# Beheerportal

21.10

Gids voor bedrijfbeheerders

REVISIE: 1-11-2021

# Inhoudsopgave

# 1 Over dit document

Dit document is bedoeld voor klantbeheerders die de cloudbeheerportal willen gebruiken om gebruikersaccounts, eenheden en quota's te maken en te beheren, om de toegang tot hun cloudorganisatie te configureren en te beheren en het gebruik en de activiteiten in de cloudorganisatie te bewaken.

# 2 Over de beheerportal

De beheerportal is een webinterface voor het cloudplatform dat services biedt voor gegevensbescherming.

Elke service heeft een eigen webinterface, de zogenaamde serviceconsole, maar met de beheerportal kunnen beheerders meer doen, zoals het gebruik van services beheren, gebruikersaccounts en eenheden maken, rapporten genereren, enzovoort.

## 2.1 Accounts en eenheden

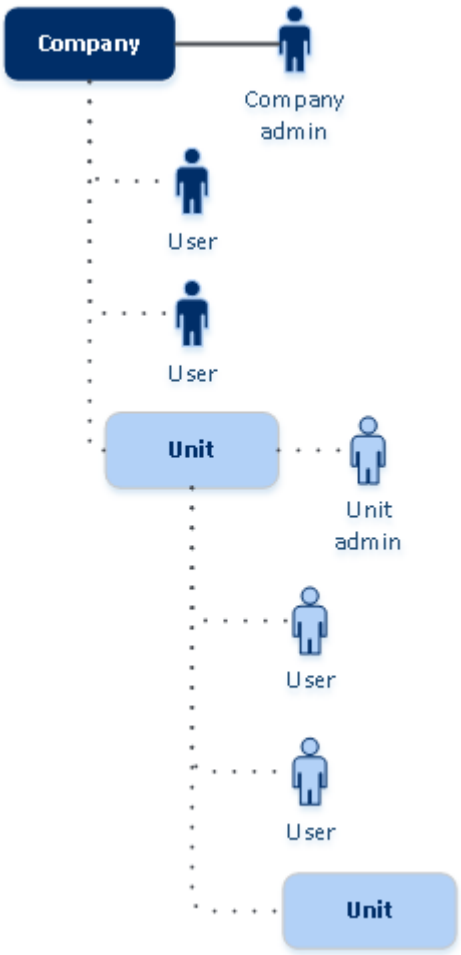
Er zijn twee typen gebruikersaccounts: beheerdersaccounts en gebruikersaccounts.

- **Beheerders** hebben toegang tot de beheerportal. Ze hebben de beheerdersrol in alle services.
- **Gebruikers** hebben geen toegang tot de beheerportal. Hun toegang tot de services een hun rollen in de services worden gedefinieerd door een beheerder.

Beheerders kunnen eenheden maken. Dit zijn meestal de eenheden of afdelingen van hun organisatie. Elk account bestaat ofwel op bedrijfsniveau of in een eenheid.

Een beheerder kan eenheden, beheerdersaccounts en gebruikersaccounts beheren op het eigen niveau in de hiërarchie of op een lager niveau.

Het volgende diagram bevat drie hiërarchieniveaus: voor het bedrijf en twee eenheden. Optionele eenheden en accounts worden weergegeven met een stippellijn.




De volgende tabel bevat een overzicht van de bewerkingen die door beheerders en gebruikers kunnen worden uitgevoerd.

| Bewerking | Gebruikers | Beheerders |
|---|---|---|
| Eenheden maken | Nee | Ja |
| Accounts maken | Nee | Ja |
| De software downloaden en installeren | Ja | Ja |
| Services gebruiken | Ja | Ja |
| Rapporten maken over het servicegebruik | Nee | Ja |

## 2.2 Quotabeheer

Met **quota's** kunt u beperkingen instellen voor het gebruik van de service door tenants.

In de beheerportal kunt u de servicequota's bekijken die door uw serviceprovider zijn toegewezen aan uw organisatie, maar u kunt deze niet beheren.

U kunt de servicequota's voor uw gebruikers beheren.

### 2.2.1 Quota's voor uw organisatie bekijken

Ga in de beheerportal naar **Overzicht** > **Gebruik**. U ziet een dashboard met de toegewezen quota's voor uw organisatie. De quota's voor elke service worden op een afzonderlijk tabblad weergegeven.

## Quota's voor back-ups

U kunt waarden opgeven voor de cloudopslagquota, de quota voor lokale back-up en het maximale aantal machines/apparaten/websites dat de gebruiker mag beveiligen. De volgende quota's zijn beschikbaar.

### Quota's voor apparaten

- **Werkstations**
- **Servers**
- **Virtuele machines**
- **Mobiele apparaten**
- **Webhostingservers** (op Linux gebaseerde fysieke of virtuele servers waarop een Plesk-, cPanel-, DirectAdmin-, VirtualMin- of ISPManager-besturingspaneel wordt uitgevoerd)
- **Websites**

Een machine/apparaat/website wordt beschouwd als beschermd zolang hierop ten minste één beschermingsschema wordt toegepast. Een mobiel apparaat is beveiligd na de eerste backup.

Wanneer de uitbreiding voor een aantal apparaten wordt overschreden, kan de gebruiker geen beschermingsschema toepassen voor meer apparaten.

### Quota's voor cloudgegevensbronnen

- **Microsoft 365-seats**

  Deze quota wordt door de serviceprovider toegepast op het hele bedrijf. Bedrijfbeheerders kunnen de quota en het gebruik bekijken in de beheerportal.

  Licenties voor de Microsoft 365-seats zijn afhankelijk van de geselecteerde factureringsmodus voor Cyber Protection.

  Meer informatie over de beschikbare licentieopties voor de factureringsmodus per gigabyte vindt u in Cyber Protect Cloud: Licenties voor Microsoft 365 per GB.

  Meer informatie over de beschikbare licentieopties voor de factureringsmodus per workload vindt u in Cyber Protect Cloud: Wijzigingen van de licenties en prijzen voor Microsoft 365.
- **Microsoft 365 Teams**

  Deze quota wordt door de serviceprovider toegepast op het hele bedrijf. Met deze quota wordt de mogelijkheid om Microsoft 365 Teams te beschermen in- of uitgeschakeld. Daarnaast wordt ook ingesteld wat het maximale aantal teams is dat kan worden beschermd. Voor de

bescherming van één team, ongeacht het aantal leden of kanalen, is één quota vereist. Bedrijfbeheerders kunnen de quota en het gebruik bekijken in de beheerportal.

- **Microsoft 365 SharePoint Online**

  Deze quota wordt door de serviceprovider toegepast op het hele bedrijf. Met deze quota wordt de mogelijkheid om SharePoint Online-sites te beschermen in- of uitgeschakeld. Daarnaast wordt ook ingesteld wat het maximale aantal siteverzamelingen en groepssites is dat kan worden beschermd.

  Bedrijfbeheerders kunnen de quota bekijken in de beheerportal. Ze kunnen ook de quota, samen met de hoeveelheid opslagruimte voor de back-ups van SharePoint Online, bekijken in de gebruiksrapporten.
- **Google Workspace-seats**

  Deze quota wordt door de serviceprovider toegepast op het hele bedrijf. Het bedrijf kan toestemming hebben om **Gmail**-postvakken (met inbegrip van agenda en contacten), **Google Drive**-bestanden of beide te beveiligen. Bedrijfbeheerders kunnen de quota en het gebruik bekijken in de beheerportal.
- **Gedeelde Drive in Google Workspace**

  Deze quota wordt door de serviceprovider toegepast op het hele bedrijf. Met deze quota wordt de mogelijkheid om gedeelde Drives in Google Workspace te beschermen in- of uitgeschakeld. Als de quota is ingeschakeld, kan een willekeurig aantal gedeelde Drives worden beveiligd. Bedrijfbeheerders kunnen de quota in de beheerportal niet bekijken, maar kunnen in de gebruiksrapporten wel zien hoeveel opslagruimte in beslag wordt genomen door de back-ups van de gedeelde Drives.

  Een back-up van gedeelde Drives in Google Workspace is alleen beschikbaar voor klanten die daarnaast ten minste één quota voor Google Workspace-seats hebben. Deze quota wordt alleen geverifieerd en wordt niet opgenomen.

Een Microsoft 365-seat wordt beschouwd als beschermd zolang er ten minste één beschermingsschema wordt toegepast op het postvak of OneDrive van de gebruiker. Een Google Workspace-seat wordt beschouwd als beschermd zolang er ten minste één beschermingsschema wordt toegepast op het postvak of Google Drive van de gebruiker.

Wanneer de uitbreiding voor een aantal seats wordt overschreden, kan een bedrijfbeheerder geen beschermingsschema toepassen voor meer seats.

## Quota's voor opslag

- **Lokale back-up**

  De quota voor **Lokale back-up** beperkt de totale grootte van lokale back-ups die worden gemaakt met behulp van de cloudinfrastructuur. U kunt geen uitbreiding instellen voor deze quota.
- **Cloudresources**

  De quota voor **cloudresources** combineert de quota voor back-upopslag en de quota's voor noodherstel. De quota voor back-upopslag beperkt de totale omvang van de back-ups in de

cloudopslag. Wanneer de uitbreiding van de back-upopslagquota wordt overschreden, mislukken de back-ups.

## Quota's voor noodherstel

**Opmerking**
De opties voor noodherstel zijn alleen beschikbaar in de Disaster Recovery-add-on.

Deze quota's worden door de serviceprovider toegepast op het hele bedrijf. Bedrijfbeheerders kunnen de quota's en het gebruik in de beheerportal bekijken, maar kunnen geen quota's voor een gebruiker instellen.

- **Noodherstelopslag**
  Deze opslag wordt gebruikt door primaire en herstelservers. Als de maximale uitbreiding voor deze quota wordt bereikt, kunt u geen primaire en herstelservers maken, en geen schijven van de bestaande primaire servers toevoegen/uitbreiden. Als de maximale uitbreiding voor deze quota's wordt overschreden, kunt u geen failover starten en ook geen gestopte server starten. Actieve servers blijven actief.
- **Compute-punten**
  Deze quota beperkt de CPU- en RAM-resources die worden verbruikt door primaire servers en herstelservers gedurende een factureringsperiode. Als de maximale uitbreiding voor deze quota wordt bereikt, worden alle primaire en herstelservers afgesloten. U kunt deze servers pas weer gebruiken bij het begin van de volgende factureringsperiode. De standaardfactureringsperiode is een volledige kalendermaand.
  Wanneer de quota wordt uitgeschakeld, kunnen de servers niet worden gebruikt, ongeacht de factureringsperiode.
- **Openbare IP-adressen**
  Deze quota beperkt het aantal openbare IP-adressen dat kan worden toegewezen aan de primaire en herstelservers. Als de maximale uitbreiding voor deze quota wordt bereikt, kunt u geen openbare IP-adressen inschakelen voor meer servers. U kunt verhinderen dat een server een openbaar IP-adres gebruikt door het selectievakje **Openbaar IP-adres** uit te schakelen in de serverinstellingen. Vervolgens kunt u toestaan dat een andere server een openbaar IP-adres gebruikt. Dit is doorgans niet hetzelfde adres.
  Wanneer de quota wordt uitgeschakeld, maken alle servers geen gebruik meer van openbare IP-adressen, zodat ze niet meer bereikbaar zijn vanaf internet.
- **Cloudservers**
  Deze quota beperkt het totale aantal primaire en herstelservers. Als de maximale uitbreiding voor deze quota is bereikt, kunt u geen primaire of herstelservers maken.
  Wanneer de quota wordt uitgeschakeld, worden de servers weergegeven in de serviceconsole, maar de enige beschikbare bewerking is **Verwijderen**.
- **Internettoegang**
  Met deze quota wordt de internettoegang vanaf primaire en herstelservers in- of uitgeschakeld.

Wanneer de quota wordt uitgeschakeld, kunnen de primaire en herstelservers geen verbinding maken met internet.

## Quota's voor File Sync & Share

Deze quota's worden door de serviceprovider toegepast op het hele bedrijf. Bedrijfbeheerders kunnen de quota's en het gebruik bekijken in de beheerportal.

- **Gebruikers**
  Met deze quota definieert u het aantal gebruikers dat toegang krijgt tot deze service.
- **Cloudopslag**
  Dit is cloudopslag voor het opslaan van gebruikersbestanden. De quota bepaalt de toegewezen ruimte voor een tenant in de cloudopslag.

## Quota's voor Physical Data Shipping

De quota's voor de Physical Data Shipping-service worden per station verbruikt. U kunt de initiële back-ups van meerdere machines op één harde schijf opslaan.

Deze quota's worden door de serviceprovider toegepast op het hele bedrijf. Bedrijfbeheerders kunnen de quota's en het gebruik in de beheerportal bekijken, maar kunnen geen quota's voor een gebruiker instellen.

- **Naar de cloud**
  Hiermee kunt u een initiële back-up naar het clouddatacentrum verzenden via een hardeschijfstation. Met deze quota definieert u het maximale aantal stations dat wordt overgezet naar het clouddatacentrum.

## Quota's voor notarisatie

Deze quota's worden door de serviceprovider toegepast op het hele bedrijf. Bedrijfbeheerders kunnen de quota's en het gebruik bekijken in de beheerportal.

- **Notarisatieopslag**
  De notarisatieopslag is de cloudopslag waar de genotariseerde bestanden, ondertekende bestanden en bestanden die nog worden genotariseerd of ondertekend, worden opgeslagen. Deze quota definieert de maximale ruimte die door deze bestanden kan worden ingenomen.
  Als u dit quotagebruik wilt verminderen, kunt u de reeds genotariseerde of ondertekende bestanden verwijderen uit de notarisatieopslag.
- **Notarisaties**
  Deze quota definieert het maximale aantal bestanden dat kan worden genotariseerd met Notary-service. Een bestand wordt beschouwd als genotariseerd zodra het naar de notarisatieopslag wordt geüpload en de notarisatiestatus wordt gewijzigd in Wordt uitgevoerd.
  Als hetzelfde bestand meerdere keren wordt genotariseerd, telt elke keer als een nieuwe notarisatie.
- **eSignatures**

Deze quota definieert het maximale aantal bestanden dat kan worden ondertekend met Notary-service. Een bestand wordt beschouwd als ondertekend zodra het wordt verzonden voor ondertekening.

## 2.2.2 Quota's voor uw gebruikers definiëren

Met **quota's** kunt u beperkingen instellen voor het gebruik van de service door gebruikers. Als u de quota's wilt instellen voor een gebruiker, selecteert u de gebruiker op het tabblad **Gebruikers** en klikt u op het potloodpictogram in het gedeelte **Quota's**.

Wanneer de quota wordt overschreden, wordt een melding verzonden naar het e-mailadres van de gebruiker. Als u geen quota-uitbreiding instelt, wordt de quota beschouwd als '**soft**'. Dit betekent dat beperkingen voor het gebruik van de Cyber Protection-service niet worden toegepast.

Wanneer u de quota-uitbreiding opgeeft, wordt de quota beschouwd als '**hard**'. Met een **uitbreiding** kan de gebruiker de quota overschrijden met de opgegeven waarde. Wanneer de uitbreiding wordt overschreden, worden er beperkingen toegepast voor het gebruik van de service.

**Voorbeeld**

**Softe quota**: U hebt de quota voor werkstations ingesteld op 20. Zodra het aantal beschermde werkstations van de gebruiker 20 is, krijgt de gebruiker een melding per e-mail. De Cyber Protection-service blijft beschikbaar.

**Harde quota**: Als u de quota voor werkstations hebt ingesteld op 20 en de uitbreiding 5 is, dan krijgt de gebruiker een melding per e-mail zodra het aantal beveiligde werkstations 20 is. De Cyber Protection-service wordt uitgeschakeld wanneer het aantal van 25 wordt bereikt.

### Quota's voor back-ups

U kunt de quota opgeven voor back-upopslag en het maximale aantal machines/apparaten/websites dat de gebruiker mag beveiligen. De volgende quota's zijn beschikbaar.

#### Quota's voor apparaten

- **Werkstations**
- **Servers**
- **Virtuele machines**
- **Mobiele apparaten**
- **Webhostingservers** (op Linux gebaseerde fysieke of virtuele servers waarop een Plesk-, cPanel-, DirectAdmin-, VirtualMin- of ISPManager-besturingspaneel wordt uitgevoerd)
- **Websites**

Een machine/apparaat/website wordt beschouwd als beschermd zolang hierop ten minste één beschermingsschema wordt toegepast. Een mobiel apparaat is beveiligd na de eerste backup.

Wanneer de uitbreiding voor een aantal apparaten wordt overschreden, kan de gebruiker geen beschermingsschema toepassen voor meer apparaten.

### Quota's voor opslag

- **Back-upopslag**

De quota voor back-upopslag beperkt de totale omvang van de back-ups in de cloudopslag. Wanneer de uitbreiding van de back-upopslagquota wordt overschreden, mislukken de back-ups.

### Quota's voor File Sync & Share

U kunt de volgende quota's voor File Sync & Share instellen voor een gebruiker:

- **Persoonlijke opslagruimte**
  Dit is cloudopslag voor het opslaan van de bestanden van een gebruiker. De quota bepaalt de toegewezen ruimte voor een gebruiker in de cloudopslag.

### Quota's voor notarisatie

U kunt de volgende notarisatiequota's definiëren voor een gebruiker:

- **Notarisatieopslag**
  De notarisatieopslag is de cloudopslag waar de genotariseerde bestanden, ondertekende bestanden en bestanden die nog worden genotariseerd of ondertekend, worden opgeslagen. Deze quota definieert de maximale ruimte die door deze bestanden kan worden ingenomen.
  Als u dit quotagebruik wilt verminderen, kunt u de reeds genotariseerde of ondertekende bestanden verwijderen uit de notarisatieopslag.
- **Notarisaties**
  Deze quota definieert het maximale aantal bestanden dat kan worden genotariseerd met Notary-service. Een bestand wordt beschouwd als genotariseerd zodra het naar de notarisatieopslag wordt geüpload en de notarisatiestatus wordt gewijzigd in Wordt uitgevoerd.
  Als hetzelfde bestand meerdere keren wordt genotariseerd, telt elke keer als een nieuwe notarisatie.
- **eSignatures**
  Deze quota definieert het maximale aantal bestanden dat kan worden ondertekend met Notary-service. Een bestand wordt beschouwd als ondertekend zodra het wordt verzonden voor ondertekening.

## 2.3 Ondersteunde webbrowsers

De webinterface ondersteunt de volgende webbrowsers:

- Google Chrome 29 of later
- Mozilla Firefox 23 of later
- Opera 16 of later

- Windows Internet Explorer 11 of later
- Microsoft Edge 25 of later
- Safari 8 of later uitgevoerd op de besturingssystemen macOS en iOS

Het is mogelijk dat de gebruikersinterface in andere webbrowsers (inclusief Safari-browsers die worden uitgevoerd op andere besturingssystemen) niet goed wordt weergegeven of dat bepaalde functies niet beschikbaar zijn.

# 3 Stapsgewijze instructies

De volgende stappen helpen u de basisfuncties van de beheerportal te gebruiken. Hierin wordt het volgende beschreven:

- Uw account activeren
- Toegang tot de beheerportal en de services
- Een eenheid maken
- Een gebruikersaccount maken

## 3.1 Een beheerdersaccount activeren

Nadat u zich hebt aangemeld voor een service, ontvangt u een e-mailbericht met de volgende informatie:

- **Een activeringslink voor het account**. Klik op de link en stel het wachtwoord voor het beheerdersaccount in. Het wachtwoord moet minimaal acht tekens lang zijn. Onthoud de gebruikersnaam die wordt weergegeven op de activeringspagina voor het account.
- **Een link naar de aanmeldingspagina**. De gebruikersnaam en het wachtwoord zijn hetzelfde als in de vorige stap.

## 3.2 Toegang tot de beheerportal en de services

1. Ga naar de aanmeldingspagina van de serviceconsole.
2. Typ de gebruikersnaam en klik op **Volgende**.
3. Typ het wachtwoord en klik op **Volgende**.
4. Voer een van de volgende handelingen uit:
   - Klik op **Beheerportal** om u aan te melden bij de beheerportal.
   - Klik op de naam van een service om u aan te melden bij de service.

De time-outperiode voor de beheerportal is 24 uur voor actieve sessies en 1 uur voor niet-actieve sessies.

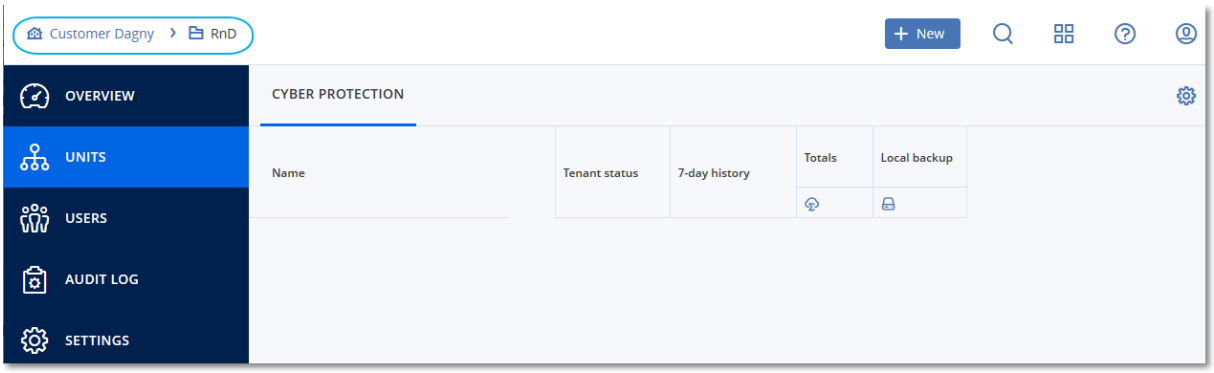
### 3.2.1 Schakelen tussen de beheerportal en de serviceconsoles

Als u wilt schakelen tussen de beheerportal en de serviceconsoles, klikt u op het -pictogram in de rechterbovenhoek en selecteert u vervolgens **Beheerportal** of de service die u wilt openen.

## 3.3 Navigatie in de beheerportal

Wanneer u de beheerportal gebruikt, werkt u steeds binnen het bedrijf of binnen een eenheid. Dit wordt aangegeven in de linkerbovenhoek.

Standaard wordt het bovenste hiërarchische niveau geselecteerd dat beschikbaar is voor u. Klik op de naam van de eenheid om in te zoomen op de hiërarchie. Klik op een naam in de linkerbovenhoek om terug te navigeren naar een hoger niveau.




Alleen het bedrijf of de eenheid waarin u op dat moment werkt, wordt weergegeven en beïnvloed door de diverse delen van de gebruikersinterface. Bijvoorbeeld:

- Met de knop **Nieuw** kunt u alleen een eenheid of gebruikersaccount maken in dit bedrijf of in deze eenheid.
- Op het tabblad **Eenheden** worden alleen de eenheden weergegeven die directe onderliggende eenheden zijn van dit bedrijf of deze eenheid.
- Op het tabblad **Gebruikers** worden alleen de gebruikersaccounts weergegeven die bestaan in dit bedrijf of deze eenheid.

## 3.4 Een eenheid maken

Sla deze stap over als u uw accounts niet wilt organiseren in eenheden.

Als u van plan bent later eenheden te maken, denk er dan aan dat bestaande accounts niet kunnen worden verplaatst tussen eenheden of tussen het bedrijf en eenheden. U moet eerst een eenheid maken en hierin vervolgens de accounts laden.

***Een eenheid maken***

1. Meld u aan bij de beheerportal.
2. Navigeer naar de eenheid waarvoor u een nieuwe eenheid wilt maken.
3. Klik in de rechterbovenhoek op **Nieuw** > **Eenheid**.
4. Geef bij **Naam** een naam op voor de nieuwe eenheid.
5. [Optioneel] Selecteer bij **Taal** de standaardtaal voor meldingen, rapporten en de software die binnen deze eenheid wordt gebruikt.
6. Voer een van de volgende handelingen uit:
   - Als u een eenheidbeheerder wilt maken, klikt u op **Volgende** en volgt u de stappen (vanaf stap 4) die worden beschreven in 'Een gebruikersaccount maken'.
   - Klik op **Opslaan en sluiten** om een eenheid zonder beheerder te maken. U kunt beheerders en gebruikers later toevoegen aan de eenheid.

De zojuist gemaakte eenheid wordt weergegeven op het tabblad **Eenheden**.

Als u de eenheidinstellingen wilt bewerken of de contactgegevens wilt opgeven, selecteert u de eenheid op het tabblad **Eenheden** en klikt u op het potloodpictogram in het gedeelte dat u wilt bewerken.

## 3.5 Een gebruikersaccount maken

Sla deze stap over als u geen aanvullende gebruikersaccounts wilt maken.

In de volgende gevallen kan het handig zijn om aanvullende accounts te maken:

- Accounts voor bedrijfbeheerders: hiermee kunt u de beheertaken delen met andere mensen.
- Accounts voor eenheidbeheerders: hiermee kunt u het beheer delegeren aan andere mensen van wie de toegangsrechten zijn beperkt tot de betreffende eenheden.
- Gebruikersaccounts: hiermee kunt u instellen dat gebruikers alleen toegang hebben tot een subset van de services.

***Een gebruikersaccount maken***

1. Meld u aan bij de beheerportal.
2. Navigeer naar de eenheid waarvoor u een nieuwe gebruikersaccount wilt maken.
3. Klik in de rechterbovenhoek op **Nieuw** > **Gebruiker**.
4. Geef de volgende informatie op voor het account:
   - **Gebruikersnaam**

     **Belangrijk**
     Elk account moet een unieke gebruikersnaam hebben.

   - **E-mail**
   - [Optioneel]**Voornaam**
   - [Optioneel] **Achternaam**
   - Selecteer bij **Taal** de standaardtaal voor meldingen, rapporten en de software die wordt gebruikt voor dit account.
5. Selecteer de services waartoe de gebruiker toegang heeft en de rollen in iedere service.
   - Als u het selectievakje **Bedrijfbeheerder** inschakelt, heeft de gebruiker toegang tot de beheerportal en de beheerdersrol in alle services.
   - Als u het selectievakje **Eenheidbeheerder** inschakelt, heeft de gebruiker toegang tot de beheerportal, maar mogelijk niet tot de beheerdersrol voor de service. Dit hangt af van de service.
   - Anders heeft de gebruiker de rollen die u selecteert in de geselecteerde services.
6. Klik op **Maken**.

Het zojuist gemaakte gebruikersaccount wordt weergegeven op het tabblad **Gebruikers**.

Als u de gebruikersinstellingen wilt bewerken of de instellingen voor meldingen en quota's voor de gebruiker wilt opgeven, selecteert u de gebruiker op het tabblad **Gebruikers** en klikt u op het potloodpictogram in het gedeelte dat u wilt bewerken.

***Het wachtwoord van een gebruiker opnieuw instellen***

1. Ga in de beheerportal naar **Gebruikers**.
2. Selecteer de gebruiker van wie u het wachtwoord opnieuw wilt instellen en klik vervolgens op het ellipspictogram  > **Wachtwoord opnieuw instellen**.
3. Bevestig uw actie door te klikken op **Opnieuw instellen**.

De gebruiker kan het proces voor opnieuw instellen nu voltooien door de instructies in de ontvangen e-mail te volgen.

## 3.6 Gebruikersrollen beschikbaar voor elke service

Een gebruiker kan meerdere rollen hebben, maar slechts één rol per service.

Voor elke service kunt u definiëren welke rol aan een gebruiker wordt toegewezen.

| Service | Rol | Beschrijving |
|---|---|---|
| N.v.t. | Bedrijfbeheerder | Met deze rol worden ook beheerdersrechten voor alle services verleend.<br><br>Deze rol geeft toegang tot de acceptatielijst van het bedrijf. Als de Disaster Recovery-functie van de Bescherming-service is ingeschakeld voor het bedrijf, biedt deze rol ook toegang tot die functie. |
| Beheerportal | Beheerder | Met deze rol wordt toegang verkregen tot de beheerportal waar de beheerder gebruikers binnen de hele organisatie kan beheren. |
| | Alleen-lezen beheerder | De rol biedt alleen-lezen toegang tot alle objecten in de beheerportal. Dergelijke gebruikers hebben alleen-lezen toegang tot gegevens van andere gebruikers binnen de organisatie. |
| Bescherming | Beheerder | Met deze rol kunt u Bescherming configureren en beheren voor uw klanten.<br>De rol is vereist voor het configureren en beheren van de Disaster Recovery-functie en de acceptatielijst van het bedrijf. |
| | Alleen-lezen beheerder | De rol biedt alleen-lezen toegang tot alle objecten van de Bescherming-service. Dergelijke gebruikers hebben alleen-lezen toegang tot gegevens van andere gebruikers binnen de organisatie.<br>De alleen-lezen beheerder kan de Disaster Recovery-functie en de acceptatielijst van het bedrijf niet configureren en beheren. |

| | | |
|---|---|---|
| | Operator herstellen | De rol biedt toegang tot back-ups van Microsoft 365- en Google Workspace-organisaties en maakt herstel mogelijk, terwijl de toegang tot gevoelige inhoud wordt beperkt. |
| | Gebruiker | Met deze rol kunt u de Bescherming-service gebruiken, maar zonder administratorbevoegdheden. Dergelijke gebruikers hebben geen toegang tot gegevens van andere gebruikers binnen de organisatie. |
| File Sync & Share | Beheerder | Met deze rol kunt u File Sync & Share configureren en beheren voor uw gebruikers. |
| | Gebruiker | Met deze rol kan de service voor File Sync & Share worden gebruikt. Dergelijke gebruikers hebben geen toegang tot gegevens van andere gebruikers binnen de organisatie. |
| Notarisatie | Beheerder | Met deze rol kunt u Notary configureren en beheren voor uw gebruikers. |
| | Gebruiker | Met deze rol kunt u de Notary-service gebruiken, maar zonder administratorbevoegdheden. Dergelijke gebruikers hebben geen toegang tot gegevens van andere gebruikers binnen de organisatie. |

### 3.6.1 Rol van alleen-lezen beheerder

Een account met deze rol biedt alleen-lezen toegang tot de Cyberbescherming-webconsole en kan:

- Diagnostische gegevens verzamelen, zoals systeemrapporten.
- De herstelpunten van een back-up zien, maar niet de gedetailleerde inhoud van back-ups en geen bestanden, mappen of e-mails zien.

Een alleen-lezen beheerder kan niet:

- Taken starten of stoppen.
  Een alleen-lezen-beheerder kan bijvoorbeeld geen herstelbewerking starten en geen actieve back-up stoppen.
- Het bestandssysteem openen op bron- of doelmachines.
  Een alleen-lezen-beheerder kan bijvoorbeeld geen bestanden, mappen of e-mails zien op een machine waarvan een back-up is gemaakt.
- De instellingen wijzigen.
  Een alleen-lezen-beheerder kan bijvoorbeeld geen beschermingsschema maken of de instellingen ervan wijzigen.
- Gegevens maken, bijwerken of verwijderen.
  Een alleen-lezen-beheerder kan bijvoorbeeld geen back-ups verwijderen.

Alle UI-objecten die niet toegankelijk zijn voor een alleen-lezen beheerder, worden verborgen, met uitzondering van de standaardinstellingen van het beschermingsschema. Deze instellingen worden weergegeven, maar de knop **Opslaan** is niet actief.

Eventuele wijzigingen van de accounts en rollen worden weergegeven op het tabblad **Activiteiten**, inclusief de volgende details:

- Nieuwe wijzigingen
- Wie de wijzigingen heeft gemaakt
- Datum en tijd van de wijzigingen

## 3.6.2 Operator-rol herstellen

Deze rol is alleen beschikbaar in de Cyber Protection-service en is beperkt tot Microsoft 365- en Google Workspace-back-ups.

Een hersteloperator kan het volgende doen:

- Waarschuwingen en activiteiten bekijken.
- Door de lijst met back-ups bladeren en deze vernieuwen.
- Door back-ups bladeren zonder toegang tot de inhoud. De hersteloperator kan de namen van de back-upbestanden en de onderwerpen en afzenders van e-mails in de back-up zien.
- Zoeken in back-ups (zoeken in volledige tekst wordt niet ondersteund).
- Cloud-to-cloud back-ups herstellen binnen de oorspronkelijke Microsoft 365- of Google Workspace-organisatie.

Een hersteloperator kan niet het volgende doen:

- Waarschuwingen verwijderen.
- Microsoft 365- of Google Workspace-organisaties toevoegen of verwijderen.
- Back-uplocaties toevoegen of verwijderen of de naam ervan wijzigen.
- Back-ups verwijderen of de naam ervan wijzigen.
- Mappen maken, verwijderen of de naam ervan wijzigen tijdens het herstellen van een back-up naar een aangepaste locatie.
- Een back-upschema toepassen of een back-up uitvoeren.
- Back-upbestanden of de inhoud van e-mails in de back-up openen.
- Back-upbestanden of e-mailbijlagen downloaden.
- Cloudresources waarvan een back-up is gemaakt, zoals e-mails of agenda-items, verzenden als e-mail.
- Microsoft 365 Teams-gesprekken bekijken of herstellen.

## 3.7 De instellingen voor de meldingen voor een gebruiker wijzigen ...

Als u de instellingen voor de meldingen voor een gebruiker wilt wijzigen, selecteert u de gebruiker op het tabblad **Gebruikers** en klikt u op het potloodpictogram in het gedeelte **Instellingen**. De volgende meldingsinstellingen zijn beschikbaar als de Cyber Protection-service is ingeschakeld voor de tenant waar de gebruiker is gemaakt:

- **Meldingen over quotumoverschrijdingen** (standaard ingeschakeld)
  Meldingen over quotaoverschrijdingen.
- **Geplande gebruiksrapporten** (standaard ingeschakeld)
  Gebruiksrapporten die op de eerste dag van elke maand worden verzonden.
- **Foutmeldingen**, **waarschuwingsmeldingen** en **gereedmeldingen** (standaard uitgeschakeld)
  Meldingen over de uitvoeringsresultaten van beschermingsschema's en de resultaten van noodherstelbewerkingen voor elk apparaat.
- **Dagelijkse samenvatting over actieve waarschuwingen** (standaard ingeschakeld)
  De dagelijkse samenvatting wordt gegenereerd op basis van de lijst met actieve waarschuwingen die aanwezig zijn in de serviceconsole op het moment dat de samenvatting wordt gegenereerd. De samenvatting wordt één keer per dag gegenereerd en verzonden tussen 10:00 en 23:59 uur UTC. Het tijdstip waarop het rapport wordt gegenereerd en verzonden, is afhankelijk van de workload in het datacentrum. Als er op dat moment geen actieve waarschuwingen zijn, wordt de samenvatting niet verzonden. De samenvatting bevat geen informatie over eerdere waarschuwingen die niet meer actief zijn. Als een gebruiker bijvoorbeeld een mislukte back-up vindt en de waarschuwing wist, of als de back-up opnieuw met succes wordt geprobeerd voordat de samenvatting wordt gegenereerd, dan is de waarschuwing niet meer aanwezig en wordt deze niet opgenomen in de samenvatting.
- **Meldingen van apparaatbeheer** (standaard uitgeschakeld)
  Meldingen over pogingen om randapparatuur en poorten te gebruiken die zijn beperkt door beschermingsschema's (alleen wanneer de apparaatbeheermodule is ingeschakeld).
- **Herstelmeldingen** (standaard uitgeschakeld)
  Meldingen over herstelacties voor de volgende resources: e-mailberichten van gebruikers en volledige mailbox, openbare mappen, OneDrive/GoogleDrive: volledige OneDrive en bestanden of mappen, SharePoint-bestanden, Teams: kanalen, hele team, e-mailberichten, en teamsite.
  In het kader van deze meldingen worden de volgende acties als herstelacties beschouwd: verzenden als e-mail, downloaden, of een herstelbewerking starten.

Alle meldingen worden verzonden naar het e-mailadres van de gebruiker.

### 3.7.1 Meldingen ontvangen door gebruikersrol

Welke meldingen worden verzonden door Cyber Protection hangt af van de gebruikersrol.

| Type melding\Gebruikersrol | Gebruiker | Klantbeheerder |
|---|---|---|
| Meldingen voor eigen apparaten | Ja | Ja |
| Meldingen voor alle apparaten in de organisatie | N.v.t. | Ja |
| Meldingen voor Microsoft 365, Google Workspace en andere back-ups in de cloud | N.v.t. | Ja |

## 3.8 Een gebruikersaccount uitschakelen en inschakelen

Mogelijk moet u een gebruikersaccount uitschakelen om de toegang tot het cloudplatform tijdelijk te beperken.

***Een gebruikersaccount uitschakelen***

1. Ga in de beheerportal naar **Gebruikers**.
2. Selecteer het gebruikersaccount dat u wilt uitschakelen en klik vervolgens op het ellipspictogram  > **Uitschakelen**.
3. Bevestig uw actie door te klikken op **Uitschakelen**.

Deze gebruiker kan het cloudplatform dan niet gebruiken en geen meldingen ontvangen.

Als u een uitgeschakeld gebruikersaccount wilt inschakelen, selecteert u het account in de gebruikerslijst en klikt u vervolgens op het ellipspictogram  > **Inschakelen**.

## 3.9 Een gebruikersaccount verwijderen

Mogelijk moet u een gebruikersaccount definitief verwijderen om de gebruikte resources vrij te maken, bijvoorbeeld opslagruimte of een licentie. De gebruiksstatistieken worden binnen een dag na verwijdering bijgewerkt. Voor accounts met veel gegevens kan dit langer duren.

Voordat u een gebruikersaccount verwijdert, moet u dit uitschakelen. Zie Een gebruikersaccount uitschakelen en inschakelen voor meer informatie hierover.

**Belangrijk**
Een verwijderd gebruikersaccount kan niet meer worden hersteld!

***Een gebruikersaccount verwijderen***

1. Ga in de beheerportal naar **Gebruikers**.
2. Selecteer het uitgeschakelde gebruikersaccount en klik vervolgens op het ellipspictogram  > **Verwijderen**.
3. Bevestig de actie door uw gebruikersnaam in te voeren en klik vervolgens op **Verwijderen**.

Het resultaat:

- Dit gebruikersaccount wordt verwijderd.
- Alle gegevens die bij dit gebruikersaccount horen, worden verwijderd.
- De registratie wordt ongedaan gemaakt voor alle machines die aan dit gebruikersaccount zijn gekoppeld.

## 3.10 Eigendom van een gebruikersaccount overdragen

Mogelijk moet u het eigendom van een gebruikersaccount overdragen als u toegang wilt behouden tot de gegevens van een beperkte gebruiker.

**Belangrijk**
U kunt de inhoud van een verwijderd account niet opnieuw toewijzen.

***Het eigendom van een gebruikersaccount overdragen:***

1. Ga in de beheerportal naar **Gebruikers**.
2. Selecteer het gebruikersaccount waarvan u het eigendom wilt overdragen en klik vervolgens op het potloodpictogram in het gedeelte **Algemene informatie**.
3. Vervang het bestaande e-mailadres door het e-mailadres van de toekomstige accounteigenaar en klik vervolgens op **Gereed**.
4. Bevestig uw actie door te klikken op **Ja**.
5. Laat de toekomstige accounteigenaar het e-mailadres verifiëren door de instructies te volgen die naar dat adres zijn gestuurd.
6. Selecteer het gebruikersaccount waarvan u het eigendom overdraagt en klik vervolgens op het ellipspictogram  > **Wachtwoord opnieuw instellen**.
7. Bevestig uw actie door te klikken op **Opnieuw instellen**.
8. Laat de toekomstige accounteigenaar het wachtwoord opnieuw instellen door de instructies te volgen die naar het betreffende e-mailadres zijn gestuurd.

De nieuwe eigenaar heeft nu toegang tot dit account.

## 3.11 Tweeledige verificatie instellen

**Tweeledige verificatie (2FA)** is een vorm van meervoudige verificatie waarmee een gebruikersidentiteit wordt gecontroleerd door een combinatie van twee verschillende factoren:

- Iets wat een gebruiker weet (pincode of wachtwoord)
- Iets wat een gebruiker heeft (token)
- Iets wat een gebruiker is (biometrie)

Tweeledige verificatie biedt extra beveiliging tegen ongeautoriseerde toegang tot uw account.

Het platform ondersteunt **Time-Based One-Time Password (TOTP)**-verificatie. Als de TOTP-verificatie in het systeem is ingeschakeld, moeten gebruikers hun traditionele wachtwoord en de eenmalige TOTP-code invoeren om toegang te krijgen tot het systeem. Met andere woorden: een gebruiker geeft het wachtwoord én de TOTP-code op (deze twee samen vormen de twee factoren van tweeledige verificatie). De TOTP-code wordt gegenereerd in de verificatietoepassing op een apparaat ('tweede-factor-apparaat') van de gebruiker op basis van de huidige tijd en het geheim (QR-code of alfanumerieke code) van het platform.

## 3.11.1 Zo werkt het

1. U kunt tweeledige verificatie inschakelen op het niveau van de organisatie.
2. Alle gebruikers van uw organisatie moeten een verificatietoepassing installeren op hun 'tweede-factor-apparaat' (mobiele telefoon, laptop, desktop of tablet). Deze toepassing wordt gebruikt voor het genereren van eenmalige TOTP-codes. De aanbevolen verificatietoepassingen:
   - Google Authenticator
     iOS-appversie (https://apps.apple.com/app/google-authenticator/id388497605)
     Android-versie (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2)
   - Microsoft Authenticator
     iOS-appversie (https://apps.apple.com/app/microsoft-authenticator/id983156458)
     Android-versie (https://play.google.com/store/apps/details?id=com.azure.authenticator)

   **Belangrijk**
   De tijd op het gebruikersapparaat waarop de verificatietoepassing is geïnstalleerd, moet correct zijn ingesteld en de huidige tijd weergeven.
3. De gebruikers van uw organisatie moeten zich opnieuw aanmelden bij het systeem.
4. Wanneer ze hun gebruikersnaam en wachtwoord hebben ingevoerd, wordt ze gevraagd om tweeledige verificatie in te stellen voor hun gebruikersaccount.
5. Ze moeten de QR-code scannen met hun verificatietoepassing. Als de QR-code niet kan worden gescand, kunnen ze het TOTP-geheim onder de QR-code gebruiken en dit handmatig toevoegen in de verificatietoepassing.

   **Belangrijk**
   We raden u met klem aan om de code en het geheim op te slaan (print de QR-code, schrijf het TOTP-geheim op of gebruik de toepassing waarmee een back-up van codes kan worden gemaakt in de cloud). U hebt het TOTP-geheim nodig om tweeledige verificatie opnieuw in te stellen voor het geval u uw 'tweede-factor-apparaat' kwijtraakt.
6. De eenmalige TOTP-code wordt gegenereerd in de verificatietoepassing. De code wordt om de 30 seconden automatisch opnieuw gegenereerd.
7. Wanneer gebruikers hun wachtwoord hebben ingevoerd, moeten ze vervolgens de TOTP-code

invoeren op het scherm 'Tweeledige verificatie instellen'.

8. Hierdoor wordt tweeledige verificatie voor de gebruikers ingesteld.

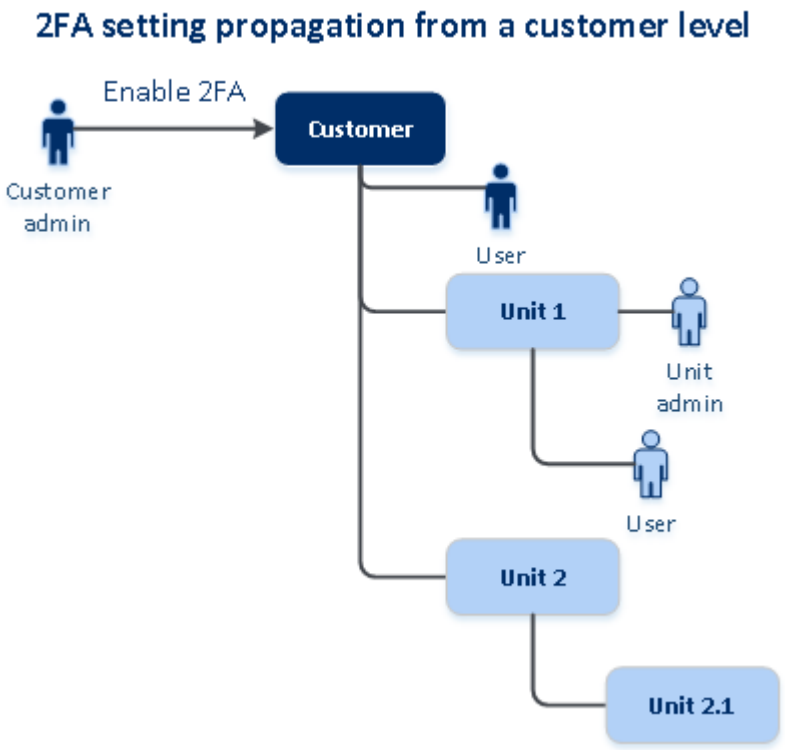
Wanneer gebruikers zich dan aanmelden bij het systeem, wordt ze gevraagd om de gebruikersnaam en het wachtwoord in te voeren, plus de eenmalige TOTP-code die wordt gegenereerd in de verificatietoepassing. Als gebruikers de browser als vertrouwd markeren wanneer ze zich aanmelden bij het systeem, wordt niet meer om de TOTP-code gevraagd bij de volgende aanmelding via deze browser.

## 3.11.2 Tweeledige verificatie doorvoeren bij de tenants

Tweeledige verificatie wordt ingesteld op **organisatieniveau**. U kunt tweeledige verificatie alleen instellen voor uw eigen organisatie.

De instellingen voor tweeledige verificatie worden als volgt doorgevoerd op tenantniveau:

- Voor eenheden worden automatisch de instellingen voor tweeledige verificatie van de betreffende klantorganisatie overgenomen.




**Opmerking**

1. Het is niet mogelijk om tweeledige verificatie in te stellen op het niveau van eenheden.
2. U kunt de instellingen voor tweeledige verificatie beheren voor gebruikers van de onderliggende organisaties (eenheden).

## 3.11.3 Tweeledige verificatie instellen voor uw tenant

### Tweeledige verificatie inschakelen voor uw tenant

1. Ga in de beheerportal naar **Instellingen** > **Beveiliging**.
2. Schakel de schuifregelaar in om tweeledige verificatie in te schakelen. Klik op **Inschakelen** om te bevestigen.

Op de voortgangsbalk ziet u hoeveel gebruikers tweeledige verificatie hebben ingesteld voor hun accounts. Tweeledige verificatie is dan ingeschakeld voor uw organisatie. Alle gebruikers van de organisatie moeten dan tweeledige verificatie instellen voor hun accounts. Daarna wordt aan de gebruikers gevraagd om hun gebruikersnaam en wachtwoord én de TOTP-code in te voeren om zich aan te melden bij het systeem.

Op het tabblad **Gebruikers** wordt de kolom **Status van tweeledige verificatie** weergegeven. U kunt volgen welke gebruikers tweeledige verificatie hebben ingesteld voor hun accounts.

### Tweeledige verificatie uitschakelen voor uw tenant

1. Ga in de beheerportal naar **Instellingen** > **Beveiliging**.
2. Schakel de schuifregelaar uit om tweeledige verificatie uit te schakelen. Klik op **Uitschakelen** om te bevestigen.
3. [Als ten minste één gebruiker in de organisatie tweeledige verificatie heeft geconfigureerd] Voer de TOTP-code in die is gegenereerd in uw verificatietoepassing op het mobiele apparaat.

Tweeledige verificatie wordt dan uitgeschakeld voor uw organisatie, alle geheimen worden verwijderd en alle vertrouwde browsers worden uit het geheugen gewist. Alle gebruikers kunnen zich dan bij het systeem aanmelden met alleen hun gebruikersnaam en wachtwoord. Op het tabblad **Gebruikers** wordt de kolom **Status van tweeledige verificatie** verborgen.

## 3.11.4 Configuratie voor tweeledige verificatie beheren voor gebruikers

U kunt de instellingen voor tweeledige verificatie voor al uw gebruikers controleren en opnieuw configureren op het tabblad **Gebruikers** in de beheerportal.

### Controle

In de beheerportal, op het tabblad **Gebruikers**, ziet u een lijst met alle gebruikers binnen uw organisatie. Bij **Status van tweeledige verificatie** ziet u of tweeledige verificatie is ingesteld voor een gebruiker.

## Tweeledige verificatie opnieuw instellen voor een gebruiker

1. Als u de instellingen voor een gebruiker wilt wijzigen, gaat u in de beheerportal naar het tabblad **Gebruikers** en vervolgens selecteert u de gebruiker en klikt u op de ellips.
2. Klik op **Tweeledige verificatie opnieuw instellen**.
3. Voer de TOTP-code in die is gegenereerd in uw verificatietoepassing op uw 'tweede-factor-apparaat' en klik op **Opnieuw instellen**.

De gebruiker kan tweeledige verificatie dan opnieuw instellen.

## De vertrouwde browser opnieuw instellen voor een gebruiker

1. Als u de instellingen voor een gebruiker wilt wijzigen, gaat u in de beheerportal naar het tabblad **Gebruikers** en vervolgens selecteert u de gebruiker en klikt u op de ellips.
2. Klik op **Alle vertrouwde browsers opnieuw instellen**.
3. Voer de TOTP-code in die is gegenereerd in de verificatietoepassing op uw 'tweede-factor-apparaat' en klik op **Opnieuw instellen**.

Gebruikers voor wie u alle vertrouwde browsers opnieuw hebt ingesteld, moeten de TOTP-code opgeven wanneer ze zich opnieuw aanmelden.

Gebruikers kunnen zelf alle vertrouwde browsers en de instellingen voor tweeledige verificatie opnieuw configureren. Wanneer ze zich aanmelden bij het systeem, kunnen ze op de betreffende link klikken en de TOTP-code invoeren om de bewerking te bevestigen.

## Tweeledige verificatie uitschakelen voor een gebruiker

Het kan nodig zijn om tweeledige verificatie uit te schakelen voor een gebruiker, terwijl de andere gebruikers van het account tweeledige verificatie blijven gebruiken. Dit is het geval als deze gebruiker wordt gebruikt om toegang te krijgen tot de API.

**Belangrijk**
Zet normale gebruikers niet om naar servicegebruikers om tweeledige verificatie uit te schakelen, want anders kunnen de gebruikers zich mogelijk niet aanmelden.

1. Als u de instellingen voor een gebruiker wilt wijzigen, gaat u in de beheerportal naar het tabblad **Gebruikers** en vervolgens selecteert u de gebruiker en klikt u op de ellips.
2. Klik op **Markeren als serviceaccount**. De gebruiker krijgt dan een speciale status voor tweeledige verificatie, genaamd **Serviceaccount.**
3. [Als ten minste één gebruiker binnen een tenant tweeledige verificatie heeft geconfigureerd] Bevestig het uitschakelen door de TOTP-code in te voeren die is gegenereerd in de verificatietoepassing op uw 'tweede-factor-apparaat'.

### Tweeledige verificatie inschakelen voor een gebruiker

Mogelijk moet u tweeledige verificatie inschakelen voor een bepaalde gebruiker voor wie u tweeledige verificatie eerder hebt uitgeschakeld.

1. Als u de instellingen voor een gebruiker wilt wijzigen, gaat u in de beheerportal naar het tabblad **Gebruikers** en vervolgens selecteert u de gebruiker en klikt u op de ellips.
2. Klik op **Markeren als gewoon account**. De gebruiker moet tweeledige verificatie dan opnieuw instellen of de TOTP-code invoeren voor toegang tot het systeem.

## 3.11.5 Tweeledige verificatie opnieuw instellen voor het geval u uw 'tweede-factor-apparaat' kwijtraakt

Als u uw 'tweede-factor-apparaat' bent kwijtgeraakt en u de toegang tot uw account opnieuw wilt instellen, volgt u een van de aangegeven methoden:

- Herstel uw TOTP-geheim (QR-code of alfanumerieke code) vanuit een back-up.
  Gebruik een ander 'tweede-factor-apparaat' en voeg het opgeslagen TOTP-geheim toe aan de verificatietoepassing die op dit apparaat is geïnstalleerd.
- Vraag uw beheerder om de instellingen voor tweeledige verificatie opnieuw te configureren voor u.

## 3.11.6 Bescherming tegen beveiligingsaanvallen

Een beveiligingsaanval is een aanval waarbij een indringer probeert toegang te krijgen tot het systeem door veel wachtwoorden in te voeren, in de hoop bij toeval het juiste wachtwoord te vinden.

Voor de bescherming van het platform tegen beveiligingsaanvallen wordt gebruikgemaakt van apparaatcookies.

De instellingen voor de bescherming tegen beveiligingsaanvallen die op het platform worden gebruikt, zijn vooraf gedefinieerd:

| Parameter | Wachtwoord invoeren | TOTP-code invoeren |
|---|---|---|
| Maximaal aantal pogingen | 10 | 5 |
| Maximale periode voor de pogingen (deze limiet wordt opnieuw ingesteld na een time-out) | 15 min (900 sec) | 15 min (900 sec) |
| Vergrendeling vindt plaats na | Maximaal aantal pogingen +1 (11e poging) | Maximaal aantal pogingen |
| Vergrendelingsperiode | 5 min (300 sec) | 5 min (300 sec) |

Als u tweeledige verificatie hebt ingeschakeld, krijgt een client(browser) alleen een apparaatcookie nadat verificatie met beide factoren (wachtwoord en TOTP-code) is uitgevoerd.

Voor vertrouwde browsers volstaat een verificatie met slechts één factor (wachtwoord) om de appraatcookie te krijgen.

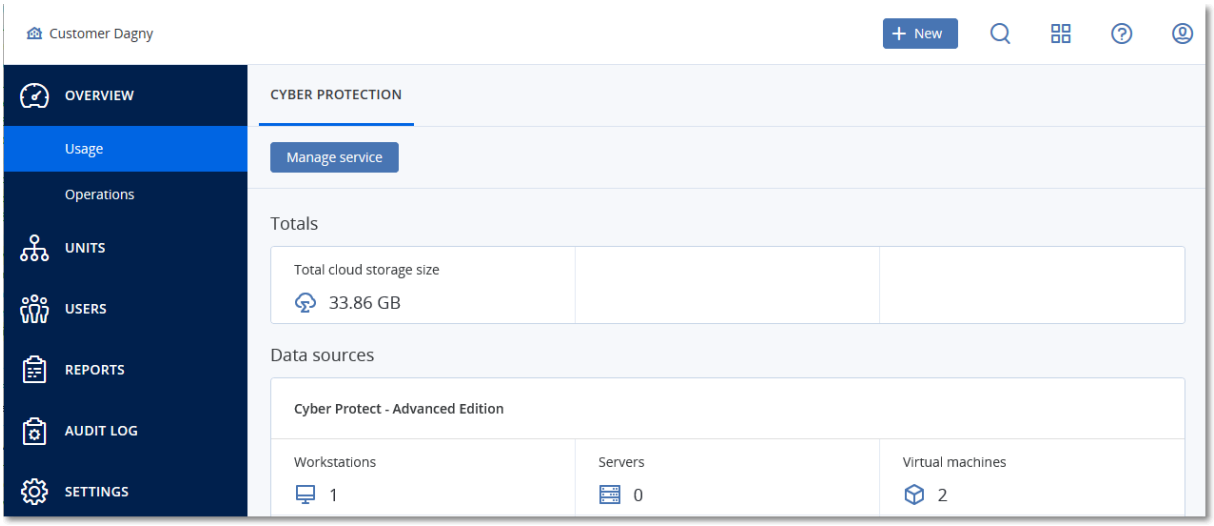
Het aantal pogingen om de TOTP-code in te voeren wordt geregistreerd per gebruiker, niet per apparaat. Dus gebruikers worden geblokkeerd, zelfs als ze proberen de TOTP-code in te voeren via verschillende apparaten.

# 4 Controle

Klik op **Overzicht** voor toegang tot informatie over het gebruik en de bewerkingen van services.

## 4.1 Gebruik

Het tabblad **Gebruik** bevat een overzicht van het servicegebruik (met inbegrip van eventuele quota's). Op dit tabblad hebt u toegang tot de serviceconsoles.



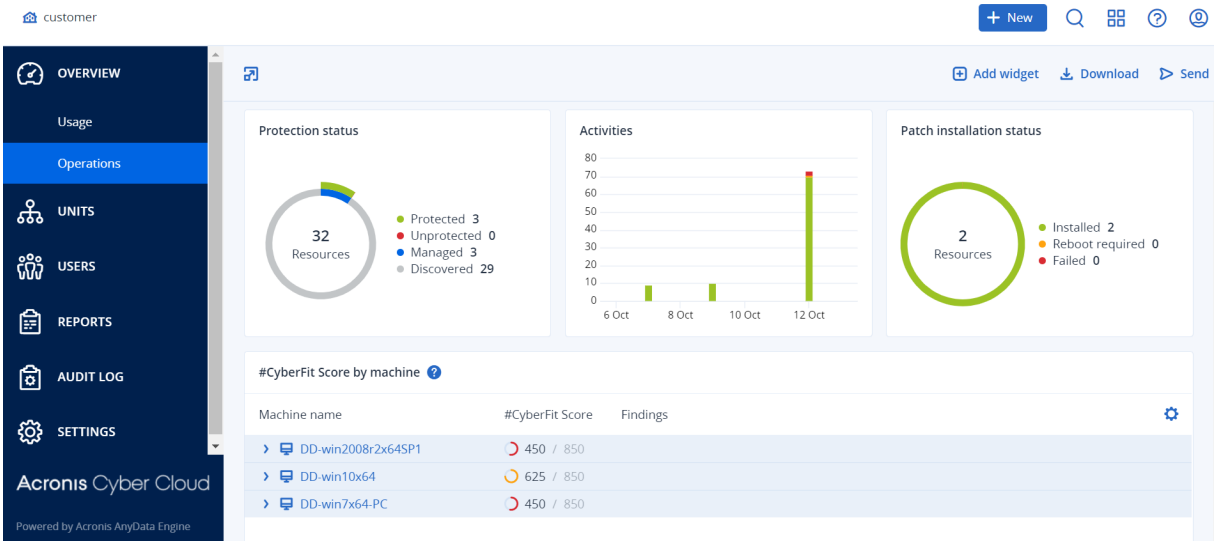

## 4.2 Dashboards voor bewerkingen

Het dashboard **Bewerkingen** is alleen beschikbaar voor bedrijfbeheerders wanneer op bedrijfsniveau wordt gewerkt.

Het dashboard **Bewerkingen** bevat enkele aanpasbare widgets die een overzicht bieden van de bewerkingen voor de Cyber Protection-service.

De widgets worden elke twee minuten bijgewerkt. De widgets hebben klikbare elementen waarmee u problemen kunt onderzoeken en oplossen. U kunt de huidige status van het dashboard downloaden of in PDF- en/of XLSX-indeling via e-mail verzenden.

U kunt kiezen uit verschillende widgets in de vorm van tabellen, cirkeldiagrammen, staafdiagrammen, lijsten en structuurkaarten. U kunt meerdere widgets van hetzelfde type toevoegen met verschillende filters.




***De widgets op het dashboard opnieuw indelen***

Versleep de widgets door op de betreffende namen te klikken.

***Een widget bewerken***

Klik op het potloodpictogram naast de naam van de widget. Wanneer u een widget bewerkt, kunt u de naam ervan wijzigen, het tijdsbereik wijzigen en filters instellen.

***Een widget toevoegen***

Klik op **Widget toevoegen** en voer vervolgens een van de volgende acties uit:

- Klik op de widget die u wilt toevoegen. De widget wordt toegevoegd met de standaardinstellingen.
- Als u de widget wilt bewerken voordat u deze toevoegt, klikt u op het potloodpictogram wanneer de widget is geselecteerd. Wanneer u de widget hebt bewerkt, klikt u op **Gereed**.

***Een widget verwijderen***

Klik op de X naast de naam van de widget.

## 4.2.1 Beveiligingsstatus

### Beveiligingsstatus

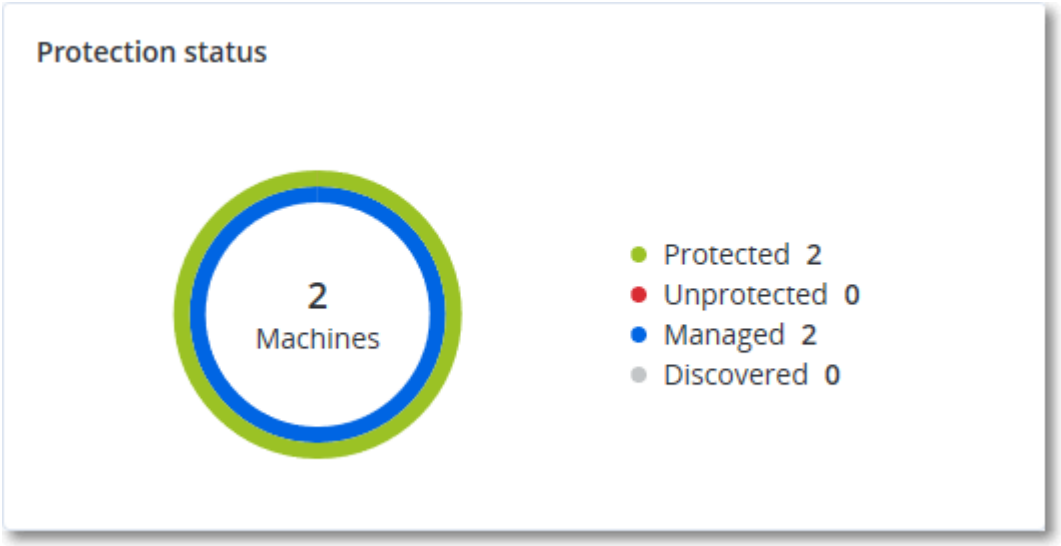
Deze widget geeft de huidige beveiligingsstatus voor alle machines weer.

Een machine kan een van de volgende statussen hebben:

- **Beschermd**: machines met toegepast beschermingsschema.
- **Onbeschermd**: machines zonder toegepast beschermingsschema. Dit kunnen zowel gedetecteerde als beheerde machines zonder beschermingsschema zijn.

- **Beheerd**: machines met geïnstalleerde beveiligingsagent.
- **Gedetecteerd**: machines waarop geen beveiligingsagent is geïnstalleerd.

Als u op de machinestatus klikt, wordt u voor meer informatie omgeleid naar de lijst met machines die deze status hebben.




## Gedetecteerde machines

Deze widget geeft de lijst met gedetecteerde machines tijdens het opgegeven tijdbereik weer.

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 |

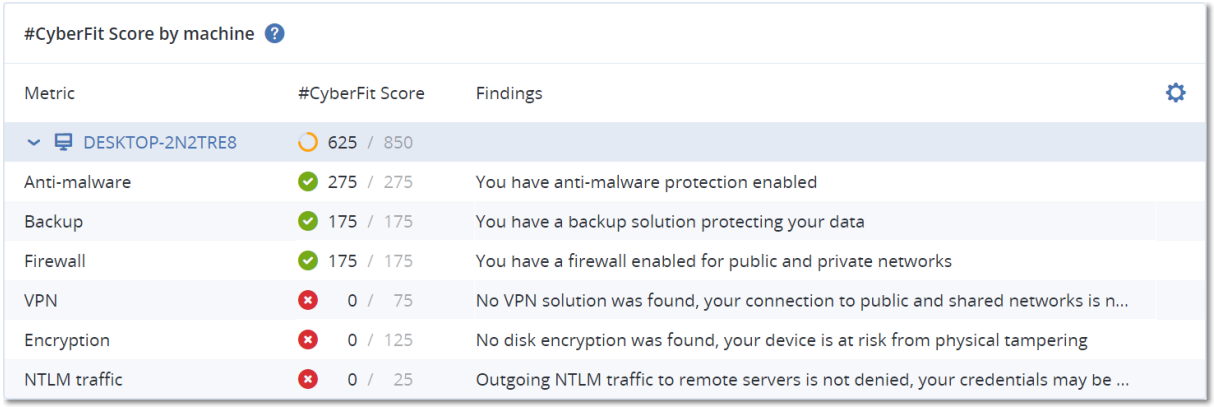
## 4.2.2 #CyberFit-score per machine

In deze widget ziet u voor elke machine de totale #CyberFit-score, de samengestelde scores en de bevindingen voor elk van de beoordeelde metrieken:

- Antimalware
- Back-up
- Firewall
- VPN
- Versleuteling
- NTLM-verkeer

Als u de score voor de verschillende metrieken wilt verbeteren, kunt u de aanbevelingen in het rapport bekijken.

Raadpleeg '#CyberFit-score voor machines' voor meer informatie over de #CyberFit-score.




## 4.2.3 Schijfintegriteitscontrole

Schijfintegriteitscontrole geeft informatie over de huidige status van de schijfintegriteit en een prognose daarover, zodat u gegevensverlies door een eventuele schijffout kunt voorkomen. Zowel HDD- als SSD-schijven worden ondersteund.

### Beperkingen

- Prognose van schijfintegriteit wordt alleen ondersteund voor machines met Windows.
- Alleen schijven van fysieke machines worden gecontroleerd. De schijven van virtuele machines kunnen niet worden gecontroleerd en weergegeven in de widgets voor schijfintegriteit.
- RAID-configuraties worden niet ondersteund.
- Op NVMe-stations wordt schijfintegriteitscontrole alleen ondersteund voor stations die de SMART-gegevens via de Windows-API communiceren. Schijfintegriteitscontrole wordt niet ondersteund voor NVMe-stations waarop de SMART-gegevens rechtstreeks van het station moeten worden gelezen.

Schijfintegriteit kan een van de volgende statussen hebben:

- **OK**
  : de schijfintegriteit is tussen de 70 en 100%.

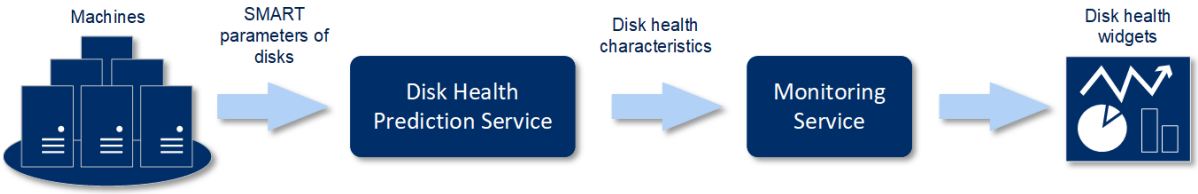
- **Waarschuwing**
  : de schijfintegriteit is tussen de 30 en 70%.
- **Kritiek**
  : de schijfintegriteit is tussen de 0 en 30%.
- **Schijfgegevens berekenen**
  : de huidige schijfstatus en -prognose worden berekend.

## Zo werkt het

De service Voorspelling van schijfintegriteit maakt gebruik van een op kunstmatige intelligentie gebaseerd voorspellingsmodel.

1. De agent verzamelt de SMART-parameters van de schijven en geeft deze gegevens door aan de service Voorspelling van schijfintegriteit:
   - SMART 5: aantal opnieuw toegewezen sectoren.
   - SMART 9: uren ingeschakeld.
   - SMART 187: gerapporteerde niet-corrigeerbare fouten.
   - SMART 188: time-out van opdrachten.
   - SMART 197: huidig aantal sectoren in behandeling.
   - SMART 198: aantal offline niet-corrigeerbare sectoren.
   - SMART 200: percentage schrijffouten.
2. De service Voorspelling van schijfintegriteit verwerkt de ontvangen SMART-parameters, maakt prognoses en genereert de volgende kenmerken van de schijfintegriteit:
   - Huidige status van schijfintegriteit: OK, Waarschuwing, Kritiek.
   - Prognose van schijfintegriteit: negatief, stabiel, positief.
   - Prognose van schijfintegriteit, waarschijnlijkheid uitgedrukt als percentage.

   De periode van de voorspelling is één maand.
3. De controleservice ontvangt deze kenmerken en toont vervolgens de relevante informatie in de widgets voor schijfintegriteit in de serviceconsole.




## Widgets voor schijfintegriteit

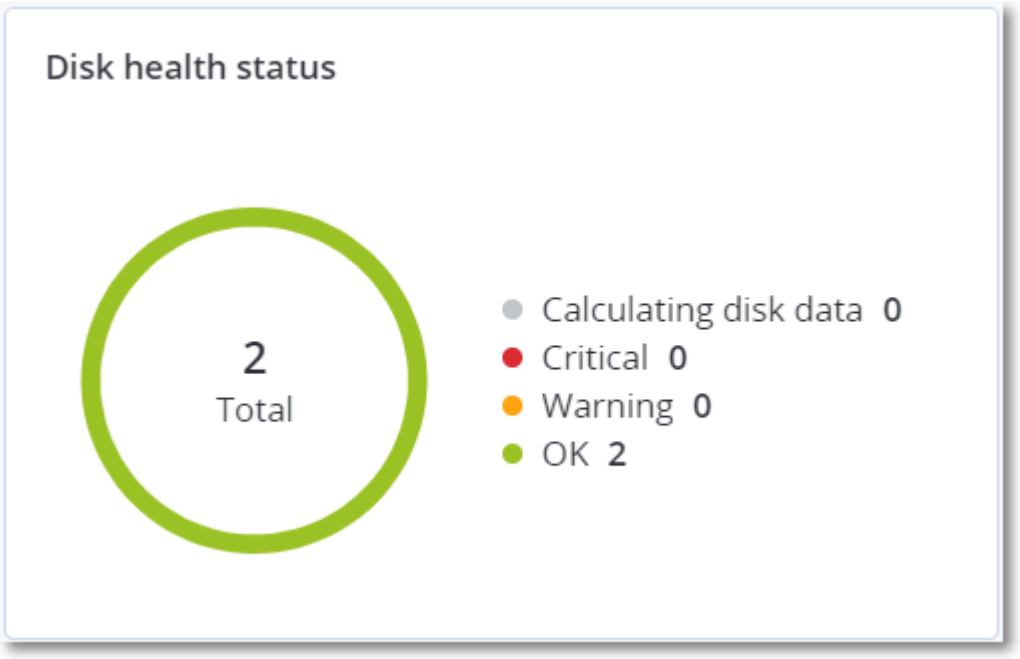
De resultaten van de schijfintegriteitscontrole worden weergegeven in de volgende widgets die beschikbaar zijn in de serviceconsole.

- **Overzicht van schijfintegriteit**: een widget met een structuurkaart op twee detailniveaus waartussen kan worden geschakeld.
  - Machineniveau
    : Geeft samengevatte informatie weer over de status van de schijfintegriteit van de geselecteerde klantmachines. Alleen de meest kritieke schijfstatus wordt weergegeven. De andere statussen worden in een knopinfo weergegeven wanneer u het betreffende blok aanwijst met de muis. Hoe groot het blok van de machine is, hangt af van de totale grootte van alle schijven van de machine. Welke kleur het blok van de machine heeft, hangt af van de meest kritieke schijfstatus die is gevonden.


  - Schijfniveau
    : Geeft de huidige status van de schijfintegriteit weer van alle schijven voor de geselecteerde machine. Elk schijfblok toont een van de volgende prognoses van schijfintegriteit en de waarschijnlijkheid ervan in procenten:
    - Zal minder worden
    - Zal stabiel blijven

- Zal beter worden


- **Status van schijfintegriteit**: Een widget met een cirkeldiagram met het aantal schijven voor elke status.



### Waarschuwingen over de status van de schijfintegriteit

De controle van de schijfintegriteit wordt elke 30 minuten uitgevoerd en de bijbehorende waarschuwing wordt een keer per dag gegenereerd. Wanneer de status van de schijfintegriteit verandert van **Waarschuwing** in **Kritiek**, wordt er altijd een waarschuwing gegenereerd.

| Naam van de waarschuwing | Ernstgraad | Status van schijfintegriteit | Beschrijving |
|---|---|---|---|
| Schijffout is mogelijk | Waarschuwing | (30 – 70) | De schijf <schijfnaam> op deze machine zal waarschijnlijk defect raken in de toekomst. Voer zo snel mogelijk een volledige systeemkopieback-up van deze schijf uit, vervang deze en herstel de systeemkopie vervolgens op de nieuwe schijf. |
| Schijf zal binnenkort defect raken | Kritiek | (0 – 30) | De status van de schijf <schijfnaam> op deze machine is kritiek en de schijf zal waarschijnlijk binnenkort defect raken. Een imageback-up van deze schijf wordt op dit moment niet aanbevolen, omdat de schijf defect kan raken door de extra belasting. Maak nu meteen een back-up van de belangrijkste bestanden op deze schijf en vervang de schijf. |

## 4.2.4 Overzicht van gegevensbescherming

Met de functie Overzicht van gegevensbescherming kunt u alle gegevens vinden die belangrijk voor u zijn en gedetailleerde informatie krijgen over het aantal, de grootte, de locatie en de beveiligingsstatus van alle belangrijke bestanden in een schaalbare weergave met structuurkaart.

De grootte van elke blok hangt af van het totale aantal/de grootte van alle belangrijke bestanden die bij een klant/machine horen.

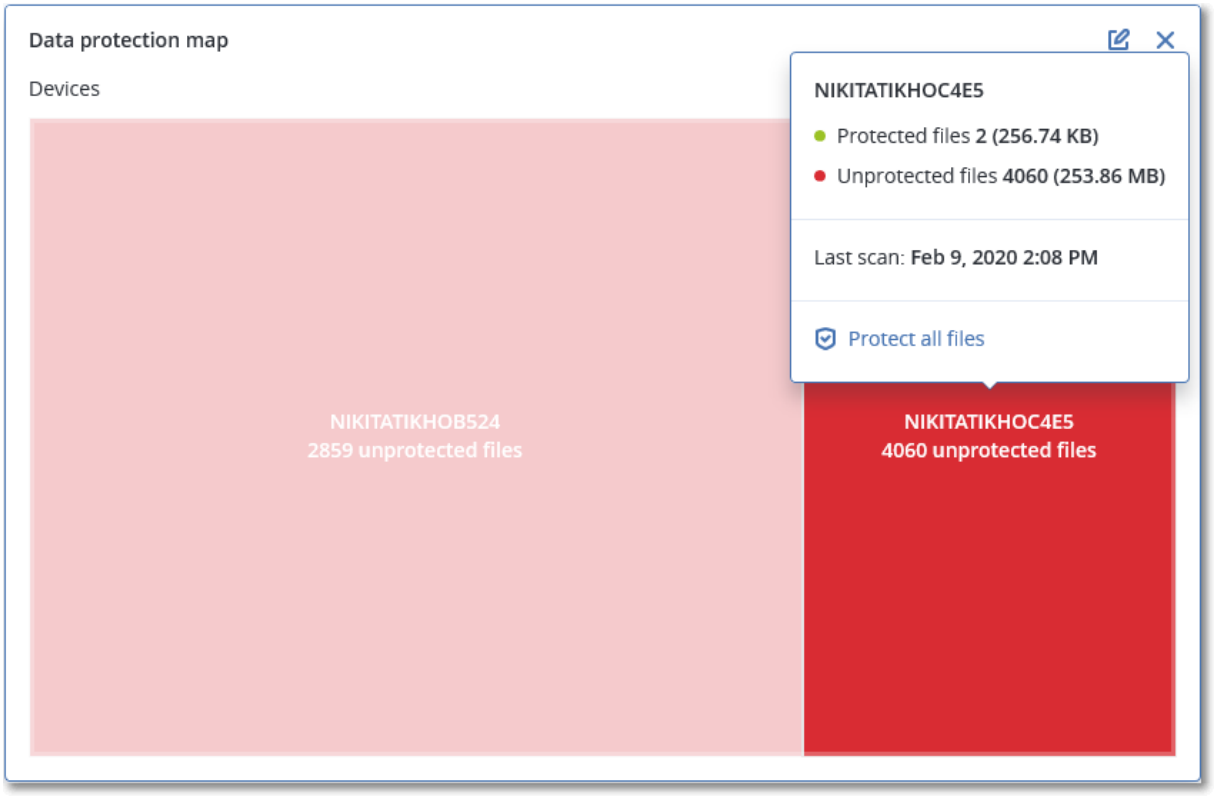
Bestanden kunnen een van de volgende beveiligingsstatussen hebben:

- **Kritiek** – er zijn 51-100% onbeschermde bestanden met de door u opgegeven extensies waarvan geen back-up wordt gemaakt met de bestaande back-upinstellingen voor de geselecteerde machine/locatie.
- **Laag** – er zijn 21-50% onbeschermde bestanden met de door u opgegeven extensies waarvan geen back-up wordt gemaakt met de bestaande back-upinstellingen oor de geselecteerde machine/locatie.
- **Medium**: er zijn 1-20% onbeschermde bestanden met de door u opgegeven extensies waarvan geen back-up wordt gemaakt met de bestaande back-upinstellingen oor de geselecteerde machine/locatie.

- **Hoog** – alle bestanden met de door u opgegeven extensies worden beschermd (er wordt een back-up van gemaakt) voor de geselecteerde machine/locatie.

De resultaten van het gegevensbeschermingsonderzoek zijn te vinden op het dashboard in de widget Overzicht van gegevensbescherming, een widget met een structuurkaart waarin de detailniveaus op machineniveau worden weergegeven:

- Machineniveau: geeft samengevatte informatie weer over de beveiligingsstatus van belangrijke bestanden per geselecteerde klant.




Als u onbeschermde bestanden wilt beschermen, wijst u het blok aan en klikt u op **Alle bestanden beschermen**. In het dialoogvenster vindt u informatie over het aantal onbeschermde bestanden en de locatie hiervan. Klik op **Alle bestanden beschermen** om ze te beschermen.

U kunt ook een gedetailleerd rapport in CSV-indeling downloaden.

## 4.2.5 Widgets voor evaluatie van beveiligingsproblemen

### Machines met beveiligingsproblemen

Deze widget geeft de machines met beveiligingsproblemen weer per ernstgraad.

Het gevonden beveiligingsprobleem kan een van de volgende ernstgraden hebben volgens het Common Vulnerability Scoring System (CVSS) v3.0:

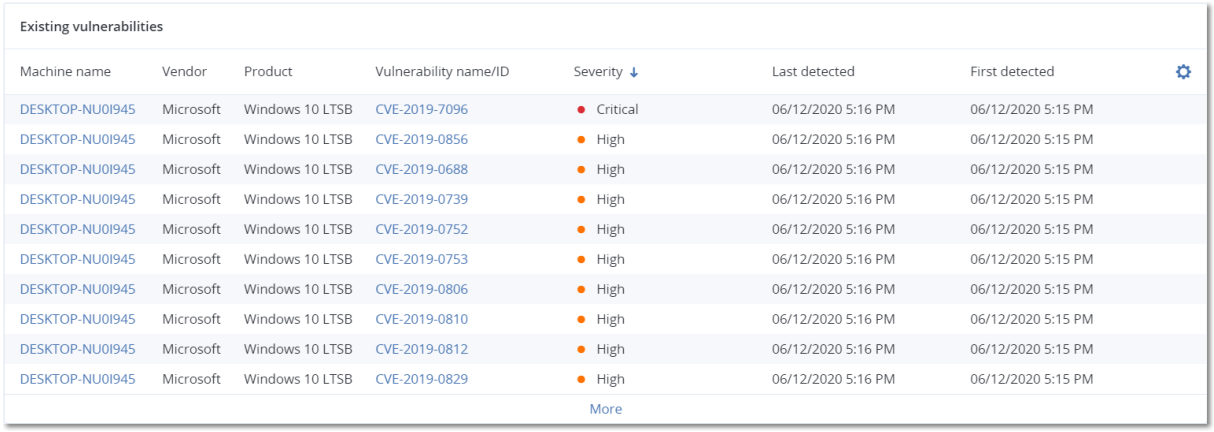
- Beveiligd: geen beveiligingsproblemen gevonden
- Kritiek: 9,0 – 10,0 CVSS

- Hoog: 7,0 – 8,9 CVSS
- Medium: 4,0 – 6,9 CVSS
- Laag: 0,1 – 3,9 CVSS
- Geen: 0,0 CVSS


## Bestaande kwetsbaarheden

Deze widget geeft de momenteel bestaande beveiligingsproblemen op machines weer. De widget **Bestaande beveiligingsproblemen** bevat twee kolommen met tijdstempels:

- **Eerst gedetecteerd**: datum en tijd waarop een beveiligingsprobleem voor het eerst is gedetecteerd op de machine.
- **Laatst gedetecteerd**: datum en tijd waarop een beveiligingsprobleem voor het laatst is gedetecteerd op de machine.


Existing vulnerabilities

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

More

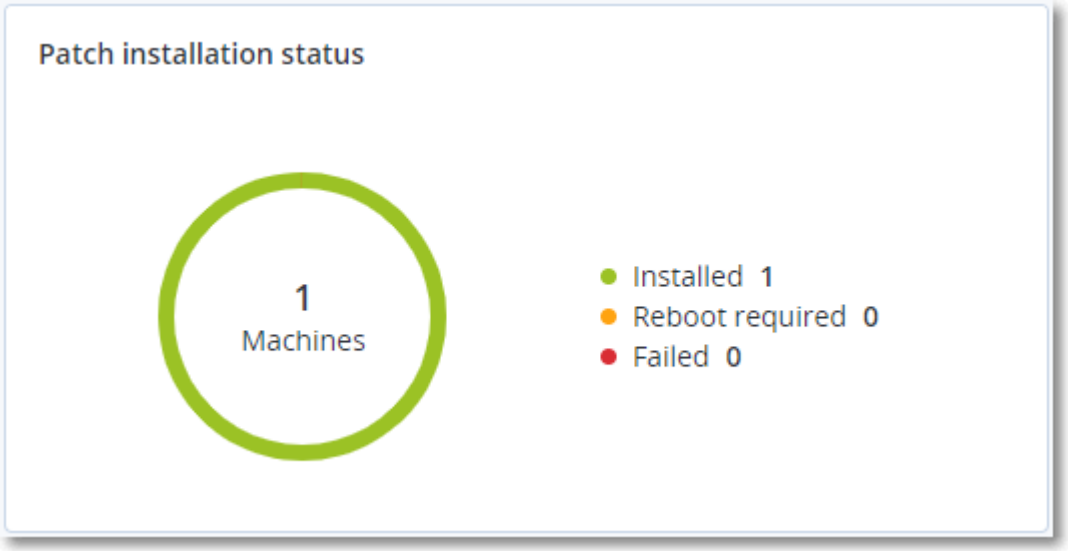
## 4.2.6 Widgets voor patchinstallatie

Er zijn vier widgets gerelateerd aan de functionaliteit voor patchbeheer.

## Status van patchinstallatie

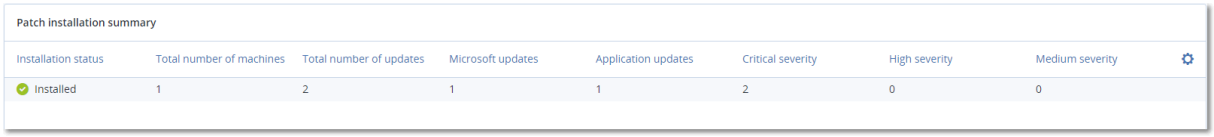
Deze widget geeft het aantal machines weer, gegroepeerd op status van de patchinstallatie.

- **Geïnstalleerd**: alle beschikbare patches zijn geïnstalleerd op een machine
- **Opnieuw opstarten vereist**: opnieuw opstarten is vereist voor een machine na de patchinstallatie
- **Mislukt**: patchinstallatie is mislukt op een machine




## Overzicht van patchinstallatie

Deze widget geeft een overzicht van de patches op machines weer, gesorteerd op de status van de patchinstallatie.



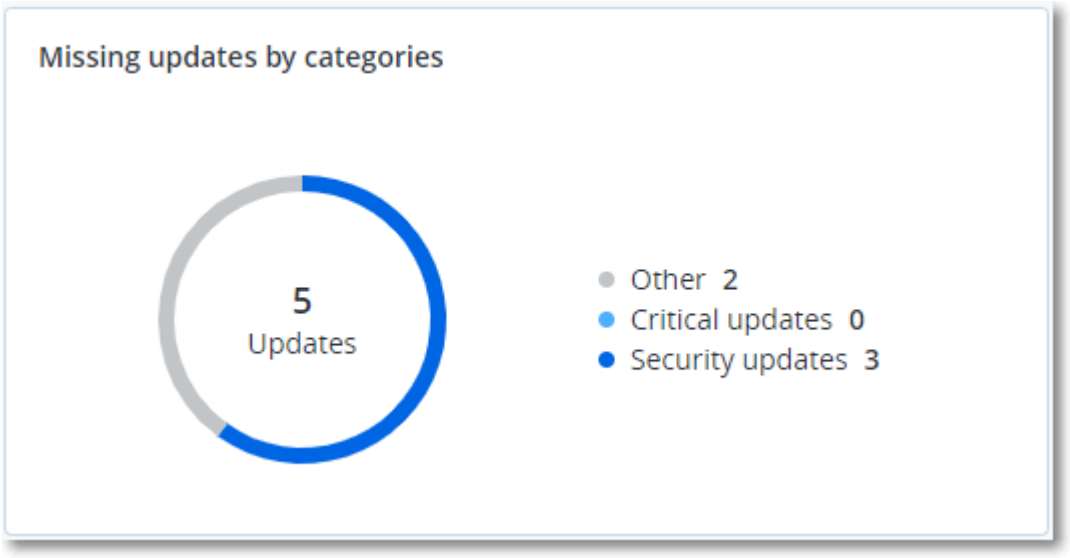

## Geschiedenis van patchinstallatie

Deze widget geeft gedetailleerde informatie over patches op machines weer.

### Ontbrekende updates per categorie

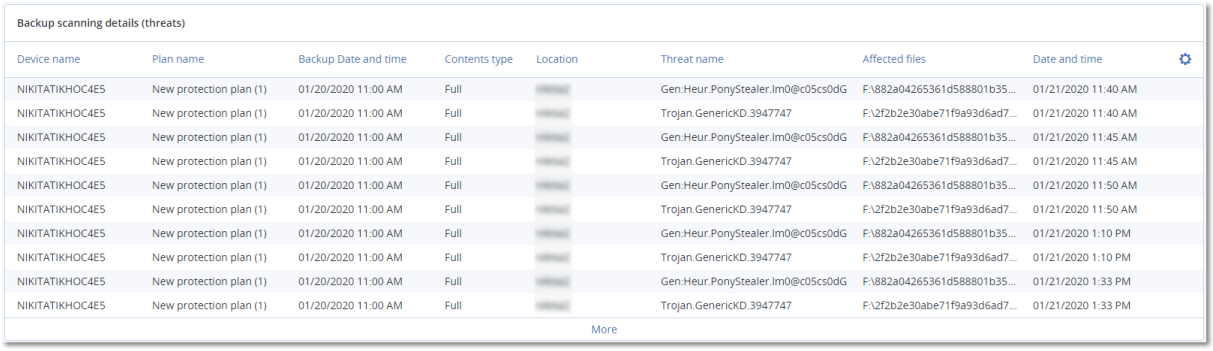
Deze widget geeft het aantal ontbrekende updates per categorie weer. De volgende categorieën worden weergegeven:

- Beveiligingsupdates
- Kritieke updates
- Anders




## 4.2.7 Gegevens van back-upscan

Deze widget geeft gedetailleerde informatie over de gedetecteerde bedreigingen in back-ups weer.

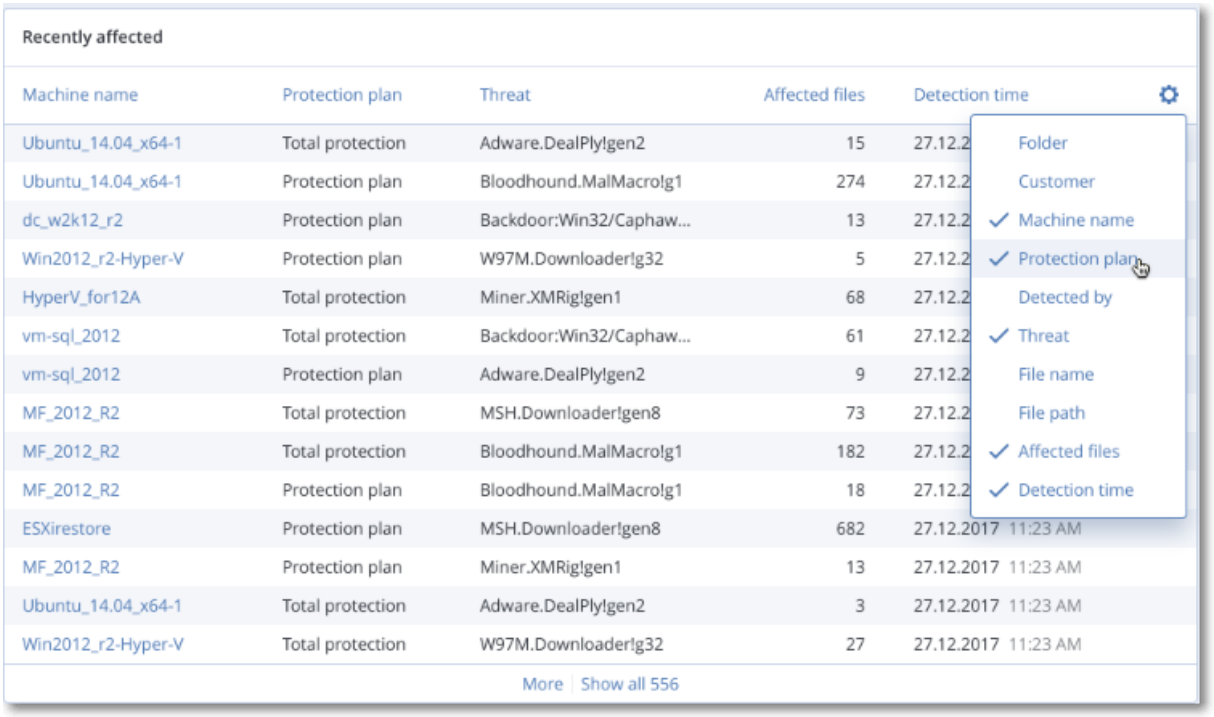

Backup scanning details (threats)

| 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

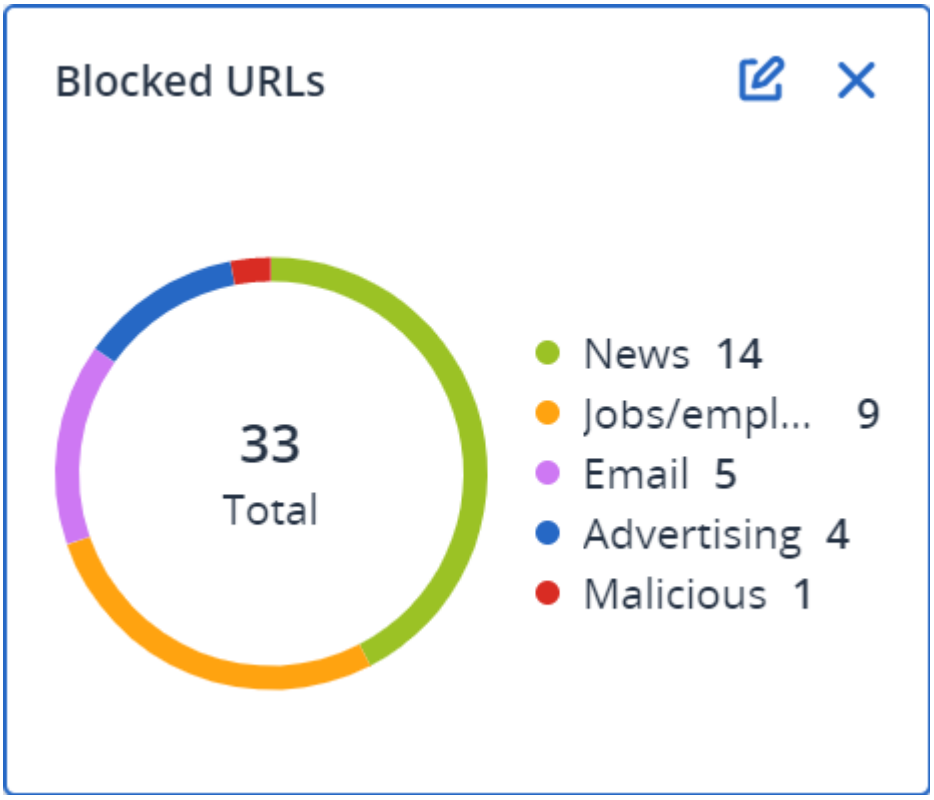
## 4.2.8 Onlangs beïnvloed

Deze widget geeft gedetailleerde informatie over recent geïnfecteerde machines weer. U kunt informatie vinden over welke bedreiging is gedetecteerd en hoeveel bestanden zijn geïnfecteerd.



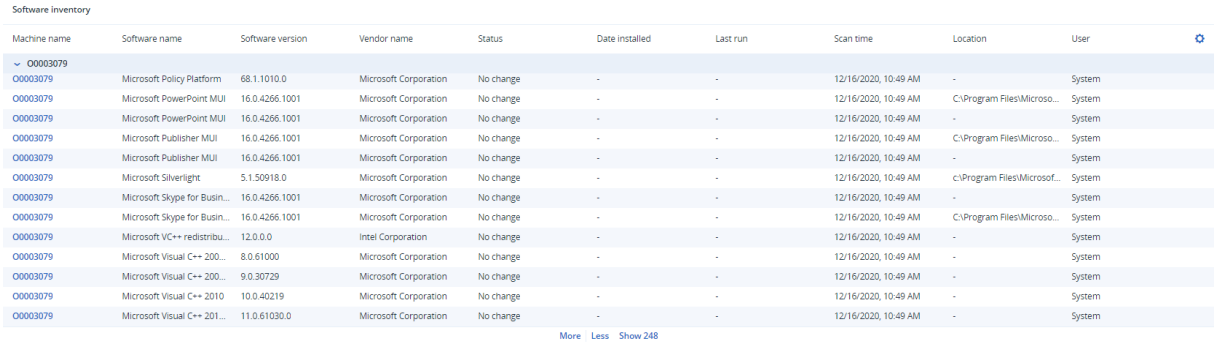

## 4.2.9 Geblokkeerde URL's

De widget geeft de statistieken van geblokkeerde URL's per categorie weer. Zie de Cyber Protection-gebruikershandleiding voor meer informatie over URL-filtering en -categorisering.

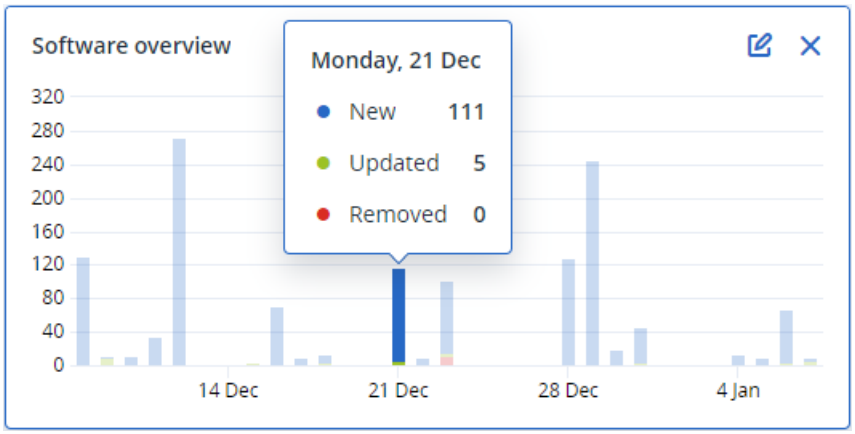


## 4.2.10 Widgets voor software-inventaris

De widget voor de tabel **Software-inventaris** geeft gedetailleerde informatie weer over alle software die is geïnstalleerd op Windows- en macOS-apparaten in uw organisatie.




De widget **Softwareoverzicht** geeft het aantal nieuwe, bijgewerkte en verwijderde toepassingen weer gedurende een bepaalde periode (7 dagen, 30 dagen of de huidige maand) op Windows- en macOS-apparaten in uw organisatie.




Wanneer u met de muis een bepaalde balk in het diagram aanwijst, wordt er knopinfo weergegeven met de volgende informatie:

**Nieuw**: het aantal nieuw geïnstalleerde toepassingen.

**Bijgewerkt**: het aantal bijgewerkte toepassingen.

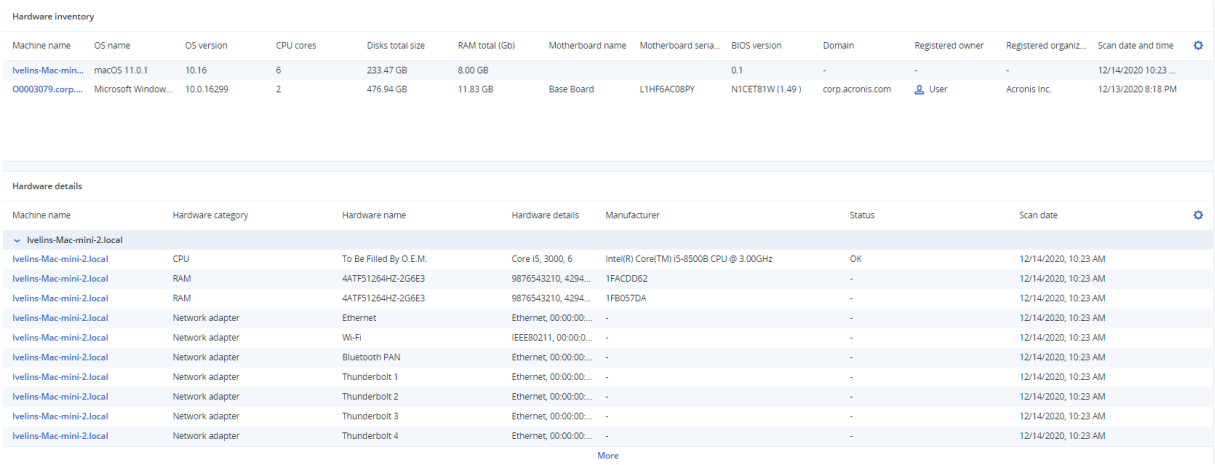
**Verwijderd**: het aantal verwijderde toepassingen.

Wanneer u op het gedeelte van de balk klikt voor een bepaalde status, wordt u omgeleid naar de pagina **Softwarebeheer** -> **Software-inventaris**. De informatie op de pagina wordt gefilterd op de betreffende datum en status.

## 4.2.11 Widgets voor hardware-inventaris

De widgets voor de tabel **Hardware-inventaris** en **Hardwaregegevens** geven informatie weer over alle hardware die is geïnstalleerd op fysieke en virtuele Windows- en macOS-apparaten in uw

organisatie.



Hardware inventory

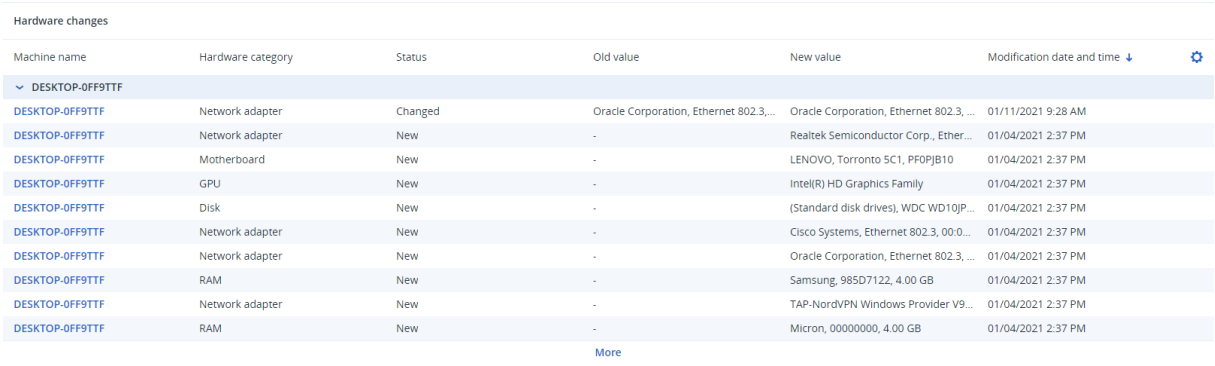
| Machine name | OS name | OS version | CPU cores | Disks total size | RAM total (Gb) | Motherboard name | Motherboard seria... | BIOS version | Domain | Registered owner | Registered organiz... | Scan date and time |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ivelins-Mac-min... | macOS 11.0.1 | 10.16 | 6 | 233.47 GB | 8.00 GB | | | 0.1 | - | - | - | 12/14/2020 10:23 ... |
| O0003079.corp.... | Microsoft Window... | 10.0.16299 | 2 | 476.94 GB | 11.83 GB | Base Board | L1HF6AC08PY | N1CET81W (1.49 ) | corp.acronis.com | User | Acronis Inc. | 12/13/2020 8:18 PM |

Hardware details

| Machine name | Hardware category | Hardware name | Hardware details | Manufacturer | Status | Scan date |
|---|---|---|---|---|---|---|
| Ivelins-Mac-mini-2.local | | | | | | |
| Ivelins-Mac-mini-2.local | CPU | To Be Filled By O.E.M. | Core i5, 3000, 6 | Intel(R) Core(TM) i5-8500B CPU @ 3.00GHz | OK | 12/14/2020, 10:23 AM |
| Ivelins-Mac-mini-2.local | RAM | 4ATF51264HZ-2G6E3 | 9876543210, 4294... | 1FACDD62 | - | 12/14/2020, 10:23 AM |
| Ivelins-Mac-mini-2.local | RAM | 4ATF51264HZ-2G6E3 | 9876543210, 4294... | 1FB057DA | - | 12/14/2020, 10:23 AM |
| Ivelins-Mac-mini-2.local | Network adapter | Ethernet | Ethernet, 00:00:00:... | - | - | 12/14/2020, 10:23 AM |
| Ivelins-Mac-mini-2.local | Network adapter | Wi-Fi | IEEE80211, 00:00:0... | - | - | 12/14/2020, 10:23 AM |
| Ivelins-Mac-mini-2.local | Network adapter | Bluetooth PAN | Ethernet, 00:00:00:... | - | - | 12/14/2020, 10:23 AM |
| Ivelins-Mac-mini-2.local | Network adapter | Thunderbolt 1 | Ethernet, 00:00:00:... | - | - | 12/14/2020, 10:23 AM |
| Ivelins-Mac-mini-2.local | Network adapter | Thunderbolt 2 | Ethernet, 00:00:00:... | - | - | 12/14/2020, 10:23 AM |
| Ivelins-Mac-mini-2.local | Network adapter | Thunderbolt 3 | Ethernet, 00:00:00:... | - | - | 12/14/2020, 10:23 AM |
| Ivelins-Mac-mini-2.local | Network adapter | Thunderbolt 4 | Ethernet, 00:00:00:... | - | - | 12/14/2020, 10:23 AM |

More

De widget voor de tabel **Hardwarewijzigingen** geeft informatie weer over de hardware die gedurende een bepaalde periode (7 dagen, 30 dagen of de huidige maand) is toegevoegd, verwijderd of gewijzigd op fysieke en virtuele Windows- en macOS-apparaten in uw organisatie.



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

# 5 Rapportage

Klik op **Rapporten** voor toegang tot rapporten over het gebruik en de bewerkingen van services.

**Opmerking**
Deze functionaliteit is niet beschikbaar in de Standard-edities van de Cyber Protection-service.

## 5.1 Gebruiksrapporten

Gebruiksrapporten bevatten historische gegevens over het gebruik van de services.
Gebruiksrapporten zijn beschikbaar in zowel CSV- als HTML-indeling.

### 5.1.1 Type rapport

U kunt een van de volgende rapporttypen selecteren:

- **Huidig gebruik**
  Het rapport bevat de huidige gebruiksmetrieken van de service.
- **Samenvatting voor de hele periode**
  Het rapport bevat de gebruiksmetrieken van de service voor het einde van de opgegeven periode, en het verschil tussen de metrieken aan het begin en aan het einde van de opgegeven periode.
- **Elke dag gedurende de periode**
  Het rapport bevat de gebruiksmetrieken van de service en de wijzigingen voor elke dag van de opgegeven periode.

### 5.1.2 Bereik van het rapport

Voor het bereik van het rapport kunt u een van de volgende waarden selecteren:

- **Directe klanten en partners**
  Dit rapport bevat alleen de servicegebruiksmetrieken voor de directe onderliggende eenheden van het bedrijf of de eenheid waarin u werkt.
- **Alle klanten en partners**
  Dit rapport bevat de servicegebruiksmetrieken voor alle onderliggende eenheden van het bedrijf of de eenheid waarin u werkt.
- **Alle klanten, partners en gebruikers**
  Dit rapport bevat de servicegebruiksmetrieken voor alle onderliggende eenheden van het bedrijf of de eenheid waarin u werkt, en voor alle gebruikers binnen de eenheden.

### 5.1.3 Geplande rapporten

Een gepland rapport bevat de servicegebruiksmetrieken voor de laatste volledige kalendermaand. De rapporten worden gegenereerd om 23:59:59 UTC op de eerste dag van een maand en verzonden op de tweede dag van die maand. De rapporten worden verzonden naar alle beheerders van uw

bedrijf of eenheid die het selectievakje **Geplande gebruiksrapporten** hebben ingeschakeld in de gebruikersinstellingen.

***Een gepland rapport inschakelen of uitschakelen***

1. Meld u aan bij de beheerportal.
2. Controleer of u werkt in het bedrijf of de eenheid op het hoogste niveau dat beschikbaar is voor u.
3. Klik op **Rapporten** > **Gebruik**.
4. Klik op **Gepland**.
5. Schakel het selectievakje **Een maandelijks overzichtsrapport verzenden** in of uit.
6. Ga naar **Detailniveau** en selecteer een van de eerder vermelde opties voor het bereik van het rapport.

## 5.1.4 Aangepaste rapporten

Een aangepast rapport wordt op aanvraag gegenereerd en kan niet worden gepland. Het rapport wordt verzonden naar uw e-mailadres.

***Een aangepast rapport genereren***

1. Meld u aan bij de beheerportal.
2. Navigeer naar de eenheid waarvoor u een rapport wilt maken.
3. Klik op **Rapporten** > **Gebruik**.
4. Klik op **Aangepast**.
5. Ga naar **Type** en selecteer het rapporttype zoals eerder beschreven.
6. [Niet beschikbaar voor het rapporttype **Huidig gebruik**] Ga naar **Periode** en selecteer de rapportageperiode:
   - **Huidige kalendermaand**
   - **Vorige kalendermaand**
   - **Aangepast**
7. [Niet beschikbaar voor het rapporttype **Huidig gebruik**] Als u een aangepaste rapportageperiode wilt opgeven, selecteert u de begin- en einddatum. Anders kunt u deze stap overslaan.
8. Ga naar **Detailniveau** en selecteer een van de eerder vermelde opties voor het bereik van het rapport.
9. Klik op **Genereren en verzenden** om het rapport te genereren.

## 5.1.5 Gegevens in gebruiksrapporten

Het rapport over het gebruik van de Cyber Protection-service bevat de volgende gegevens over een bedrijf of een eenheid:

- Grootte van de back-ups per eenheid, per gebruiker en per type apparaat.
- Aantal beschermde apparaten per eenheid, per gebruiker en per type apparaat.
- Prijswaarde per eenheid, per gebruiker en per type apparaat.
- De totale grootte van de back-ups.
- Het totale aantal beschermde apparaten.
- De totale prijswaarde.

**Opmerking**
Als de Cyber Protection-service een apparaattype niet kan detecteren, wordt dat apparaat weergegeven als **onbekend type** in het rapport.

## 5.2 Rapporten over bewerkingen

De rapporten van **Bewerkingen** zijn alleen beschikbaar voor bedrijfbeheerders wanneer op bedrijfsniveau wordt gewerkt.

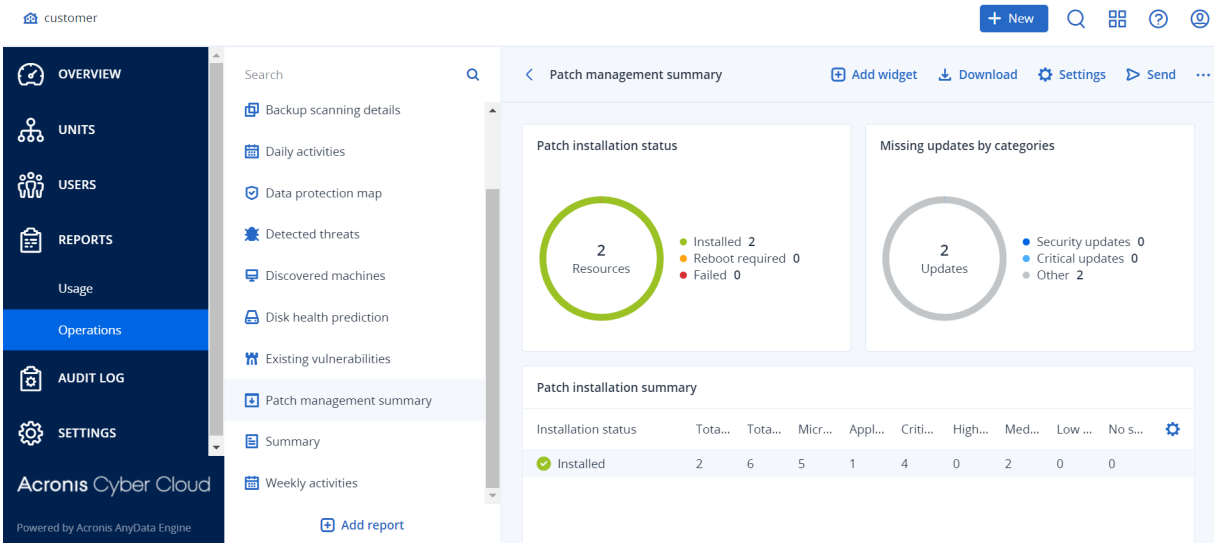
Een rapport over bewerkingen kan elke serie van de dashboardwidgets voor **Bewerkingen** bevatten. Alle widgets tonen samenvattende informatie voor het hele bedrijf.
Afhankelijk van het widgettype bevat het rapport gegevens voor een tijdbereik of voor het moment van browsen of het genereren van rapporten. Zie "Gerapporteerde gegevens per type widget" (p. 64).

Alle historische widgets tonen gegevens voor hetzelfde tijdbereik. U kunt dit bereik wijzigen in de rapportinstellingen.

Als u een rapport wilt bekijken, klikt u op de naam ervan.

U kunt een rapport over de activiteiten in Excel- (XLSX) of PDF-indeling downloaden of per e-mail verzenden.

Als u bewerkingen met een rapport wilt openen, klikt u op het ellipspictogram op de rapportregel. Dezelfde bewerkingen zijn beschikbaar vanuit het rapport.




U kunt vooraf gedefinieerde rapporten maken of een aangepast rapport maken.

De standaardrapporten worden hieronder weergegeven:

| Naam van rapport | Beschrijving |
|---|---|
| #CyberFit-score per machine | Geeft de #CyberFit-score weer, gebaseerd op de evaluatie van de beveiligingsmetrieken en -configuraties voor elke machine, en geeft aanbevelingen voor verbeteringen. |
| Waarschuwingen | Geeft de waarschuwingen weer die zijn gegenereerd tijdens een bepaalde periode. |
| Gegevens van back-upscan | Geeft gedetailleerde informatie weer over gedetecteerde bedreigingen in de back-ups. |
| Dagelijkse activiteiten | Geeft de overzichtsinformatie weer over activiteiten die zijn uitgevoerd tijdens een bepaalde periode. |
| Overzicht van gegevensbescherming | Geeft gedetailleerde informatie weer over het aantal, de grootte, de locatie en de beveiligingsstatus van alle belangrijke bestanden op machines. |
| Gedetecteerde bedreigingen | Geeft details weer over de betroffen machines en het aantal geblokkeerde bedreigingen, en over de machines die in orde zijn en de machines met beveiligingsproblemen. |
| Gedetecteerde machines | Geeft alle gevonden machines in het organisatienetwerk weer. |
| Voorspelling van schijfintegriteit | Geeft voorspellingen weer over wanneer uw HDD/SSD zal uitvallen en de huidige schijfstatus. |
| Bestaande kwetsbaarheden | Geeft de bestaande beveiligingsproblemen voor het besturingssysteem en de toepassingen in uw organisatie weer. Het rapport geeft ook de details van de betroffen machines in uw netwerk weer voor elk product dat wordt vermeld. |

| | |
|---|---|
| Overzicht van patchbeheer | Geeft het aantal ontbrekende patches, geïnstalleerde patches en toepasselijke patches weer. U kunt de rapporten analyseren om de gegevens over ontbrekende/geïnstalleerde patches en de details van alle systemen te krijgen. |
| Overzicht | Geeft de overzichtsinformatie over de beschermde apparaten tijdens een bepaalde periode weer. |
| Wekelijkse activiteiten | Geeft de overzichtsinformatie weer over activiteiten die zijn uitgevoerd tijdens een bepaalde periode. |
| Software-inventaris | Geeft gedetailleerde informatie weer over alle software die is geïnstalleerd op Windows- en macOS-machines in uw organisatie. |
| Hardware-inventaris | Geeft gedetailleerde informatie weer over alle hardware die beschikbaar is op fysieke en virtuele Windows- en macOS-machines in uw organisatie. |

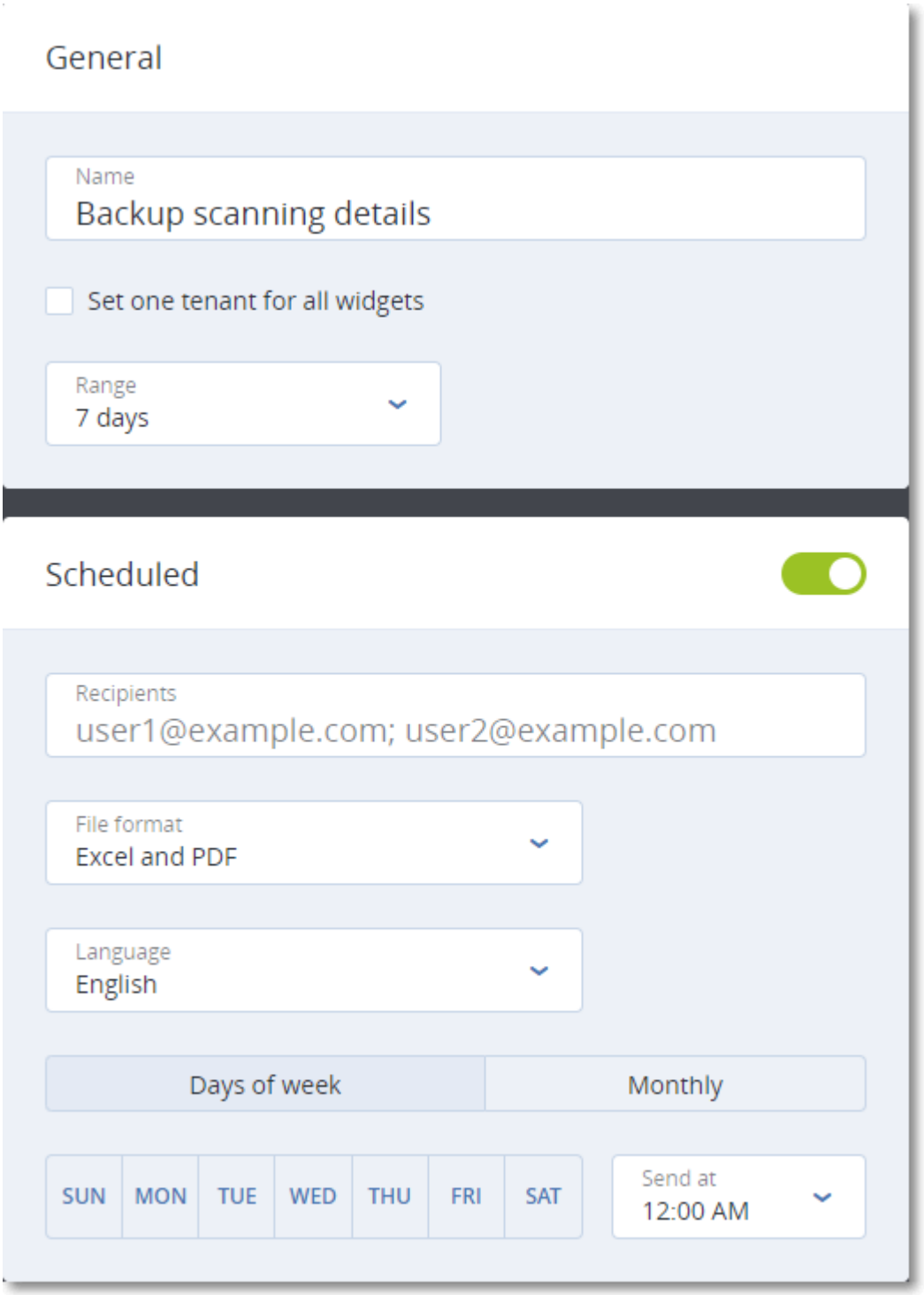
## Rapport toevoegen

1. Klik op **Rapport toevoegen**.
2. Voer een van de volgende handelingen uit:
   - Als u een vooraf gedefinieerd rapport wilt toevoegen, klikt u op de naam ervan.
   - Als u een aangepast rapport wilt toevoegen, klikt u op **Aanpassen**, klikt u op de naam van het rapport (de standaard toegewezen namen zien eruit als **Aangepast (1)**) en vervolgens voegt u widgets toe aan het rapport.
3. [Optioneel] Versleep de widgets om ze opnieuw te rangschikken.
4. [Optioneel] Bewerk het rapport zoals hieronder beschreven.

## Rapport bewerken

Als u een rapport wilt bewerken, klikt u op de naam ervan en vervolgens klikt u op **Instellingen**. Wanneer u een rapport bewerkt, kunt u het volgende doen:

- De naam van het rapport wijzigen
- Het tijdbereik voor alle widgets in het rapport wijzigen
- Plannen om het rapport in PDF- en/of Excel-indeling te verzenden via e-mail




## Een rapport plannen

1. Klik op de naam van het rapport en klik vervolgens op **Instellingen**.
2. Schakel de switch **Gepland** in.
3. Geef de e-mailadressen van de ontvangers op.
4. Selecteer de rapportindeling: PDF, Excel of beide.

5. Selecteer de dagen en het tijdstip waarop het rapport wordt verzonden.
6. Klik op **Opslaan** in de rechterbovenhoek.

## De rapportstructuur exporteren en importeren

U kunt de rapportstructuur (de set widgets en de rapportinstellingen) exporteren en importeren naar een JSON-bestand.

Als u de rapportstructuur wilt exporteren, klikt u op de naam van het rapport, klikt u op het ellipspictogram in de rechterbovenhoek en klikt u vervolgens op **Exporteren**.

Als u de rapportstructuur wilt importeren, klikt u op **Rapport toevoegen** en vervolgens op **Importeren**.

## Een rapport downloaden

U kunt een rapport downloaden. Klik op **Downloaden** en selecteer de gewenste indelingen:

- Excel en PDF
- Excel
- PDF

**Opmerking**
Voor beide indelingen kunt u tot 1000 rijen downloaden voor op tabellen gebaseerde widgets.

## Een dump maken van de rapportgegevens

U kunt een dump van de rapportgegevens in een CSV-bestand verzenden via e-mail. De dump bevat alle rapportgegevens (zonder dat deze gefilterd zijn) voor een aangepast tijdbereik. De tijdstempels in CSV-rapporten geven de tijd in UTC weer. De tijdstempels in Excel- en PDF-rapporten geven de huidige tijdzone van het systeem weer.

De software genereert de gegevensdump binnen een mum van tijd. Als u een lange tijdsduur opgeeft, kan deze actie lang duren.

***Een dump maken van de rapportgegevens***

1. Klik op de naam van het rapport.
2. Klik op het ellipspictogram in de rechterbovenhoek en klik vervolgens op **Dumpgegevens**.
3. Geef de e-mailadressen van de ontvangers op.
4. Geef in **Tijdbereik** het tijdbereik op.
   De onbewerkte historische gegevens worden permanent bewaard, maar er kunnen enkele beperkingen gelden voor de doelindeling van de export.
5. Klik op **Verzenden**.

# 5.3 Overzicht

Het overzichtsrapport bevat een overzicht van de beschermingsstatus van de omgeving en de beschermde apparaten van uw organisatie voor een bepaald tijdbereik.

Het overzichtsrapport bevat aanpasbare secties met dynamische widgets die de belangrijkste prestatiegegevens tonen over het gebruik van de volgende cloudservices: Back-up, antimalwarebeveiliging, evaluatie van beveiligingsproblemen, patchbeheer, Notary, noodherstel en Files Sync & Share.

U kunt het rapport op verschillende manieren aanpassen.

- Secties toevoegen of verwijderen.
- De volgorde van secties wijzigen.
- De naam van secties wijzigen.
- Widgets verplaatsen naar een andere sectie.
- Wijzig de volgorde van de widgets in elke sectie.
- Voeg widgets toe of verwijder ze.
- Pas widgets aan.

U kunt overzichtsrapporten genereren in PDF- en Excel-indeling, en deze naar de belanghebbenden of eigenaren van uw organisatie sturen, zodat zij gemakkelijk de technische en zakelijke waarde van de geleverde services kunnen zien.

## 5.3.1 Widgets voor het overzichtsrapport

U kunt secties en widgets toevoegen aan of verwijderen uit het overzichtsrapport en zo bepalen welke informatie wordt opgenomen in het rapport.

### Widgets voor overzicht van workloads

De volgende tabel bevat meer informatie over de widgets in het gedeelte **Overzicht van workloads**.

| Widget | Beschrijving |
|---|---|
| **Overzicht van cyberbescherming** | De widget toont de belangrijkste prestatiegegevens van cyberbescherming voor het opgegeven tijdbereik.<br>**Gegevens met back-up**: de totale grootte van de archieven die zijn gemaakt in de cloudopslag en lokale opslag.<br>**Verholpen bedreigingen**: het totale aantal keren dat malware is geblokkeerd op alle apparaten.<br>**Schadelijke URL's geblokkeerd**: het totale aantal URL's dat is |

| Widget | Beschrijving |
|---|---|
| | geblokkeerd op alle apparaten.<br><br>**Gepatchte beveiligingsproblemen**: het totale aantal beveiligingsproblemen dat is verholpen door de installatie van softwarepatches op alle apparaten.<br><br>**Geïnstalleerde patches**: het totale aantal geïnstalleerde patches op alle apparaten.<br><br>**Servers beschermd door DR**: het totale aantal servers dat wordt beschermd door Disaster Recovery.<br><br>**File Sync & Share-gebruikers**: het totale aantal eind- en gastgebruikers dat gebruikmaakt van Cyber Files.<br><br>**Genotariseerde bestanden**: het totale aantal genotariseerde bestanden.<br><br>**Elektronisch ondertekende documenten**: het totale aantal elektronisch ondertekende documenten.<br><br>**Geblokkeerde randapparaten**: het totale aantal geblokkeerde randapparaten. |
| **Beveiligingsstatus van workloads** | De widget toont de beschermde en niet-beschermde workloads per type op het moment dat het rapport werd gegenereerd. Beschermde workloads zijn workloads waarop ten minste één beschermings- of back-upschema wordt toegepast. Niet-beschermde workloads zijn workloads waarop geen beschermings- of back-upschema wordt toegepast. De volgende workloads worden meegeteld:<br>**Servers**: fysieke servers en domeincontrollerservers.<br><br>**Werkstations**: fysieke werkstations.<br><br>**Virtuele machines**: zowel virtuele machines met agent als zonder agent.<br><br>**Webhostingservers**: virtuele of fysieke server met geïnstalleerde cPanel of Plesk.<br><br>**Mobiele apparaten**: fysieke mobiele apparaten.<br><br>Een workload kan tot meer dan één categorie behoren. Een webhostingserver wordt bijvoorbeeld in twee categorieën ondergebracht: **Servers** en **Webhostingservers**. |
| **Beveiligingsstatus van workloads in de cloud** | **Beveiligingsstatus van workloads in de cloud**<br>De widget toont het aantal beschermde en niet-beschermde workloads in de cloud per type op het moment dat het rapport werd gegenereerd. Beschermde cloudworkloads zijn cloudworkloads waarop ten minste één back-upschema wordt toegepast. Niet-beschermde cloudworkloads zijn cloudworkloads waarop geen back- |

| Widget | Beschrijving |
|---|---|
| | upschema wordt toegepast. De volgende typen cloudworkloads worden weergegeven in het diagram (in alfabetische volgorde van A tot Z):<br>• Google Workspace Drive<br>• Google Workspace Gmail<br>• Google Workspace - Gedeelde Drive<br>• Gehoste Exchange-postvakken<br>• Microsoft 365-postvakken<br>• Microsoft 365 OneDrive<br>• Microsoft 365 SharePoint Online<br>• Microsoft Teams<br>• Websites<br>Voor sommige workloadtypen worden de volgende workloadgroepen gebruikt:<br>• Microsoft 365: Gebruikers, groepen, openbare mappen, teams en siteverzamelingen<br>• Google Workspace: Gebruikers en Shared Drives<br>• Gehoste Exchange: Gebruikers<br>Als er in een workloadgroep meer dan 10.000 workloads zijn, toont de widget geen gegevens voor de betreffende workloads.<br>Als de klant bijvoorbeeld een Microsoft 365-account heeft met 10.000 postvakken en OneDrive-service voor 500 gebruikers, behoren deze allemaal tot de workloadgroep. De som van deze workloads is 10.500, waardoor de limiet van 10.000 per workloadgroep wordt overschreden. Daarom worden de betreffende workloads verborgen in de widget: Microsoft 365-postvakken en Microsoft 365 OneDrive. |

## Widgets voor antimalwarebeveiliging

De volgende tabel bevat meer informatie over de widgets in het gedeelte **Antimalwarebeveiliging**.

| Widget | Beschrijving |
|---|---|
| **Antimalwarescan van bestanden** | De widget toont de resultaten van de antimalwarescan op aanvraag van de apparaten binnen het opgegeven datumbereik.<br>**Bestanden**: het totale aantal gescande bestanden<br>**Opschonen**: het totale aantal schone bestanden<br>**Gedetecteerd, in quarantaine geplaatst**: het totale aantal geïnfecteerde bestanden die in quarantaine zijn geplaatst<br>**Gedetecteerd, niet in quarantaine geplaatst**: het totale |

| Widget | Beschrijving |
|---|---|
| | aantal geïnfecteerde bestanden die niet in quarantaine zijn geplaatst<br><br>**Beschermde apparaten**: het totale aantal apparaten waarop een beleid voor antimalwarebeveiliging wordt toegepast<br><br>**Totaal aantal geregistreerde apparaten**: het totale aantal geregistreerde apparaten op het moment dat het rapport wordt gegenereerd |
| **Geblokkeerde URL's** | De widget toont het aantal geblokkeerde URL's gegroepeerd per websitecategorie voor het opgegeven datumbereik.<br><br>De widget geeft de zeven websitecategorieën weer met het grootste aantal geblokkeerde URL's en combineert de rest van de websitecategorieën in **Overige**.<br><br>Zie het onderwerp URL-filtering in Cyber Protection voor meer informatie over de websitecategorieën. |
| **Bedreigingen gedetecteerd door beschermingstechnologie** | De widget toont het aantal gedetecteerde bedreigingen voor het opgegeven datumbereik, gegroepeerd per beschermingstechnologie:<br>• Antimalwarescan<br>• Gedragengine<br>• Bescherming tegen cryptomining<br>• Preventie tegen aanvallen<br>• Actieve bescherming tegen ransomware<br>• Realtime bescherming<br>• URL-filtering |
| **Antimalwarescan van back-ups** | De widget toont de resultaten van de antimalwarescans van de back-ups voor het opgegeven datumbereik, op basis van de volgende metrieken:<br>• Totale aantal gescande herstelpunten<br>• Aantal schone herstelpunten<br>• Aantal schone herstelpunten met niet-ondersteunde partities<br>• Aantal geïnfecteerde herstelpunten. Deze metriek omvat het aantal geïnfecteerde herstelpunten met niet-ondersteunde partities. |

## Back-upwidgets

De volgende tabel bevat meer informatie over de widgets in het gedeelte **Back-up**.

| Widget | Beschrijving |
|---|---|
| **Workloads waarvan een back-up is gemaakt** | De widget toont het totaal aantal geregistreerde workloads per back-upstatus.<br><br>**Back-up gemaakt**: het aantal workloads waarvan een back-up is gemaakt (ten minste één back-up is uitgevoerd) gedurende het datumbereik van het rapport.<br><br>**Geen back-up gemaakt**: het aantal workloads waarvan geen back-up is gemaakt (er is geen enkele back-up uitgevoerd) gedurende het datumbereik van het rapport. |
| **Status van schijfintegriteit per fysiek apparaat** | De widget toont de geaggregeerde integriteitsstatus van fysieke apparaten, gebaseerd op de integriteitsstatus van hun schijven.<br><br>**OK**: deze status van de schijfintegriteit wordt gebruikt voor de waarden [70-100]. De status van het apparaat is **OK** wanneer alle schijven de status **OK** hebben.<br><br>**Waarschuwing**: deze status van de schijfintegriteit wordt gebruikt voor de waarden [30-70]. De status van een apparaat is **Waarschuwing** wanneer de status van ten minste een van de schijven **Waarschuwing** is en wanneer er geen schijven de status **Fout** hebben.<br><br>**Fout**: deze status van de schijfintegriteit wordt gebruikt voor de waarden [0-30]. De status van het apparaat is **Fout** wanneer de status van ten minste een van de schijven de status **Fout** heeft.<br><br>**Schijfgegevens berekenen**: de status van het apparaat is **Schijfgegevens berekenen** wanneer de statussen van de schijven van het apparaat nog niet zijn berekend. |
| **Opslaggebruik voor back-ups** | De widget toont het totale aantal en de totale grootte van de back-ups in de cloud en de lokale opslag voor het opgegeven tijdbereik. |

## Widgets voor evaluatie van beveiligingsproblemen en patchbeheer

De volgende tabel bevat meer informatie over de widgets in het gedeelte **Evaluatie van beveiligingsproblemen en patchbeheer**.

| Widget | Beschrijving |
|---|---|
| **Gepatchte beveiligingsproblemen** | De widget toont de prestatieresultaten van de evaluatie van beveiligingsproblemen voor het opgegeven datumbereik.<br><br>**Totaal**: het totale aantal gepatchte beveiligingsproblemen.<br><br>**Microsoft-softwarebeveiligingsproblemen**: het totale aantal verholpen problemen met de Microsoft-beveiliging op alle Windows-apparaten.<br><br>**Beveiligingsproblemen van Windows-software van derden**: |

| Widget | Beschrijving |
|---|---|
| | het totale aantal verholpen beveiligingsproblemen met Windows-software van derden op alle Windows-apparaten.<br><br>**Gescande workloads**: het totale aantal apparaten dat minstens eenmaal is gescand op beveiligingsproblemen binnen het opgegeven datumbereik. |
| **Geïnstalleerde patches** | De widget toont de prestatieresultaten van het patchbeheer voor het opgegeven datumbereik.<br><br>**Geïnstalleerd**: het totaal getal patches dat is geïnstalleerd op alle apparaten.<br><br>**Microsoft-softwarepatches**: het totale aantal Microsoft-softwarepatches dat is geïnstalleerd op alle Windows-apparaten.<br><br>**Patches voor Windows-software van derden**: het totale aantal patches voor Windows-software van derden dat is geïnstalleerd op alle Windows-apparaten.<br><br>**Gepatchte workloads**: het totale aantal apparaten dat is gepatcht (ten minste één patch is geïnstalleerd binnen het opgegeven datumbereik). |

## Widgets voor noodherstel

De volgende tabel bevat meer informatie over de widgets in het gedeelte **Noodherstel**.

| Widget | Beschrijving |
|---|---|
| **Disaster Recovery-statistieken** | De widget toont de belangrijkste prestatiegegevens van noodherstel voor het opgegeven datumbereik.<br><br>**Productiefailovers**: het aantal productiefailoverbewerkingen voor het opgegeven tijdbereik.<br><br>**Testfailovers**: het totale aantal testfailoverbewerkingen in het opgegeven tijdbereik.<br><br>**Primaire servers**: het totale aantal primaire servers op het moment dat het rapport werd gegenereerd.<br><br>**Herstelservers**: het totale aantal herstelservers op het moment dat het rapport werd gegenereerd.<br><br>**Openbare IP's**: het totale aantal openbare IP-adressen (op het moment dat het rapport werd gegenereerd).<br><br>**Totaal verbruikte compute-punten**: het totale aantal compute-punten dat is verbruikt in het opgegeven tijdbereik. |
| **Disaster** | De widget toont informatie over de servers die zijn beschermd door Disaster |

| Widget | Beschrijving |
|---|---|
| **Recovery - Servers getest** | Recovery en zijn getest met testfailover.<br><br>De widget toont de volgende metrieken:<br><br>**Server beschermd**: het aantal servers dat wordt beschermd door Disaster Recovery (servers die ten minste één herstelserver hebben) op het moment dat het rapport werd gegenereerd.<br><br>**Getest**: het aantal door Disaster Recovery beschermde servers dat is getest met testfailover gedurende het geselecteerde tijdbereik, ten opzichte van alle door Disaster Recovery beschermde servers.<br><br>**Niet getest**: het aantal door Disaster Recovery beschermde servers dat niet is getest met testfailover gedurende het geselecteerde tijdbereik, ten opzichte van alle door Disaster Recovery beschermde servers.<br><br>De widget toont ook de grootte van de Disaster Recovery-opslag (in GB) op het moment dat het rapport werd gegenereerd. Het is de som van de back-upgrootten van de cloudservers. |
| **Servers beschermd door Disaster Recovery** | De widget toont informatie over de servers die zijn beschermd door Disaster Recovery en de niet-beschermde servers.<br><br>De widget toont de volgende metrieken:<br><br>Het totale aantal servers geregistreerd in de klanttenant op het moment dat het rapport werd gegenereerd.<br><br>**Beschermd**: het aantal servers dat wordt beschermd door Disaster Recovery (servers die ten minste één herstelserver en een volledige serverback-up hebben), ten opzichte van alle geregistreerde servers op het moment dat het rapport werd gegenereerd.<br><br>**Niet beschermd**: het totale aantal niet-beschermde servers ten opzichte van alle geregistreerde servers op het moment dat het rapport werd gegenereerd. |

## Widget voor de preventie van gegevensverlies

Het volgende onderwerp bevat meer informatie over de geblokkeerde randapparaten in het gedeelte **Preventie van gegevensverlies**.

De widget toont het totale aantal geblokkeerde apparaten en het totale aantal geblokkeerde apparaten per apparaattype voor het opgegeven datumbereik.

- Verwisselbare opslag
- Versleuteld verwisselbaar
- Printers
- Klembord: omvat de apparaattypen Klembord en Schermopname.

- Mobiele apparaten
- Bluetooth
- Optische stations
- Diskettestations
- USB: omvat de apparaattypen USB-poort en Omgeleide USB-poort.
- FireWire
- Toegewezen stations
- Omgeleid klembord: omvat de apparaattypen Omgeleid klembord inkomend en Omgeleid klembord uitgaand.

De widget toont de eerste zeven apparaattypen met het hoogste aantal geblokkeerde apparaten, en combineert de rest van de apparaattypen in het apparaattype **Overige**.

## Widgets voor File Sync & Share

De volgende tabel bevat informatie over de widgets in het gedeelte **File Sync & Share**.

| Widget | Beschrijving |
|---|---|
| **File Sync & Share-statistieken** | De widget toont de volgende metrieken:<br>**Totaal gebruikte cloudopslag**: het totale opslaggebruik van alle gebruikers.<br>**Eindgebruikers**: het totale aantal eindgebruikers.<br>**Gemiddeld gebruikte opslag per eindgebruiker**: het gemiddelde opslaggebruik per eindgebruiker.<br>**Gastgebruikers**: het totale aantal gastgebruikers. |
| **File Sync & Share-opslaggebruik door eindgebruikers** | De widget toont het totale aantal File Sync & Share-eindgebruikers die een opslaggebruik hebben in de volgende bereiken:<br>• 0 – 1 GB<br>• 1 – 5 GB<br>• 5 – 10 GB<br>• 10 – 50 GB<br>• 50 – 100 GB<br>• 100 – 500 GB<br>• 500 GB – 1 TB<br>• 1+ TB |

## Widgets voor Notary

De volgende tabel bevat meer informatie over de widgets in het gedeelte **Notary**.

| Widget | Beschrijving |
|---|---|
| **Cyber Notary-statistieken** | De widget toont de volgende Notary-metrieken:<br>**Gebruikte cloudopslag voor Notary**: de totale grootte van de gebruikte opslag voor Notary-services.<br>**Genotariseerde bestanden**: het totale aantal genotariseerde bestanden.<br>**Elektronisch ondertekende documenten**: het totale aantal elektronisch ondertekende documenten en elektronisch ondertekende bestanden. |
| **Genotariseerde bestanden van eindgebruikers** | Geeft het totale aantal genotariseerde bestanden van alle eindgebruikers weer. De gebruikers worden gegroepeerd op basis van het aantal genotariseerde dat ze hebben.<br>• Maximaal 10 bestanden<br>• 11 – 100 bestanden<br>• 101 – 500 bestanden<br>• 501 – 1000 bestanden<br>• 1000+ bestanden |
| **Elektronisch ondertekende documenten van eindgebruikers** | De widget toont het totale aantal elektronisch ondertekende documenten en elektronisch ondertekende bestanden van alle eindgebruikers. De gebruikers worden gegroepeerd op basis van het aantal elektronisch ondertekende documenten en bestanden dat ze hebben.<br>• Maximaal 10 bestanden<br>• 11 – 100 bestanden<br>• 101 – 500 bestanden<br>• 501 – 1000 bestanden<br>• 1000+ bestanden |

## 5.3.2 De instellingen van het overzichtsrapport configureren

U kunt de rapportinstellingen bijwerken die zijn geconfigureerd toen het overzichtsrapport werd gemaakt.

***De instellingen van het overzichtsrapport bijwerken***

1. Ga in de beheerconsole naar **Rapporten**>**Overzichtsrapport**.
2. Klik op de naam van het overzichtsrapport dat u wilt bijwerken.
3. Klik op **Instellingen**.
4. Wijzig de waarden van de velden zoals gewenst.
5. Klik op **Opslaan**.

## 5.3.3 Een overzichtsrapport maken

U kunt een overzichtsrapport maken, de inhoud ervan bekijken, de ontvangers van het rapport configureren en plannen wanneer het automatisch wordt verzonden.

***Een overzichtsrapport maken***

1. Ga in de beheerconsole naar **Rapporten**>**Overzichtsrapport**.
2. Klik op **Overzichtsrapport maken**.
3. Typ bij **Naam van rapport** de naam van het rapport.
4. Selecteer de ontvangers van het rapport.
   - Als u het rapport naar alle contacten en gebruikers wilt sturen, selecteert u **Verzenden naar alle contacten en gebruikers**.
   - Als u het rapport naar specifieke contacten en gebruikers wilt sturen
     a. Schakel **Verzenden naar alle contacten en gebruikers** uit.
     b. Klik op **Contacten selecteren**.
     c. Selecteer de specifieke contacten en gebruikers. U kunt de zoekfunctie gebruiken om gemakkelijk een specifiek contact te vinden.
     d. Klik op **Selecteren**.
5. Selecteer een bereik: **30 dagen** of **Deze maanden**
6. Selecteer een bestandsindeling: **PDF**, **Excel** of **Excel en PDF**.
7. Configureer de planningsinstellingen.
   - Als u het rapport op een bepaalde datum en tijd naar de ontvangers wilt sturen:
     a. Schakel de optie **Gepland** in.
     b. Klik op het veld **Dag van de maand**, wis het veld Laatste dag en klik op de datum die u wilt instellen.
     c. Geef in het veld **Tijd** de tijd op die u wilt instellen.
     d. Klik op **Toepassen**.
   - Als u het rapport wilt maken zonder het naar de ontvangers te sturen, schakelt u de optie **Gepland** uit.
8. Klik op **Opslaan**.

## 5.3.4 Het overzichtsrapport aanpassen

U kunt bepalen welke informatie in het overzichtsrapport moet worden opgenomen. U kunt secties toevoegen of verwijderen, widgets toevoegen of verwijderen, de naam van secties wijzigen, widgets

aanpassen, en widgets en secties slepen en neerzetten om de volgorde te wijzigen waarin de informatie in het rapport wordt weergegeven.

***Een sectie toevoegen***

1. Klik op **Item toevoegen** > **Sectie toevoegen**.
2. Typ in het venster **Sectie toevoegen** een sectienaam of gebruik de standaard sectienaam.
3. Klik op **Toevoegen aan rapport**.

***De naam van een sectie wijzigen***

1. Klik in de sectie waar u de naam wilt wijzigen, op **Bewerken**.
2. Typ de nieuwe naam in het venster **Sectie bewerken**.
3. Klik op **Opslaan**.

***Een sectie verwijderen***

1. Klik in de sectie waar u wilt verwijderen, op **Sectie verwijderen**.
2. Klik in het bevestigingsvenster voor **Sectie verwijderen** op **Verwijderen**.

***Een widget met standaardinstellingen toevoegen aan een sectie***

1. Klik in de sectie waar u de widget wilt toevoegen, op **Widget toevoegen**.
2. Klik in het venster **Widget toevoegen** op de widget die u wilt toevoegen.

***Een aangepaste widget toevoegen aan een sectie***

1. Klik in de sectie waar u de widget wilt toevoegen, op **Widget toevoegen**.
2. Zoek in het venster **Widget toevoegen** naar de widget die u wilt toevoegen en klik op **Aanpassen**.
3. Configureer de velden indien nodig.
4. Klik op **Widget toevoegen**.

***Een widget met standaardinstellingen toevoegen aan het rapport***

1. Klik op **Item toevoegen** > **Widget toevoegen**.
2. Klik in het venster **Widget toevoegen** op de widget die u wilt toevoegen.

***Een aangepaste widget toevoegen aan het rapport***

1. Klik op **Widget toevoegen**.
2. Zoek in het venster **Widget toevoegen** naar de widget die u wilt toevoegen en klik op **Aanpassen**.
3. Configureer de velden indien nodig.
4. Klik op **Widget toevoegen**.

***De standaardinstellingen van een widget herstellen***

1. Klik in de widget die u wilt aanpassen, op **Bewerken**.
2. Klik op **Terugzetten naar standaardwaarden**.
3. Klik op **Gereed**.

***Een widget aanpassen***

1. Klik in de widget die u wilt aanpassen, op **Bewerken**.
2. Bewerk de velden zoals gewenst.
3. Klik op **Gereed**.

### 5.3.5 Overzichtsrapporten verzenden

U kunt een overzichtsrapport op aanvraag verzenden. In dit geval wordt de instelling **Planning** genegeerd en wordt het rapport onmiddellijk verzonden. Bij het verzenden van het rapport gebruikt het systeem de waarden voor Ontvangers, Bereik en Bestandsindeling die zijn geconfigureerd in **Instellingen**. U kunt deze instellingen handmatig wijzigen voordat u het rapport verzendt. Zie "De instellingen van het overzichtsrapport configureren" (p. 60) voor meer informatie.

***Een overzichtsrapport verzenden***

1. Ga in de beheerportal naar **Rapporten**>**Overzichtsrapport**.
2. Klik op de naam van het overzichtsrapport dat u wilt verzenden.
3. Klik op **Nu verzenden**.
   Het overzichtsrapport wordt automatisch verzonden naar de geselecteerde ontvangers.

## 5.4 Tijdzones in rapporten

De tijdzones die in rapporten worden gebruikt, zijn afhankelijk van het rapporttype. De volgende tabel bevat informatie ter referentie.

| Locatie en type van het rapport | Tijdzone gebruikt in het rapport |
|---|---|
| Beheerportal> Overzicht> Bewerkingen<br>(widgets) | De tijd waarop rapporten worden gemaakt, komt overeen met de tijdzone van de machine met de gebruikte browser. |
| Beheerportal> Overzicht> Bewerkingen<br>(geëxporteerd naar PDF of xslx) | • De tijdstempel van het geëxporteerde rapport komt overeen met de tijdzone van de machine die is gebruikt om het rapport te exporteren.<br>• De tijdzone van de activiteiten die in het rapport worden weergegeven, is UTC. |
| Beheerportal> Rapporten> Gebruik> Geplande rapporten | • Het rapport is gegenereerd op de eerste dag van de maand om 23:59:59 UTC.<br>• Het rapport wordt verzonden op de tweede dag van de maand. |

| | |
|---|---|
| Beheerportal> Rapporten> Gebruik> Aangepaste rapporten | De tijdzone en datum van het rapport is UTC. |
| Beheerportal> Rapporten> Bewerkingen<br>(widgets) | • De tijd waarop rapporten worden gemaakt, komt overeen met de tijdzone van de machine met de gebruikte browser.<br>• De tijdzone van de activiteiten die in het rapport worden weergegeven, is UTC. |
| Beheerportal> Rapporten> Bewerkingen<br>(geëxporteerd naar PDF of xslx) | • De tijdstempel van het geëxporteerde rapport komt overeen met de tijdzone van de machine die is gebruikt om het rapport te exporteren.<br>• De tijdzone van de activiteiten die in het rapport worden weergegeven, is UTC. |
| Beheerportal> Rapporten> Bewerkingen<br>(geplande levering) | • De tijdzone van de rapportlevering is UTC.<br>• De tijdzone van de activiteiten die in het rapport worden weergegeven, is UTC. |
| Beheerportal> Gebruikers> Dagelijks overzicht van actieve waarschuwingen | • Dit rapport wordt één keer per dag verzonden tussen 10:00 en 23:59 UTC. Het tijdstip waarop het rapport wordt verzonden, is afhankelijk van de workload in het datacentrum.<br>• De tijdzone van de activiteiten die in het rapport worden weergegeven, is UTC. |
| Beheerportal> Gebruikers> Statusmeldingen over cyberbeveiliging | • Dit rapport wordt verzonden wanneer een activiteit is voltooid.<br>**Opmerking**<br>Afhankelijk van de workload in het datacentrum kunnen sommige rapporten vertraagd worden verzonden.<br>• De tijdzone van de activiteit in het rapport is UTC. |

## 5.5 Gerapporteerde gegevens per type widget

Er zijn twee typen widgets op het dashboard, afhankelijk van het gegevensbereik dat ze weergeven:

- Widgets die actuele gegevens weergeven op het moment van browsen of het genereren van rapporten.
- Widgets die historische gegevens weergeven.

Wanneer u een datumbereik in de rapportinstellingen configureert om gegevens voor een bepaalde periode te dumpen, is het geselecteerde tijdbereik alleen van toepassing op widgets die historische gegevens weergeven. Voor widgets die actuele gegevens weergeven op het moment van browsen, is de parameter tijdbereik niet van toepassing.

In de volgende tabel worden de beschikbare widgets weergegeven, met de respectievelijke gegevensbereiken.

| Naam van widget | Gegevens weergegeven in widget en rapporten |
|---|---|
| #CyberFit-score per machine | Actueel |
| 5 meest recente waarschuwingen | Actueel |
| Gegevens van actieve waarschuwingen | Actueel |
| Overzicht van waarschuwingen activeren | Actueel |
| Activiteiten | Historisch |
| Activiteitenlijst | Historisch |
| Geschiedenis van waarschuwingen | Historisch |
| Antimalwarescan van back-ups | Historisch |
| Antimalwarescan van bestanden | Historisch |
| Back-upscangegevens (bedreigingen) | Historisch |
| Back-upstatus | Historisch: in de kolommen **Totaal aantal uitgevoerde bewerkingen** en **Aantal voltooide bewerkingen**<br>Actueel: in alle andere kolommen |
| Opslaggebruik voor back-ups | Historisch |
| Geblokkeerde randapparaten | Historisch |
| Geblokkeerde URL's | Actueel |
| Cloudtoepassingen | Actueel |
| Beveiligingsstatus van workloads in de cloud | Actueel |
| Cyberbescherming | Actueel |
| Overzicht van cyberbescherming | Historisch |
| Overzicht van gegevensbescherming | Historisch |
| Apparaten | Actueel |
| Disaster Recovery - Servers getest | Historisch |
| Disaster Recovery-statistieken | Historisch |
| Gedetecteerde machines | Actueel |
| Overzicht van schijfintegriteit | Actueel |

| | |
|---|---|
| Status van schijfintegriteit | Actueel |
| Status van schijfintegriteit per fysiek apparaat | Actueel |
| Elektronisch ondertekende documenten van eindgebruikers | Actueel |
| Bestaande kwetsbaarheden | Historisch |
| File Sync & Share-statistieken | Actueel |
| File Sync & Share-opslaggebruik door eindgebruikers | Actueel |
| Hardwarewijzigingen | Historisch |
| Hardwaredetails | Actueel |
| Hardware-inventaris | Actueel |
| Overzicht van historische waarschuwingen | Historisch |
| Locatieoverzicht | Actueel |
| Ontbrekende updates per categorie | Actueel |
| Niet beschermd | Actueel |
| Genotariseerde bestanden van eindgebruikers | Actueel |
| Notary-statistieken | Actueel |
| Geschiedenis van patchinstallatie | Historisch |
| Status van patchinstallatie | Historisch |
| Overzicht van patchinstallatie | Historisch |
| Gepatchte beveiligingsproblemen | Historisch |
| Geïnstalleerde patches | Historisch |
| Beveiligingsstatus | Actueel |
| Onlangs beïnvloed | Historisch |
| Servers beschermd door Disaster Recovery | Actueel |
| Software-inventaris | Actueel |
| Softwareoverzicht | Historisch |

| | |
|---|---|
| Bedreigingen gedetecteerd door beschermingstechnologie | Historisch |
| Machines met beveiligingsproblemen | Actueel |
| Workloads waarvan een back-up is gemaakt | Historisch |
| Beveiligingsstatus van workloads | Actueel |

# 6 Auditlogboek

Als u het auditlogboek wilt bekijken, klikt u op **Auditlogboek**.

Het auditlogboek geeft een chronologisch overzicht van de volgende gebeurtenissen:

- Bewerkingen uitgevoerd door gebruikers in de beheerportal
- Bewerkingen met cloud-to-cloud resources die door gebruikers worden uitgevoerd in de Cyber Protection-serviceconsole
- Systeemberichten over bereikte quota en quotagebruik

Het logboek bevat gebeurtenissen voor de organisatie of eenheid waarin u momenteel werkt, met de onderliggende eenheden. U kunt op een gebeurtenis klikken als u meer informatie wilt zien.

Het logboek wordt dagelijks opgeschoond. De gebeurtenissen worden na 180 dagen verwijderd.

## 6.1 Velden van het auditlogboek

Het logboek bevat de volgende informatie voor elke gebeurtenis:

- **Gebeurtenis**
  Korte beschrijving van de gebeurtenis. Bijvoorbeeld: **Tenant is gemaakt**, **Tenant is verwijderd**, **Gebruiker is gemaakt**, **Gebruiker is verwijderd**, **Quotum is bereikt**, **Back-upinhoud is doorzocht**.
- **Ernstgraad**
  Kan een van de volgende waarden zijn:
  - **Fout**
    Geeft een fout aan.
  - **Waarschuwing**
    Geeft een mogelijk negatieve actie aan. Bijvoorbeeld: **Tenant is verwijderd**, **Gebruiker is verwijderd**, **Quotum is bereikt**.
  - **Kennisgeving**
    Geeft een gebeurtenis aan die mogelijk uw aandacht vereist. Bijvoorbeeld: **Tenant is bijgewerkt**, **Gebruiker is bijgewerkt**.
  - **Informatie**
    Geeft neutrale informatie aan over een verandering of actie. Bijvoorbeeld: **Tenant is gemaakt**, **Gebruiker is gemaakt**, **Quotum is bijgewerkt**.
- **Datum**
  De datum en tijd waarop de gebeurtenis zich heeft voorgedaan.
- **Naam van object**
  Het object waarvoor de bewerking is uitgevoerd. Bijvoorbeeld: het object van de gebeurtenis **Gebruiker is bijgewerkt** is de gebruiker van wie de eigenschappen zijn gewijzigd. Voor gebeurtenissen die zijn gerelateerd aan een quotum, is het quotum het object.
- **Tenant**

De naam van de eenheid waarvan het object deel uitmaakt. Bijvoorbeeld: de tenant van de gebeurtenis **Gebruiker is bijgewerkt** is de eenheid waarvan de gebruiker deel uitmaakt. De tenant van de gebeurtenis **Quotum is bereikt** is de gebruiker van wie het quotum is bereikt.

- **Initiator**

  De gebruikersnaam van de gebruiker die de gebeurtenis heeft geïnitieerd. Voor systeemberichten en gebeurtenissen die worden geïnitieerd door beheerders op het hoogste niveau, wordt **Systeem** gebruikt als waarde voor de initiator.
- **Tenant van initiator**

  De naam van de eenheid waarvan de initiator deel uitmaakt. Voor systeemberichten en gebeurtenissen die worden geïnitieerd door beheerders op het hoogste niveau, wordt dit veld leeg gelaten.
- **Methode**

  Geeft aan of de gebeurtenis is geïnitieerd via de webinterface of via de API.
- **IP**

  Het IP-adres van de machine van waaraf de gebeurtenis is geïnitieerd.

## 6.2 Filteren en zoeken

U kunt de gebeurtenissen filteren op beschrijving, ernstgraad of datum. U kunt ook naar de gebeurtenissen zoeken per object, eenheid, initiator en eenheid van de initiator.

# 7 Geavanceerde scenario's

## 7.1 Toegang tot de webinterface beperken

U kunt toegang tot de webinterface beperken door een lijst met IP-adressen op te geven die de gebruikers kunnen gebruiken om zich aan te melden.

Deze beperking is ook van toepassing op toegang tot de beheerportal via de API.

Deze beperking is alleen van toepassing op het niveau waar het is ingesteld. De beperking wordt *niet* toegepast op de leden van de onderliggende eenheden.

***Toegang tot de webinterface beperken***

1. Meld u aan bij de beheerportal.
2. Navigeer naar de eenheid waarvoor u de toegang wilt beperken.
3. Klik op **Instellingen** > **Beveiliging**.
4. Schakel het selectievakje **Aanmeldingsbeheer inschakelen** in.
5. Ga naar **Toegestane IP-adressen** en geef de toegestane IP-adressen op.
   U kunt de volgende parameters opgeven, gescheiden door puntkomma's:
   - IP-adres, bijvoorbeeld: 192.0.2.0
   - IP-bereik, bijvoorbeeld: 192.0.2.0-192.0.2.255
   - Subnetten, bijvoorbeeld: 192.0.2.0/24
6. Klik op **Opslaan**.

## 7.2 Toegang tot uw bedrijf beperken

Bedrijfbeheerders kunnen de toegang tot het bedrijf beperken voor beheerders op een hoger niveau.

Als toegang tot het bedrijf is beperkt, kunnen beheerders op een hoger niveau alleen de eigenschappen van het bedrijf wijzigen. Ze krijgen de gebruikersaccounts en onderliggende eenheden niet te zien.

***Toegang tot het bedrijf beperken***

1. Meld u aan bij de beheerportal.
2. Klik op **Instellingen** > **Beveiliging**.
3. Schakel de optie **Toegang tot ondersteuning** uit.
4. Klik op **Opslaan**.

## 7.3 API-clients beheren

Systemen van derden kunnen worden geïntegreerd met  Cyber Cloud door gebruik te maken van de Application Programming Interfaces (API's). Toegang tot deze API's wordt ingeschakeld via API-clients, een integraal onderdeel van het OAuth 2.0-autorisatieframework van het platform.

### 7.3.1 Wat is een API-client?

Een API-client is een speciaal platformaccount dat is bedoeld om een systeem van derden te vertegenwoordigen dat moet worden geverifieerd en geautoriseerd om toegang te krijgen tot gegevens in de API's van het platform en de bijbehorende services.

De toegang van de client is beperkt tot een tenant, waarbij een beheerder de client en bijbehorende sub-tenants maakt.

Wanneer de client wordt gemaakt, worden hiervoor de servicerollen van het beheerdersaccount overgenomen en deze rollen kunnen later niet worden gewijzigd. Als de rollen van het beheerdersaccount worden gewijzigd of uitgeschakeld, heeft dit geen invloed op de client.

De clientreferenties bestaan uit de unieke identificatie (id) en de geheime waarde. De referenties verlopen niet en kunnen niet worden gebruikt om u aan te melden op de beheerportal of bij een serviceconsole. De geheime waarde kan opnieuw worden ingesteld.

Het is niet mogelijk tweeledige verificatie voor de client in te schakelen.

### 7.3.2 Typische integratieprocedure

1. Een beheerder maakt een API-client in een tenant die wordt beheerd door een systeem van derden.
2. De beheerder activeert de stroom van de OAuth 2.0-clientreferenties in het systeem van derden.
   Volgens deze stroom moet het systeem eerst de referenties van de gemaakte client naar het platform sturen met behulp van de autorisatie-API voordat toegang kan worden verkregen tot de tenant en bijbehorende services via de API. Het platform genereert en retourneert een beveiligingstoken (de unieke cryptische tekenreeks die aan deze specifieke client is toegewezen). Vervolgens moet het systeem dit token toevoegen aan alle API-aanvragen.
   Met een beveiligingstoken hoeft u geen clientreferenties meer door te geven bij de API-aanvragen. Voor extra veiligheid verloopt het token binnen twee uur. Daarna mislukken alle API-aanvragen met het verlopen token en moet het systeem een nieuw token aanvragen vanaf het platform.

Raadpleeg de handleiding voor ontwikkelaars op https://developer.acronis.com/doc/account-management/v2/guide/index voor meer informatie over het gebruik van de autorisatie- en platform-API's.

### 7.3.3 Een API-client maken

1. Meld u aan bij de beheerportal.
2. Klik op **Instellingen** > **API-clients** > **API-client maken**.
3. Voer een naam in voor de API-client.
4. Klik op **Volgende**.
   De API-client wordt standaard gemaakt met de status **Actief**.
5. Kopieer en bewaar de id en de geheime waarde van de client en de datacenter-URL. U hebt ze nodig wanneer u de stroom van de OAuth 2.0-clientreferenties inschakelt in het systeem van derden.

   **Belangrijk**
   Om veiligheidsredenen wordt de geheime waarde slechts één keer weergegeven. Er is geen manier om deze waarde op te halen als u deze kwijtraakt. U kunt deze alleen opnieuw instellen.

6. Klik op **Gereed**.

### 7.3.4 De geheime waarde van een API-client opnieuw instellen

1. Meld u aan bij de beheerportal.
2. Klik op **Instellingen** > **API-clients**.
3. Zoek de gewenste client in de lijst.
4. Klik op  en klik vervolgens op **Geheim opnieuw instellen**.
5. Bevestig uw beslissing door op **Volgende** te klikken.
   Er wordt een nieuwe geheime waarde gegenereerd. De client-id en datacenter-URL veranderen niet.
   Alle beveiligingstokens die aan deze client zijn toegewezen, verlopen onmiddellijk en API-aanvragen met deze tokens mislukken.
6. Kopieer en bewaar de nieuwe geheime waarde van de client.

   **Belangrijk**
   Om veiligheidsredenen wordt de geheime waarde slechts één keer weergegeven. Er is geen manier om deze waarde op te halen als u deze kwijtraakt. U kunt deze alleen opnieuw instellen.

7. Klik op **Gereed**.

### 7.3.5 Een API-client uitschakelen

1. Meld u aan bij de beheerportal.
2. Klik op **Instellingen** > **API-clients**.

3. Zoek de gewenste client in de lijst.
4. Klik op  en vervolgens op **Uitschakelen**.
5. Bevestig uw beslissing.
   De status van de client verandert in **Uitgeschakeld**.
   API-aanvragen met beveiligingstokens die aan deze client zijn toegewezen, mislukken, maar de tokens zullen niet onmiddellijk verlopen. Het uitschakelen van de client heeft geen invloed op de vervaltijd van tokens.
   U kunt de client op elk gewenst moment opnieuw inschakelen.

## 7.3.6 Een uitgeschakelde API-client inschakelen

1. Meld u aan bij de beheerportal.
2. Klik op **Instellingen** > **API-clients**.
3. Zoek de gewenste client in de lijst.
4. Klik op  en vervolgens op **Inschakelen**.
   De status van de client verandert in **Actief**.
   API-aanvragen met beveiligingstokens die aan deze client zijn toegewezen, lukken nog zolang deze tokens nog niet zijn verlopen.

## 7.3.7 Een API-client verwijderen

1. Meld u aan bij de beheerportal.
2. Klik op **Instellingen** > **API-clients**.
3. Zoek de gewenste client in de lijst.
4. Klik op  en vervolgens op **Verwijderen**.
5. Bevestig uw beslissing.
   Alle beveiligingstokens die aan deze client zijn toegewezen, verlopen onmiddellijk en API-aanvragen met deze tokens mislukken.

**Belangrijk**
Er is geen manier om een verwijderde client te herstellen.

# Index

**V**



**W**



**Z**