sie zum Erstellen eines neuen Backups den Schutzplan entweder manuell oder über eine Planung aus.

   Warnung!
   Wenn Sie ein Backup löschen, bevor Sie bewirkt haben, dass das Archiv den unveränderlichen Storage unterstützt, wird das Backup endgültig gelöscht.

So können Sie den unveränderlichen Storage deaktivieren

1. Melden Sie sich als Administrator am Management-Portal an und gehen Sie dann zu **Einstellungen** –> **Sicherheit**.
2. Deaktivieren Sie den Schalter **Unveränderlicher Storage**.

Hinweis
Sie können unveränderlichen Storage nur im Governance-Modus deaktivieren.

Warnung!
Eine Deaktivierung des unveränderlichen Storage tritt nicht sofort in Kraft. Der unveränderliche Storage bleibt für eine Frist von 14 Tagen aktiv, sodass Sie entsprechend der ursprünglichen Aufbewahrungsdauer auf die entsprechenden gelöschten Backups zugreifen können. Wenn die Frist endet, werden alle Backups im unveränderlichen Storage dauerhaft gelöscht.

3. Bestätigen Sie Ihre Auswahl, indem Sie auf **Deaktivieren** klicken.

Unterstützte Storages und Agenten

- Der unveränderliche Storage wird nur auf dem Cloud Storage unterstützt.

  Der unveränderliche Storage ist sowohl für von Acronis gehostete als auch für von Partnern gehostete Cloud Storages verfügbar, die Cyber Infrastructure 4.7.1 oder höher verwenden.

  Alle Storages, die mit dem Cyber Infrastructure Backup Gateway verwendet werden können, werden unterstützt. Zum Beispiel der Cyber Infrastructure Storage, Amazon S3- und EC2-Storages sowie der Microsoft Azure Storage.

  Der unveränderliche Storage erfordert, dass der TCP-Port 40440 für den Backup Gateway Service in Cyber Infrastructure geöffnet ist. Ab Version 4.7.1 wird der TCP-Port 40440 automatisch mit dem Traffic-Typ **Backup (ABGW) öffentlich** geöffnet. Weitere Informationen über die Traffic-Typen finden Sie in der Acronis Cyber Infrastructure-Dokumentation.
- Für den unveränderlichen Storage muss der Protection Agent in Version 21.12 (Build 15.0.28532) oder höher installiert sein.
- Es werden nur TIBX-Backups (Version 12) unterstützt.

Task-Verwaltung

Wenn Ihr Konto Zugriff auf den Advanced Automation Service beinhaltet, können Sie auf **Task-Verwaltung** klicken, wenn Sie Ihre Service Desk-Tickets einsehen und verwalten möchten.

Hinweis
Benutzer, denen in Advanced Automation die Rolle 'Client-Manager' zugewiesen wurde, können alle Service Desk-Tickets innerhalb der Organisation einsehen und verwalten. Benutzer, denen die Rolle 'Kunde' zugewiesen wurde, können nur ihre eigenen Tickets einsehen und aktualisieren.

Service Desk-Tickets einsehen

Wenn Sie auf die vorhandenen Service Desk-Tickets einsehen wollen, gehen Sie im Management-Portal zu **Task-Verwaltung –> Service Desk**. Es werden Informationen zu jedem Ticket angezeigt. Wie etwa:

- Ein Link zum Ticket.
- Der aktuelle Status des Tickets.
- Die insgesamt für das Ticket aufgewendete Zeit.
- Der Antragsteller des Tickets.
- Der Kunde.
- Die Priorität des Tickets.
- Der zugewiesene Support-Agent.
- Die zugewiesene Service-Level-Vereinbarung (SLA), wann die SLA verletzt wird und wann die nächste Aktualisierung durch einen Ticket-Techniker zu erwarten ist.
- Das Datum, an dem das Ticket zuletzt aktualisiert wurde.

Wenn Sie die Ticket-Daten exportieren wollen, klicken Sie auf **Exportieren**. Es wird eine XSL-Datei mit der Bezeichnung **Tickets** auf Ihren Workload heruntergeladen.

Sie können die angezeigte Liste auch filtern oder sortieren, um ein spezifisches Ticket zu finden. Wenn Sie eine erweiterte Filterung benötigen, können Sie mit dem Tool **Filter** genauer definieren, welche spezifischen Tickets angezeigt werden sollen.

Ein Service Desk-Ticket erstellen

So können Sie ein neues Ticket erstellen

1. Gehen Sie zu **Task-Verwaltung –> Service Desk**. Es wird eine Liste mit den offenen Tickets angezeigt.

   Hinweis
   Benutzer, denen in Advanced Automation die Rolle 'Client-Manager' zugewiesen wurde, können alle Service Desk-Tickets innerhalb der Organisation einsehen. Benutzer, denen die Rolle 'Kunde' zugewiesen wurde, können nur ihre eigenen Tickets einsehen.

2. Klicken Sie auf **+ Neu**. Das Fenster 'Neues Ticket erstellen' wird angezeigt.
3. Definieren Sie Folgendes:
   - Geben Sie im Feld **Ticket-Titel** den Titel für das Ticket ein.
   - Wählen Sie im Feld **Antragsteller** (nur für Benutzer mit der Rolle 'Client-Manager' aktiviert) den betreffenden Benutzer aus der Liste der aktiven Benutzer und Kontakte des Kunden. Beachten Sie, dass das Feld **Kundenname** sowohl für Client-Manager als auch für Benutzer vom Typ Kunden deaktiviert ist.
   - (Optional) Fügen Sie in das Feld **Telefonnummer** eine relevante Telefonnummer ein. Beachten Sie: Wenn Sie die angezeigte Standardnummer aktualisieren, wird die neue Nummer als Standardtelefonnummer dieses Benutzers gespeichert.
   - Wählen Sie im Feld **Vorgesetzter** den relevanten Benutzer aus der Liste der aktiven Kundenbenutzer (z.B. Benutzer, denen die Rolle 'Client-Manager' zugewiesen wurde).
   - Wählen Sie im Bereich **Konfigurationselement oder Service** entweder **Verwalteter Service** oder **IT-Service**:
     - **Verwalteter Service**: Diese Option wird ausgewählt und mit den relevanten Details vorausgefüllt, wenn der Produkttyp 'Verwalteter Service' im betreffenden Vertrag verfügbar ist. Beachten Sie, dass diese Option deaktiviert ist, wenn der Vertrag keine Produkte des Typs 'Verwalteter Service' enthält.
     - **IT-Service**: Diese Option wird ausgewählt und mit den relevanten Details vorausgefüllt, wenn der Produkttyp 'IT-Service' im betreffenden Vertrag verfügbar ist. Beachten Sie, dass diese Option deaktiviert ist, wenn der Vertrag keine Produkte des Typs 'IT-Service' enthält.
     - Das Feld **Konfigurationselement** zeigt die Geräte an, die mit dem ausgewählten 'Verwalteten Service' oder 'IT-Service' verbunden sind (wenn das Gerät unbekannt ist, wird **Unbekanntes KE** angezeigt). Die Auswahl eines Geräts nach der Auswahl eines Services ist optional (wenn Sie in diesem Szenario ein Gerät auswählen, wird die SLA nicht geändert, sondern bleibt die SLA, die zu dem Service gehört).

Hinweis
Zu den aufgelisteten Geräten gehören die von Cyber Protect bereitgestellten. Wenn Cyber Protection eine Remote-Steuerungsoption für ein aufgeführtes Gerät bietet, können Sie vom Ticket aus eine Remote-Verbindung über das RDP-Protokoll oder den HTML5-Client herstellen.

  - Sie können auch eine Kategorie im Feld **Kategorie** auswählen und eine Priorität im Feld **Priorität** definieren. Das Feld **SLA** kennzeichnet die SLA-Vereinbarung mit Ihrem Managed Service Provider.
- Im Bereich **Ticket-Aktualisierung** können Sie ausführliche Textbeschreibungen und Kommentare (einschließlich Bilder und andere Mediendateien mit einer maximalen Größe von 25 MB; die unterstützten Formate und Typen sind nachfolgend im Abschnitt **Anhänge** aufgeführt) in das angezeigte Textfeld eingeben. Beachten Sie, dass der Ticket-Status standardmäßig mit **Neu** festgelegt ist und nicht geändert werden kann.
- Aktivieren Sie den Optionsschalter **E-Mail an den Antragsteller senden**, um sicherzustellen, dass alle Ticket-Aktualisierungen per E-Mail an den Antragsteller gesendet werden.
- Fügen Sie im Bereich **Anhänge** alle relevanten Anhänge hinzu, indem Sie diese per Maus bzw. per Drag & Drop hinzufügen.
  Die Anhänge können jedes der folgenden Formate und Typen umfassen (bis zu einem Maximum von 25 MB):
  - Medien: .avi, .mp4, .mp3
  - E-Mails: .eml, .msg
  - Bilder: .png, .gif, .jpeg, .jpg, .heic, .bmp, .tiff, .svg
  - Dokument- und Protokolldateien: .doc, .docx, .xls, .xlsx, .ppt, .pptx, .txt, .log, .pdf
  - Archive: .zip, .rar

4. Klicken Sie auf **Fertig**. Wenn das Ticket generiert wird, wird es zur Liste der offenen Tickets hinzugefügt.

Service Desk-Tickets aktualisieren

So können Sie ein Ticket aktualisieren

1. Gehen Sie zu **Task-Verwaltung –> Service Desk**. Es wird eine Liste mit den derzeit offenen Tickets angezeigt.

Hinweis
Benutzer, denen in Advanced Automation die Rolle 'Client-Manager' zugewiesen wurde, können alle Service Desk-Tickets innerhalb der Organisation einsehen. Benutzer, denen die Rolle 'Kunde' zugewiesen wurde, können nur ihre eigenen Tickets einsehen.

2. (Optional) Wenn Sie eine große Anzahl von Tickets haben, können Sie den Filter verwenden, um ein bzw. mehrere relevante Tickets zu finden.

   Klicken Sie auf **Filter** (oder **Gespeicherte Filter**, wenn Sie bereits einen Filter definiert haben) und wählen Sie die relevanten Werte in den angezeigten Feldern aus. Beachten Sie, dass Sie auf den Optionsschalter **Zu gespeicherten Filtern hinzufügen** klicken können, wenn Sie den definierten Filter zur späteren Verwendung speichern wollen.

   Alternativ können Sie auch die Leiste **Suchen** verwenden, um ein bzw. mehrere relevante Tickets zu finden.
3. Klicken Sie auf den Link der relevanten Ticket-Zeile und nehmen Sie die gewünschten Änderungen auf den angezeigten Registerkarten vor:
   - **Aktivitäten**: Zeigt die jüngsten Aktivitäten zu einem Ticket an – darunter den aktuellen Status und die Kommentare, die zu diesem Ticket abgegeben wurden.

     Hinweis
     Wenn Sie den Status eines Tickets, das durch einen Alarm in der Cyber Protect-Konsole erstellt wurde, auf **Geschlossen** ändern, wird auch der entsprechende Alarm in der Cyber Protect-Konsole geschlossen.

   - **Überblick**: Zeigt allgemeine Ticket-Einstellungen an, die nach Bedarf geändert werden können. Weitere Informationen finden Sie im Abschnitt '"Ein Service Desk-Ticket erstellen" (S. 42)'.

     Beachten Sie, dass Sie auf dieser Registerkarte den Status des Tickets ändern können. Wenn Sie beispielsweise mit der Bearbeitung des Tickets beginnen, können Sie den Status zu **Wird bearbeitet** ändern oder ihn zu **Geschlossen** ändern, wenn das Ticket beendet werden kann. Sie können auch Geräte ändern, die mit einem Ticket verknüpft sind. Wenn beispielsweise ein Ticket erstellt wird, das nicht das richtige Gerät enthält, können Sie auf das Listenfeld **Konfigurationselement** klicken, um das relevante Gerät auszuwählen.

   Weitere Informationen über die verschiedenen Felder, die bei der Bearbeitung eines Tickets verfügbar sind, finden Sie im Abschnitt '"Ein Service Desk-Ticket erstellen" (S. 42)'.
4. Klicken Sie auf **Änderungen speichern**.

   Beachten Sie: Wenn der Umschalter **E-Mail an den Antragsteller senden** aktiviert ist, wird eine E-Mail an den betreffenden Benutzer gesendet.

Monitoring

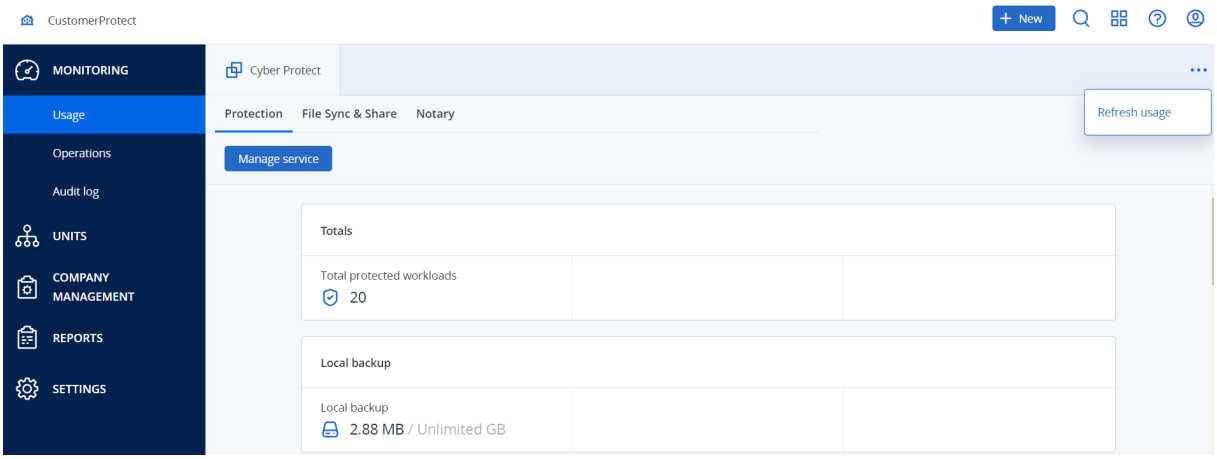
Klicken Sie auf **Monitoring**, wenn Sie Informationen über die Service-Nutzung und durchgeführte Aktionen erhalten wollen.

Nutzung

Die Registerkarte **Nutzung** ermöglicht Ihnen einen Überblick über die Service-Nutzung (inkl. Quotas, falls zutreffend) und auf die Service-Konsolen zuzugreifen.

Wenn Sie die auf der Registerkarte angezeigten Nutzungsdaten aktualisieren wollen, klicken Sie im oberen rechten Teil des Bildschirms auf das Drei-Punkte-Symbol und wählen Sie **Nutzung aktualisieren**.

Hinweis
Das Abrufen der Daten kann bis zu 10 Minuten dauern. Laden Sie die Seite neu, damit die aktualisierten Daten angezeigt werden.



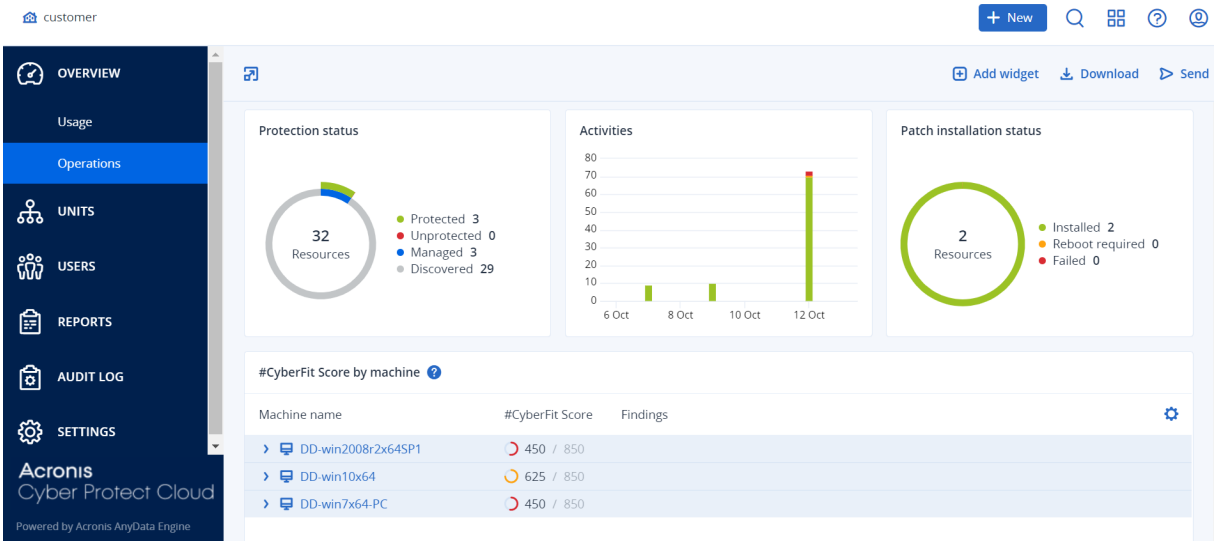
Aktionen-Dashboard

Das Dashboard **Aktionen** ist nur für Firmenadministratoren verfügbar, wenn diese auf Firmenebene arbeiten.

Das Dashboard **Aktionen** enthält eine Reihe benutzerdefinierbarer Widgets, die Ihnen einen Überblick über diejenigen Aktionen geben, die im Zusammenhang mit dem Cyber Protection Service stehen.

Die Widgets werden alle zwei Minuten aktualisiert. Die Widgets haben anklickbare Elemente, über die Sie Probleme untersuchen und beheben können. Sie können den aktuellen Zustand des Dashboards in Form einer .pdf- und/oder .xlsx-Datei herunterladen oder als E-Mail versenden.

Sie können aus einer Vielzahl von Widgets wählen, die als Tabellen, Torten- und Balkendiagramme, Listen und Treemaps (Kacheldiagramm mit Baumstruktur) angezeigt werden. Sie können mehrere Widgets desselben Typs hinzufügen, die aber unterschiedliche Filter verwenden.



So können Sie die Widgets auf dem Dashboard neu anordnen

Verschieben Sie die Widgets per Drag & Drop-Aktion, indem Sie zuvor auf deren Namen klicken.

So können Sie ein Widget bearbeiten

Klicken Sie neben dem Widget-Namen auf das Stiftsymbol. Mit der Funktion 'Bearbeiten' können Sie ein Widget umbenennen, den Zeitraum ändern und Filter festlegen.

So können Sie ein Widget hinzufügen

Klicken Sie auf **Widget hinzufügen** und gehen Sie dann nach einer der folgenden Möglichkeiten vor:

- Klicken Sie auf das hinzuzufügende Widget. Das Widget wird daraufhin mit den Standardeinstellungen hinzugefügt.
- Wenn Sie das Widgeht vor dem Hinzufügen bearbeiten wollen, dann klicken Sie nach der Auswahl des Widgets auf das Stiftsymbol. Klicken Sie, nachdem Sie das Widget bearbeitet haben, auf **Fertig**.

So können Sie ein Widget entfernen

Klicken Sie neben dem Widget-Namen auf das X-Symbol.

Schutzstatus

Schutzstatus

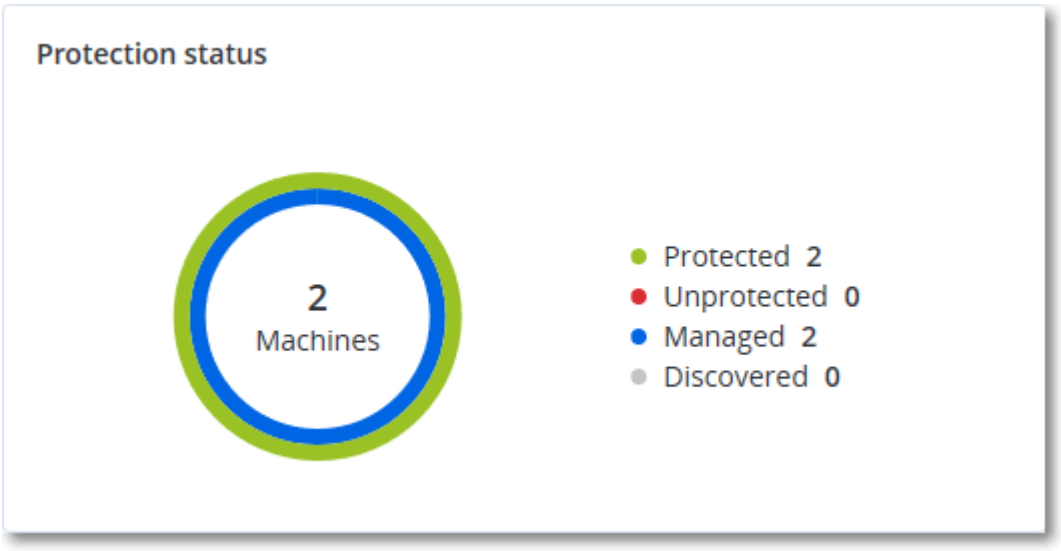
Dieses Widget zeigt den aktuellen Sicherungsstatus für alle Maschinen an.

Eine Maschine kann sich in einem der folgenden Statuszustände befinden:

- **Geschützt** – Maschinen, auf die ein Schutzplan angewendet wurde.

- **Ungeschützt** – Maschinen, auf die noch kein Schutzplan angewendet wurde. Dazu gehören sowohl erkannte als auch verwaltete Maschinen, auf die noch kein Schutzplan angewendet wurde.
- **Verwaltet** – Maschinen, auf denen ein Protection Agent installiert ist.
- **Erkannt** – Maschinen, auf denen kein Protection Agent installiert ist.

Wenn Sie auf den Maschinenstatus klicken, werden Sie zu der Liste der Maschinen mit diesem Status weitergeleitet, um weitere Details zu erhalten.



Erkannte Maschinen

Dieses Widget zeigt die Liste der erkannten Maschinen während eines spezifizierten Zeitraums an.

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

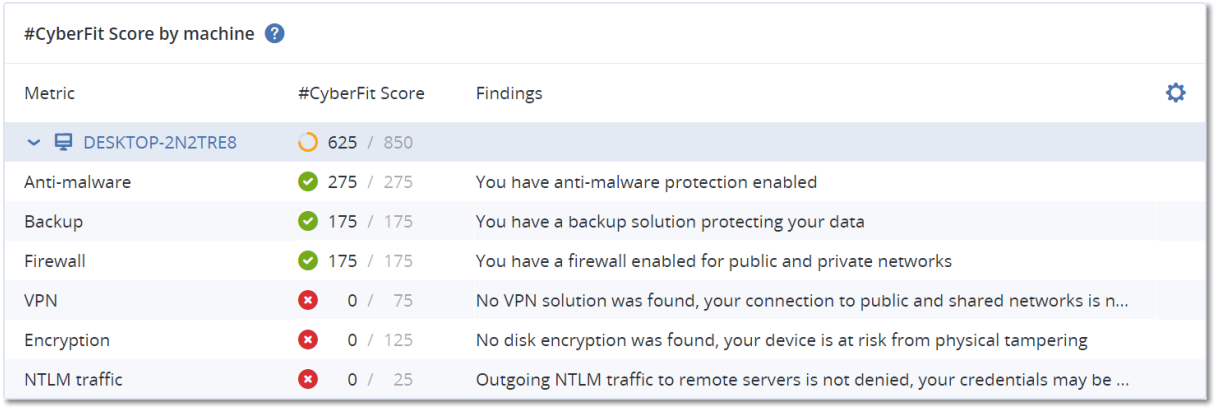
#CyberFit-Score pro Maschine

Dieses Widget zeigt für jede Maschine den #CyberFit-Gesamt-Score und die Einzel-Scores an, aus denen sich dieser Gesamtwert zusammensetzt – sowie die Ergebnisse für jede der bewerteten Metriken:

- Antimalware
- Backup
- Firewall
- VPN
- Verschlüsselung
- NTLM-Traffic

Wenn Sie den Score einer einzelnen Metrik verbessern wollen, können Sie die Empfehlungen einsehen, die in Form eines Berichts verfügbar sind.

Weitere Informationen über den #CyberFit-Score finden Sie im Abschnitt '#CyberFit-Score für Maschinen'.



Endpoint Detection & Response (EDR)-Widgets

Wichtig
Dies ist eine Early Access-Version der EDR-Dokumentation. Einige der Funktionen und Beschreibungen können daher noch unvollständig sein.

Die Endpoint Detection & Response (EDR)-Funktionalität umfasst eine Reihe von Widgets, auf die über das Dashboard **Aktionen** zugegriffen werden kann.

Folgende Widgets sind verfügbar:

- Spitzenverteilung der Vorfälle pro Workload
- MTTR (Mittlere Problemlösungszeit) für Vorfälle

- Sicherheitsvorfall-Burndown
- Workload-Netzwerkstatus

Spitzenverteilung der Vorfälle pro Workload

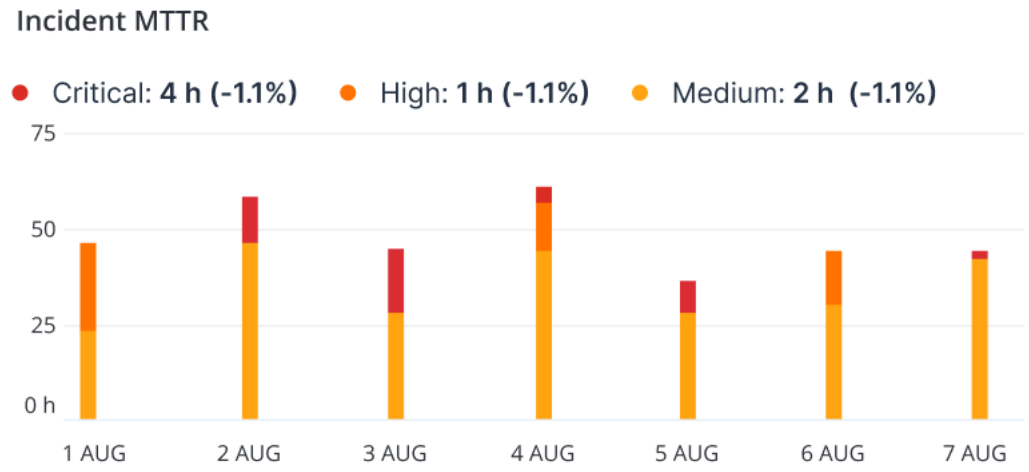
Dieses Widget zeigt die fünf Workloads mit den meisten Vorfällen an (klicken Sie auf **Alle anzeigen**, um zur Vorfallsliste zu gelangen, die entsprechend den Widget-Einstellungen gefiltert wird).

Bewegen Sie den Mauszeiger über eine Workload-Zeile, um eine Aufschlüsselung des aktuellen Untersuchungsstadiums für die Vorfälle angezeigt zu bekommen; die Untersuchungsstadien sind **Nicht gestartet**, **Wird untersucht**, **Geschlossen** und **Falsch positiv**. Klicken Sie anschließend auf einen Workload, den Sie weiter analysieren wollen, und wählen Sie den entsprechenden Kunden im angezeigten Pop-up-Fenster aus. Die Vorfallsliste wird entsprechend den Einstellungen des Widgets aktualisiert.

MTTR (Mittlere Problemlösungszeit) für Vorfälle

Dieses Widget zeigt die durchschnittliche Problemlösungszeit für Sicherheitsvorfälle an. Sie gibt an, wie schnell Vorfälle untersucht und gelöst werden.

Klicken Sie auf eine Spalte, um die Vorfälle nach ihrem Schweregrad (**Kritisch**, **Hoch** und **Mittel**) aufzuschlüsseln und zu sehen, wie lange es dauerte, die verschiedenen Schweregrade zu beheben. Der in Klammern angegebene Prozentwert gibt den Anstieg bzw. den Rückgang im Vergleich zum vorherigen Zeitraum an.

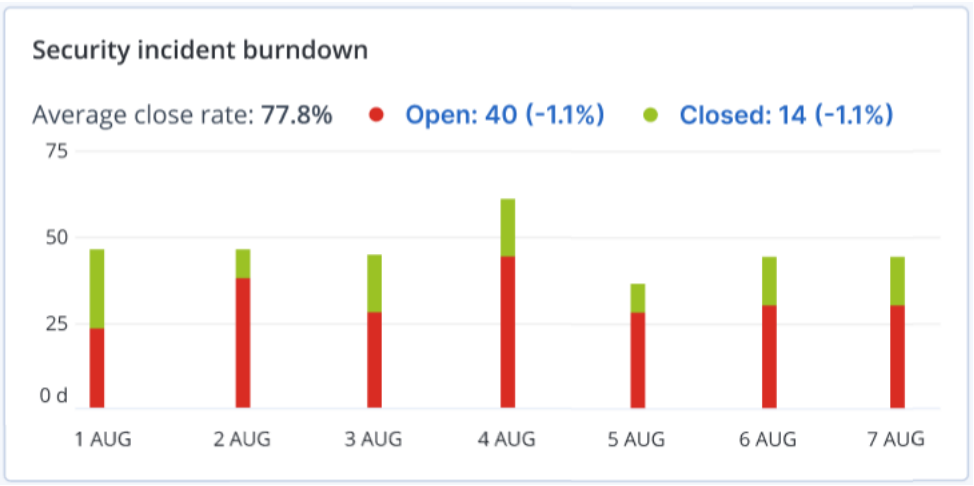


Sicherheitsvorfall-Burndown

Dieses Widget zeigt die Effizienzrate bei der Schließung von Vorfällen an; die Anzahl der offenen Vorfälle wird dabei mit der Anzahl der geschlossenen Vorfälle über einen bestimmten Zeitraum abgeglichen.

Bewegen Sie den Mauszeiger über eine Spalte, um eine Aufschlüsselung der geschlossenen und offenen Vorfälle für den jeweiligen Tag angezeigt zu bekommen. Wenn Sie auf das Element 'Öffnen' klicken, wird ein Pop-up-Fenster angezeigt, in dem Sie den entsprechenden Mandanten auswählen können. Daraufhin wird die gefilterte Vorfallsliste für den betreffenden Mandanten aufgerufen, um die derzeit offenen Vorfälle anzuzeigen (die das Stadium **Wird untersucht** oder **Nicht gestartet** haben). Wenn Sie auf das Element "Geschlossen" klicken, wird die Vorfallsliste für den betreffenden Mandanten angezeigt und so gefiltert, dass nur noch die Vorfälle angezeigt werden, die nicht mehr offen sind (die also das Stadium **Geschlossen** oder **Falsch positiv** haben).

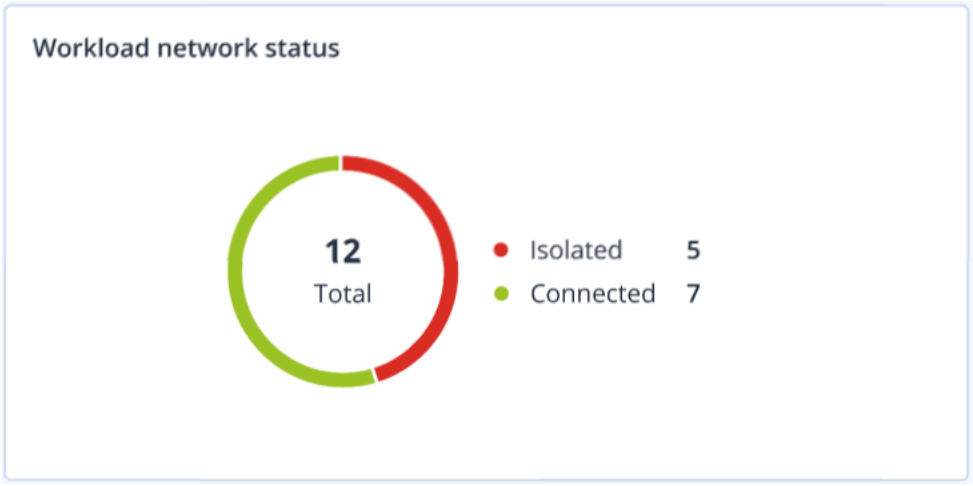
Der in Klammern angegebene Prozentwert gibt den Anstieg bzw. den Rückgang im Vergleich zum vorherigen Zeitraum an.



Workload-Netzwerkstatus

Dieses Widget zeigt den aktuellen Netzwerkstatus für Ihre Workloads an und informiert darüber, wie viele Workloads isoliert und wie viele verbunden sind.

Wenn Sie auf das Element 'Isoliert' klicken, wird ein Pop-up-Fenster angezeigt, in dem Sie den entsprechenden Mandanten auswählen können. Die dargestellte Workload-Ansicht wird gefiltert, sodass nur noch die isolierten Workloads angezeigt werden. Wenn Sie auf das Element 'Verbunden' klicken, wird die Liste 'Workload mit Agenten' angezeigt, die so gefiltert ist, dass die verbundenen Workloads (für den ausgewählten Mandanten) angezeigt werden.



Überwachung der Laufwerksintegrität

Die Überwachung der Laufwerksintegrität liefert Informationen über den aktuellen Laufwerksintegritätsstatus sowie eine Vorhersage über diesen. Dadurch können Sie Datenverluste vorab verhindern, die durch einen Laufwerksausfall verursacht werden könnten. Es werden sowohl Laufwerke vom Typ HDD (klassische Festplatten) als auch SSD (Flash-Speicher basierte Laufwerke) unterstützt.

Einschränkungen

- Die Vorhersage zur Laufwerksintegrität wird nur für Maschinen unterstützt, die unter Windows laufen.
- Es können nur Laufwerke von physischen Maschinen überwacht werden. Die Laufwerke von virtuellen Maschinen können nicht überwacht werden und werden daher auch nicht in den Laufwerksintegrität-Widgets angezeigt.
- RAID-Konfigurationen werden nicht unterstützt. Die Laufwerksintegrität-Widgets enthalten keine Informationen über Maschinen mit RAID-Implementierung.
- NVMe-SSDs werden nicht unterstützt.

Die Laufwerksintegrität wird durch folgende Statuszustände dargestellt:

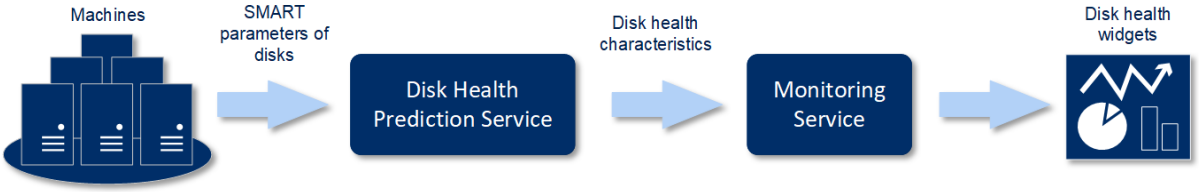
- **OK**
  Die Laufwerksintegrität liegt zwischen 70% und 100%.
- **Warnung**
  Die Laufwerksintegrität liegt zwischen 30% und 70%.
- **Kritisch**
  Die Laufwerksintegrität liegt zwischen 0% und 30%.
- **Laufwerksdaten werden berechnet**
  Der aktuelle Laufwerksstatus und die Vorhersage werden ermittelt.

Und so funktioniert es

Der Disk Health Prediction Service verwendet ein auf künstlicher Intelligenz (KI) basierendes Vorhersagemodell.

1. Der Protection Agent sammelt die SMART-Parameter der Laufwerke und übermittelt diese Daten an den Disk Health Prediction Service:
   - SMART 5 – Reallocated Sectors Count (Anzahl neu zugewiesener Sektoren).
   - SMART 9 – Power-On Hours (Einschaltzeit).
   - SMART 187 – Reported Uncorrectable Errors (Gemeldete unkorrigierbare Fehler).
   - SMART 188 – Command Timeout (Befehls-Timeout, wegen Zeitüberschreitung abgebrochene Befehle).
   - SMART 197 – Current Pending Sector Count (Anzahl derzeit ausstehender Sektoren).
   - SMART 198 – Offline Uncorrectable Sector Count (Anzahl nicht korrigierbarer Sektoren).
   - SMART 200 – Write Error Rate (Fehlerrate beim Schreiben).
2. Der Disk Health Prediction Service verarbeitet die empfangenen SMART-Parameter, trifft Vorhersagen und stellt dann folgende Laufwerksintegritätsmerkmale bereit:
   - Aktueller Laufwerksintegritätsstatus: OK, Warnung, Kritisch.
   - Vorhersage zur Laufwerksintegrität: negativ, stabil, positiv.
   - Vorhersage-Wahrscheinlichkeit der Laufwerksintegrität in Prozent.

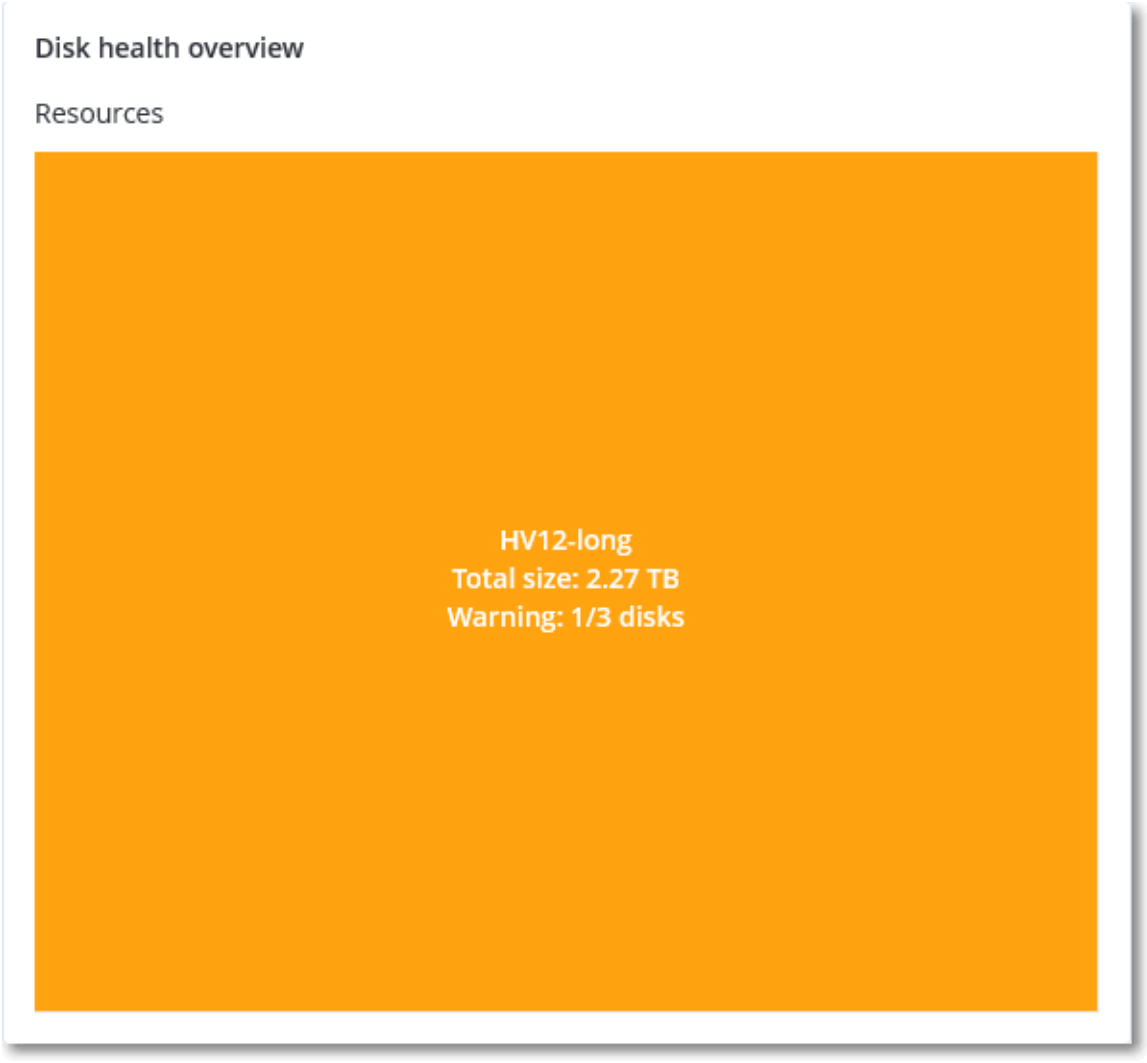
   Der Vorhersagezeitraum beträgt ein Monat.
3. Der Monitoring Service empfängt diese Merkmale und zeigt die entsprechenden Informationen dann in den Laufwerksintegrität-Widgets der Cyber Protect-Konsole an.



Laufwerksintegrität-Widgets

Die Ergebnisse der Laufwerksintegritätsüberwachung werden in folgenden Widgets dargestellt, die in der Cyber Protect-Konsole verfügbar sind.

- **Überblick der Laufwerksintegrität** ist ein Treemap-Widget (Kacheldiagramm mit Baumstruktur) mit zwei Detailebenen, zwischen denen umgeschaltet werden kann.
  - Maschinenebene
    Zeigt zusammengefasste Informationen über den Laufwerksintegritätsstatus für die ausgewählten Kundenmaschinen an. Es werden nur die kritischsten Laufwerkstatuszustände angezeigt. Die anderen Statuszustände werden in einem Tooltip angezeigt, wenn Sie mit dem Mauszeiger über einen bestimmten Block fahren. Die Blockgröße der Maschine hängt von der Gesamtgröße aller Laufwerke dieser Maschine ab. Die Blockfarbe der Maschine hängt vom kritischsten Laufwerksstatus ab, der gefunden wurde.

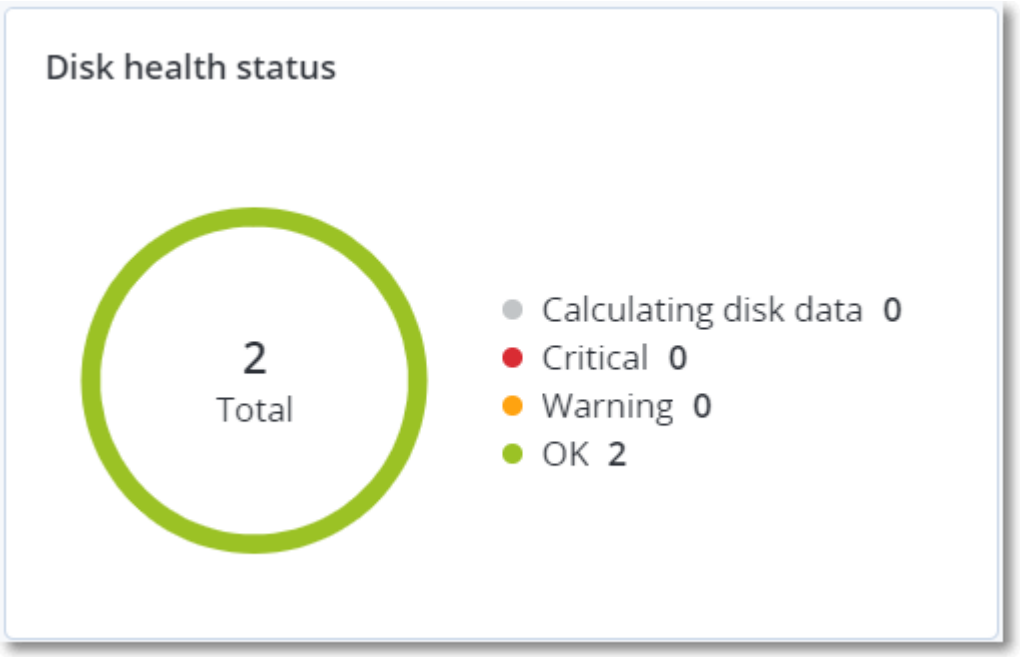


  - Laufwerksebene
    Zeigt den aktuellen Laufwerksintegritätsstatus aller Laufwerke für die ausgewählte Maschine an. Jeder Laufwerksblock zeigt eine der nachfolgenden Vorhersagen zur Laufwerksintegrität

sowie die dazugehörige Wahrscheinlichkeit (in Prozent) an:

- Wird heruntergestuft
- Wird stabil bleiben
- Wird verbessert

- **Laufwerksintegritätsstatus** ist ein Kreisdiagramm-Widget, welches die Anzahl der Laufwerke für jeden Status anzeigt.



Alarmmeldungen zum Laufwerksintegritätsstatus

Die Laufwerksintegritätsprüfung wird alle 30 Minuten durchgeführt, während die entsprechende Alarmmeldung nur einmal täglich generiert wird. Wenn sich der Laufwerksintegritätsstatus von **Warnung** zu **Kritisch** ändert, wird immer ein Alarm generiert.

Alarmbezeichnung	Schweregrad	Laufwerksintegritätsstatus	Beschreibung
Laufwerksausfall ist möglich	Warnung	(30 – 70)	Das Laufwerk <Laufwerksname> auf dieser Maschine wird wahrscheinlich demnächst ausfallen. Sichern Sie das Laufwerk möglichst bald mit einem vollständigen Image-Backup. Bauen Sie dann ein Ersatzlaufwerk ein und stellen Sie das Image auf diesem wieder her.
Laufwerksausfall steht unmittelbar bevor	Kritisch	(0 – 30)	Das Laufwerk <Laufwerksname> auf dieser Maschine befindet sich in einem kritischen Zustand und wird höchstwahrscheinlich sehr bald ausfallen. Wir raten davon ab, jetzt noch ein Image-Backup des

			Laufwerks zu erstellen, da die zusätzliche Belastung zum endgültigen Laufwerksausfall führen könnte. Versuchen Sie, die wichtigsten Dateien auf dem Laufwerk umgehend zu sichern und es dann auszutauschen.

Data Protection-Karte

Die Funktion 'Data Protection-Karte' ermöglicht es Ihnen, alle für Sie wichtigen Daten zu ermitteln sowie ausführliche Informationen über Anzahl, Größe, Speicherort und Sicherungsstatus aller wichtigen Dateien in Form einer skalierbaren Treemap-Anzeige (Kacheldiagramm mit Baumstruktur) zu erhalten.

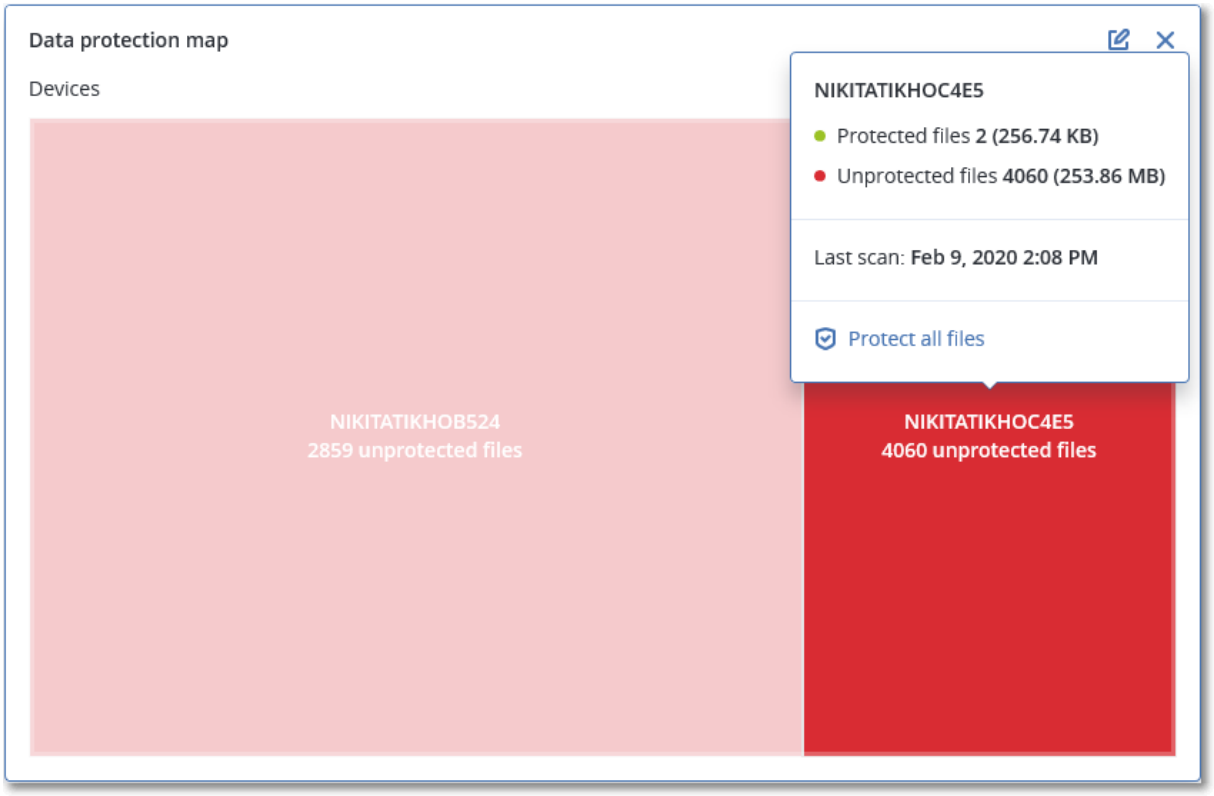
Jede Blockgröße hängt von der Gesamtzahl/Größe aller wichtigen Dateien ab, die zu einem Kunden/einer Maschine gehören.

Dateien können einen der folgenden Schutzstatus-Zustände haben:

- **Kritisch** – es gibt 1-20% ungeschützte Dateien mit den von Ihnen spezifizierten Erweiterungen, die für die/den ausgewählte(n) Maschine/Speicherort nicht per Backup gesichert wurden und mit den vorhandenen Backup-Einstellungen nicht gesichert werden.
- **Niedrig** – es gibt 21-50% ungeschützte Dateien mit den von Ihnen spezifizierten Erweiterungen, die für die/den ausgewählte(n) Maschine/Speicherort nicht per Backup gesichert wurden und mit den vorhandenen Backup-Einstellungen nicht gesichert werden.
- **Mittel** – es gibt 1-20% ungeschützte Dateien mit den von Ihnen spezifizierten Erweiterungen, die für die/den ausgewählte(n) Maschine/Speicherort nicht per Backup gesichert wurden und mit den vorhandenen Backup-Einstellungen nicht gesichert werden.
- **Hoch** – alle Dateien mit den von Ihnen spezifizierten Erweiterungen wurden für die/den ausgewählte(n) Maschine/Speicherort per Backup gesichert.

Alle Ergebnisse der Data Protection-Untersuchtung können auf dem Dashboard im Data Protection-Karten-Widget gefunden werden – einem Treemap-Widget, welches die Details auf Maschinenebene anzeigt:

- Maschinenebene – zeigt Informationen über den Schutzstatus wichtiger Dateien für die Maschinen des ausgewählten Kundens an.



Wenn Sie bisher noch ungesicherte Dateien schützen wollen, müssen Sie mit dem Mauszeiger über den Block fahren und dann auf den Befehl **Alle Dateien schützen** klicken. Im Dialogfenster finden Sie Informationen zur Anzahl der ungeschützten Dateien und zu deren Speicherort. Wenn Sie diese sichern wollen, klicken Sie auf **Alle Dateien schützen**.

Sie können außerdem einen ausführlichen Bericht im CSV-Format herunterladen.

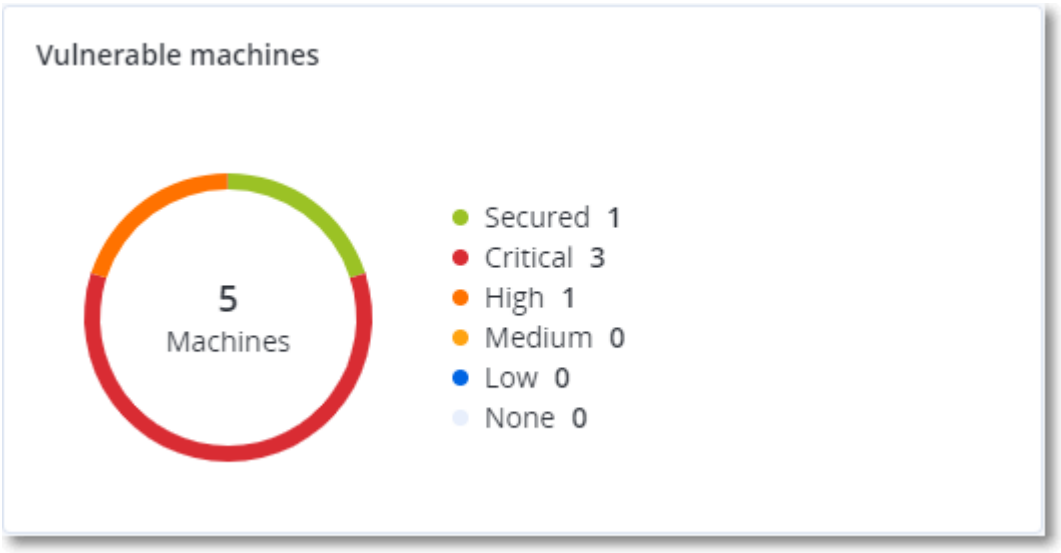
Widget für Schwachstellenbewertung

Verwundbare Maschinen

Dieses Widget zeigt die verwundbaren Maschinen nach dem Verwundbarkeitsgrad an.

Die gefundene Schwachstelle kann gemäß CVSS v3.0 (Common Vulnerability Scoring System) einen der folgenden Schweregrade haben:

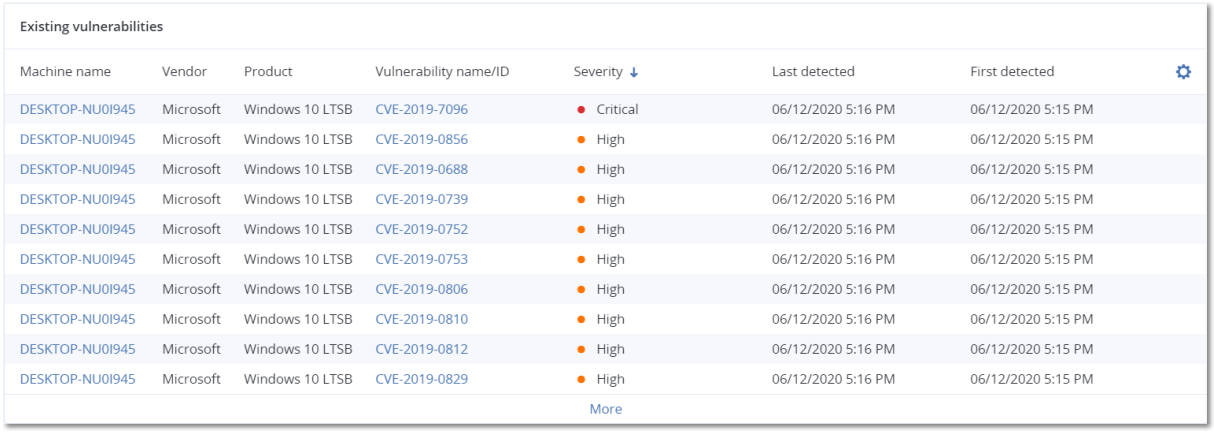
- Gesichert: es wurden keine Schwachstellen gefunden
- Kritisch: 9.0 - 10.0 CVSS
- Hoch: 7.0 - 8.9 CVSS
- Mittel: 4.0 - 6.9 CVSS
- Niedrig: 0.1 - 3.9 CVSS
- Ohne: 0.0 CVSS



Vorhandene Schwachstellen

Dieses Widget zeigt die derzeit vorhandenen Schwachstellen auf Maschinen an. Im Widget **Vorhandene Schwachstellen** gibt es zwei Spalten mit Zeitstempeln:

- **Zuerst erkannt** – Datum und Uhrzeit, als die Schwachstelle erstmals auf der Maschine erkannt wurde.
- **Zuletzt erkannt** – Datum und Uhrzeit, als die Schwachstelle das letzte Mal auf der Maschine erkannt wurde.



Widgets für Patch-Installation

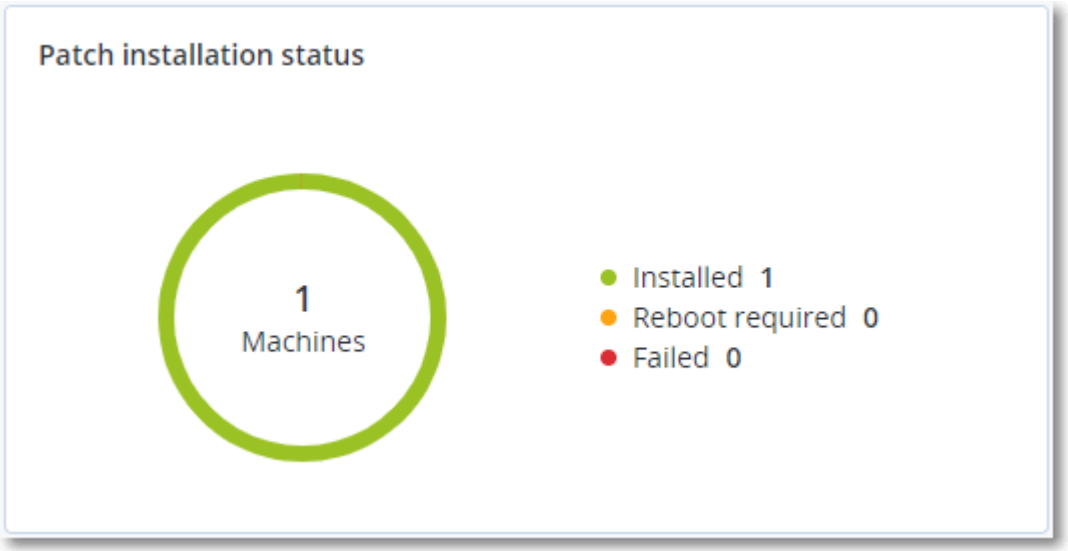
Es gibt vier Widgets im Zusammenhang mit der Patch-Verwaltungsfunktionalität.

Status der Patch-Installation

Dieses Widget zeigt die Anzahl der Maschinen gruppiert nach dem Status des Patch-Installation an.

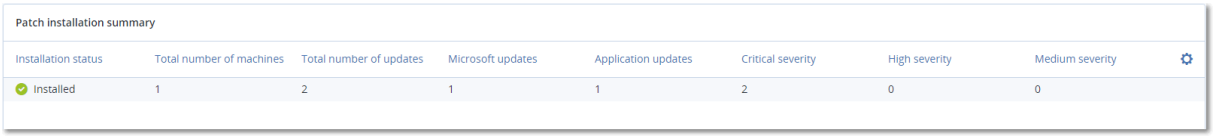
- **Installiert** – alle verfügbaren Patches sind auf einer Maschine installiert
- **Neustart erforderlich** – nach einer Patch-Installation muss eine Maschine neu gestartet werden

- **Fehlgeschlagen** – die Patch-Installation ist auf einer Maschine fehlgeschlagen



Übersicht der Patch-Installation

Dieses Widget zeigt eine Übersicht der Patches auf den Maschinen an, gruppiert nach dem Status des Patch-Installation.



Verlauf der Patch-Installation

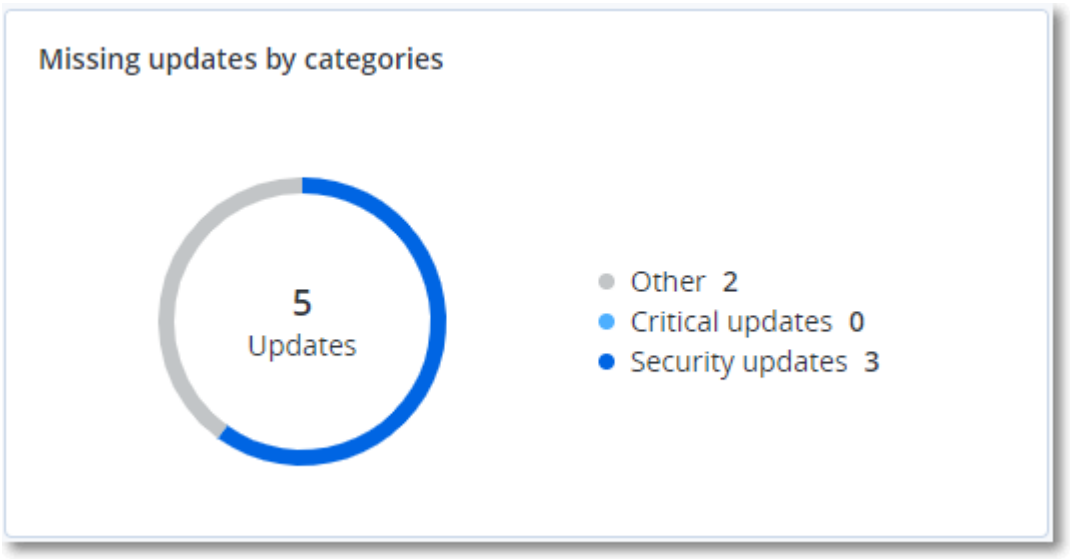
Dieses Widget zeigt ausführliche Informationen über die Patches auf den Maschinen an.

Fehlende Updates nach Kategorie

Dieses Widget zeigt die Anzahl der fehlenden Updates nach Kategorie an. Folgende Kategorien werden angezeigt:

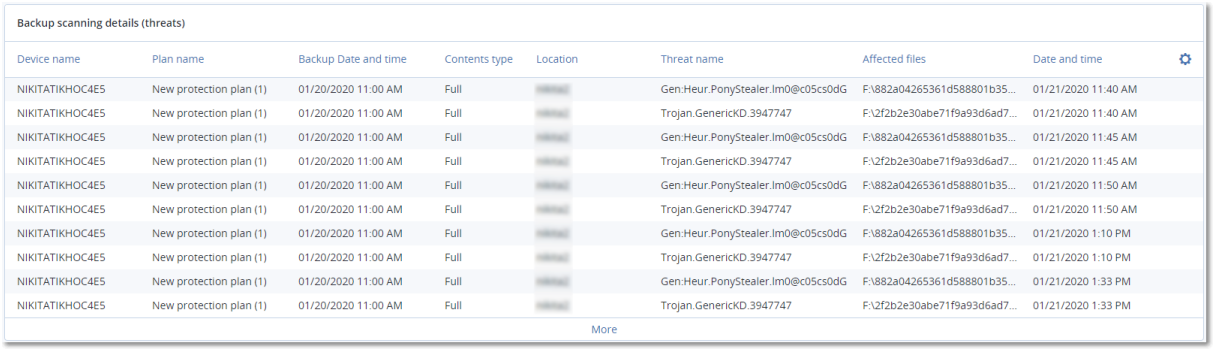
- Sicherheitsupdates
- Kritische Updates

- Anderer



Backup-Scanning-Details

Dieses Widget zeigt ausführliche Informationen über erkannte Bedrohungen in den Backups an.

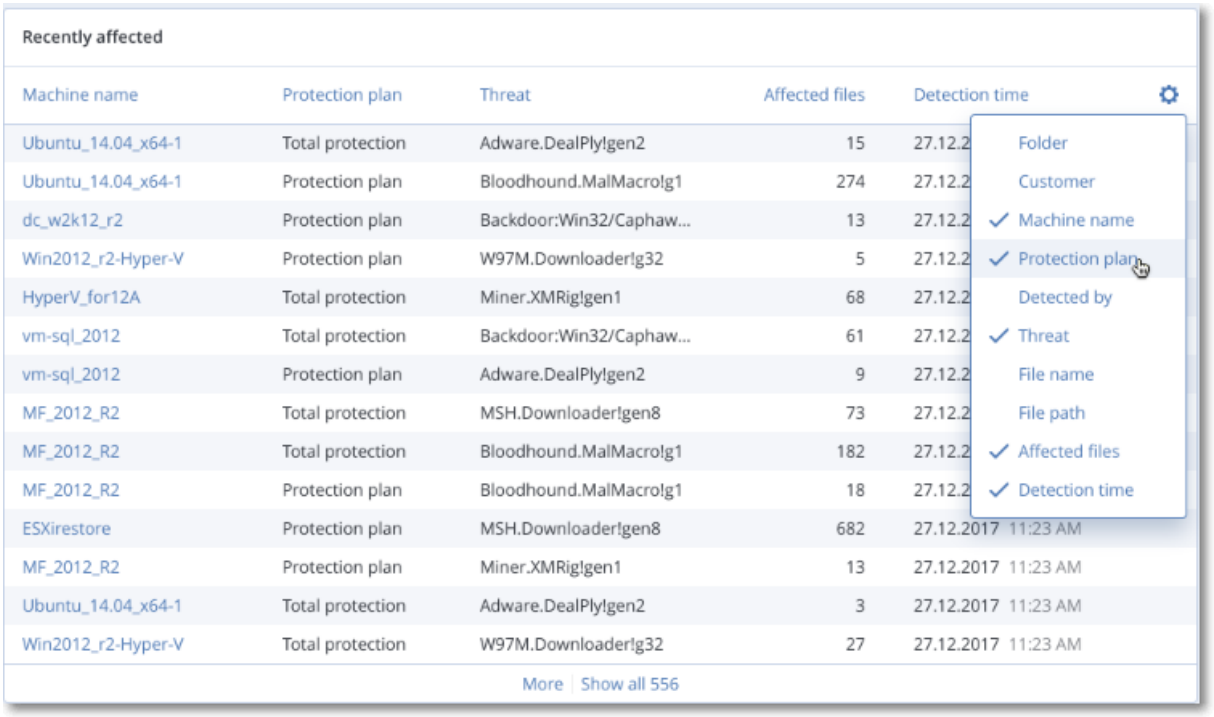

Backup scanning details (threats)

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	[redacted]	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	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	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	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	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	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	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	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	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	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:33 PM

More

Kürzlich betroffen

Dieses Widget zeigt detaillierte Informationen über Workloads an, die von Bedrohungen wie Viren, Malware und Ransomware betroffen waren. Sie können hier Informationen über die erkannten Bedrohungen, den Zeitpunkt der Erkennung sowie die Anzahl der betroffenen Dateien finden.



Daten für kürzlich betroffene Workloads herunterladen

Sie können die Daten für kürzlich betroffene Workloads herunterladen, eine CSV-Datei generieren und diese dann an die von Ihnen spezifizierten Empfänger senden.

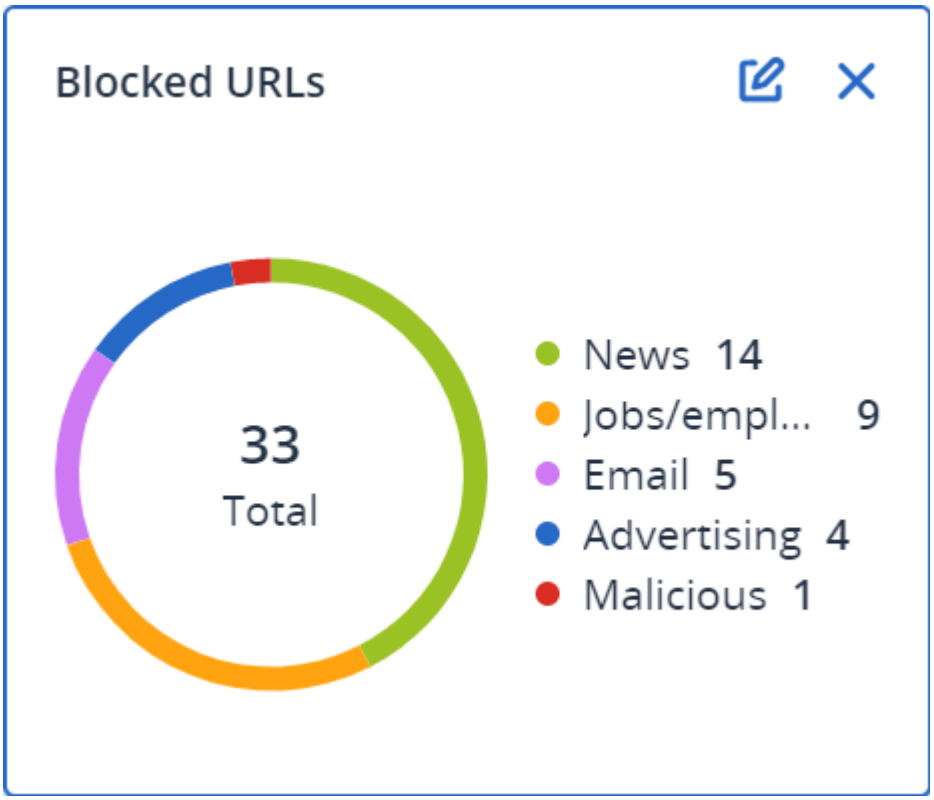
So laden Sie die Daten für kürzlich betroffene Workloads herunter

1. Klicken Sie im Widget **Kürzlich betroffen** auf den Befehl **Daten herunterladen**.
2. Geben Sie im Feld **Zeitraum** die Anzahl der Tage ein, für die Sie Daten herunterladen wollen. Die maximale Anzahl der Tage, die Sie eingeben können, beträgt 200.
3. Geben Sie im Feld **Empfänger** die E-Mail-Adressen aller Personen ein, die eine E-Mail mit einem Link zum Herunterladen der CSV-Datei erhalten sollen.
4. Klicken Sie auf **Download**.

   Das System beginnt dann damit, die CSV-Datei mit den Daten für diejenigen Workloads zu generieren, die in dem von Ihnen spezifizierten Zeitraum betroffen waren. Wenn die CSV-Datei vollständig ist, sendet das System eine E-Mail an die Empfänger. Jeder Empfänger kann dann diese CSV-Datei herunterladen.

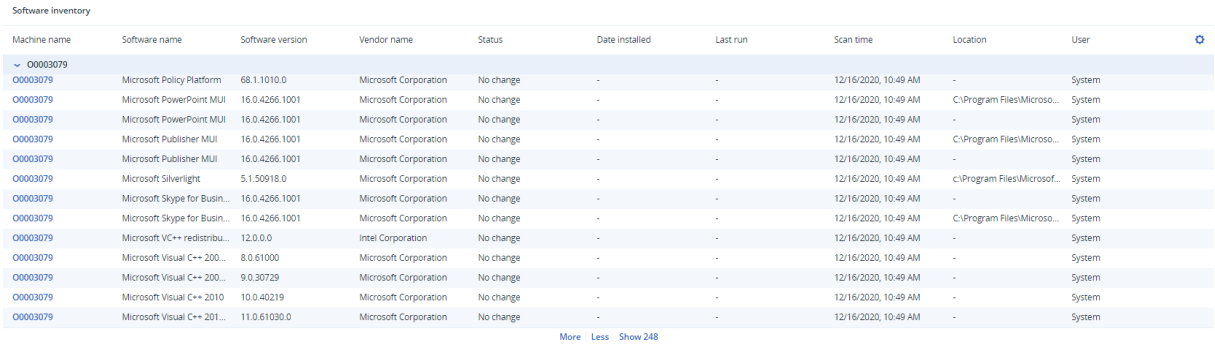
Blockierte URLs

Das Widget zeigt die Statistiken der blockierten URLs nach Kategorie an. Weitere Informationen zum Filtern und Kategorisieren von URLs/Websites finden Sie in der Cyber Protection-Benutzeranleitung.



Widgets für Software-Inventarisierung

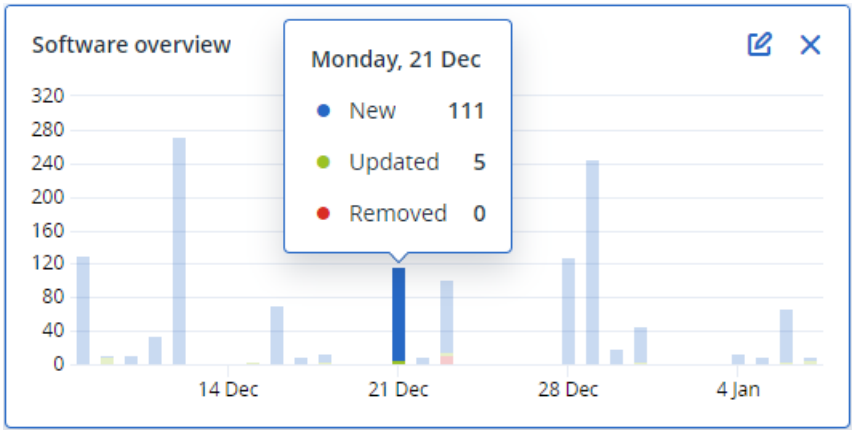
Das Tabellen-Widget **Software-Inventarisierung** zeigt ausführliche Informationen über die gesamte Software an, die auf den physischen Windows- und macOS-Maschinen in Ihrem Unternehmen installiert ist.


Software inventory

Machine name	Software name	Software version	Vendor name	Status	Date installed	Last run	Scan time	Location	User
O0003079									
O0003079	Microsoft Policy Platform	68.1.1010.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft PowerPoint MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
O0003079	Microsoft PowerPoint MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Publisher MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
O0003079	Microsoft Publisher MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Silverlight	5.1.50918.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	c:\Program Files\Microsof...	System
O0003079	Microsoft Skype for Busin...	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Skype for Busin...	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
O0003079	Microsoft VC++ redistribu...	12.0.0.0	Intel Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Visual C++ 200...	8.0.61000	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Visual C++ 200...	9.0.30729	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Visual C++ 2010	10.0.40219	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Visual C++ 201...	11.0.61030.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System

More Less Show 248

Das Widget **Software-Überblick** zeigt die Anzahl der neuen, aktualisierten oder gelöschten Applikationen auf Windows- und macOS-Maschinen in Ihrem Unternehmen für einen spezifizierten Zeitraum (7 Tage, 30 Tage oder den aktuellen Monat) an.



Wenn Sie den Mauszeiger über einen bestimmten Balken im Diagramm halten, wird ein Tooltip mit folgenden Informationen angezeigt:

Neu – die Anzahl der neu installierten Applikationen.

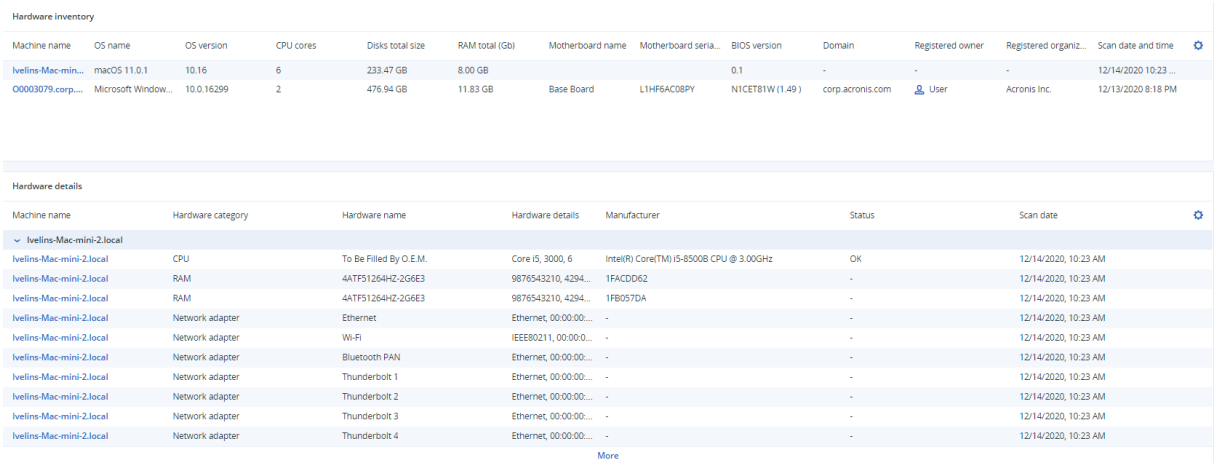
Aktualisiert – die Anzahl der aktualisierten Applikationen.

Entfernt – die Anzahl der entfernten Applikationen.

Wenn Sie auf den Balkenteil für einen bestimmten Status klicken, werden Sie zur Seite **Software-Verwaltung** –> **Software-Inventarisierung** weitergeleitet. Die Informationen auf dieser Seite werden nach dem entsprechenden Datum und Status gefiltert.

Widgets für Hardware-Inventarisierung

Die Tabellen-Widgets **Hardware-Inventarisierung** und **Hardware-Details** zeigen Informationen über alle Hardware an, die von den physischen und virtuellen Windows- sowie macOS-Geräten in Ihrem Unternehmen verwendet wird.



Das Tabellen-Widget **Hardware-Änderungen** zeigt Informationen über hinzugefügte, entfernte oder geänderte Hardware auf physischen und virtuellen Windows- sowie macOS-Geräten in Ihrem Unternehmen für einen spezifizierten Zeitraum (7 Tage, 30 Tage oder den aktuellen Monat) an.

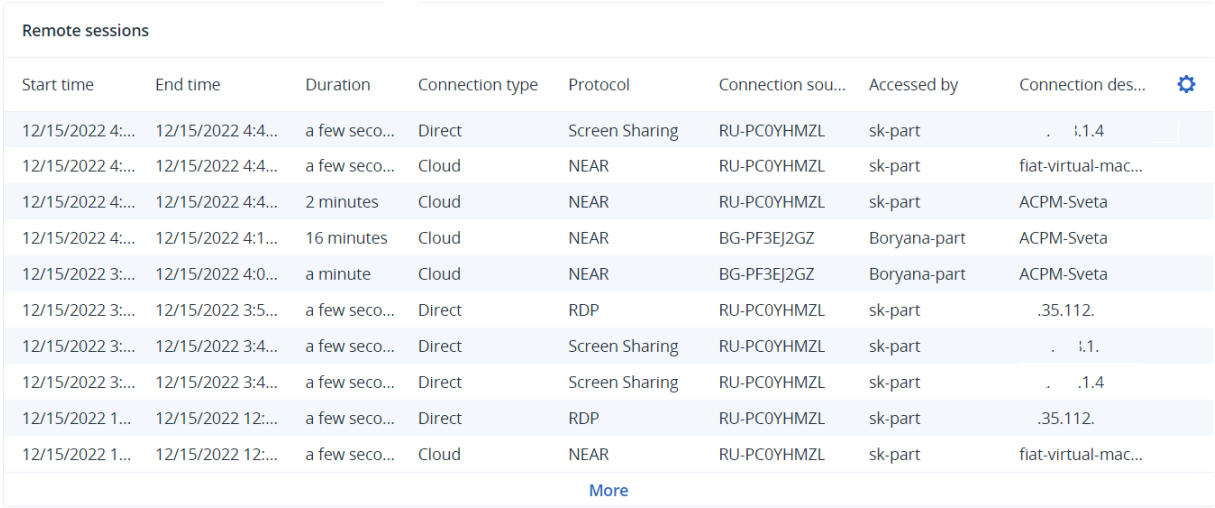
Hardware changes

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, Torronto 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

Sitzungsverlauf

Das Widget zeigt detaillierte Informationen über die Remote-Desktop- und Dateiübertragungssitzungen an, die in Ihrer Organisation während eines bestimmten Zeitraums durchgeführt wurden.



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	. .1.4
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.
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

Überwachungsprotokoll

So können Sie das Überwachungsprotokoll (Audit-Log) einsehen wollen, gehen Sie zu **Monitoring** –> **Überwachungsprotokoll**

Das Überwachungsprotokoll stellt eine chronologische Aufzeichnung über folgende Ereignisse bereit:

- Aktionen, die von den Benutzern im Management-Portal durchgeführt werden
- Aktionen mit Cloud-zu-Cloud-Ressourcen, die von Benutzern in der Cyber Protect-Konsole durchgeführt werden
- Cyber Scripting-Aktionen, die von Benutzern in der Cyber Protect-Konsole durchgeführt werden
- Systemmeldungen über erreichte Quotas und deren Nutzung

Das Protokoll (Log) zeigt Ereignisse für die Organisation oder die Abteilung (und deren Unterabteilungen) an, in der Sie sich gerade befinden. Klicken Sie auf ein Ereignis, wenn Sie mehr Informationen darüber erhalten wollen.

Überwachungsprotokolle (Audit-Logs) werden im Datacenter gespeichert, sodass deren Verfügbarkeit nicht durch Probleme auf den Endbenutzer-Maschinen beeinträchtigt werden kann.

Das Protokoll wird einmal täglich bereinigt. Die Ereignisse werden nach 180 Tagen gelöscht.

Felder im Überwachungsprotokoll

Für jedes Ereignis zeigt das Protokoll Folgendes an:

- **Ereignis**
  Eine kurze Beschreibung des Ereignisses. Beispiele: **Mandant wurde erstellt**, **Mandant wurde gelöscht**, **Benutzer wurde erstellt**, **Benutzer wurde gelöscht**, **Quota wurde erreicht**, **Backup-Inhalt wurde durchsucht**, **Skript wurde geändert**.
- **Schweregrad**
  Folgende Werte sind möglich:
  - **Fehler**
    Kennzeichnet einen Fehler.
  - **Warnung**
    Kennzeichnet eine potenziell negative Aktion. Beispiele: **Mandant wurde gelöscht**, **Benutzer wurde gelöscht**, **Quota wurde erreicht**.
  - **Hinweis**
    Kennzeichnet ein Ereignis, das möglicherweise eine Benutzerinteraktion erfordert. Beispiele: **Tenant wurde aktualisiert**, **Benutzer wurde aktualisiert**.
  - **Informationell**
    Kennzeichnet eine neutrale Information oder Aktion. Beispiele: **Mandant wurde erstellt**, **Benutzer wurde erstellt**, **Quota wurde aktualisiert**, **Skripting-Plan wurde gelöscht**.
- **Datum**
  Datum und Zeitpunkt, als das Ereignis auftrat.
- **Objektname**
  Das Objekt, mit dem die Aktion durchgeführt wurde. Beispiel: das Objekt des Ereignisses **Benutzer wurde aktualisiert** ist derjenige Benutzer, dessen Eigenschaften geändert wurden. Bei Ereignissen, die sich auf eine Quota beziehen, ist die Quota das Objekt.
- **Mandant**
  Der Name der Abteilung, zu welcher das Objekt gehört. Beispiel: der Mandant des Ereignisses **Benutzer wurde aktualisiert** ist diejenige Abteilung, zu welcher der Benutzer gehört. Der Mandant des Ereignisses **Quota wurde erreicht** ist der Benutzer, dessen Quota erreicht wurde.
- **Initiator**

Der Anmeldename des Benutzers, der das Ereignis initiiert hat. Bei Systemmeldungen und Ereignissen, die von einem übergeordneten Administratoren initiiert wurden, wird **System** als Inititator angezeigt.

- **Mandant des Initiators**
  Der Name der Abteilung, zu welcher der Initiator gehört. Bei Systemmeldungen und Ereignissen, die von einem übergeordneten Administrator initiiert wurden, bleibt dieses Feld leer.
- **Methode**
  Zeigt an, ob das Ereignis über das Weboberfläche oder über die API ausgelöst wurde.
- **IP**
  Die IP-Adresse der Maschine, von der aus das Ereignis ausgelöst wurde.

Filter und Suche

Sie können die Ereignisse nach Typ, Schweregrad oder Datum filtern. Sie können die Ereignisse auch nach Name, Objekt, Mandant, Initiator und Mandant des Initiators durchsuchen.

Berichte

Klicken Sie auf **Berichte**, wenn Sie Berichte über die Service-Nutzung und durchgeführte Aktionen zugreifen wollen.

Hinweis
Diese Funktionalität ist nicht in den Standard-Editionen des Cyber Protection Service verfügbar.

Nutzungsberichte

Nutzungsberichte stellen Daten über die zurückliegende Nutzung der Services zur Verfügung. Nutzungsberichte sind im CSV- und HTML-Format verfügbar.

Berichtstyp

Sie können einen der folgenden Berichtstypen wählen:

- **Aktuelle Nutzung**
  Der Bericht enthält die aktuellen Service-Nutzungsmetriken.
- **Zusammenfassung für Zeitraum**
  Der Bericht enthält die Service-Nutzungsmetriken für das Ende des spezifizierten Zeitraums und den Unterschied zwischen den Metriken zu Beginn und Ende des spezifizierten Zeitraums.
- **Täglich für einen Zeitraum**
  Der Bericht enthält die Service-Nutzungsmetriken und deren Änderungen für jeden Tag des spezifizierten Zeitraums.

Berichtsumfang

Sie können den Umfang des Berichts über die folgenden Werte bestimmen:

- **Direkte Kunden und Partner**
  Der Bericht wird nur Service-Nutzungsmetriken für die direkten Unterabteilungen derjenigen Firma oder Abteilung enthalten, in welcher Sie gerade arbeiten.
- **Alle Kunden und Partner**
  Der Bericht wird Service-Nutzungsmetriken für alle untergeordneten Abteilungen derjenigen Firma oder Abteilung enthalten, in welcher Sie gerade arbeiten.
- **Alle Kunden und Partner (einschließlich Benutzerdetails)**
  Der Bericht wird Service-Nutzungsmetriken für alle untergeordneten Abteilung derjenigen Firma oder Abteilung enthalten, in welcher Sie gerade arbeiten, und für alle Benutzer innerhalb der Abteilungen.

Metriken mit einer Nutzung von Null

Sie können die Anzahl der Zeilen im Bericht verringern, indem Sie nur Informationen über solche

Metriken auflisten lassen, deren Nutzung ungleich Null ist, und zudem Informationen über Metriken ausblenden lassen, die keine Nutzung aufweisen (gleich Null ist).

Geplante Nutzungsberichte konfigurieren

Ein geplanter Bericht umfasst die Service-Nutzungsmetriken für den letzten vollen Kalendermonat. Die Berichte werden um 23:59:59 Uhr (UTC-Zeit) am ersten Tag eines Monats generiert und dann am zweiten Tag desselben Monats gesendet. Die Berichte werden an alle Administratoren Ihrer Firma oder Abteilung gesendet, die in den Benutzereinstellungen das Kontrollkästchen **Geplante Nutzungsberichte** aktiviert haben.

So (de)aktivieren Sie einen geplanten Bericht

1. Melden Sie sich am Management-Portal an.
2. Stellen Sie sicher, dass Sie in der Firma oder obersten Abteilung arbeiten, die für Sie verfügbar ist.
3. Klicken Sie auf **Berichte** –> **Nutzung**.
4. Klicken Sie auf **Geplant**.
5. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Einen monatlichen Übersichtsbericht senden**.
6. Bestimmen Sie bei **Detail-Level**, welchen Umfang der Bericht haben soll.
7. [Optional] Wählen Sie **Metriken mit einer Nutzung von Null ausblenden**, wenn Sie Metriken ausschließen wollen, bei denen es keine Nutzung gibt.

Benutzerdefinierte Nutzungsberichte konfigurieren

Ein benutzerdefinierter Bericht wird auf Anforderung generiert und kann nicht geplant werden. Der Bericht wird an Ihre E-Mail-Adresse gesendet.

So erstellen Sie einen benutzerdefinierten Bericht

1. Melden Sie sich am Management-Portal an.
2. Gehen Sie zu der Abteilung, für die Sie einen Bericht erstellen wollen.
3. Klicken Sie auf **Berichte** –> **Nutzung**.
4. Klicken Sie auf **Benutzerdefiniert**.
5. Wählen Sie im Feld **Typ** den Berichtstyp ausk.
6. [Nicht verfügbar für den Berichtstyp **Aktuelle Nutzung**] Wählen Sie bei **Zeitraum** den Berichtszeitraum.
   - **Aktueller Kalendermonat**
   - **Vorheriger Kalendermonat**
   - **Benutzerdefiniert**

7. [Nicht verfügbar für den Berichtstyp **Aktuelle Nutzung**] Wenn Sie einen benutzerdefinierten Berichtszeitraum spezifizieren wollen, müssen Sie die entsprechenden Start- und Endzeiten festlegen. Ansonsten können Sie diesen Schritt überspringen.
8. Bestimmen Sie bei **Detail-Level**, welchen Umfang der Bericht haben soll.
9. [Optional] Wählen Sie **Metriken mit einer Nutzung von Null ausblenden**, wenn Sie Metriken ausschließen wollen, bei denen es keine Nutzung gibt.
10. Um einen Bericht zu generieren, klicken Sie auf **Generieren und senden**.

Daten in Nutzungsberichten

Ein Bericht über die Nutzung des Cyber Protection Service enthält folgende Daten über eine Firma oder Abteilung:

- Die Größe von Backups pro Abteilung, pro Benutzer, pro Gerätetyp.
- Die Anzahl von geschützten Geräten pro Abteilung, pro Benutzer, pro Gerätetyp.
- Der Preis pro Abteilung, pro Benutzer, pro Gerätetyp.
- Die Gesamtgröße der Backups.
- Die Gesamtzahl der geschützten Geräte.
- Der Gesamtpreis.

Hinweis
Wenn der Cyber Protection Service einen Gerätetyp nicht erkennen kann, wird dieses Gerät im Bericht als **Nicht typisiert** aufgeführt.

Aktionen-Berichte

Die Berichte **Aktionen** sind nur für Firmenadministratoren verfügbar, wenn diese auf Firmenebene arbeiten.

Ein Bericht über Aktionen kann einen beliebigen Satz von Dashboard-Widgets des Typs '**Aktionen**' enthalten. Alle Widgets zeigen zusammengefasste Informationen für die komplette Firma an.
Je nach Widget-Typ enthält der Bericht Daten für einen bestimmten Zeitraum oder für den Zeitpunkt des Durchsuchens oder der Berichtserstellung. Siehe Abschnitt '"Berichtsdaten je nach Widget-Typ" (S. 86)'.

Alle historischen Widgets zeigen Daten für den gleichen Zeitraum an. Sie können diesen Zeitraum in den Berichtseinstellungen ändern.

Sie können vorgegebene Berichte (Standardberichte) verwenden oder einen benutzerdefinierten Bericht erstellen.

Sie können einen Bericht herunterladen oder per E-Mail im XLSX-Format (Excel) oder PDF-Format versenden.

Die Standardberichte sind nachfolgend aufgelistet:

Berichtsname	Beschreibung
#CyberFit-Score pro Maschine	Zeigt den #CyberFit-Score, der auf der Evaluierung von Sicherheitsmetriken und Sicherheitskonfigurationen für jede Maschine basiert, und Empfehlungen für deren Verbesserungen an.
Alarmmeldungen	Zeigt Alarmmeldungen an, die während eines bestimmten Zeitraums aufgetreten sind.
Backup-Scanning-Details	Zeigt ausführliche Informationen über erkannte Bedrohungen in den Backups an.
Tägliche Aktivitäten	Zeigt Übersichtsinformationen zu Aktivitäten an, die während eines bestimmten Zeitraums durchgeführt wurden.
Data Protection-Karte	Zeigt ausführliche Informationen über Anzahl, Größe, Speicherort und Sicherungsstatus aller wichtigen Dateien auf den Maschinen an.
Erkannte Bedrohungen	Zeigt Details der betroffenen Maschinen anhand der Anzahl der blockierten Bedrohungen sowie der fehlerfreien und verwundbaren Maschinen an.
Erkannte Maschinen	Zeigt alle gefundene Maschinen im Organisationsnetzwerk an.
Vorhersage der Laufwerksintegrität	Zeigt den aktuellen Laufwerksstatus an sowie eine Prognose dazu, wann Ihre HDD/SSD vermutlich ausfallen wird.
Vorhandene Schwachstellen	Zeigt die existierenden Verwundbarkeiten des Betriebssystems und der Applikationen in Ihrem Unternehmen an. Der Bericht zeigt zudem Details der betroffenen Maschinen in Ihrem Netzwerk für jedes aufgelistete Produkt an.
Übersicht zur Patch-Verwaltung	Zeigt die Anzahl der fehlenden, installierten und anwendbaren Patches an. Sie können sich Detailinformationen zu den Berichten anzeigen lassen, um Informationen und Details zu den fehlenden/installierten Patches für alle Systeme zu erhalten.
Übersicht	Zeigt Übersichtsinformationen zu geschützten Geräten für einen bestimmten Zeitraum an.
Wöchentliche Aktivitäten	Zeigt Übersichtsinformationen zu Aktivitäten an, die während eines bestimmten Zeitraums durchgeführt wurden.
Software-Inventarisierung	Zeigt ausführliche Informationen über die gesamte Software an, die auf den Windows- und macOS-Geräten in Ihrem Unternehmen installiert ist.
Hardware-Inventarisierung	Zeigt ausführliche Informationen über die gesamte Hardware an, die für die physischen und virtuellen Windows- sowie macOS-Geräte in Ihrem Unternehmen verfügbar ist.

Remote-Sitzungen	Zeigt detaillierte Informationen über die Remote-Desktop- und Dateiübertragungssitzungen an, die in Ihrer Organisation während eines bestimmten Zeitraums durchgeführt wurden.

Aktionen mit Berichten

Wenn Sie einen Bericht einsehen wollen, klicken Sie auf dessen Namen.

So können Sie einen neuen Bericht hinzufügen

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Klicken Sie unter der Liste der verfügbaren Berichte auf **Bericht hinzufügen**.
3. [Um einen vordefinierten Bericht hinzuzufügen] Klicken Sie auf den Namen des vordefinierten Berichts.
4. [Um einen benutzerdefinierten Bericht hinzuzufügen] Klicken Sie auf **Benutzerdefiniert** und fügen Sie dann Widgets zum Bericht hinzu.
5. [Optional] Ordnen Sie die Widgets per Drag & Drop nach Ihren Vorstellungen neu an.

So können Sie eine Bericht bearbeiten

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie aus der Liste der Berichte denjenigen Bericht aus, den Sie bearbeiten wollen.
   Sie können Folgendes tun:
   - Den Bericht umbenennen.
   - Den Zeitraum für alle Widgets im Report ändern.
   - Die Berichtsempfänger spezifizieren sowie den Zeitpunkt, an dem der Bericht an diese gesendet werden soll. Die verfügbaren Formate sind PDF und XLSX.

So können Sie einen Bericht löschen

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie aus der Liste der Berichte denjenigen Bericht aus, den Sie löschen wollen.
3. Klicken Sie auf das Drei-Punkte-Symbol (...) und dann auf den Befehl **Löschen**.
4. Bestätigen Sie Ihre Auswahl, indem Sie auf **Löschen** klicken.

So können Sie eine Bericht planen

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie in der Liste der Berichte denjenigen Bericht aus, den Sie planen wollen, und klicken Sie anschließend auf **Einstellungen**.
3. Aktivieren Sie den Schalter **Geplant**.
   - Spezifizieren Sie die E-Mail-Adressen der Empfänger.
   - Bestimmen Sie das Format des Berichts.

Hinweis
Sie können bis zu 1000 Elemente in eine PDF-Datei und bis zu 10.000 Elemente in eine XLSX-Datei exportieren. Die Zeitstempel in den PDF- und XLSX-Dateien basieren auf der lokalen Zeit Ihrer Maschine.

- Bestimmen Sie die Sprache des Berichts.
- Konfigurieren Sie die Planung.

4. Klicken Sie auf **Speichern**.

So können Sie einen Bericht herunterladen

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie in der Liste der Berichte den gewünschten Bericht aus und klicken Sie dann auf **Download**.
3. Bestimmen Sie das Format des Berichts.

So können Sie einen Bericht senden

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie in der Liste der Berichte den gewünschten Bericht aus und klicken Sie dann auf **Senden**.
3. Spezifizieren Sie die E-Mail-Adressen der Empfänger.
4. Bestimmen Sie das Format des Berichts.
5. Klicken Sie auf **Senden**.

So können Sie die Berichtsstruktur exportieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie in der Liste der Berichte den gewünschten Bericht aus.
3. Klicken Sie auf das Drei-Punkte-Symbol (...) und dann auf den Befehl **Exportieren**.

Als Ergebnis wird die Berichtsstruktur als JSON-Datei auf Ihrer Maschine gespeichert.

So können Sie die Berichtsdaten sichern

Mit dieser Option können Sie alle Daten für einen benutzerdefinierten Zeitraum (ohne Filterung) in eine CSV-Datei exportieren und diese an einen E-Mail-Empfänger senden.

Hinweis
Sie können bis zu 150.000 Elemente in eine CSV-Datei exportieren. Die Zeitstempel in der CSV-Datei verwenden die koordinierte Weltzeit (UTC).

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie aus der Liste der Berichte denjenigen Bericht aus, dessen Daten Sie sichern wollen.

3. Klicken Sie auf das Drei-Punkte-Symbol (...) und dann auf **Sicherungsdaten**.
4. Spezifizieren Sie die E-Mail-Adressen der Empfänger.
5. Spezifizieren Sie bei **Zeitraum** den benutzerdefinierten Zeitraum, für den Sie die Daten sichern wollen.

   Hinweis
   CSV-Dateien für längere Zeiträume vorzubereiten, kostet mehr Zeit.

6. Klicken Sie auf **Senden**.

Kurzübersicht

Der Kurzübersichtsbericht bietet einen Überblick über den Schutzstatus der Umgebung und der geschützten Geräte Ihres Unternehmens für einen spezifizierten Zeitraum.

Der Kurzübersichtsbericht enthält anpassbare Abschnitte mit dynamischen Widgets, die wichtige Performance-Metriken in Bezug auf die Nutzung folgender Cloud-Services anzeigen: Backup, Antimalware Protection, Schwachstellenbewertung, Patch-Verwaltung, Notary Service, Disaster Recovery und File Sync & Share.

Sie können den Bericht auf vielfältige Weise anpassen.

- Ändern oder löschen Sie Abschnitte.
- Ändern Sie die Reihenfolge von Abschnitten.
- Benennen Sie Abschnitte um.
- Verschieben Sie Widgets von einem Abschnitt zu einem anderen.
- Ändern Sie die Reihenfolge der Widgets in jedem Abschnitt.
- Fügen Sie Widgets hinzu oder entfernen Sie diese.
- Passen Sie die Widgets an.

Sie können die Kurzübersichtsberichte im PDF- und Excel-Format generieren und diese an die Eigentümer oder andere Projektbeteiligte Ihres Unternehmens senden, damit diese den technischen und geschäftlichen Wert der bereitgestellten Services leichter erkennen können.

Kurzübersicht-Widgets

Sie können Bereiche und Widgets im Kurzübersichtsbericht hinzufügen oder entfernen und dadurch bestimmen, welche Informationen im Bericht enthalten sein sollen.

Workloads-Überblick-Widgets

In der nachfolgenden Tabelle finden Sie weitere Informationen zu den Widgets im Bereich **Workloads-Überblick**.

Widget	Beschreibung
Cloud-Workloads Schutzstatus	Dieses Widget zeigt die Anzahl der geschützten und ungeschützten Cloud-Workloads nach Typ und zum Zeitpunkt der Berichtserstellung an. Geschützte Cloud-Workloads sind Cloud-Workloads, auf die mindestens ein Backup-Plan angewendet wurde. Ungeschützte Cloud-Workloads sind Cloud-Workloads, auf die (bisher) kein Backup-Plan angewendet wurde. Folgende Cloud-Workload-Typen sind im Diagramm dargestellt (in alphabetischer Reihenfolge von A bis Z): • Google Workspace Drive • Google Workspace Gmail • Google Workspace Shared Drive • Hosted Exchange-Postfächer • Microsoft 365-Postfächer • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • Websites Für einige Workload-Typen werden folgende Workload-Gruppen verwendet: • Microsoft 365: Benutzer, Gruppen, Öffentliche Ordner, Teams und Website-Sammlungen • Google Workspace: Benutzer und Shared Drives • Hosted Exchange: Benutzer Wenn es in einer Workload-Gruppe mehr als 10.000 Workloads gibt, zeigt das Widget keine Daten für die entsprechenden Workloads an. Wenn der Kunde beispielsweise ein Microsoft 365-Konto mit 10.000 Postfächern sowie je einen OneDrive-Service für 500 Benutzer hat, so gehören diese alle zur Workload-Gruppe 'Benutzer'. Die Summe dieser Workloads beträgt 10.500, wodurch die Begrenzung von 10.000 für eine Workload-Gruppe überschritten wird. Daher wird das Widget die entsprechenden Workload-Typen ausblenden: Microsoft 365-Postfächer und Microsoft 365 OneDrive.
Cyber Protection-Übersicht	Das Widget zeigt die wichtigsten Metriken zur Cyber Protection-Performance für den spezifizierten Zeitraum an. **Gesicherte Daten** – die Gesamtgröße der Archive, die in den lokalen Storages und Cloud Storages und erstellt wurden. **Abgemilderte Bedrohungen** – die Gesamtzahl der Malware, die insgesamt auf allen Geräten blockiert wurden. **Schädliche URLs blockiert** – die Gesamtzahl der blockierten URLs auf allen Geräten.

Widget	Beschreibung
	Gepatchte Schwachstellen – die Gesamtzahl der Schwachstellen, die durch die Installation von Software-Patches auf allen Geräten behoben wurden. **Installierte Patches** – die Gesamtzahl der Patches, die auf allen Geräten installiert wurden. **Server geschützt durch DR** – die Gesamtzahl der Server, die per Disaster Recovery geschützt werden. **File Sync & Share-Benutzer** – die Gesamtzahl der End- und Gastbenutzer, die die Cyber Files Funktionalität verwenden. **Beglaubigte Dateien** – die Gesamtzahl der beglaubigten Dateien. **Elektronisch signierte Dokumente** – die Gesamtzahl der elektronisch signierten Dokumente. **Blockierte Peripheriegeräte** – die Gesamtzahl der Peripheriegeräte, auf die der Zugriff blockiert wird.
Workload-Netzwerkstatus	Dieses Widget informiert darüber, wie viele Workloads isoliert sind und wie viele verbunden sind (das normale Stadium des Workloads). Wählen Sie den gewünschten Kunden aus. Die dargestellte Workload-Ansicht wird gefiltert, sodass nur noch isolierte Workloads angezeigt werden. Wenn Sie auf das Element 'Verbunden' klicken, wird die Liste 'Workload mit Agenten' angezeigt, die so gefiltert ist, dass die verbundenen Workloads (für den ausgewählten Kunden) angezeigt werden.
Workloads-Schutzstatus	Das Widget zeigt die geschützten und ungeschützten Workloads nach Typ und zum Zeitpunkt der Berichtserstellung an. Geschützte Workloads sind Workloads, auf die mindestens ein Schutz- oder Backup-Plan angewendet wurde. Ungeschützte Workloads sind Workloads, auf die (bisher) kein Schutz- oder Backup-Plan angewendet wurde. Folgende Workloads werden gezählt: **Server** – physische Server und Domain-Controller-Server. **Workstations** – physische Workstations. **Virtuelle Maschinen** – sowohl agentenbasierte als auch agentenlose virtuelle Maschinen. **Webhosting-Server** – virtueller oder physischer Server, auf denen cPanel oder Plesk installiert ist. **Mobilgeräte** – physische Mobilgeräte (wie Smartphones). Ein Workload kann zu mehreren Kategorien gehören. Ein Webhosting-Server wird beispielsweise zu zwei Kategorien gezählt – **Server** und **Webhosting-Server**.

Antimalware Protection-Widgets

In der nachfolgenden Tabelle finden Sie weitere Informationen zu den Widgets im Bereich **Threat Defense**.

Widget	Beschreibung
Antimalware-Scan von Dateien	Das Widget zeigt die Ergebnisse der On-Demand-Antimalware-Scans von den jeweiligen Geräten für den spezifizierten Datumsbereich an. **Dateien** – die Gesamtzahl der gescannten Dateien **Sauber** – die Gesamtzahl der sauberen Dateien **Erkannt, unter Quarantäne gestellt** – die Gesamtzahl der infizierten Dateien, die unter Quarantäne gestellt wurden **Erkannt, nicht unter Quarantäne gestellt** – die Gesamtzahl der infizierten Dateien, die nicht unter Quarantäne gestellt wurden **Geräte geschützt** – die Gesamtzahl der Geräte, auf die eine Antimalware Protection-Richtlinie angewendet wurde **Gesamtzahl an registrierten Geräten** – Die Gesamtzahl der registrierten Geräte zum Zeitpunkt der Berichtserstellung
Antimalware-Scan von Backups	Das Widget zeigt die Ergebnisse der Antimalware-Scans von Backups für den spezifizierten Datumsbereich an und verwendet dabei folgende Metriken: • Gesamtzahl der gescannten Recovery-Punkte • Anzahl der sauberen Recovery-Punkte • Anzahl der sauberen Recovery-Punkte mit nicht unterstützten Partitionen • Anzahl der infizierten Recovery-Punkte. Diese Metrik beinhaltet die Anzahl der infizierten Recovery-Punkte mit nicht unterstützten Partitionen (Volumes).
Blockierte URLs	Das Widget zeigt für den spezifizierten Datumsbereich die Anzahl der blockierten URLs an, gruppiert nach Website-Kategorie. Das Widget listet die sieben Website-Kategorien mit der größten Anzahl blockierter URLs auf und fasst die übrigen Website-Kategorien unter **Andere(s)** zusammen. Weitere Informationen zu den Website-Kategorien finden Sie unter dem Thema 'URL-Filterung in Cyber Protection'.
Sicherheitsvorfall-Burndown	Dieses Widget zeigt die Effizienzrate bei der Schließung von Vorfällen für die ausgewählte Firma an; die Anzahl der offenen Vorfälle wird dabei mit der Anzahl der geschlossenen Vorfälle über einen bestimmten Zeitraum abgeglichen. Bewegen Sie den Mauszeiger über eine Spalte, um eine

Widget	Beschreibung
	Aufschlüsselung der geschlossenen und offenen Vorfälle für den jeweiligen Tag angezeigt zu bekommen. Der in Klammern angegebene Prozentwert gibt den Anstieg bzw. den Rückgang im Vergleich zum vorherigen Zeitraum an.
MTTR (Mittlere Problemlösungszeit) für Vorfälle	Dieses Widget zeigt die durchschnittliche Problemlösungszeit für Sicherheitsvorfälle an. Sie gibt an, wie schnell Vorfälle untersucht und gelöst werden. Klicken Sie auf eine Spalte, um die Vorfälle nach ihrem Schweregrad (**Kritisch**, **Hoch** und **Mittel**) aufzuschlüsseln und zu sehen, wie lange es dauerte, die verschiedenen Schweregrade zu beheben. Der in Klammern angegebene Prozentwert gibt den Anstieg bzw. den Rückgang im Vergleich zum vorherigen Zeitraum an.
Bedrohungsstatus	Dieses Widget zeigt den aktuellen Bedrohungsstatus für die Workloads einer Firma an (unabhängig von der Anzahl der Workloads) und hebt dabei die aktuelle Anzahl der Vorfälle hervor, die nicht abgeschwächt wurden und die noch untersucht werden müssen. Das Widget gibt auch die Anzahl der Vorfälle an, die (manuell und/oder automatisch vom System) abgeschwächt wurden.
Erkannten Bedrohungen nach Schutztechnologie	Das Widget zeigt für den spezifizierten Datumsbereich die Anzahl der erkannten Bedrohungen an, gruppiert nach folgenden Schutztechnologien: • Antimalware-Scanning • Behavior Engine • Cryptomining Protection • Exploit-Prävention • Ransomware Active Protection • Echtzeitschutz • URL-Filterung

Backup-Widgets

In der nachfolgenden Tabelle finden Sie weitere Informationen zu den Widgets im Bereich **Backup**.

Widget	Beschreibung
Workloads gesichert	Das Widget zeigt die Gesamtzahl der registrierten Workloads nach dem jeweiligen Backup-Status an. **Gesichert** – die Anzahl der Workloads, die während des Berichtszeitraums per Backup geschützt wurden (es muss mindestens ein erfolgreiches Backup durchgeführt worden sein). **Nicht gesichert** – die Anzahl der Workloads, die während des

Widget	Beschreibung
	Berichtszeitraums nicht per Backup geschützt wurden (es wurde kein erfolgreiches Backup durchgeführt).
Laufwerksintegritätstatus nach physischen Geräten	Das Widget zeigt den aggregierten Integritätstatus von physischen Geräte an, basierend auf den Integritätstatuszuständen von deren Laufwerken. **OK** – Dieser Laufwerksintegritätsstatus bezieht sich auf bestimmte Werte [70-100]. Der Status eines Gerätes ist **OK**, wenn all seine Laufwerke den Status **OK** haben. **Warnung** – Dieser Laufwerksintegritätsstatus bezieht sich auf bestimmte Werte [30-70]. Der Status eines Gerätes ist **Warnung**, wenn mindestens eines seiner Laufwerke den Status **Warnung** und kein Laufwerk den Status **Fehler** hat. **Fehler** – Dieser Laufwerksintegritätsstatus bezieht sich auf bestimmte Werte [0-30]. Der Status eines Gerätes ist **Fehler**, wenn mindestens eines seiner Laufwerke den Status **Fehler** hat. **Laufwerksdaten werden berechnet** – Der Status eines Gerätes ist **Laufwerksdaten werden berechnet**, wenn die Statuszustände seiner Laufwerke noch nicht berechnet wurden.
Backup Storage-Nutzung	Das Widget zeigt für den spezifizierten Zeitraum die Gesamtzahl und Gesamtgröße der Backups in der Cloud sowie im lokalen Storage an.

Widgets für Schwachstellenbewertung und Patch-Verwaltung

In der nachfolgenden Tabelle finden Sie weitere Informationen zu den Widgets im Bereich **Schwachstellenbewertung und Patch-Verwaltung**.

Widget	Beschreibung
Gepatchte Schwachstellen	Das Widget zeigt die Performance-Ergebnisse der Schwachstellenbewertung für den spezifizierten Datumsbereich an. **Insgesamt** – die Gesamtzahl der gepatchten Schwachstellen. **Microsoft-Software-Schwachstellen** – die Gesamtzahl der behobenen Microsoft-Schwachstellen auf allen Windows-Geräten. **Schwachstellen in Windows-Software von Drittanbietern** – die Gesamtzahl der behobenen Schwachstellen in Windows-Programmen von Drittanbietern auf allen Windows-Geräten. **Workloads gescannt** – die Gesamtzahl der Geräte, die innerhalb des

Widget	Beschreibung
	spezifizierten Datumsbereichs mindestens einmal erfolgreich auf Schwachstellen gescannt wurden.
Patches installiert	Das Widget zeigt die Performance-Ergebnisse der Patch-Verwaltung für den spezifizierten Datumsbereich an. **Installiert** – die Gesamtzahl der Patches, die erfolgreich auf allen Geräten installiert wurden. **Microsoft-Software-Patches** – die Gesamtzahl der Patches für Software-Programme von Microsoft, die auf allen Windows-Geräten installiert wurden. **Patches für Windows-Software von Drittanbietern** – die Gesamtzahl der Patches für Software-Programme von Drittanbietern, die auf allen Windows-Geräten installiert wurden. **Workloads gepatcht** – die Gesamtzahl der Geräte, die erfolgreich gepatcht wurden (im spezifizierten Datumsbereich wurde mindestens ein Patch erfolgreich installiert).

Disaster Recovery-Widgets

In der nachfolgenden Tabelle finden Sie weitere Informationen zu den Widgets im Bereich **Disaster Recovery**.

Widget	Beschreibung
Disaster Recovery-Statistiken	Das Widget zeigt die wichtigsten Metriken zur Disaster Recovery-Performance für den spezifizierten Datumsbereich an. **Produktions-Failover** – die Anzahl der Produktions-Failover-Aktionen für den spezifizierten Zeitraum. **Test-Failover** – die Gesamtzahl der Test-Failover-Aktionen, die während des spezifizierten Zeitraums durchgeführt wurden. **Primäre Server** – die Gesamtzahl der primären Server zum Zeitpunkt der Berichtserstellung. **Recovery-Server** – die Gesamtzahl der Recovery-Server zum Zeitpunkt der Berichtserstellung. **Öffentliche IPs** – die Gesamtzahl der öffentlichen IP-Adresse (zum Zeitpunkt der Berichtserstellung). **Verbrauchte Berechnungspunkte insgesamt** – die Gesamtzahl der Berechnungspunkte, die während des spezifizierten Zeitraums verbraucht wurden.
Disaster	Das Widget zeigt Informationen über die Server an, die per Disaster Recovery

Widget	Beschreibung
Recovery-Server getestet	geschützt werden und per Test-Failover getestet wurden. Das Widget zeigt folgende Metriken an: **Server geschützt** – die Anzahl der per Disaster Recovery geschützten Server (Server, die mindestens einen Recovery-Server haben) zum Zeitpunkt der Berichtserstellung. **Getestet** – die Anzahl der per Disaster Recovery geschützten Server, die während des festgelegten Zeitraums per Test-Failover getestet wurden (von allen per Disaster Recovery geschützten Servern). **Nicht getestet** – die Anzahl der per Disaster Recovery geschützten Server, die während des festgelegten Zeitraums nicht per Test-Failover getestet wurden (von allen per Disaster Recovery geschützten Servern). Das Widget zeigt auch die Größe des Disaster Recovery Storage (in GB) zum Zeitpunkt der Berichtserstellung an. Dies entspricht der Summe der Backup-Größen der Cloud Server.
Server geschützt mit Disaster Recovery	Das Widget zeigt Informationen über die per Disaster Recovery geschützten Server sowie die ungeschützten Server an. Das Widget zeigt folgende Metriken an: Die Gesamtzahl der im Kunden-Mandanten registrierten Server zum Zeitpunkt der Berichtserstellung. **Geschützt** – die Anzahl der per Disaster Recovery geschützten Server (die mindestens einen Recovery-Server sowie ein Backup des kompletten Servers haben) von allen registrierten Servern und zum Zeitpunkt der Berichtserstellung. **Ungeschützt** – die Gesamtzahl der ungeschützten Server von allen registrierten Servern zum Zeitpunkt der Berichtserstellung.

Data Loss Prevention-Widget

Im nachfolgenden Abschnitt finden Sie weitere Informationen über die blockierten Peripheriegeräte im Bereich **Data Loss Prevention**.

Das Widget zeigt die Gesamtanzahl der blockierten Geräte sowie die Gesamtanzahl der blockierten Geräte an, nach Gerätetyp und für den spezifizierten Datumsbereich.

- Wechselmedien
- Verschlüsseltes Wechsellaufwerk
- Drucker
- Zwischenablage – enthält die Gerätetypen 'Zwischenablage' und 'Screenshot-Aufnahme'.
- Mobilgeräte

- Bluetooth
- Optische Laufwerke
- Diskettenlaufwerke
- USB – enthält die Gerätetypen 'USB-Port' und 'Umgeleiteter USB-Port'.
- FireWire
- Zugeordnete Laufwerke
- Umgeleitete Zwischenablage – enthält die Gerätetypen 'Umgeleitete Zwischenablage eingehend' und 'Umgeleitete Zwischenablage ausgehend'.

Das Widget zeigt die ersten sieben Gerätetypen an, die die höchste Anzahl an blockierten Geräten haben, und fasst die übrigen Gerätetypen unter dem Gerätetyp **Andere(s)** zusammen.

File Sync & Share-Widgets

In der nachfolgenden Tabelle finden Sie weitere Informationen zu den Widgets im Bereich **File Sync & Share**.

Widget	Beschreibung
File Sync & Share-Statistiken	Das Widget zeigt folgende Metriken an: **Verwendeter Cloud Storage insgesamt** – Die gesamte Storage-Nutzung aller Benutzer. **Endbenutzer** – die Gesamtzahl der Endbenutzer. **Durchschnittliche Storage-Nutzung pro Benutzer** – die durchschnittliche Storage-Nutzung pro Endbenutzer. **Gastbenutzer** – die Gesamtzahl der Gastbenutzer.
File Sync & Share-Storage-Nutzung durch Endbenutzer	Das Widget zeigt die Gesamtzahl der File Sync & Share-Endbenutzer an, die eine Storage-Nutzung in folgenden Bereichen haben: • 0–1 GB • 1–5 GB • 5–10 GB • 10–50 GB • 50–100 GB • 100–500 GB • 500 GB – 1 TB • Mehr als 1 TB

Notary-Widgets

In der nachfolgenden Tabelle finden Sie weitere Informationen zu den Widgets im Bereich **Notary**.

Widget	Beschreibung
Cyber Notary-Statistiken	Das Widget zeigt folgende Notary-Metriken an: **Notary Cloud Storage verwendet** – die Gesamtgröße des Storage, der für Notary Services verwendet wird. **Beglaubigte Dateien** – die Gesamtzahl der beglaubigten Dateien. **Elektronisch signierte Dokumente** – die Gesamtzahl der elektronisch signierten Dokumente und Dateien.
Beglaubigte Dateien über alle Endbenutzer hinweg	Zeigt die Gesamtzahl der beglaubigten Dateien für alle Endbenutzer an. Die Benutzer werden nach der Anzahl der beglaubigten Dateien gruppiert, die diese haben. • Bis zu 10 Dateien • 11–100 Dateien • 101–500 Dateien • 501–1000 Dateien • Mehr als 1000 Dateien
Elektronisch signierte Dokumente über alle Endbenutzer hinweg an	Das Widget zeigt die Gesamtzahl der elektronisch signierten Dokumente und Dateien für alle Endbenutzer an. Die Benutzer werden nach der Anzahl der elektronisch signierten Dokumente und Dateien gruppiert, die diese haben. • Bis zu 10 Dateien • 11–100 Dateien • 101–500 Dateien • 501–1000 Dateien • Mehr als 1000 Dateien

Die Einstellungen des Kurzübersichtsberichts konfigurieren

Sie können die Berichtseinstellungen aktualisieren, die beim Erstellen des Kurzübersichtsberichts konfiguriert wurden.

So können Sie die Einstellungen des Kurzübersichtsberichts aktualisieren

1. Gehen Sie in der Management-Konsole zu **Berichte** –> **Kurzübersicht**.
2. Klicken Sie auf den Namen des Kurzübersichtsberichts, den Sie aktualisieren wollen.
3. Klicken Sie auf **Einstellungen**.
4. Ändern Sie die Werte der Felder nach Bedarf.
5. Klicken Sie auf **Speichern**.

Einen Kurzübersichtsbericht erstellen

Sie können einen Kurzübersichtsbericht erstellen, eine Vorschau seiner Inhalte anzeigen, die Empfänger des Berichts konfigurieren und den Zeitpunkt für den automatischen Versand planen.

So können Sie einen Kurzübersichtsbericht erstellen

1. Gehen Sie in der Management-Konsole zu **Berichte** –> **Kurzübersicht**.
2. Klicken Sie auf **Kurzübersichtsbericht erstellen**.
3. Geben Sie bei **Berichtsname** eine Bezeichnung für den Bericht ein.
4. Bestimmen Sie die Empfänger des Berichts.
   - Wenn Sie den Bericht an alle Kontakte und Benutzer senden wollen, wählen Sie **An alle Kontakte und Benutzer senden** aus.
   - Wenn Sie den Bericht an bestimmte Kontakte und Benutzer senden wollen
     a. Deaktivieren Sie die Auswahl **An alle Kontakte und Benutzer senden**.
     b. Klicken Sie auf **Kontakte wählen**.
     c. Wählen Sie die gewünschten Kontakte und Benutzer aus. Sie können die Suchfunktion verwenden, um bestimmte Kontakte leichter zu finden.
     d. Klicken Sie auf **Auswählen**.
5. Wählen Sie den Bereich: **30 Tage** oder **Dieser Monat**
6. Bestimmen Sie das Dateiformat: **PDF**, **Excel** oder **Excel und PDF**.
7. Konfigurieren Sie die Planungseinstellungen.
   - Wenn Sie den Bericht an einem bestimmten Datum und zu einer bestimmten Uhrzeit an die Empfänger senden wollen:
     a. Aktivieren Sie die Option **Geplant**.
     b. Klicken Sie auf das Feld **Tag des Monats**, deaktivieren Sie das Feld 'Letzter Tag' und klicken Sie auf das Datum, das Sie festlegen wollen.
     c. Geben Sie im Feld **Zeit** die Stunde an, die Sie festlegen wollen.
     d. Klicken Sie auf **Anwenden**.
   - Wenn Sie den Bericht nur erstellen wollen, ohne ihn an die Empfänger zu senden, müssen Sie die Option **Geplant** deaktivieren.
8. Klicken Sie auf **Speichern**.

Den Kurzübersichtsbericht anpassen

Sie können bestimmen, welche Informationen in den Kurzübersichtsbericht aufgenommen werden sollen. Sie können Abschnitte hinzufügen oder löschen, Widgets hinzufügen oder löschen,

Abschnitte umbenennen, Widgets anpassen sowie Widgets und Abschnitte per Drag & Drop verschieben, um die Reihenfolge zu ändern, in der die Informationen im Bericht erscheinen.

So können Sie einen Abschnitt hinzufügen

1. Klicken Sie auf **Element hinzufügen** –> **Abschnitt hinzufügen**.
2. Geben Sie im Fenster **Abschnitt hinzufügen** einen Namen für den Abschnitt ein oder verwenden Sie den vorgegebenen Abschnittsnamen.
3. Klicken Sie auf **Zu Bericht hinzufügen**.

So können Sie einen Abschnitt umbenennen

1. Klicken Sie in dem Abschnitt, den Sie umbenennen wollen, auf den Befehl **Bearbeiten**.
2. Geben Sie im Fenster **Abschnitt bearbeiten** den neuen Namen ein.
3. Klicken Sie auf **Speichern**.

So können Sie einen Abschnitt löschen

1. Klicken Sie in dem Abschnitt, den Sie löschen wollen, auf den Befehl **Abschnitt löschen**.
2. Klicken Sie im Bestätigungsfenster **Abschnitt löschen** auf **Löschen**.

So können Sie ein Widget mit Standardeinstellungen zu einem Abschnitt hinzufügen

1. Klicken Sie in dem Abschnitt, in dem Sie das Widget einfügen wollen, auf den Befehl **Widget hinzufügen**.
2. Klicken Sie im Fenster **Widget hinzufügen** auf dasjenige Widget, welches Sie hinzufügen wollen.

So können Sie ein benutzerdefiniertes Widget zu einem Abschnitt hinzufügen

1. Klicken Sie in dem Abschnitt, in dem Sie das Widget einfügen wollen, auf den Befehl **Widget hinzufügen**.
2. Suchen Sie im Fenster **Widget hinzufügen** das Widget, welches Sie hinzufügen wollen, und klicken Sie dann auf **Anpassen**.
3. Konfigurieren Sie die Felder nach Bedarf.
4. Klicken Sie auf **Widget hinzufügen**.

So können Sie ein Widget mit Standardeinstellungen dem Bericht hinzufügen

1. Klicken Sie auf **Element hinzufügen** –> **Widget hinzufügen**.
2. Klicken Sie im Fenster **Widget hinzufügen** auf dasjenige Widget, welches Sie hinzufügen wollen.

So können Sie ein benutzerdefiniertes Widget dem Bericht hinzufügen

1. Klicken Sie auf **Widget hinzufügen**.
2. Suchen Sie im Fenster **Widget hinzufügen** das Widget, welches Sie hinzufügen wollen, und klicken Sie dann auf **Anpassen**.

3. Konfigurieren Sie die Felder nach Bedarf.
4. Klicken Sie auf **Widget hinzufügen**.

So können Sie die Standardeinstellungen eines Widgets zurücksetzen

1. Klicken Sie in dem anzupassenden Widget auf den Befehl **Bearbeiten**.
2. Klicken Sie auf **Auf Standard zurücksetzen**.
3. Klicken Sie auf **Fertig**.

So können Sie ein Widget anpassen

1. Klicken Sie in dem anzupassenden Widget auf den Befehl **Bearbeiten**.
2. Bearbeiten Sie die Felder nach Ihrem Bedarf.
3. Klicken Sie auf **Fertig**.

Kurzübersichtsberichte senden

Sie können einen Kurzübersichtsbericht auch manuell nach Bedarf versenden. In diesem Fall wird die Einstellung **Geplant** ignoriert und der Bericht umgehend versendet. Beim Versenden des Berichts wird das System auf die Werte für Empfänger, Bereich und Dateiformat zurückgreifen, die in den entsprechenden **Einstellungen** konfiguriert wurden. Sie können diese Einstellungen vor dem Versenden des Berichts aber noch manuell ändern. Weitere Informationen finden Sie im Abschnitt '"Die Einstellungen des Kurzübersichtsberichts konfigurieren" (S. 82)'.

So können Sie einen Kurzübersichtsbericht senden

1. Gehen Sie im Management-Portal zu **Berichte** –> **Kurzübersicht**.
2. Klicken Sie auf den Namen des Kurzübersichtsberichts, den Sie versenden wollen.
3. Klicken Sie auf **Jetzt senden**.
   Das System wird den Kurzübersichtsbericht an die ausgewählten Empfänger senden.

Zeitzonen in Berichten

Die Zeitzonen, die in Berichten verwendet werden, hängen vom jeweiligen Berichtstyp ab. Die Informationen in der nachfolgenden Tabelle sollen Ihnen als Referenz dienen.

Berichtsort und -typ	Im Bericht verwendete Zeitzone
Management-Portal –> Überblick –> Aktionen (Widgets)	Die Zeit der Berichtserstellung entspricht der Zeitzone der Maschine, auf welcher der Webbrowser ausgeführt wird.
Management-Portal –> Überblick –> Aktionen (als PDF oder XSLX exportiert)	• Der Zeitstempel des exportierten Berichts entspricht der Zeitzone der Maschine, die zum Exportieren des Berichts verwendet wurde.

	• Die Zeitzone der im Bericht angezeigten Aktivitäten ist UTC.
Management-Portal –> Berichte –> Nutzung –> Geplante Berichte	• Der Bericht wird um 23:59:59 UTC am ersten Tag des Monats erstellt. • Der Bericht wird am zweiten Tag des Monats gesendet.
Management-Portal –> Berichte –> Nutzung –> Benutzerdefinierte Berichte	Die Zeitzone und das Datum des Berichts ist UTC.
Management-Portal –> Berichte –> Aktionen (Widgets)	• Die Zeit der Berichtserstellung entspricht der Zeitzone der Maschine, auf welcher der Webbrowser ausgeführt wird. • Die Zeitzone der im Bericht angezeigten Aktivitäten ist UTC.
Management-Portal –> Berichte –> Aktionen (als PDF oder XSLX exportiert)	• Der Zeitstempel des exportierten Berichts entspricht der Zeitzone der Maschine, die zum Exportieren des Berichts verwendet wurde. • Die Zeitzone der im Bericht angezeigten Aktivitäten ist UTC.
Management-Portal –> Berichte –> Aktionen (geplante Übermittlung)	• Die Zeitzone und die Berichtsübermittlung ist UTC. • Die Zeitzone der im Bericht angezeigten Aktivitäten ist UTC.
Management-Portal –> Benutzer –> Tägliche Zusammenfassung über aktive Alarmmeldungen	• Der Bericht wird einmal am Tag zwischen 10:00 und 23:59 UTC gesendet. Der genaue Zeitpunkt der Berichtsübermittlung hängt vom Workload im Datacenter ab. • Die Zeitzone der im Bericht angezeigten Aktivitäten ist UTC.
Management-Portal –> Benutzer –> Cyber Protection-Status-Benachrichtigungen	• Der Bericht wird gesendet, wenn eine Aktivität abgeschlossen wurde. **Hinweis** In Abhängigkeit vom Workload des Datacenters können einige Berichte verzögert gesendet werden. • Die Zeitzone der im Aktivität im Bericht ist UTC.

Berichtsdaten je nach Widget-Typ

Je nach dem Datenbereich, den sie anzeigen, gibt es zwei Arten von Widgets auf dem Dashboard:

- Widgets, die aktuelle Daten für den Zeitpunkt des Durchsuchens oder der Berichtserstellung anzeigen.
- Widgets, die historische Daten anzeigen.

Wenn Sie in den Berichtseinstellungen einen Datumsbereich konfigurieren, um Daten für einen bestimmten Zeitraum auszugeben, gilt der gewählte Zeitraum nur für Widgets, die historische Daten

anzeigen. Für Widgets, die aktuelle Daten für den Zeitpunkt des Durchsuchens anzeigen, ist der Parameter Zeitraum nicht anwendbar.

Die nachfolgende Tabelle führt die verfügbaren Widgets und deren Datenbereiche auf.

Widget-Name	Daten, die im Widget und in Berichten angezeigt werden
#CyberFit-Score pro Maschine	Aktuell
5 neueste Alarmmeldungen	Aktuell
Details zu aktiven Alarmmeldungen	Aktuell
Aktive Alarmmeldungen – Übersicht	Aktuell
Aktivitäten	Historisch
Aktivitätsliste	Historisch
Alarmverlauf	Historisch
Antimalware-Scan von Backups	Historisch
Antimalware-Scan von Dateien	Historisch
Backup-Scanning-Details (Bedrohungen)	Historisch
Backup-Status	Historisch – in den Spalten **Ausführungen insgesamt** und **Anzahl erfolgreiche Ausführungen** Aktuell – in allen anderen Spalten
Backup Storage-Nutzung	Historisch
Blockierte Peripheriegeräte	Historisch
Blockierte URLs	Aktuell
Cloud-Applikationen	Aktuell
Cloud-Workloads Schutzstatus	Aktuell
Cyber protection	Aktuell
Cyber Protection-Übersicht	Historisch
Data Protection-Karte	Historisch
Geräte	Aktuell
Disaster Recovery-Server getestet	Historisch
Disaster Recovery-Statistiken	Historisch
Erkannte Maschinen	Aktuell

Überblick der Laufwerksintegrität	Aktuell
Laufwerksintegritätsstatus	Aktuell
Laufwerksintegritätstatus nach physischen Geräten	Aktuell
Elektronisch signierte Dokumente über alle Endbenutzer hinweg an	Aktuell
Vorhandene Schwachstellen	Historisch
File Sync & Share-Statistiken	Aktuell
File Sync & Share-Storage-Nutzung durch Endbenutzer	Aktuell
Hardware-Änderungen	Historisch
Hardware-Details	Aktuell
Hardware-Inventarisierung	Aktuell
Übersicht der historischen Alarmmeldungen	Historisch
Speicherorteübersicht	Aktuell
Fehlende Updates nach Kategorie	Aktuell
Nicht geschützt	Aktuell
Beglaubigte Dateien über alle Endbenutzer hinweg	Aktuell
Notary-Statistiken	Aktuell
Verlauf der Patch-Installation	Historisch
Status der Patch-Installation	Historisch
Übersicht der Patch-Installation	Historisch
Gepatchte Schwachstellen	Historisch
Patches installiert	Historisch
Schutzstatus	Aktuell
Kürzlich betroffen	Historisch
Remote-Sitzungen	Historisch
Sicherheitsvorfall-Burndown	Historisch
Sicherheitsvorfall-MTTR (Mittlere	Historisch

Problemlösungszeit)	
Server geschützt mit Disaster Recovery	Aktuell
Software-Inventarisierung	Aktuell
Software-Überblick	Historisch
Bedrohungsstatus	Aktuell
Erkannten Bedrohungen nach Schutztechnologie	Historisch
Spitzenverteilung der Vorfälle pro Workload	Aktuell
Verwundbare Maschinen	Aktuell
Workload-Netzwerkstatus	Aktuell
Workloads gesichert	Historisch
Workloads-Schutzstatus	Aktuell

Integrationen

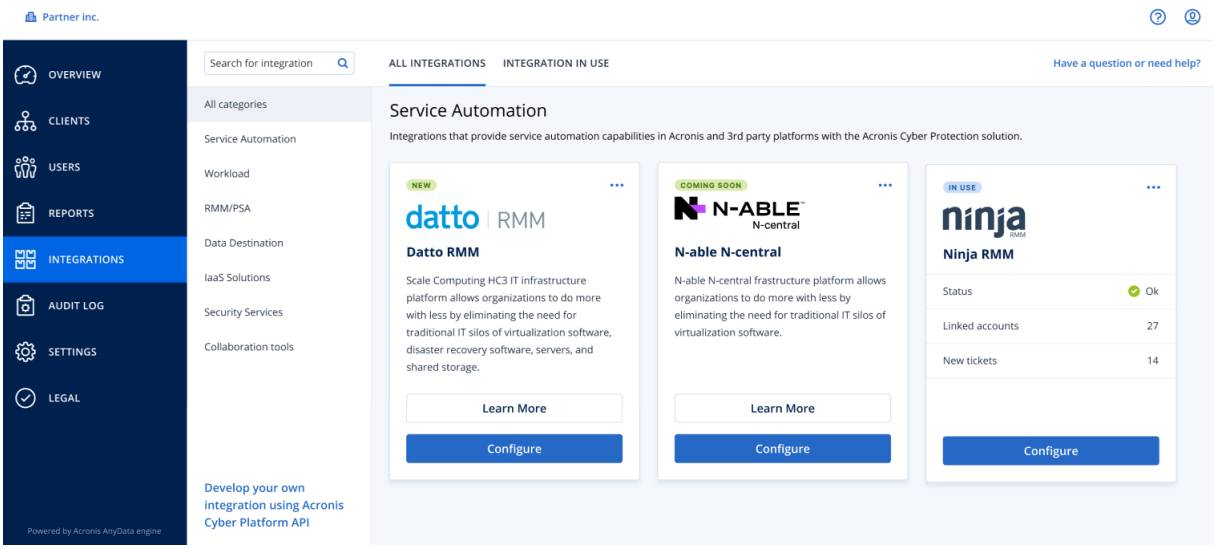
Katalog der Integrationen

Diese Seite dient als globaler Ort, an dem alle integrierbaren Applikationen registriert und die Informationen zu diesen aktualisiert werden.
Von hier aus können neue Integrationen hinzugefügt oder vorhandene geändert werden.

Hinweis
Nur Benutzer mit der Rolle **Firmenadministrator** dürfen die Integrationskonfiguration ändern.

Alle Integrationen

Auf der Registerkarte **Alle Integrationen** wird eine Liste mit allen derzeit verfügbaren Integrationen angezeigt, die als Kacheln nebeneinander angeordnet sind.



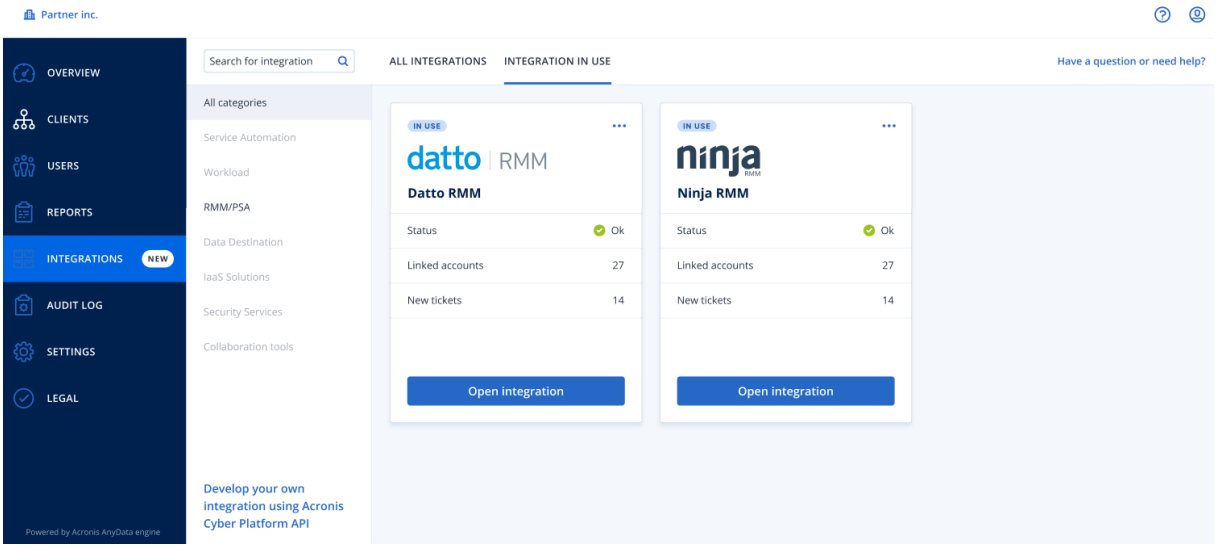
Auf jeder Kachel werden eine kurze Produktbeschreibung und zwei zusätzliche Optionen angezeigt:

- **Mehr erfahren** – klicken Sie auf diese Schaltfläche, wenn Sie mehr Informationen über die jeweilige Integration erhalten wollen:
  - **Integrationsfunktionen**
  - **Dokumentations-Links**
  - **Support-Kontakte**
- **Konfigurieren** – verwenden Sie diese Option, wenn Sie einige Integrationseinstellungen bearbeiten wollen.

Kacheln, die inaktive Integrationen darstellen, werden grau dargestellt und sind deaktiviert. Sie können außerdem mit dem Hinweis '**Demnächst verfügbar**' gekennzeichnet sein.

Verwendete Integrationen

Auf der Registerkarte **Verwendete Integrationen** wird eine Liste aller Integrationen angezeigt, die derzeit aktiv verwendet werden – jeweils ergänzt um einige allgemeine Informationen.



Klicken Sie auf **Integration öffnen**, um direkt auf die entsprechende Applikation zuzugreifen.

Auf der linken Seite finden Sie eine Liste der Integrationskategorien, in der alle vorhandenen Applikationen in bestimmte Gruppen (wie Service-Automatisierung, Workload, RMM/PSA usw.) eingeteilt sind. Wenn Sie auf eine einzelne Kategorie klicken, werden diejenigen Integrationen angezeigt, die zu dieser bestimmten Gruppe gehören. Eine Kategorie, die Sie sich gerade anzeigen lassen, wird hervorgehoben.

Verwenden Sie die Option **Suchen**, wenn Sie Abfragen durchführen und nach bestimmten Integration suchen wollen.

Sie können die Liste der Integrationen nach Kategorien und Bezeichnungen (Labels) filtern. Die Bezeichnungen (Labels) werden alphabetisch sortiert. Wenn keine Ergebnisse gefunden werden, können Sie Ihre Suche auf weitere Kategorien ausdehnen.

Wenn Sie eine Applikation deaktivieren wollen, klicken Sie in der rechten oberen Kachel-Ecke auf das Drei-Punkte-Symbol (...) und wählen Sie den Befehl **Deaktivieren**.

Falls Sie daran interessiert sind, Ihre eigene Integration zu entwickeln, wird außerdem ein Link zur Acronis API-Dokumentation bereitgestellt.

Zugriff auf die Weboberfläche beschränken

Sie können den Zugriff auf die Weboberfläche einschränken, indem Sie eine Liste von IP-Adressen spezifizieren, über die sich die Benutzer an der Weboberfläche anmelden dürfen.

Diese Beschränkung gilt auch für Zugriffe auf das Verwaltungsportal über die API.

Diese Beschränkung gilt nur für die Ebene, für die sie eingerichtet wurde. Sie gilt *nicht* für die Mitglieder untergeordneter Abteilungen.

So beschränken Sie den Zugriff auf die Weboberfläche

1. Melden Sie sich am Management-Portal an.
2. Gehen Sie zu der Abteilung, für die Sie den Zugriff beschränken wollen.
3. Klicken Sie auf **Einstellungen** –> **Sicherheit**.
4. Wählen Sie das Kontrollkästchen **Anmeldekontrolle aktivieren** aus.
5. Spezifizieren Sie bei **Zulässige IP-Adressen** diejenigen IP-Adressen, die Zugriff erhalten sollen. Sie können für Ihre Eingabe jeden der folgenden Parameter verwenden, jeweils per Semikolon abgetrennt:
   - IP-Adressen, beispielsweise: 192.0.2.0
   - IP-Bereiche, beispielsweise: 192.0.2.0-192.0.2.255
   - Subnetze, beispielsweise: 192.0.2.0/24
6. Klicken Sie auf **Speichern**.

Den Zugriff auf Ihre Firma beschränken

Firmenadministratoren können den Zugriff von höherstufigen Administratoren auf die Firma beschränken.

Wenn der Zugriff auf die Firma beschränkt ist, können die Administratoren des übergeordneten Mandanten nur noch die Eigenschaften der Firma ändern. Sie können weder die Benutzerkonten noch untergeordneten Abteilungen sehen.

So beschränken Sie den Zugriff auf die Firma

1. Melden Sie sich am Management-Portal an.
2. Klicken Sie auf **Einstellungen** –> **Sicherheit**.
3. Deaktivieren Sie die Option **Support-Zugang**.
4. Klicken Sie auf **Speichern**.

API-Clients verwalten

Sie können Drittherstellersysteme in Cyber Protect Cloud integrieren, indem Sie dessen APIs (Application Programming Interfaces, Anwendungsprogrammierschnittstellen) verwenden. Der Zugriff auf diese APIs wird über API-Clients ermöglicht, die ein integraler Bestandteil des OAuth 2.0-Autorisierungsframeworks der Plattform sind.

Was ist ein API-Client?

Ein API-Client ist ein spezielles Plattform-Konto, welches ein Drittherstellersystem repräsentieren soll, welches authentifiziert und autorisiert werden muss, um auf Daten in den APIs der Plattform und deren Services zugreifen zu können.

Der Zugriff des Clients ist auf einem Mandanten beschränkt, wo ein Administrator den Client und dessen Untermandanten erstellt.

Bei seiner Erstellung erbt der Client die Service-Rollen des Administratorkontos. Diese Rollen können später nicht mehr geändert werden. Eine Änderung der Rollen des Administratorkontos oder dessen Deaktivierung hat keine Auswirkungen auf den Client.

Die Client-Anmeldedaten bestehen aus dem eindeutigen Bezeichner (der ID) und einem geheimen Wert (auch kurz 'Geheimnis' genannt). Die Anmeldedaten verfallen nicht und können auch nicht verwendet werden, um sich am Management-Portal oder einer der Service-Konsolen anzumelden. Der geheime Wert kann zurückgesetzt werden.

Für den Client kann keine Zwei-Faktor-Authentifizierung aktiviert werden.

Eine typische Integrationsprozedur

1. Ein Administrator erstellt einen API-Client in einem Mandanten, den ein Drittherstellersystem verwalten soll.
2. Der Administrator aktiviert den OAuth 2.0-Client-Anmeldeinformationsfluss in dem Drittherstellersystem.

   Gemäß diesem Informationsfluss sollte das System, bevor es über die API auf den Mandanten und dessen Services zugreift, zunächst die Anmeldedaten des erstellten Clients mithilfe der Autorisierungs-API an die Plattform übermitteln. Die Plattform generiert ein Sicherheitstoken und sendet dieses zurück – eine eindeutige kryptische Zeichenfolge, die diesem speziellen Client zugewiesen wird. Das System muss dieses Token dann allen API-Anforderungen hinzufügen.

   Ein solches Sicherheitstoken macht es unnötig, dass die Anmeldedaten des Clients mit den API-Anforderungen übermittelt werden müssen. Zur Erhöhung der Sicherheit verfällt das entsprechende Token nach zwei Stunden. Nach diesem Zeitraum schlagen alle API-Anfragen mit dem abgelaufenen Token fehl, sodass das System ein neues Token von der Plattform anfordern muss.

Weitere Informationen zur hier verwendeten Autorisierung und den Plattform-APIs finden Sie in der Anleitung für Entwickler (Developer's Guide) unter https://developer.acronis.com/doc/account-management/v2/guide/index.

Einen API-Client erstellen

1. Melden Sie sich am Management-Portal an.
2. Klicken Sie auf **Einstellungen** –> **API-Clients** –> **API-Client erstellen**.

3. Geben Sie einen Namen für den API-Client ein.
4. Klicken Sie auf **Weiter**.
   Der API-Client wird standardmäßig mit dem Status **Aktiv** erstellt.
5. Kopieren und speichern Sie die ID und den geheimen Wert (das 'Geheimnis') des Clients sowie die Datacenter-URL. Diese benötigen Sie, wenn Sie den OAuth 2.0-Client-Anmeldeinformationsfluss in dem Drittherstellersystem aktivieren wollen.

   Wichtig
   Der geheime Wert wird aus Sicherheitsgründen nur einmal anzeigt! Dieser Wert kann nicht wiederhergestellt werden, wenn Sie ihn verlieren. Sie können ihn nur zurücksetzen.

6. Klicken Sie auf **Fertig**.

Den geheimen Wert eines API-Clients zurücksetzen

1. Melden Sie sich am Management-Portal an.
2. Klicken Sie auf **Einstellungen** –> **API-Clients**.
3. Suchen Sie in der Liste nach dem gewünschten Client.
4. Klicken Sie auf und anschließend auf **Geheimnis zurücksetzen**.
5. Klicken Sie auf **Weiter**, um Ihre Entscheidung zu bestätigen.
   Es wird ein neuer geheimer Wert generiert. Die Client-ID und Datacenter-URL werden nicht geändert.
   Alle Sicherheitstoken, die diesem Client zugewiesen wurden, verfallen sofort und alle weitere API-Anforderungen, die mit diesen Tokens erfolgen, werden fehlschlagen.
6. Kopieren und speichern Sie den neuen geheimen Wert (das 'Geheimnis') des Clients.

   Wichtig
   Der geheime Wert wird aus Sicherheitsgründen nur einmal anzeigt! Dieser Wert kann nicht wiederhergestellt werden, wenn Sie ihn verlieren. Sie können ihn nur zurücksetzen.

7. Klicken Sie auf **Fertig**.

Einen API-Client deaktivieren

1. Melden Sie sich am Management-Portal an.
2. Klicken Sie auf **Einstellungen** –> **API-Clients**.
3. Suchen Sie in der Liste nach dem gewünschten Client.
4. Klicken Sie auf und anschließend auf **Deaktivieren**.
5. Bestätigen Sie Ihre Entscheidung.
   Der Status des Clients wird zu **Deaktiviert** geändert.

Alle API-Anforderungen mit Sicherheitstokens, die diesem Client zugewiesen wurden, werden fehlschlagen. Aber die Tokens verfallen nicht sofort. Die Deaktivierung des Clients hat keinen Einfluss auf den Ablaufzeitpunkt der Tokens.

Sie können den Client jederzeit wieder reaktivieren.

Einen deaktivierten API-Client wieder aktivieren

1. Melden Sie sich am Management-Portal an.
2. Klicken Sie auf **Einstellungen** –> **API-Clients**.
3. Suchen Sie in der Liste nach dem gewünschten Client.
4. Klicken Sie auf und anschließend auf **Aktivieren**.

   Der Status des Clients wird zu **Aktiv** geändert.

   Alle API-Anforderungen mit Sicherheitstokens, die diesem Client zugewiesen wurden, sind erfolgreich, solange diese Tokens noch nicht abgelaufen sind.

Einen API-Client löschen

1. Melden Sie sich am Management-Portal an.
2. Klicken Sie auf **Einstellungen** –> **API-Clients**.
3. Suchen Sie in der Liste nach dem gewünschten Client.
4. Klicken Sie auf und anschließend auf **Löschen**.
5. Bestätigen Sie Ihre Entscheidung.

   Alle Sicherheitstoken, die diesem Client zugewiesen wurden, verfallen sofort und alle weitere API-Anforderungen, die mit diesen Tokens erfolgen, werden fehlschlagen.

Wichtig

Ein einmal gelöschter Client kann nicht wiederhergestellt werden!

Index

#

#CyberFit-Score pro Maschine 48

A

Agenten automatisch aktualisieren 36

Aktionen-Berichte 69

Aktionen-Dashboard 45

Alarmmeldungen zum Laufwerksintegritätsstatus 55

Alle Integrationen 90

Anforderungen an das Kennwort 17

Antimalware Protection-Widgets 76

API-Clients verwalten 92

Auf das Management-Portal und die Services zugreifen 18

B

Backup-Quotas 8, 14

Backup-Scanning-Details 60

Backup-Widgets 77

Benutzerdefinierte Nutzungsberichte konfigurieren 68

Berichte 67

Berichtsdaten je nach Widget-Typ 86

Berichtstyp 67

Berichtsumfang 67

Blockierte URLs 61

D

Data Loss Prevention-Widget 80

Data Protection-Karte 56

Daten für kürzlich betroffene Workloads herunterladen 61

Daten in Nutzungsberichten 69

Den geheimen Wert eines API-Clients zurücksetzen 94

Den Kurzübersichtsbericht anpassen 83

Den Zugriff auf Ihre Firma beschränken 92

Die Benachrichtigungseinstellungen für einen Benutzer ändern 25

Die Eigentümerschaft eines Benutzerkontos übertragen 28

Die Einstellungen des Kurzübersichtsberichts konfigurieren 82

Die Zwei-Faktor-Authentifizierung bei Verlust des Zweit-Faktor-Gerätes zurücksetzen 35

Die Zwei-Faktor-Authentifizierung für Benutzer verwalten 33

Die Zwei-Faktor-Authentifizierung für Ihren Mandanten einrichten 32

Die Zwei-Faktoren-Einrichtung zwischen Mandantenebenen weitergeben 31

Disaster Recovery-Quotas 11

Disaster Recovery-Widgets 79

E

Ein Administratorkonto aktivieren 17

Ein Benutzerkonto deaktivieren und aktivieren 27

Ein Benutzerkonto erstellen 19

Ein Benutzerkonto löschen 27

Ein Service Desk-Ticket erstellen 42

Eine Abteilung erstellen 19

Eine typische Integrationsprozedur 93

Einen API-Client deaktivieren 94

Einen API-Client erstellen 93

Einen API-Client löschen 95

Einen deaktivierten API-Client wieder aktivieren 95

Einen Kurzübersichtsbericht erstellen 83

Einschränkungen 51

Endpoint Detection & Response (EDR)-Widgets 48

Erkannte Maschinen 47

F

Fehlende Updates nach Kategorie 59

Felder im Überwachungsprotokoll 65

File Sync & Share-Quotas 13, 15

File Sync & Share-Widgets 81

Filter und Suche 66

Für jeden Service verfügbare Benutzerrollen 21

G

Geplante Nutzungsberichte konfigurieren 68

I

Im Management-Portal navigieren 18

Integrationen 90

J

Je nach Benutzerrolle empfangene Benachrichtigungen 27

K

Katalog der Integrationen 90

Konten und Abteilungen 6

Kürzlich betroffen 60

Kurzübersicht 73

Kurzübersicht-Widgets 73

Kurzübersichtsberichte senden 85

L

Laufwerksintegrität-Widgets 53

M

Metriken mit einer Nutzung von Null 67

Monitoring 33, 45

MTTR (Mittlere Problemlösungszeit) für Vorfälle 49

N

Notary-Quotas 13, 15

Notary-Widgets 81

Nutzung 45

Nutzungsberichte 67

P

Physischer Datenversand-Quotas 13

Q

Quota-Verwaltung 7

Quota für Storage 15

Quotas für Cloud-Datenquellen 8

Quotas für Ihr Unternehmen einsehen 8

Quotas für Ihre Benutzer definieren 14

Quotas für Storage 10

S

Schritt-für-Schritt-Anleitungen 17

Schutz vor Brute-Force-Angriffen 35

Schutzstatus 46

Service Desk-Tickets aktualisieren 43

Service Desk-Tickets einsehen 41

Sicherheitsvorfall-Burndown 50

Sitzungsverlauf 64

So können Sie Agenten automatisch aktualisieren lassen 37

So können Sie die Agenten-Updates überwachen 38

So können Sie die vertrauenswürdigen Browser eines Benutzers zurücksetzen 34

So können Sie die Zwei-Faktor-Authentifizierung für einen Benutzer aktivieren 35

So können Sie die Zwei-Faktor-Authentifizierung für einen Benutzer deaktivieren 34

So können Sie die Zwei-Faktor-Authentifizierung für einen Benutzer zurücksetzen 33

So können Sie die Zwei-Faktor-Authentifizierung für Ihren Mandanten aktivieren 32

So können Sie die Zwei-Faktor-Authentifizierung für Ihren Mandanten deaktivieren 33

Spitzenverteilung der Vorfälle pro Workload 49

Status der Patch-Installation 58

T

Task-Verwaltung 41

U

Über das Management-Portal 6

Über dieses Dokument 5

Übersicht der Patch-Installation 59

Überwachung der Laufwerksintegrität 51

Überwachungsprotokoll 64

Und so funktioniert es 29, 52

Unterstützte Webbrowser 16

Unveränderlichen Storage konfigurieren 38

V

Verhindern, dass sich nicht lizenzierte Microsoft 365-Benutzer anmelden können 11

Verlauf der Patch-Installation 59

Verwendete Integrationen 91

Verwundbare Maschinen 57

Vorhandene Schwachstellen 58

W

Was ist ein API-Client? 93

Widget für Schwachstellenbewertung 57

Widgets für Hardware-Inventarisierung 63

Widgets für Patch-Installation 58

Widgets für Schwachstellenbewertung und Patch-Verwaltung 78

Widgets für Software-Inventarisierung 62

Workload-Netzwerkstatus 51

Workloads-Überblick-Widgets 73

Z

Zeitzonen in Berichten 85

Zugriff auf die Weboberfläche beschränken 91

Zwei-Faktor-Authentifizierung einrichten 29

Zwischen dem Management-Portal und den Service-Konsolen umschalten 18