Portal zarządzania

24.03

Podręcznik administratora firmy

WERSJA: 10.04.2024

Spis treści

Informacje na temat niniejszego dokumentu

Ten dokument jest przeznaczony dla administratorów klientów, którzy chcą używać portalu zarządzania w chmurze do tworzenia kont użytkowników, jednostek i limitów oraz zarządzania nimi w celu konfigurowania i kontrolowania dostępu oraz monitorowania wykorzystania i operacji w swojej organizacji w chmurze.

Informacje o portalu zarządzania

Portal zarządzania to interfejs internetowy platformy chmurowej, która udostępnia usługi ochrony danych.

Choć każda usługa ma własny interfejs internetowy, nazywany konsolą usługi, portal zarządzania umożliwia administratorom kontrolowanie wykorzystania usług, tworzenie kont użytkowników i jednostek, generowanie raportów i nie tylko.

Konta i jednostki

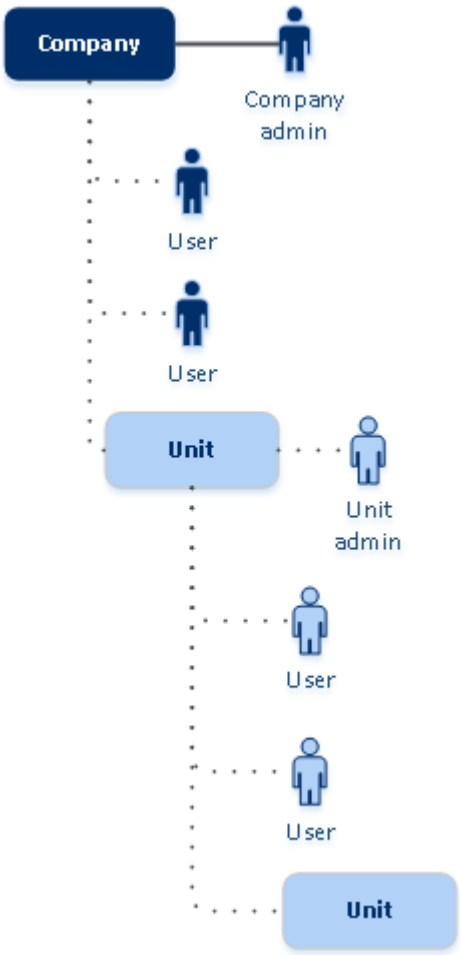
Dostępne są dwa rodzaje kont użytkowników: konta administratorów oraz konta użytkowników.

- **Administratorzy** mają dostęp do portalu zarządzania. Mają rolę administratora we wszystkich usługach.
- **Użytkownicy** nie mają dostępu do portalu zarządzania. Ich dostęp do usług oraz role są określane przez administratora.

Administratorzy mogą tworzyć jednostki, które zwykle odpowiadają jednostkom organizacyjnym lub działom organizacji. Każde konto istnieje albo na poziomie firmy, albo w ramach jednostki.

Administrator może zarządzać jednostkami, kontami administratorów i kontami użytkowników na własnym lub niższym poziomie hierarchii.

Poniższy diagram ilustruje trzy poziomy hierarchii — firmę i dwie jednostki. Opcjonalne jednostki i konta są oznaczone linią kropkowaną.



Poniższa tabela zawiera zestawienie operacji, które mogą wykonywać administratorzy oraz użytkownicy.

Operacja	Użytkownicy	Administratorzy
Tworzenie jednostki	Nie	Tak
Tworzenie kont	Nie	Tak
Pobieranie i instalacja oprogramowania	Tak	Tak
Korzystanie z usług	Tak	Tak
Tworzenie raportów dotyczących użytkowania usługi	Nie	Tak

Zarządzanie limitami

Limity ograniczają możliwości korzystania z usługi przez dzierżawcę.

W portalu zarządzania można przeglądać limity usług przyznane organizacji przez dostawcę usług, ale nie można nimi zarządzać.

Można zarządzać limitami usług dotyczącymi użytkowników.

Wyświetlanie limitów organizacji

W portalu zarządzania wybierz **Przegląd** > **Wykorzystanie**. Pojawi się pulpit nawigacyjny z limitami przyznanymi organizacji. Limity dotyczące poszczególnych usług są wyświetlane na osobnych kartach.

Limity dotyczące usługi Kopia zapasowa

Możesz określić limit miejsca w chmurze, limit lokalnych kopii zapasowych oraz maksymalną liczbę komputerów / urządzeń / witryn internetowych, które może chronić użytkownik. Dostępne są niżej wymienione limity.

Limity urządzeń

- **Stacje robocze**
- **Serwery**
- **Maszyny wirtualne**
- **Urządzenia mobilne**
- **Serwery hostingu witryn internetowych** (serwery fizyczne i wirtualne z systemem Linux oraz uruchomionym panelem sterowania Plesk, cPanel, DirectAdmin, VirtualMin lub ISPManager)
- **Witryny internetowe**

Komputer, urządzenie lub witryna internetowe są uznawane za chronione, gdy jest do nich stosowany co najmniej jeden plan ochrony. Urządzenie mobilne staje się chronione po utworzeniu pierwszej kopii zapasowej.

W przypadku przekroczenia nadwyżki liczby urządzeń użytkownik nie może zastosować planu ochrony do kolejnych urządzeń.

Limity chmurowych źródeł danych

- **Stanowiska Microsoft 365**

  Dostawca usługi stosuje ten limit dla całej firmy. Administratorzy firmy mogą wyświetlać ten limit oraz monitorować poziom jego wykorzystania w portalu zarządzania.

  Licencjonowanie stanowisk Microsoft 365 zależy od wybranego trybu rozliczeniowego za rozwiązanie Cyber Protection.

Ważne

Na potrzeby agenta lokalnego i agenta w chmurze wykorzystywane są osobne limity. W przypadku tworzenia kopii zapasowych tych samych obciążeń przy użyciu obu agentów opłata zostanie naliczona dwukrotnie. Na przykład:

- Jeśli kopia zapasowa skrzynek pocztowych 120 użytkowników zostanie utworzona przy użyciu agenta lokalnego, a kopia zapasowa plików OneDrive tych samych użytkowników zostanie utworzona przy użyciu agenta w chmurze, zostanie naliczona opłata za 240 stanowisk Microsoft 365.
- Jeśli kopia zapasowa skrzynek pocztowych 120 użytkowników zostanie utworzona przy użyciu agenta lokalnego, a ponadto zostanie jeszcze utworzona kopia zapasowa tych samych skrzynek pocztowych przy użyciu agenta w chmurze, zostanie naliczona opłata za 240 stanowisk Microsoft 365.

W trybie rozliczeń **Za obciążenie** limit **Stanowiska Microsoft 365** jest liczony według liczby unikatowych użytkowników. Unikatowy użytkownik to użytkownik, który ma co najmniej jeden z następujących elementów:

- Chroniona skrzynka pocztowa
- Chronione dane OneDrive
- Uzyskaj dostęp do co najmniej jednego chronionego zasobu na poziomie firmy: Witryna Microsoft 365 SharePoint Online lub Microsoft 365 Teams.
  Aby się dowiedzieć, jak sprawdzić liczbę członków witryny Microsoft 365 SharePoint lub Teams, zapoznaj się z tym artykułem bazy wiedzy Knowledge Base.

Uwaga

Blokowani użytkownicy usług Microsoft 365, którzy nie mają chronionej osobistej skrzynki pocztowej ani konta OneDrive i mają dostęp tylko do udostępnionych zasobów (udostępnione skrzynki pocztowe, witryny SharePoint i Microsoft Teams), nie są uwzględniani w opłatach.

Blokowani użytkownicy to ci, którzy nie mają ważnej nazwy logowania i nie mogą uzyskać dostępu do usług Microsoft 365. Informacje o tym, jak zablokować wszystkich użytkowników nielicencjonowanych z organizacji Microsoft 365, można znaleźć w sekcji "Blokowanie logowania się nielicencjonowanych użytkowników usługi Microsoft 365" (s. 11).

Następujące stanowiska Microsoft 365 nie są objęte opłatą i nie wymagają licencji na stanowisko:

- Udostępnione skrzynki pocztowe
- Pomieszczenia i wyposażenie
- Użytkownicy zewnętrzni mający dostęp do witryn SharePoint i/lub Microsoft Teams uwzględnionych w kopii zapasowej

Więcej informacji na temat opcji licencjonowania w trybie rozliczeniowym za gigabajt można znaleźć w artykule Cyber Protect Cloud: licencjonowanie usługi Microsoft 365 za GB.

Więcej informacji na temat opcji licencjonowania w trybie rozliczeniowym za obciążenie można znaleźć w artykule Cyber Protect Cloud: zmiany w licencjonowaniu i cenach usługi Microsoft 365.

- **Microsoft 365 Teams**

  Dostawca usługi stosuje ten limit dla całej firmy. Ten limit powoduje włączenie lub wyłączenie funkcji ochrony instancji Microsoft 365 Teams oraz ustawienie maksymalnej liczby chronionych zespołów. Do ochrony jednego zespołu, niezależnie od liczby jego członków lub kanałów, wymagany jest jeden limit. Administratorzy firmy mogą wyświetlać ten limit oraz monitorować poziom jego wykorzystania w portalu zarządzania.
- **Microsoft 365 SharePoint Online**

  Dostawca usługi stosuje ten limit dla całej firmy. Ten limit powoduje włączenie lub wyłączenie możliwości ochrony witryn programu SharePoint Online oraz ustawienie maksymalnej liczby chronionych zbiorów witryn i witryn grup.

  Administratorzy firmy mogą wyświetlać ten limit w portalu zarządzania. Mogą też wyświetlać ten limit oraz ilość miejsca w pamięci masowej zajmowanego przez kopie zapasowe SharePoint Online w raportach dotyczących wykorzystania.
- **Stanowiska Google Workspace**

  Dostawca usługi stosuje ten limit dla całej firmy. Firma może chronić skrzynki pocztowe **Gmail** (w tym kalendarz i kontakty), pliki z **Dysku Google** lub oba te rodzaje elementów. Administratorzy firmy mogą wyświetlać ten limit oraz monitorować poziom jego wykorzystania w portalu zarządzania.
- **Dysk współdzielony Google Workspace**

  Dostawca usługi stosuje ten limit dla całej firmy. Ten limit powoduje włączenie lub wyłączenie funkcji ochrony Dysków współdzielonych Google Workspace. W przypadku jego włączenia można chronić dowolną liczbę Dysków współdzielonych. Administratorzy firmy nie mogą przeglądać limitu w portalu zarządzania, ale mogą przeglądać ilość miejsca w pamięci masowej zajmowanego przez kopie zapasowe Dysków współdzielonych w raportach dotyczących wykorzystania.

  Tworzenie kopii zapasowych Dysków współdzielonych Google Workspace jest dostępne tylko dla klientów, którzy dodatkowo mają co najmniej jeden limit stanowisk Google Workspace. Limit ten jest tylko sprawdzany — nie jest wykorzystywany.

Stanowisko Microsoft 365 jest uznawane za chronione, gdy do skrzynki pocztowej lub danych OneDrive użytkownika jest stosowany co najmniej jeden plan ochrony. Stanowisko Google Workspace jest uznawane za chronione, gdy do skrzynki pocztowej lub danych Dysku Google użytkownika jest stosowany co najmniej jeden plan ochrony.

W przypadku przekroczenia nadwyżki stanowisk administrator firmy nie może zastosować planu ochrony do kolejnych stanowisk.

Limity miejsca w pamięci masowej

- **Lokalne kopie zapasowe**

  Limit **Lokalnych kopii zapasowych** ogranicza łączny rozmiar lokalnych kopii zapasowych tworzonych za pomocą infrastruktury chmury. Dla tego limitu nie można ustawić nadwyżki.
- **Zasoby chmury**

  Limit **Zasoby chmury** łączy w sobie limit miejsca w pamięci masowej na kopie zapasowe oraz limity odzyskiwania po awarii. Limit miejsca w pamięci masowej na kopie zapasowe wyznacza

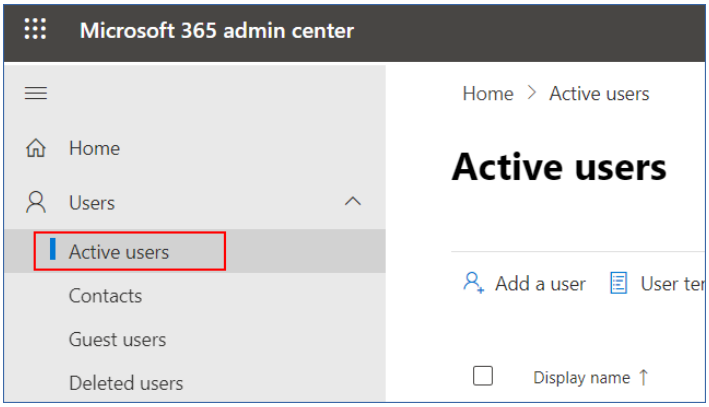
łączny rozmiar kopii zapasowych znajdujących się w danej chmurze. W przypadku przekroczenia nadwyżki limitu miejsca w pamięci masowej na kopie zapasowe tworzenie kopii zapasowej zakończy się niepowodzeniem.

Blokowanie logowania się nielicencjonowanych użytkowników usługi Microsoft 365

Aby uniemożliwić logowanie się wszystkim użytkownikom nielicencjonowanym z organizacji Microsoft 365, należy edytować ich status logowania.

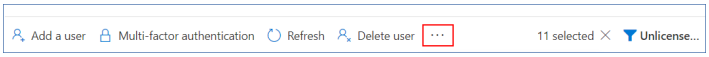
Aby zablokować logowanie się użytkowników nielicencjonowanych

1. Zaloguj się do centrum administracyjnego usługi Microsoft 365 (https://admin.microsoft.com) jako administrator globalny.
2. W menu nawigacyjnym wybierz **Użytkownicy** > **Aktywni użytkownicy**.



3. Kliknij **Filtruj**, a następnie wybierz **Użytkownicy nielicencjonowani**.

4. Zaznacz pola wyboru obok nazw użytkowników, a następnie kliknij ikonę wielokropka (...).



5. W menu wybierz **Edytuj status logowania**.
6. Zaznacz pole wyboru **Blokuj logowanie się użytkowników** i kliknij **Zapisz**.

Limity dotyczące usługi Odzyskiwanie po awarii

Uwaga
Pozycje ofert usługi odzyskiwania po awarii są dostępne tylko wraz z dodatkiem Disaster Recovery.

Dostawca usługi stosuje te limity dla całej firmy. Administratorzy firmy mogą przeglądać limity oraz monitorować wykorzystanie w portalu zarządzania, ale nie mogą ustawiać limitów użytkowników.

- **Magazyn odzyskiwania po awarii**

  W magazynie odzyskiwania po awarii wyświetlany jest rozmiar magazynu kopii zapasowych serwerów chronionych za pomocą usługi odzyskiwania po awarii. Wykorzystanie magazynu odzyskiwania po awarii jest równe wykorzystaniu magazynu kopii zapasowych obciążeń chronionych za pomocą serwerów odzyskiwania po awarii. Wielkość tego magazynu jest

obliczana od chwili utworzenia serwera odzyskiwania, niezależnie od tego, czy ten serwer jest aktualnie uruchomiony. W przypadku osiągnięcia nadwyżki tego limitu nie będzie można tworzyć serwerów podstawowych bądź serwerów odzyskiwania ani dodawać/rozszerzać dysków już istniejących serwerów podstawowych. W przypadku przekroczenia nadwyżki tego limitu nie będzie można inicjować przełączania awaryjnego ani uruchamiać zatrzymanego serwera. Działające serwery kontynuują pracę.

- **Punkty obliczeniowe**

  Limit ogranicza zasoby procesora i pamięci RAM wykorzystywane przez serwery podstawowe oraz serwery odzyskiwania podczas okresu rozliczeniowego. W przypadku osiągnięcia nadwyżki tego limitu wszystkie serwery podstawowe i serwery odzyskiwania są wyłączane. Nie można użyć tych serwerów aż do rozpoczęcia następnego okresu rozliczeniowego. Domyślny okres rozliczeniowy to pełny miesiąc kalendarzowy.

  W przypadku wyłączenia tego limitu nie można korzystać z serwerów — niezależnie od okresu rozliczeniowego.
- **Publiczne adresy IP**

  Ten limit ogranicza liczbę publicznych adresów IP, które można przypisać serwerom podstawowym i serwerom odzyskiwania. W przypadku osiągnięcia nadwyżki tego limitu nie można włączać publicznych adresów IP dla kolejnych serwerów. Możesz zablokować możliwość używania publicznego adresu IP na danym serwerze, odznaczając pole wyboru **Publiczny adres IP** w ustawieniach serwera. Następnie możesz pozwolić innemu serwerowi używać publicznego adresu IP, który najczęściej będzie inny.

  W przypadku wyłączenia tego limitu wszystkie serwery przestają używać publicznych adresów IP, przez co stają się niedostępne z Internetu.
- **Serwery chmurowe**

  Ten limit ogranicza łączną liczbę serwerów podstawowych i serwerów odzyskiwania. W przypadku wyczerpania nadwyżki tego limitu nie można tworzyć serwerów podstawowych ani serwerów odzyskiwania.

  W przypadku wyłączenia limitu serwery są widoczne w konsoli Cyber Protect, ale dostępna jest jedynie opcja **Usuń**.
- **Dostęp do Internetu**

  Ten limit umożliwia włączanie lub wyłączanie dostępu do Internetu z serwerów podstawowych i serwerów odzyskiwania.

  W przypadku wyłączenia tego limitu serwery podstawowe i serwery odzyskiwania nie będą mogły nawiązać połączenia z Internetem.

Limity dotyczące usługi File Sync & Share

Dostawca usługi stosuje te limity dla całej firmy. Administratorzy firmy mogą przeglądać te limity oraz monitorować poziomy ich wykorzystania w portalu zarządzania.

- **Użytkownicy**

  Ten limit określa liczbę użytkowników mających dostęp do usługi.

  Konta administratorów nie są wliczane do tego limitu.

- **Chmura**
  To ustawienie dotyczy pamięci w chmurze przeznaczonej na pliki użytkowników. Limit określa ilość miejsca w chmurze przydzielonego dzierżawcy.

Limity dotyczące usługi Fizyczne dostarczanie danych

Wykorzystanie limitów dotyczących usługi Fizyczne dostarczanie danych jest szacowane na podstawie liczby dysków. Na jednym dysku można zapisać początkowe kopie zapasowe wielu komputerów.

Dostawca usługi stosuje te limity dla całej firmy. Administratorzy firmy mogą przeglądać limity oraz monitorować wykorzystanie w portalu zarządzania, ale nie mogą ustawiać limitów użytkowników.

- **W chmurze**
  Umożliwia wysłanie początkowej kopii zapasowej do chmurowego centrum danych na dysku twardym. Ten limit określa maksymalną liczbę dysków, które można przesłać do chmurowego centrum danych.

Limity dotyczące usługi Notary

Dostawca usługi stosuje te limity dla całej firmy. Administratorzy firmy mogą przeglądać te limity oraz monitorować poziomy ich wykorzystania w portalu zarządzania.

- **Magazyn Notary**
  Określa maksymalną ilość miejsca w chmurze na pliki notaryzowane, pliki podpisane oraz pliki w trakcie notaryzacji lub podpisywania.
  Aby zmniejszyć wykorzystanie tego limitu, można usunąć z magazynu Notary pliki już notaryzowane lub podpisane.
- **Notaryzacje**
  Określa maksymalną liczbę plików, które można notaryzować przy użyciu usługi Notary.
  Plik jest uznawany za notaryzowany, gdy tylko zostanie przesłany do magazynu Notary i jego status notaryzacji zostanie zmieniony na **W toku**.
  W przypadku kilkukrotnej notaryzacji tego samego pliku każda notaryzacja jest liczona osobno.
- **E-podpisy**
  Określa maksymalną liczbę e-podpisów cyfrowych.

Określanie limitów dla użytkowników

Limity pozwalają ograniczać możliwości korzystania z usługi przez użytkownika. Aby ustawić limity dla użytkownika, wybierz go na karcie **Użytkownicy** w sekcji **Zarządzanie firmą**, a następnie kliknij ikonę ołówka w sekcji **Limity**.

W przypadku przekroczenia limitu na adres e-mail użytkownika jest wysyłane stosowne powiadomienie. Jeśli nie zostanie ustawiona nadwyżka limitu, limit jest uznawany za „**elastyczny**". Oznacza to, że ograniczenia dotyczące korzystania z usługi Cyber Protection nie są stosowane.

Jeśli zostanie ustawiona nadwyżka limitu, limit jest uznawany za „**sztywny**". **Nadwyżka** umożliwia użytkownikowi przekroczenie limitu o określoną wartość. W przypadku przekroczenia nadwyżki zostaną zastosowane ograniczenia dotyczące korzystania z usługi.

Przykład

Elastyczny limit: Został ustawiony limit 20 stacji roboczych. Gdy liczba chronionych stacji roboczych użytkownika sięgnie 20, użytkownik otrzyma stosowne powiadomienie pocztą e-mail, ale usługa Cyber Protection nadal będzie dostępna.

Sztywny limit: Jeśli ustawiono limit 20 stacji roboczych, a nadwyżka wynosi 5, to gdy liczba chronionych stacji roboczych sięgnie 20, użytkownik otrzyma powiadomienie pocztą e-mail, ale gdy liczba ta wyniesie 25, usługa Cyber Protection zostanie wyłączona.

Limity dotyczące usługi Kopia zapasowa

Możesz określić limit miejsca na kopie zapasowe oraz maksymalną liczbę komputerów, urządzeń lub witryn internetowych, które użytkownik może chronić. Dostępne są niżej wymienione limity.

Limity urządzeń

- **Stacje robocze**
- **Serwery**
- **Maszyny wirtualne**
- **Urządzenia mobilne**
- **Serwery hostingu witryn internetowych** (serwery fizyczne i wirtualne z systemem Linux oraz uruchomionym panelem sterowania Plesk, cPanel, DirectAdmin, VirtualMin lub ISPManager)
- **Witryny internetowe**

Komputer, urządzenie lub witryna internetowe są uznawane za chronione, gdy jest do nich stosowany co najmniej jeden plan ochrony. Urządzenie mobilne staje się chronione po utworzeniu pierwszej kopii zapasowej.

W przypadku przekroczenia nadwyżki liczby urządzeń użytkownik nie może zastosować planu ochrony do kolejnych urządzeń.

Limit miejsca

- **Magazyn kopii zapasowych**

Limit miejsca w pamięci masowej na kopie zapasowe wyznacza łączny rozmiar kopii zapasowych znajdujących się w danej chmurze. W przypadku przekroczenia nadwyżki limitu miejsca w pamięci masowej na kopie zapasowe tworzenie kopii zapasowej zakończy się niepowodzeniem.

Ważne
Na potrzeby agenta lokalnego i agenta w chmurze wykorzystywane są osobne limity. W przypadku tworzenia kopii zapasowych tych samych obciążeń przy użyciu obu agentów opłata zostanie naliczona dwukrotnie. Na przykład:

- Jeśli kopia zapasowa skrzynek pocztowych 120 użytkowników zostanie utworzona przy użyciu agenta lokalnego, a kopia zapasowa plików OneDrive tych samych użytkowników zostanie utworzona przy użyciu agenta w chmurze, zostanie naliczona opłata za 240 stanowisk Microsoft 365.
- Jeśli kopia zapasowa skrzynek pocztowych 120 użytkowników zostanie utworzona przy użyciu agenta lokalnego, a ponadto zostanie jeszcze utworzona kopia zapasowa tych samych skrzynek pocztowych przy użyciu agenta w chmurze, zostanie naliczona opłata za 240 stanowisk Microsoft 365.

Limity dotyczące usługi File Sync & Share

W przypadku użytkownika można określić następujące limity dotyczące usługi File Sync & Share:

- **Osobiste miejsce w pamięci masowej**
  Określa ilość miejsca w chmurze przydzielonego na pliki użytkownika.

Limity dotyczące usługi Notary

W przypadku użytkownika można określić następujące limity dotyczące usługi Notary:

- **Magazyn Notary**
  Określa maksymalną ilość miejsca w chmurze na pliki notaryzowane, pliki podpisane oraz pliki w trakcie notaryzacji lub podpisywania.
  Aby zmniejszyć wykorzystanie tego limitu, można usunąć z magazynu Notary pliki już notaryzowane lub podpisane.
- **Notaryzacje**
  Określa maksymalną liczbę plików, które można notaryzować przy użyciu usługi Notary.
  Plik jest uznawany za notaryzowany, gdy tylko zostanie przesłany do magazynu Notary i jego status notaryzacji zostanie zmieniony na **W toku**.
  W przypadku kilkukrotnej notaryzacji tego samego pliku każda notaryzacja jest liczona osobno.
- **E-podpisy**
  Określa maksymalną liczbę e-podpisów cyfrowych.

Obsługiwane przeglądarki internetowe

Interfejs internetowy obsługuje następujące przeglądarki internetowe:

- Google Chrome 29 lub nowsza
- Mozilla Firefox 23 lub nowsza
- Opera 16 lub nowsza

- Microsoft Edge 25 lub nowsza
- Safari 8 lub nowsza w systemach operacyjnych macOS oraz iOS

W innych przeglądarkach internetowych (oraz w programie Safari działającym w innych systemach operacyjnych) interfejs użytkownika może być wyświetlany niepoprawnie lub niektóre funkcje mogą być niedostępne.

Szczegółowe instrukcje

Opisane poniżej czynności stanowią wskazówki dotyczące użytkowania portalu zarządzania w podstawowym zakresie. Opisano wykonywanie następujących zadań:

- Aktywowanie konta administratora
- Dostęp do portalu zarządzania i usług
- Tworzenie jednostki
- Tworzenie konta użytkownika

Aktywacja konta administratora

Po rejestracji w celu uzyskania dostępu do usługi otrzymasz wiadomość e-mail zawierającą następujące informacje:

- **Nazwa logowania.** Nazwa użytkownika, której używasz do logowania się. Nazwa logowania jest też widoczna na stronie aktywacji konta.
- Przycisk **Aktywuj konto**. Kliknij ten przycisk i ustaw hasło do konta. Hasło musi się składać z co najmniej dziewięciu znaków. Dodatkowe informacje na temat hasła można znaleźć w sekcji "Wymagania dotyczące hasła" (s. 17).

Wymagania dotyczące hasła

Hasło do konta użytkownika musi się składać z co najmniej 9 znaków. Hasła są też sprawdzane pod kątem złożoności i oceniane przy użyciu jednej z następujących kategorii:

- Słabe
- Średni
- Silne

Nie można zapisać słabego hasła, nawet jeśli składa się ono z 9 lub większej liczby znaków. Hasła, w których jest powtarzana nazwa użytkownika, nazwa logowania, adres e-mail użytkownika lub nazwa dzierżawcy, do którego przynależy konto użytkownika, są zawsze uważane za słabe. Za słabe też uznaje się najpopularniejsze hasła.

Aby zwiększyć siłę hasła, należy dodać do niego kolejne znaki. Stosowanie różnych rodzajów znaków, na przykład cyfr, małych i wielkich liter oraz znaków specjalnych, nie jest konieczne, ale pozwala uzyskać większą siłę hasła przy mniejszej liczbie znaków.

Dostęp do portalu zarządzania i usług

1. Przejdź do strony logowania do konsoli usługi.
2. Wpisz nazwę logowania i kliknij **Dalej**.
3. Wpisz hasło i kliknij **Dalej**.

4. Wykonaj jedną z następujących czynności:
   - Aby się zalogować do portalu zarządzania, kliknij **Portal zarządzania**.
   - Aby się zalogować do usługi, kliknij jej nazwę.

Limit czasu w portalu zarządzania wynosi 24 godziny w przypadku sesji aktywnych i 1 godzinę w przypadku sesji nieaktywnych.

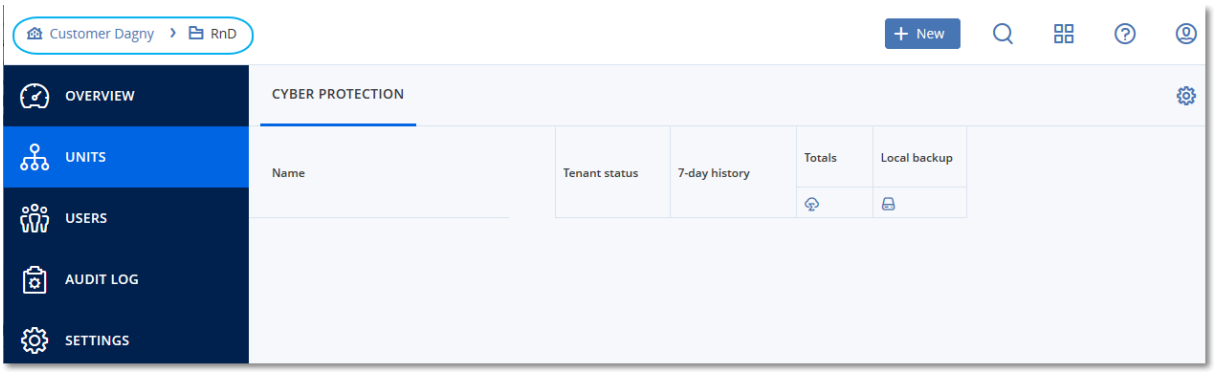
Przełączanie między portalem zarządzania a konsolami usług

Aby przełączyć między portalem zarządzania a konsolami usług, kliknij ikonę w prawym górnym rogu, a następnie wybierz **Portal zarządzania** lub usługę, do której chcesz przejść.

Nawigacja po portalu zarządzania

Korzystając z portalu zarządzania, cały czas działasz w ramach jakiegoś firmy lub jakiejś jednostki. Jest to sygnalizowane w lewym górnym rogu ekranu.

Domyślnie jest wybrany najwyższy dostępny dla Ciebie poziom w hierarchii. Kliknij nazwę jednostki, aby przejść na niższe poziomy hierarchii. Aby wrócić na najwyższy poziom, kliknij jego nazwę w lewym górnym rogu.



Wszystkie elementy interfejsu użytkownika wyświetlają tylko dane dotyczące firmy i jednostki, w ramach której aktualnie działasz, i tylko na niego mają wpływ. Na przykład:

- Za pomocą przycisku **Nowe** możesz utworzyć jednostkę lub konto użytkownika tylko w tej firmie lub jednostce.
- Na karcie **Jednostki** są wyświetlane tylko te jednostki będące bezpośrednimi elementami podrzędnymi tej firmy lub jednostki.
- Na karcie **Użytkownicy** są wyświetlane tylko te konta użytkowników, które znajdują się w tej firmie lub jednostce.

Tworzenie jednostki

Pomiń ten krok, jeśli nie chcesz organizować kont w ramach jednostek.

Jeśli planujesz utworzyć jednostki później, pamiętaj, że utworzonych kont nie można przenosić między jednostkami ani między firmą a jednostkami. Najpierw należy utworzyć jednostkę, a potem dodać do niej konta.

Aby utworzyć jednostkę

1. Zaloguj się do portalu zarządzania.
2. Przejdź do jednostki, w której chcesz utworzyć nową jednostkę.
3. W prawym górnym rogu kliknij **Nowe** > **Jednostka**.
4. W polu **Nazwa** określ nazwę nowej jednostki.
5. [Opcjonalnie] W polu **Język** zmień domyślny język powiadomień, raportów i oprogramowania, który będzie używany w przypadku danej jednostki.
6. Wykonaj jedną z następujących czynności:
   - Aby utworzyć administratora jednostki, kliknij **Dalej** i wykonaj czynności opisane w sekcji „Tworzenie konta użytkownika”, począwszy od kroku 4.
   - Aby utworzyć jednostkę bez administratora, kliknij **Zapisz i zamknij**. Administratorów i użytkowników możesz dodać do jednostki później.

Nowo utworzona jednostka pojawi się na karcie **Jednostki**.

Jeśli zechcesz edytować ustawienia jednostki lub określić informacje kontaktowe, zaznacz tę jednostkę na karcie **Jednostki**, a następnie kliknij ikonę ołówka w sekcji, którą chcesz edytować.

Tworzenie konta użytkownika

Pomiń ten krok, jeśli nie chcesz utworzyć dodatkowych kont użytkowników.

Być może zechcesz utworzyć dodatkowe konta w następujących sytuacjach:

- Konta administratorów firm — w celu podzielenia się obowiązkiem zarządzania z innymi osobami.
- Konta administratorów jednostek — w celu przekazania zarządzania usługami innym osobom, których uprawnienia dostępu będą ograniczone do odpowiednich jednostek.
- Konta użytkowników — w celu umożliwienia użytkownikom dostępu tylko do określonej części usług.

Aby utworzyć konto użytkownika

1. Zaloguj się do portalu zarządzania.
2. Przejdź do jednostki, w której chcesz utworzyć nowe konto użytkownika.
3. W prawym górnym rogu kliknij **Nowe** > **Użytkownik**.
4. Określ następujące informacje na potrzeby konta:

- **Nazwa logowania**

  Ważne
  Każde konto musi mieć unikatową nazwę logowania.

- **E-mail**

  Ważne
  Jeśli użytkownik jest zarejestrowany w usłudze File Sync & Share, podaj adres e-mail użyty do rejestracji w usłudze File Sync & Share.
  Należy pamiętać, że każde konto użytkownika klienta musi mieć unikatowy adres e-mail.

- [Opcjonalnie] **Imię**
- [Opcjonalnie] **Nazwisko**
- W polu **Język** zmień domyślny język powiadomień, raportów i oprogramowania, który będzie używany na danym koncie.

5. Wybierz usługi, do których użytkownik będzie mieć dostęp, oraz role w każdej z usług.
   - Jeśli zaznaczysz pole wyboru **Administrator firmy**, użytkownik będzie mieć dostęp do portalu zarządzania i rolę administratora we wszystkich usługach.
   - Jeśli zaznaczysz pole wyboru **Administrator jednostki**, użytkownik będzie mieć dostęp do portalu zarządzania, ale może nie mieć roli administratora usługi — w zależności od usługi.
   - Jeśli go nie zaznaczysz, użytkownik będzie mieć wybrane przez Ciebie role w wybranych usługach.
6. Kliknij **Utwórz**.

Nowo utworzone konto użytkownika pojawi się na karcie **Użytkownicy**.

Jeśli zechcesz edytować ustawienia użytkownika lub określić dla niego ustawienia powiadomień i limity, zaznacz tego użytkownika na karcie **Użytkownicy**, a następnie kliknij ikonę ołówka w sekcji, którą chcesz edytować.

Aby zresetować hasło użytkownika

1. W portalu zarządzania przejdź do karty **Zarządzanie firmą** > **Użytkownicy**.
2. Zaznacz użytkownika, którego hasło chcesz zresetować, a następnie kliknij ikonę wielokropka > **Resetuj hasło**.
3. Potwierdź czynność, klikając **Resetuj**.

Teraz użytkownik może zresetować hasło, postępując zgodnie z instrukcjami zawartymi w otrzymanej wiadomości e-mail.

W przypadku usług, które nie obsługują uwierzytelniania dwuskładnikowego (na przykład rejestracji w rozwiązaniu Cyber Infrastructure), może być konieczne przekonwertowanie konta użytkownika na *konto usługi* — takie konto nie wymaga uwierzytelniania dwuskładnikowego.

Aby przekonwertować konto użytkownika na konto usługi

1. W portalu zarządzania przejdź do karty **Zarządzanie firmą** > **Użytkownicy**.
2. Wybierz użytkownika, którego konto chcesz przekonwertować na konto usługi, a następnie kliknij ikonę wielokropka > **Oznacz jako konto usługi**.
3. W oknie z monitem o potwierdzenie wprowadź kod uwierzytelniania dwuskładnikowego i potwierdź czynność.

Tego konta można teraz używać na potrzeby usług, które nie obsługują uwierzytelniania dwuskładnikowego.

Role użytkowników dostępne w przypadku poszczególnych usług

Jeden użytkownik może mieć kilka ról, ale tylko jedną rolę w ramach danej usługi.

Rolę użytkownika można definiować dla każdej usługi z osobna.

Usługa	Rola	Opis
n/d	Administrator firmy	Ta rola oznacza przyznanie pełnych praw administratora w przypadku wszystkich usług. Ta rola zapewnia dostęp do firmowej listy dozwolonych. Jeśli dla firmy włączono funkcję Odzyskiwanie po awarii usługi Ochrona, rola ta zapewnia również dostęp do funkcji odzyskiwania po awarii.
Portal zarządzania	Administrator	Ta rola zapewnia dostęp do portalu zarządzania, gdzie administrator może zarządzać użytkownikami w całej organizacji. Na przykład rola ta przyznaje pełne uprawnienia w przypadku ekranów modułu Endpoint Detection and Response, w tym widżetów.
	Administrator w trybie tylko do odczytu Poziom partnera	Ta rola zapewnia dostęp tylko do odczytu do wszystkich obiektów w portalu zarządzania partnera i portalu zarządzania wszystkich klientów tego partnera. Tacy użytkownicy mogą uzyskiwać dostęp do danych innych użytkowników z organizacji w trybie tylko do odczytu. Mogą edytować plany ochrony, ale nie mogą zapisywać żadnych zmian w planach skryptów, planach monitorowania ani planach agentów.
	Administrator w trybie tylko do odczytu Poziom klienta	Ta rola zapewnia dostęp tylko do odczytu do wszystkich obiektów w portalu zarządzania całej firmy. Użytkownicy z tą rolą mają dostęp do danych innych użytkowników z organizacji w trybie tylko do odczytu.

	Administrator w trybie tylko do odczytu Poziom jednostki	Ta rola zapewnia dostęp tylko do odczytu do wszystkich obiektów w portalu zarządzania jednostki i podjednostek firmy. Użytkownicy z tą rolą mają dostęp do danych innych użytkowników z organizacji w trybie tylko do odczytu.
Ochrona	Administrator środowiska cybernetycznego	Oprócz praw roli Administrator rola ta daje możliwość konfigurowania usługi Cyber Protection i zarządzania nią oraz zatwierdzania czynności w ramach funkcji Skrypty cybernetyczne. Rola Administrator środowiska cybernetycznego jest dostępna tylko w przypadku dzierżawców, którzy mają włączony pakiet Advanced Management.
	Administrator	Ta rola umożliwia konfigurowanie usługi Ochrona dla klientów i zarządzanie nią. Na przykład ta rola jest wymagana do konfigurowania funkcji pakietu Disaster Recovery, funkcji pakietu Endpoint Detection and Response i firmowej listy dozwolonych, a także zarządzania nimi.
	Administrator w trybie tylko do odczytu	Ta rola zapewnia dostęp tylko do odczytu do wszystkich obiektów usługi Ochrona. Użytkownicy z tą rolą mają dostęp do danych innych użytkowników z organizacji w trybie tylko do odczytu. Administrator w trybie tylko do odczytu nie może konfigurować funkcji pakietu Disaster Recovery, funkcji pakietu Endpoint Detection and Response i firmowej listy dozwolonych ani nimi zarządzać.
	Operator przywracania	Ta rola umożliwia uzyskiwanie dostępu do kopii zapasowych organizacji Microsoft 365 i Google Workspace oraz ich odzyskiwanie przy jednoczesnym ograniczeniu dostępu do wrażliwej zawartości.
	Użytkownik	Ta rola umożliwia korzystanie z usługi Ochrona, jednak bez uprawnień administracyjnych. Zapewniony jest dostęp m.in. do funkcji pakietu Endpoint Detection and Response, ale użytkownicy przypisani do tej roli nie mają dostępu do danych innych użytkowników z organizacji.
File Sync & Share	Administrator	Ta rola umożliwia konfigurowanie usługi File Sync & Share dla swoich użytkowników i zarządzanie nią. Konto z tą rolą nie jest wliczane do limitu **Użytkownicy**, ponieważ nie zapewnia dostępu do funkcji usługi File Sync & Share.
	Użytkownik	Ta rola umożliwia korzystanie z usługi File Sync & Share. Użytkownicy mają dostęp wyłącznie do własnych oraz

		udostępnionych im danych.
	Gość	Konto z tą rolą jest tworzone, gdy użytkownik usługi File Sync & Share udostępni jakąś zawartość użytkownikowi platformy Cyber Protect Cloud, który nie ma dostępu do usługi File Sync & Share, albo osobie niebędącej użytkownikiem platformy Cyber Protect Cloud. Rola Gość nie obejmuje folderu synchronizacji, nie pozwala na korzystanie z miejsca w chmurze i nie jest wliczana do limitu **Użytkownicy**, ponieważ nie zapewnia dostępu do funkcji usługi File Sync & Share. Uprawnienia konta z rolą Gość można rozszerzyć przez przypisanie mu roli Użytkownik lub Administrator.
Notary	Administrator	Ta rola umożliwia konfigurowanie usługi Notary dla użytkowników i zarządzanie nią.
	Użytkownik	Ta rola umożliwia korzystanie z usługi Notary, jednak bez uprawnień administracyjnych. Użytkownicy z tą rolą nie mają dostępu do danych innych użytkowników z organizacji.

Rola Administrator w trybie tylko do odczytu

Konto z tą rolą ma dostęp tylko do odczytu do konsoli Cyber Protect i umożliwia wykonywanie następujących operacji:

- Zbieranie danych diagnostycznych, na przykład raportów systemowych.
- Przeglądanie punktów odzyskiwania kopii zapasowej, ale bez możliwości przejścia do zawartości kopii zapasowej i przeglądania plików, folderów oraz wiadomości e-mail.

Administrator w trybie tylko do odczytu nie może:

- Uruchamiać ani zatrzymywać żadnych zadań.
  Na przykład administrator w trybie tylko do odczytu nie może rozpocząć odzyskiwania ani zatrzymać rozpoczętej operacji tworzenia kopii zapasowej.
- Uzyskiwać dostępu do systemu plików na komputerze źródłowym lub docelowym.
  Na przykład administrator w trybie tylko do odczytu nie może przeglądać plików, folderów ani wiadomości e-mail na komputerze uwzględnionym w kopii zapasowej.
- Zmieniać jakichkolwiek ustawień.
  Na przykład administrator w trybie tylko do odczytu nie może utworzyć planu ochrony ani zmienić jego ustawień.
- Tworzyć, aktualizować ani usuwać jakichkolwiek danych.
  Na przykład administrator w trybie tylko do odczytu nie może usunąć kopii zapasowych.

Wszelkie obiekty interfejsy użytkownika niedostępne dla administratora w trybie tylko do odczytu są ukryte, z wyjątkiem domyślnych ustawień planu ochrony. Te ustawienia są widoczne, ale przycisk **Zapisz** jest nieaktywny.

Wszelkie zmiany dotyczące kont i ról są wyświetlane na karcie **Działania** wraz z następującymi informacjami:

- Co zostało zmienione
- Autorzy zmian
- Daty i godziny zmian

Rola Operator przywracania

Ta rola jest dostępna tylko w usłudze Cyber Protection i jest ograniczona do kopii zapasowych danych Microsoft 365 i Google Workspace.

Operator przywracania może wykonywać następujące czynności:

- Wyświetlanie alertów i działań.
- Przeglądanie i odświeżanie listy kopii zapasowych.
- Przeglądanie kopii zapasowych bez uzyskiwania dostępu do ich zawartości. Operator przywracania może zobaczyć nazwy plików oraz tematy i nadawców wiadomości e-mail uwzględnionych w kopii zapasowej.
- Przeszukiwanie kopii zapasowych (wyszukiwanie pełnotekstowe nie jest obsługiwane).
- Odzyskiwanie kopii zapasowych utworzonych z chmury do chmury do ich pierwotnej lokalizacji w ramach pierwotnej organizacji Microsoft 365 lub Google Workspace.

Operator przywracania nie może wykonywać następujących czynności:

- Usuwanie alertów.
- Dodawanie lub usuwanie organizacji Microsoft 365 lub Google Workspace.
- Dodawanie, usuwanie lub zmienianie nazw lokalizacji kopii zapasowych.
- Usuwanie lub zmienianie nazw kopii zapasowych.
- Tworzenie, usuwanie lub zmienianie nazw folderów podczas odzyskiwania kopii zapasowej do niestandardowej lokalizacji.
- Stosowanie planu tworzenia kopii zapasowych lub uruchamianie operacji tworzenia kopii zapasowej.
- Uzyskiwanie dostępu do plików lub zawartości wiadomości e-mail uwzględnionych w kopii zapasowej.
- Pobieranie plików lub załączników wiadomości e-mail z kopii zapasowej.
- Wysyłanie uwzględnionych w kopii zapasowej zasobów chmury, takich jak wiadomości e-mail lub elementy kalendarza, jako wiadomości e-mail.
- Wyświetlanie lub odzyskiwanie konwersacji z usługi Microsoft 365 Teams.

- Odzyskiwanie kopii zapasowych utworzonych z chmury do chmury do innych lokalizacji niż pierwotne, na przykład do innej skrzynki pocztowej, usługi OneDrive, Dysku Google lub usługi Microsoft 365 Teams.

Zmienianie ustawień powiadomień dla użytkownika

Aby zmienić ustawienia powiadomień dla użytkownika, przejdź do karty **Zarządzanie firmą** > **Użytkownicy**. Wybierz użytkownika, dla którego chcesz skonfigurować powiadomienia, a następnie kliknij ikonę ołówka w sekcji **Ustawienia**. Jeśli usługa Cyber Protection jest włączona dla dzierżawcy, w ramach którego jest tworzony użytkownik, dostępne są następujące ustawienia powiadomień:

- **Powiadomienia o nadużyciu limitów** (domyślnie włączone)
  Powiadomienia o przekroczeniu limitów.
- **Zaplanowane raporty z wykorzystania** (domyślnie włączone)
  Raporty z wykorzystania, które są wysyłane pierwszego dnia każdego miesiąca.
- **Powiadomienia o oznaczeniu marką adresu URL** (domyślnie wyłączone)
  Powiadomienia o zbliżającym się wygaśnięciu certyfikatu używanego na potrzeby niestandardowego adresu URL dla usług Cyber Protect Cloud. Powiadomienia są wysyłane do wszystkich administratorów wybranego dzierżawcy — na 30 dni, 15 dni, 7 dni, 3 dni i 1 dzień przed wygaśnięciem certyfikatu.
- **Powiadomienia o błędach**, **Powiadomienia o ostrzeżeniach** oraz **Powiadomienia o udanych operacjach** (domyślnie wyłączone)
  Powiadomienia o wynikach wykonywania planów ochrony oraz operacji odzyskiwania po awarii w przypadku każdego urządzenia.
- **Codziennie zestawienie aktywnych alertów** (domyślnie włączone)
  Codzienne zestawienie jest generowane na podstawie listy alertów aktywnych w konsoli Cyber Protect w chwili generowania zestawienia. Takie zestawienie jest generowane i wysyłane raz dziennie między 10:00 a 23:59 czasu UTC. Godzina wygenerowania i wysłania raportu zależy od obciążenia centrum danych. Jeśli w danym czasie nie ma żadnych aktywnych alertów, zestawienie nie jest wysyłane. Zestawienie nie zawiera informacji dotyczących wcześniejszych alertów, które nie są już aktywne. Na przykład w sytuacji, gdy użytkownik wykryje nieudaną operację tworzenia kopii zapasowej i wyczyści alert lub taka operacja zostanie ponowiona i zakończy się pomyślnie, zanim zostanie wygenerowane zestawienie, dotyczący jej alert nie będzie już aktywny i nie zostanie uwzględniony w zestawieniu.
- **Powiadomienia funkcji Kontrola urządzeń** (domyślnie wyłączone)
  Powiadomienia o próbach użycia urządzeń peryferyjnych i portów, do których dostęp jest ograniczony przez plany ochrony z włączonym modułem kontroli urządzeń.
- **Powiadomienia dotyczące odzyskiwania** (domyślnie wyłączone)
  Powiadomienia o czynnościach związanych z odzyskiwaniem w odniesieniu do następujących zasobów: wiadomości e-mail i cała skrzynka pocztowa użytkownika, foldery publiczne, OneDrive / Dysk Google: cały OneDrive oraz pliki lub foldery, pliki programu SharePoint, Teams: kanały, cały zespół, wiadomości e-mail i witryna zespołu.

W kontekście tych powiadomień następujące czynności są uznawane za związane z odzyskiwaniem: wysłanie jako wiadomość e-mail, pobranie lub rozpoczęcie operacji odzyskiwania.

- **Powiadomienia funkcji Zapobieganie utracie danych** (domyślnie wyłączone)
  Powiadomienia o alertach dotyczących zapobiegania utracie danych związanych z działaniami danego użytkownika w sieci.
- **Powiadomienia dotyczące incydentów bezpieczeństwa** (domyślnie wyłączone)
  Powiadomienia o złośliwym oprogramowaniu wykrytym w ramach skanowania podczas uzyskiwania dostępu, podczas wykonywania i na żądanie, a także o zdarzeniach wykrytych przez mechanizm zachowań i mechanizm filtrowania adresów URL.
  Dostępne są dwie opcje: **Zniwelowano** i **Nie zniwelowano**. Opcje te dotyczą alertów o incydentach zgłaszanych przez pakiet Endpoint Detection and Response (EDR), alertów EDR z kanałów dotyczących zagrożeń oraz alertów indywidualnych (w przypadku obciążeń, na których nie włączono EDR).
  Po utworzeniu alertu EDR wysyłana jest wiadomość e-mail do odpowiedniego użytkownika. Jeśli status zagrożenia w ramach incydentu ulegnie zmianie, zostanie wysłana nowa wiadomość e-mail. Takie wiadomości zawierają przyciski czynności, które umożliwiają użytkownikowi zapoznanie się ze szczegółami incydentu (jeśli został on zniwelowany) lub poddanie incydentu dochodzeniu i naprawienie jego skutków (jeśli nie został on zniwelowany).
- **Powiadomienia dotyczące infrastruktury** (domyślnie wyłączone)
  Powiadomienia o problemach z infrastrukturą odzyskiwania po awarii: gdy infrastruktura odzyskiwania po awarii jest niedostępna lub tunele VPN są niedostępne.

Wszystkie powiadomienia są wysyłane na adres e-mail użytkownika.

Powiadomienia odbierane przez użytkownika z daną rolą

Powiadomienia wysyłane przez usługę Cyber Protection zależą od roli użytkownika.

Typ powiadomienia \ Rola użytkownika	Użytkownik	Administrator klienta
Powiadomienia dotyczące własnych urządzeń	Tak	Tak
Powiadomienia dotyczące wszystkich urządzeń w organizacji	n/d	Tak (z wyjątkiem kategorii **Powiadomienia dotyczące incydentów bezpieczeństwa**)
Powiadomienia dotyczące usług Microsoft 365, Google Workspace i innych operacji tworzenia kopii zapasowych w chmurze	n/d	Tak

Wyłączanie i włączanie konta użytkownika

Czasem może być konieczne wyłączenie konta użytkownika w celu tymczasowego ograniczenia jego dostępu do chmury.

Aby wyłączyć konto użytkownika

1. W portalu zarządzania przejdź do sekcji **Użytkownicy**.
2. Zaznacz konto użytkownika, które chcesz wyłączyć, a następnie kliknij ikonę wielokropka > **Wyłącz**.
3. Potwierdź operację, klikając **Wyłącz**.

Od tej pory ten użytkownik nie będzie mógł korzystać z chmury ani otrzymywać żadnych powiadomień.

Aby włączyć wyłączone konto użytkownika, zaznacz je na liście użytkowników, a następnie kliknij ikonę wielokropka > **Włącz**.

Usuwanie konta użytkownika

Czasem może być konieczne nieodwracalne usunięcie konta użytkownika w celu zwolnienia wykorzystywanych przez nie zasobów, na przykład miejsca na dysku lub licencji. Statystyki wykorzystania zostaną zaktualizowane w ciągu jednego dnia od usunięcia. W przypadku kont z dużą ilością danych może to potrwać dłużej.

Przed usunięciem konta użytkownika trzeba je wyłączyć. Więcej informacji o tym, jak to zrobić, można znaleźć w sekcji „Wyłączanie i włączanie konta użytkownika”.

Aby usunąć konto użytkownika

1. W portalu zarządzania przejdź do sekcji **Użytkownicy**.
2. Zaznacz wyłączone konto użytkownika, a następnie kliknij ikonę wielokropka > **Usuń**.
3. Aby potwierdzić operację, wprowadź swoją nazwę logowania i kliknij **Usuń**.

Wskutek tego:

- Wszystkie powiadomienia dla tego konta zostaną wyłączone.
- Wszystkie dane z tego konta użytkownika zostaną usunięte.
- Administrator nie będzie mieć dostępu do portalu zarządzania.
- Wszystkie kopie zapasowe obciążeń powiązanych z tym użytkownikiem zostaną usunięte.
- Wszystkie komputery powiązane z tym kontem użytkownika zostaną wyrejestrowane.
- Wszystkie plany ochrony zostaną odwołane ze wszystkich obciążeń powiązanych z tym użytkownikiem.
- Wszystkie dane usługi File Sync & Share należące do tego użytkownika (na przykład pliki i foldery) zostaną usunięte.
- Wszystkie dane usługi Notary należące do tego użytkownika (na przykład notaryzowane lub podpisane elektronicznie pliki) zostaną usunięte.

- W obszarze **Status** użytkownika będzie wyświetlana wartość **Usunięto**. Po wskazaniu myszą statusu **Usunięto** zostanie wyświetlona data usunięcia użytkownika i należy pamiętać, że wszystkie powiązane z nim dane oraz ustawienia można odzyskać w ciągu 30 dni od usunięcia.

Przenoszenie własności konta użytkownika

Czasem może być konieczne przeniesienie własności konta użytkownika, aby zachować dostęp do zastrzeżonych danych użytkownika.

Ważne
Zawartości usuniętego konta nie można ponownie przypisać.

Aby przenieść własność konta użytkownika

1. W portalu zarządzania przejdź do sekcji **Użytkownicy**.
2. Zaznacz konto użytkownika, którego własność chcesz przenieść, a następnie kliknij ikonę ołówka w sekcji **Informacje ogólne**.
3. Zastąp dotychczasowy adres e-mail adresem e-mail przyszłego właściciela konta, a następnie kliknij **Gotowe**.
4. Potwierdź operację, klikając **Tak**.
5. Poczekaj, aż przyszły właściciel konta zweryfikuje adres e-mail, postępując zgodnie z wysłanymi na ten adres instrukcjami.
6. Zaznacz konto użytkownika, którego własność przenosisz, a następnie kliknij ikonę wielokropka > **Resetuj hasło**.
7. Potwierdź czynność, klikając **Resetuj**.
8. Poczekaj, aż przyszły właściciel konta zresetuje hasło, postępując zgodnie z instrukcjami wysłanymi na jego adres e-mail.

Od tej pory nowy właściciel będzie mieć dostęp do konta.

Konfigurowanie uwierzytelniania dwuskładnikowego

Uwierzytelnianie dwuskładnikowe (2FA) jest typem uwierzytelniania wieloskładnikowego, w którego ramach tożsamość użytkownika jest sprawdzana na podstawie dwóch elementów:

- Czegoś, co użytkownik zna (numer PIN lub hasło)
- Czegoś, co użytkownik ma (token)
- Czegoś, co jest nieodłączną cechą użytkownika (dane biometryczne)

Uwierzytelnianie dwuskładnikowe zapewnia dodatkową ochronę przed nieuprawnionym dostępem do konta.

Ta platforma obsługuje uwierzytelnianie przy użyciu **Czasowych haseł jednorazowych (Time-based One-Time Password, TOTP)**. Jeśli w systemie jest włączone uwierzytelnianie TOTP, w celu

uzyskania dostępu do systemu użytkownicy muszą podać swoje tradycyjne hasło oraz jednorazowy kod TOTP. Innymi słowy, użytkownik podaje hasło (pierwszy składnik) i kod TOTP (drugi składnik). Kod TOTP jest generowany w aplikacji uwierzytelniającej na urządzeniu używanym do obsługi drugiego składnika uwierzytelniania na podstawie bieżącego czasu i klucza tajnego (kodu QR lub alfanumerycznego) udostępnianego przez platformę.

Sposób działania

1. Uwierzytelnianie dwuskładnikowe włącza się na poziomie organizacji.
2. W takiej sytuacji każdy użytkownik z organizacji musi zainstalować aplikację uwierzytelniającą na urządzeniu używanym do obsługi drugiego składnika uwierzytelniania (telefonie komórkowym, laptopie, komputerze stacjonarnym lub tablecie). Aplikacja ta będzie służyć do generowania jednorazowych kodów TOTP. Zalecane aplikacje uwierzytelniające:
   - Google Authenticator

     Aplikacja w wersji dla systemu iOS (https://apps.apple.com/app/google-authenticator/id388497605)

     Aplikacja w wersji dla systemu Android (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2)
   - Microsoft Authenticator

     Aplikacja w wersji dla systemu iOS (https://apps.apple.com/app/microsoft-authenticator/id983156458)

     Aplikacja w wersji dla systemu Android (https://play.google.com/store/apps/details?id=com.azure.authenticator)

   Ważne
   Użytkownik musi zadbać, aby czas na urządzeniu z zainstalowaną aplikacją uwierzytelniającą był prawidłowo ustawiony i odzwierciedlał czas bieżący.
3. Użytkownik z organizacji musi ponownie się zalogować do systemu.
4. Po wprowadzeniu nazwy logowania i hasła zostanie poproszony o skonfigurowanie uwierzytelniania dwuskładnikowego na swoim koncie.
5. Musi zeskanować kod QR przy użyciu aplikacji uwierzytelniającej. Jeśli nie można zeskanować kodu QR, można użyć 32-cyfrowego kodu widocznego pod kodem QR i podać go ręcznie w aplikacji uwierzytelniającej.

   Ważne
   Zdecydowanie warto go zachować (wydrukować kod QR, zanotować klucz tajny stanowiący tymczasowe jednorazowe hasło [TOTP], skorzystać z aplikacji do tworzenia kopii zapasowych kodów w chmurze). Tymczasowe jednorazowe hasło (TOTP) będzie potrzebne do zresetowania uwierzytelniania dwuskładnikowego w razie utraty urządzenia używanego do obsługi drugiego składnika uwierzytelniania.

6. W aplikacji uwierzytelniającej zostanie wygenerowany kod stanowiący tymczasowe jednorazowe hasło (TOTP). Jest on automatycznie generowany ponownie co 30 sekund.
7. Po wprowadzeniu hasła użytkownik musi wprowadzić kod TOTP na ekranie **Skonfiguruj uwierzytelnianie dwuskładnikowe**.
8. W ten sposób zostanie skonfigurowane uwierzytelnianie dwuskładnikowe na koncie użytkownika.

Teraz podczas logowania się do systemu użytkownik będzie monitowany o podanie nazwy logowania i hasła oraz jednorazowego kodu TOTP wygenerowanego w aplikacji uwierzytelniającej. Logując się do systemu, użytkownik może oznaczyć przeglądarkę jako zaufaną, dzięki czemu przy kolejnych operacjach logowania się przy użyciu tej przeglądarki kod TOTP nie będzie wymagany.

Aby przywrócić uwierzytelnianie dwuskładnikowe na nowym urządzeniu

Jeśli masz dostęp do wcześniej skonfigurowanej mobilnej aplikacji uwierzytelniającej:

1. Zainstaluj aplikację uwierzytelniającą na nowym urządzeniu.
2. Skorzystaj z pliku PDF zapisanego podczas konfigurowania uwierzytelniania dwuskładnikowego na urządzeniu. Plik ten zawiera 32-cyfrowy kod, który należy podać w aplikacji uwierzytelniającej, aby ponownie nawiązać połączenie między aplikacją uwierzytelniającą i kontem Acronis.

   Ważne
   Jeśli kod jest poprawny, ale nie działa, należy zsynchronizować czas w uwierzytelniającej aplikacji mobilnej.

3. Jeśli podczas konfiguracji nie zapisano pliku PDF:

a. *Kliknij **Zresetuj uwierzytelnianie dwuskładnikowe** i wprowadź jednorazowe hasło wyświetlane w uprzednio skonfigurowanej mobilnej aplikacji uwierzytelniającej.*
b. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Jeśli nie masz dostępu do wcześniej skonfigurowanej mobilnej aplikacji uwierzytelniającej:

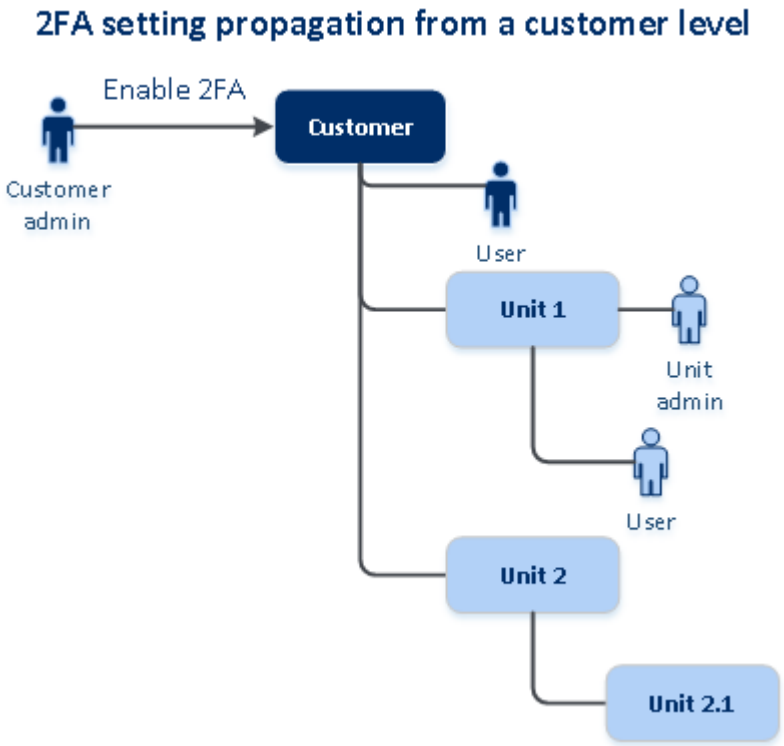
1. Skorzystaj z nowego urządzenia mobilnego.
2. Użyj zapisanego pliku PDF (domyślna nazwa pliku to `cyberprotect-2fa-backupcode.pdf`), aby powiązać nowe urządzenie.
3. Przywróć dostęp do konta z poziomu kopii zapasowej. Upewnij się, że kopie zapasowe są obsługiwane przez używaną aplikację mobilną.
4. Otwórz aplikację na tym samym koncie z innego urządzenia mobilnego, jeśli jest ono obsługiwane przez aplikację.

Propagacja konfiguracji uwierzytelniania dwuskładnikowego na wszystkich poziomach dzierżawców

Uwierzytelnianie dwuskładnikowe konfiguruje się na poziomie **organizacji**. Można skonfigurować uwierzytelnianie dwuskładnikowe tylko dla swojej organizacji.

Ustawienia uwierzytelniania dwuskładnikowego są propagowane na wszystkich poziomach dzierżawców w następujący sposób:

- Jednostki automatycznie dziedziczą ustawienia uwierzytelniania dwuskładnikowego z organizacji klienta.



Uwaga

1. Nie można skonfigurować uwierzytelniania dwuskładnikowego na poziomie jednostki.
2. Istnieje możliwość zarządzania ustawieniami uwierzytelniania dwuskładnikowego w przypadku użytkowników z organizacji podrzędnych (jednostek).

Konfigurowanie uwierzytelniania dwuskładnikowego dla dzierżawcy

Jako administrator możesz włączyć uwierzytelnianie dwuskładnikowe dla organizacji.

Aby skonfigurować uwierzytelnianie dwuskładnikowe dla dzierżawcy

1. W portalu zarządzania wybierz **Ustawienia** > **Zabezpieczenia**.
2. Przesuń przełącznik **Uwierzytelnianie dwuskładnikowe** i kliknij **Włącz**.

Teraz każdy użytkownik z organizacji musi skonfigurować uwierzytelnianie dwuskładnikowe na swoim koncie. Zostanie o to poproszony przy następnej próbie zalogowania się lub po wygaśnięciu jego bieżącej sesji.

Pasek postępu wskazuje, ilu użytkowników skonfigurowało uwierzytelnianie dwuskładnikowe na swoich kontach. Aby sprawdzić, którzy użytkownicy skonfigurowali swoje konta, przejdź do karty

Zarządzanie firmą > **Użytkownicy** i przyjrzyj się kolumnie **Status 2FA**. W przypadku użytkowników, którzy jeszcze nie skonfigurowali uwierzytelniania dwuskładnikowego na swoich kontach, w kolumnie Status 2FA jest wyświetlana wartość **Wymagana konfiguracja**.

Po pomyślnym skonfigurowaniu uwierzytelniania dwuskładnikowego użytkownicy będą musieli podawać nazwę logowania, hasło oraz kod TOTP przy każdym logowaniu się do konsoli usługi.

Aby wyłączyć uwierzytelnianie dwuskładnikowe dla dzierżawcy

1. W portalu zarządzania wybierz **Ustawienia** > **Zabezpieczenia**.
2. Aby wyłączyć uwierzytelnianie dwuskładnikowe, wyłącz przełącznik i kliknij **Wyłącz**.
3. [Jeśli co najmniej jeden użytkownik skonfigurował uwierzytelnianie dwuskładnikowe w ramach organizacji] Wprowadź kod TOTP wygenerowany w aplikacji uwierzytelniającej na urządzeniu mobilnym.

W wyniku tych działań zostanie wyłączone uwierzytelnianie dwuskładnikowe dla organizacji, zostaną usunięte wszystkie klucze tajne i zostaną zapomniane wszystkie zaufane przeglądarki. Każdy użytkownik będzie mógł się zalogować do systemu przy użyciu tylko nazwy logowania i hasła. Kolumna Status 2FA na karcie **Zarządzanie firmą** > **Użytkownicy** zostanie ukryta.

Zarządzanie uwierzytelnianiem dwuskładnikowym dla użytkowników

Na karcie **Zarządzanie firmą** > **Użytkownicy** w portalu zarządzania można monitorować i resetować ustawienia uwierzytelniania dwuskładnikowego wszystkich swoich użytkowników.

Monitorowanie

Na karcie **Zarządzanie firmą** > **Użytkownicy** w portalu zarządzania jest wyświetlana lista wszystkich użytkowników z danej organizacji. Wartość **Status 2FA** wskazuje, czy dany użytkownik ma skonfigurowane uwierzytelnianie dwuskładnikowe.

Aby zresetować uwierzytelnianie dwuskładnikowe dla użytkownika

1. W portalu zarządzania przejdź do karty **Zarządzanie firmą** > **Użytkownicy**.
2. Na karcie **Użytkownicy** znajdź użytkownika, którego ustawienia chcesz zmienić, a następnie kliknij ikonę wielokropka.
3. Kliknij **Resetuj uwierzytelnianie dwuskładnikowe**.
4. Wprowadź kod TOTP wygenerowany w aplikacji uwierzytelniającej na urządzeniu używanym do obsługi drugiego składnika uwierzytelniania i kliknij **Resetuj**.

W rezultacie użytkownik znów będzie mógł skonfigurować uwierzytelnianie dwuskładnikowe.

Aby zresetować zaufane przeglądarki użytkownika

1. W portalu zarządzania przejdź do karty **Zarządzanie firmą** > **Użytkownicy**.
2. Na karcie **Użytkownicy** znajdź użytkownika, którego ustawienia chcesz zmienić, a następnie kliknij ikonę wielokropka.
3. Kliknij **Resetuj wszystkie zaufane przeglądarki**.
4. Wprowadź kod TOTP wygenerowany w aplikacji uwierzytelniającej na urządzeniu używanym do obsługi drugiego składnika uwierzytelniania i kliknij **Resetuj**.

Użytkownik, którego wszystkie zaufane przeglądarki zostały zresetowane, przy następnym logowaniu się będzie musiał podać kod TOTP.

Użytkownicy mogą sami resetować wszystkie zaufane przeglądarki i ustawienia uwierzytelniania dwuskładnikowego. Jest to możliwe po zalogowaniu się do systemu: należy kliknąć odpowiednie łącze i wpisać kod TOTP w celu potwierdzenia operacji.

Aby wyłączyć uwierzytelnianie dwuskładnikowe na koncie użytkownika

Lepiej nie wyłączać uwierzytelniania dwuskładnikowego, ponieważ może to ułatwiać naruszenie zabezpieczeń dzierżawcy.

W drodze wyjątku można wyłączyć uwierzytelnianie dwuskładnikowe w przypadku jakiegoś użytkownika, a zachować je w kontekście pozostałych użytkowników w ramach dzierżawcy. Jest to obejście przydatne w sytuacjach, gdy uwierzytelnianie dwuskładnikowe jest włączone w ramach dzierżawcy, dla którego skonfigurowano integrację z chmurą, przy czym integracja ta autoryzuje swój dostęp do platformy przy użyciu danego konta użytkownika (hasła logowania). Aby dalej korzystać z integracji, można tymczasowo przekształcić konto użytkownika w konto usługi, w którego przypadku nie jest stosowane uwierzytelnianie dwuskładnikowe.

Ważne
Zmiana zwykłych użytkowników w użytkowników usługi w celu wyłączenia uwierzytelniania dwuskładnikowego nie jest zalecana, ponieważ zwiększa zagrożenie dla bezpieczeństwa dzierżawcy.

Zalecanym bezpiecznym rozwiązaniem umożliwiającym korzystanie z integracji z chmurą bez wyłączania uwierzytelniania dwuskładnikowego dla dzierżawców jest utworzenie klientów API i skonfigurowanie integracji z chmurą tak, aby z nimi współpracowały.

1. W portalu zarządzania przejdź do karty **Zarządzanie firmą** > **Użytkownicy**.
2. Na karcie **Użytkownicy** znajdź użytkownika, którego ustawienia chcesz zmienić, a następnie kliknij ikonę wielokropka.
3. Kliknij **Oznacz jako konto usługi**. W wyniku tego użytkownik otrzyma specjalny status uwierzytelniania dwuskładnikowego o nazwie **Konto usługi**.
4. [Jeśli co najmniej jeden użytkownik w obszarze dzierżawcy skonfigurował uwierzytelnianie dwuskładnikowe] Aby potwierdzić wyłączenie, wprowadź kod TOTP wygenerowany w aplikacji uwierzytelniającej na urządzeniu używanym do obsługi drugiego składnika uwierzytelniania.

Aby włączyć uwierzytelnianie dwuskładnikowe na koncie użytkownika

Czasem może wystąpić potrzeba włączenia uwierzytelniania dwuskładnikowego na koncie użytkownika, na którym zostało ono wcześniej wyłączone.

1. W portalu zarządzania przejdź do karty **Zarządzanie firmą** > **Użytkownicy**.
2. Na karcie **Użytkownicy** znajdź użytkownika, którego ustawienia chcesz zmienić, a następnie kliknij ikonę wielokropka.
3. Kliknij **Oznacz jako zwykłe konto**. W rezultacie użytkownik będzie musiał skonfigurować uwierzytelnianie dwuskładnikowe lub podać kod TOTP podczas logowania się do systemu.

Resetowanie uwierzytelniania dwuskładnikowego w razie utraty urządzenia używanego do obsługi drugiego składnika

Aby zresetować dostęp do konta w przypadku utraty urządzenia używanego do obsługi drugiego składnika uwierzytelniania, skorzystaj z jednej z sugerowanych metod:

- Przywróć klucz tajny TOTP (kod QR lub alfanumeryczny) z kopii zapasowej.

  Skorzystaj z innego urządzenia do obsługi drugiego składnika uwierzytelniania i wprowadź zachowany klucz tajny TOTP w aplikacji uwierzytelniającej zainstalowanej na tym urządzeniu.
- Poproś administratora o zresetowanie ustawień uwierzytelniania dwuskładnikowego na Twoim koncie.

Ochrona przed atakami brute force

Brute force to atak, podczas którego haker próbuje uzyskać dostęp do systemu, przesyłając wiele haseł z nadzieją, że jedno z nich okaże się poprawne.

Mechanizm ochrony przed atakami brute force dostępny na tej platformie jest oparty na plikach cookie urządzenia.

Stosowane są predefiniowane ustawienia ochrony przed atakami brute force:

Parametr	Wprowadzenie hasła	Wprowadzenie kodu TOTP
Limit prób	10	5
Odstęp między limitami prób (limit jest resetowany po upływie określonego czasu)	15 min (900 s)	15 min (900 s)
Aktywacja blokady	Limit prób + 1 (11. próba)	Limit prób
Okres blokady	5 min (300 s)	5 min (300 s)

W przypadku włączonego uwierzytelniania dwuskładnikowego plik cookie jest wysyłany do klienta (przeglądarki) wyłącznie po pomyślnym uwierzytelnieniu przy użyciu obu składników (hasła i kodu TOTP).

W przypadku zaufanych przeglądarek plik cookie urządzenia jest wysyłany po pomyślnym uwierzytelnieniu przy użyciu tylko jednego składnika (hasła).

Próby wprowadzenia kodu TOTP są rejestrowane w kontekście użytkownika, a nie urządzenia. Oznacza to, że blokada zostanie aktywowana nawet wtedy, gdy użytkownik będzie próbował wprowadzić kod TOTP z różnych urządzeń.

Automatyczne aktualizowanie agentów

Ważne
Obecnie dostęp do funkcji zarządzania aktualizacjami agentów jest aktywny tylko po włączeniu składnika Ochrona.

Usługa Cyber Protect udostępnia trzy typy agentów do instalowania na chronionych komputerach: agent dla systemu Windows, agent dla systemu Linux i agent dla system Mac.

Program Cyber Files Cloud udostępnia agenta komputerowego dla File Sync & Share w wersji dla systemu Windows i w wersji dla systemu MacOS. Umożliwia on synchronizację plików i folderów między komputerem a magazynem w chmurze File Sync & Share użytkownika na potrzeby promowania pracy offline, a także pracy z domu i używania do pracy własnych urządzeń (BYOD, Bring Your Own Device).

Aby ułatwić zarządzanie wieloma obciążeniami, można skonfigurować (i wyłączyć) automatyczne, nienadzorowane aktualizacje dla wszystkich agentów na wszystkich komputerach.

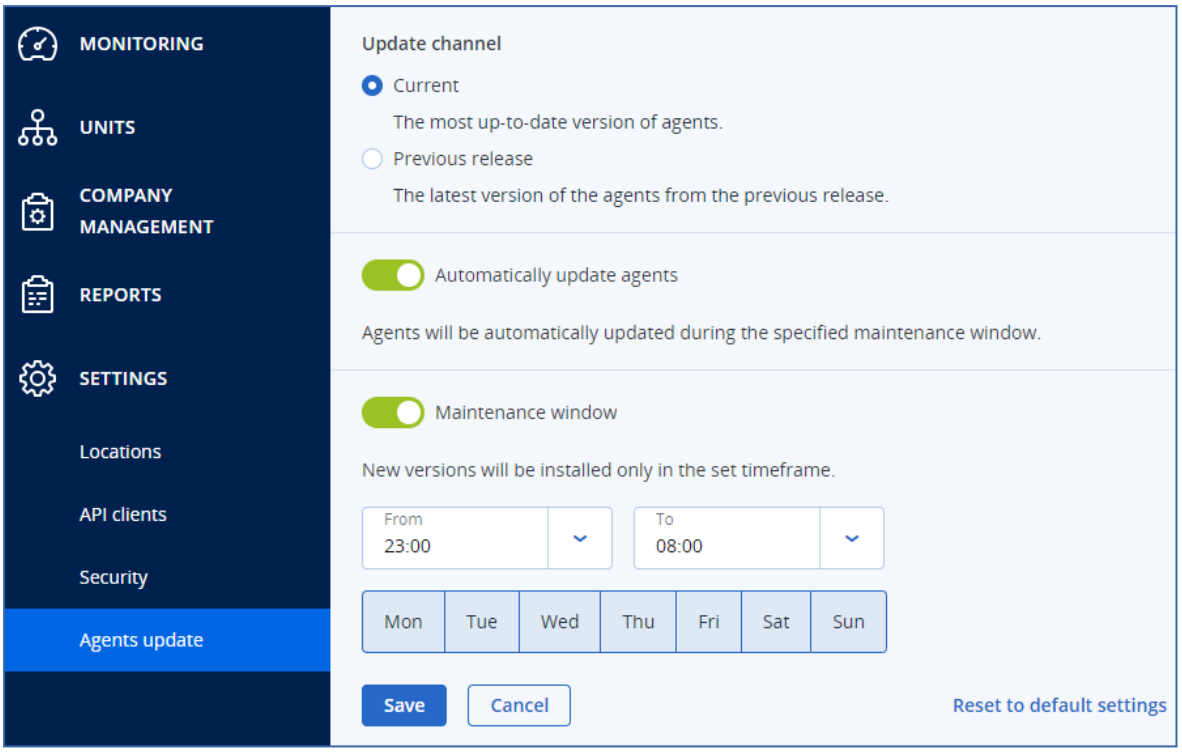
Uwaga
Aby zarządzać agentami na poszczególnych komputerach i dostosować ustawienia automatycznego aktualizowania, zapoznaj się z sekcją Podręcznika użytkownika usługi Cyber Protect dotyczącą aktualizacji agentów.

Aby automatycznie aktualizować agentów

Uwaga
Jeśli nie masz włączonej ochrony, ustawienia automatycznego aktualizowania agenta dla File Sync & Share są dziedziczone od usługodawcy.

Aby skonfigurować automatyczne aktualizowanie agentów na stronie początkowej portalu zarządzania

1. Wybierz **Ustawienia > Aktualizacja agentów**.



2. Wybierz wersję do wykrywania pod kątem aktualizacji automatycznych: **Bieżąca** lub **Poprzednia wersja**.
   (Ustawienie domyślne to **Bieżąca**).
3. Włącz opcję **Automatycznie aktualizuj agenty**.
   (Domyślnie jest ona **włączona**).
4. Ustaw ramy czasowe konserwacji.
   (Ustawienie domyślne to: od 23:00 do 08:00).

Uwaga
Mimo że procesy aktualizacji agentów zaprojektowano tak, aby były one szybkie i bezproblemowe, zalecamy wybranie takiego przedziału czasowego, w którym zakłócenia dla użytkowników będą minimalne, ponieważ użytkownicy nie mogą zapobiegać stosowaniu aktualizacji automatycznych ani ich odkładać.

5. [Opcjonalnie] Wybierz określone dni, w których mają być stosowane aktualizacje automatyczne.
6. Wybierz **Zapisz.**

Uwaga
Aktualizacje automatyczne są dostępne tylko dla:

- Agentów usługi Cyber Protect w wersji 15.0.26986 (wydanej w maju 2021 r.) lub nowszej.
- Agenta komputerowego dla File Sync & Share w wersji 15.0.30370 lub nowszej.

Aby aktualizacje automatyczne zaczęły działać, starsze agenty trzeba najpierw ręcznie zaktualizować do najnowszej wersji.

Aby monitorować aktualizacje agentów

Ważne
Monitorowanie aktualizacji agentów jest możliwe tylko pod warunkiem, że masz włączony moduł Ochrona.

Aby monitorować aktualizacje agentów, zapoznaj się z sekcjami dotyczącymi alertów i działań w Podręczniku użytkownika usługi Cyber Protect.

Konfigurowanie niezmiennego magazynu

Korzystając z niezmiennego magazynu, można uzyskiwać dostęp do usuniętych kopii zapasowych w ustawionym okresie przechowywania. Można odzyskiwać zawartość z tych kopii zapasowych, ale nie można ich zmieniać, przenosić ani usuwać. Po zakończeniu okresu przechowywania usunięte kopie zapasowe zostaną trwale usunięte.

Niezmienny magazyn zawiera następujące kopie zapasowe:

- Kopie zapasowe usunięte ręcznie.
- Kopie zapasowe usunięte automatycznie zgodnie z ustawieniami określonymi w sekcji **Okres przechowywania** w planie ochrony lub w sekcji **Reguły przechowywania** w planie czyszczenia.

Usunięte kopie zapasowe nadal zajmują miejsce w niezmiennym magazynie i są za nie naliczane odpowiednie opłaty.

Usunięci dzierżawcy nie są obciążani żadnymi opłatami za magazyny, w tym za niezmienny magazyn.

W przypadku dzierżawców-klientów niezmienny magazyn jest dostępny w następujących trybach:

- **Tryb nadzoru**
  Możesz wyłączyć i ponownie włączyć niezmienny magazyn. Możesz zmienić okres przechowywania lub przejść do trybu zgodności.
- **Tryb zgodności**

  Ostrzeżenie!
  Wybranie trybu zgodności jest nieodwracalne.

Nie można wyłączyć niezmiennego magazynu. Nie można zmienić okresu przechowywania ani wrócić do trybu nadzoru.

Konfiguracja ustawień niezmiennego magazynu jest możliwa tylko wtedy, gdy w ramach dzierżawcy, do którego należy konto administratora, jest włączone uwierzytelnianie dwuskładnikowe.

Uwaga
Aby można było uzyskiwać dostęp do usuniętych kopii zapasowych, dopilnuj, aby magazyn kopii zapasowych miał włączony port 40440 dla połączeń przychodzących.

Aby włączyć niezmienny magazyn

1. Zaloguj się do portalu zarządzania jako administrator, a następnie wybierz **Ustawienia** > **Bezpieczeństwo**.
2. Włącz przełącznik **Niezmienny magazyn**.
3. Ustaw okres przechowywania wynoszący od 14 do 3650 dni.
   Domyślny okres przechowywania to 14 dni. Dłuższy okres przechowywania danych poskutkuje zajęciem większej ilości miejsca w magazynie.
4. Wybierz tryb niezmiennego magazynu, a następnie potwierdź wybór, jeśli pojawi się wymagający tego monit.
5. Kliknij **Zapisz**.

   Ostrzeżenie!
   Wyboru opcji **Tryb zgodności** nie można cofnąć. Po wybraniu tego trybu nie będzie można wyłączyć niezmiennego magazynu ani zmienić jego trybu bądź okresu przechowywania.

6. Aby istniejące już archiwum obsługiwało niezmienny magazyn, należy utworzyć w nim nową kopię zapasową.
   Aby utworzyć nową kopię zapasową, uruchom plan ochrony ręcznie lub zgodnie z harmonogramem.

   Ostrzeżenie!
   W przypadku usunięcia kopii zapasowej przed utworzeniem archiwum obsługującego niezmienny magazyn kopia zapasowa zostanie trwale usunięta.

Aby wyłączyć niezmienny magazyn

1. Zaloguj się do portalu zarządzania jako administrator, a następnie wybierz **Ustawienia** > **Bezpieczeństwo**.
2. Wyłącz przełącznik **Niezmienny magazyn**.

   Uwaga
   Niezmienny magazyn można wyłączyć tylko w Trybie nadzoru.

Ostrzeżenie!
Wyłączenie niezmiennego magazynu nie działa od razu. W okresie prolongaty wynoszącym 14 dni niezmienny magazyn jest nadal aktywny i można uzyskać dostęp do usuniętych kopii zapasowych zgodnie z ich pierwotnym okresem przechowywania. Po zakończeniu okresu prolongaty wszystkie kopie zapasowe przechowywane w niezmiennym magazynie zostaną nieodwracalnie usunięte.

3. Potwierdź wybór, klikając **Wyłącz**.

Obsługiwane magazyny i agenty

- Niezmienny magazyn jest obsługiwany tylko w chmurze.

  Niezmienny magazyn jest dostępny w przypadku chmur hostowanych przez firmę Acronis oraz partnerów korzystających z rozwiązania Cyber Infrastructure w wersji 4.7.1 lub nowszej.

  Obsługiwane są wszystkie magazyny, których można używać razem z rozwiązaniem Cyber Infrastructure Backup Gateway. Na przykład, magazyny Cyber Infrastructure, Amazon S3 i EC2 oraz Microsoft Azure.

  Niezmienny magazyn wymaga, aby port TCP 40440 był otwarty dla usługi Backup Gateway w infrastrukturze Cyber Infrastructure. W wersji 4.7.1 lub nowszej port TCP 40440 jest automatycznie otwierany w przypadku ruchu **publicznego typu Backup (ABGW)**. Dodatkowe informacje na temat typów ruchu można znaleźć w dokumentacji infrastruktury Acronis Cyber Infrastructure.
- Niezmienny magazyn wymaga agenta ochrony w wersji 21.12 (kompilacja 15.0.28532) lub nowszej.
- Obsługiwane są tylko kopie zapasowe w formacie TIBX (Wersja 12).

Monitorowanie

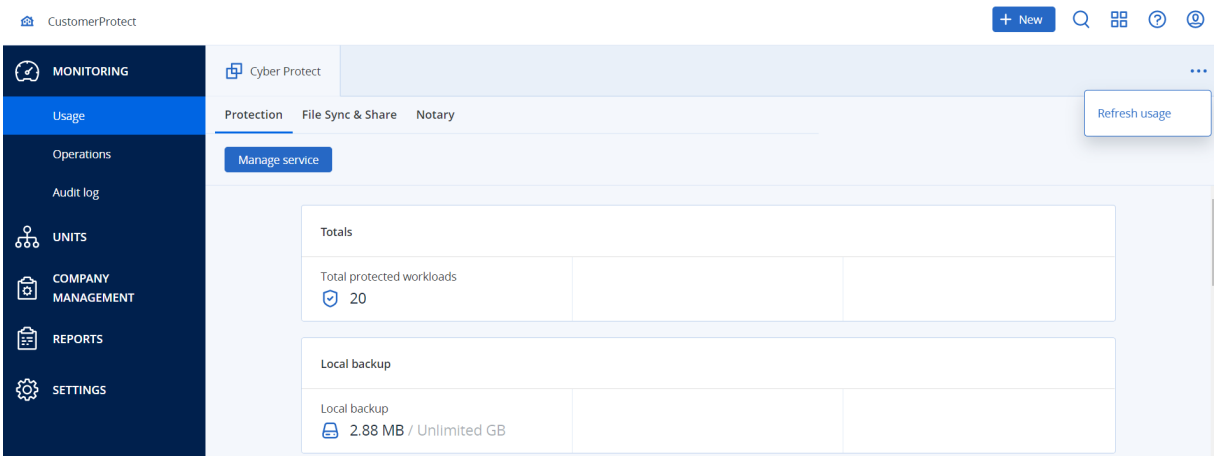
Aby uzyskać dostęp do informacji o wykorzystaniu usług i operacjach, kliknij **Monitorowanie**.

dysku

Karta **Wykorzystanie** udostępnia zestawienie informacji o wykorzystaniu usług (w tym o ewentualnych limitach) oraz umożliwia uzyskanie dostępu do konsol usług.

Aby odświeżyć dane o wykorzystaniu wyświetlane na karcie, kliknij ikonę wielokropka w prawym górnym rogu ekranu i wybierz **Odśwież dane o wykorzystaniu**.

Uwaga
Pobieranie danych może potrwać do 10 minut. Odśwież stronę, aby wyświetlić zaktualizowane dane.



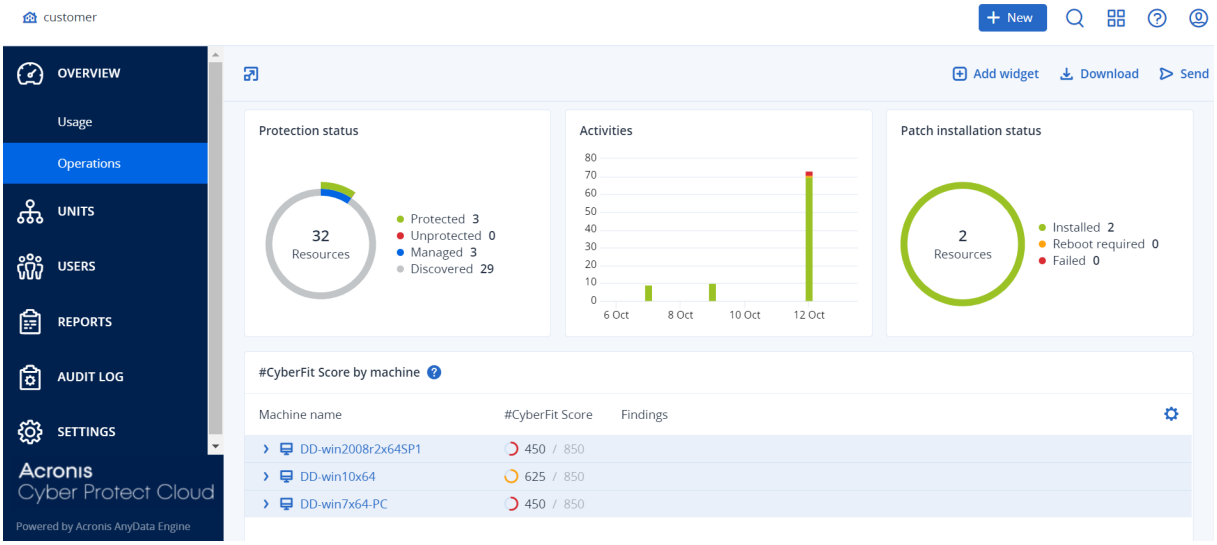
Pulpit nawigacyjny operacji

Pulpit nawigacyjny **Operacje** jest dostępny tylko dla administratorów firm podczas wykonywania operacji na poziomie firmy.

Pulpit nawigacyjny **Operacje** udostępnia szereg dostosowywalnych widżetów zapewniających ogólny obraz operacji związanych z usługą Cyber Protection.

Widżety są aktualizowane co 2 minuty. Widżety mają klikalne elementy, które pozwalają badać i rozwiązywać problemy. Możesz pobrać bieżący stan pulpitu nawigacyjnego lub przesłać go za pomocą poczty e-mail w formacie .pdf oraz/lub .xlsx.

Możesz wybierać spośród różnorodnych widżetów przedstawianych w formie tabel, wykresów kołowych, wykresów słupkowych, list i map drzew. Możesz dodać wiele widżetów tego samego typu, ale z różnymi filtrami.



Aby zmienić ustawienie widżetów na pulpicie nawigacyjnym

Klikaj nazwy widżetów i zmieniaj ich ustawienie metodą „przeciągnij i upuść”.

Aby edytować widżet

Kliknij ikonę ołówka obok nazwy widżetu. Edycja widżetu pozwala zmienić jego nazwę, zmodyfikować zakres czasu i ustawić filtry.

Aby dodać widżet

Kliknij **Dodaj widżet** i wykonaj jedną z następujących czynności:

- Kliknij widżet, który chcesz dodać. Widżet zostanie dodany z domyślnymi ustawieniami.
- Aby edytować widżet przed dodaniem, zaznacz go i kliknij ikonę ołówka. Po skończonej edycji widżetu kliknij **Gotowe**.

Aby usunąć widżet

Kliknij symbol X obok nazwy widżetu.

Status ochrony

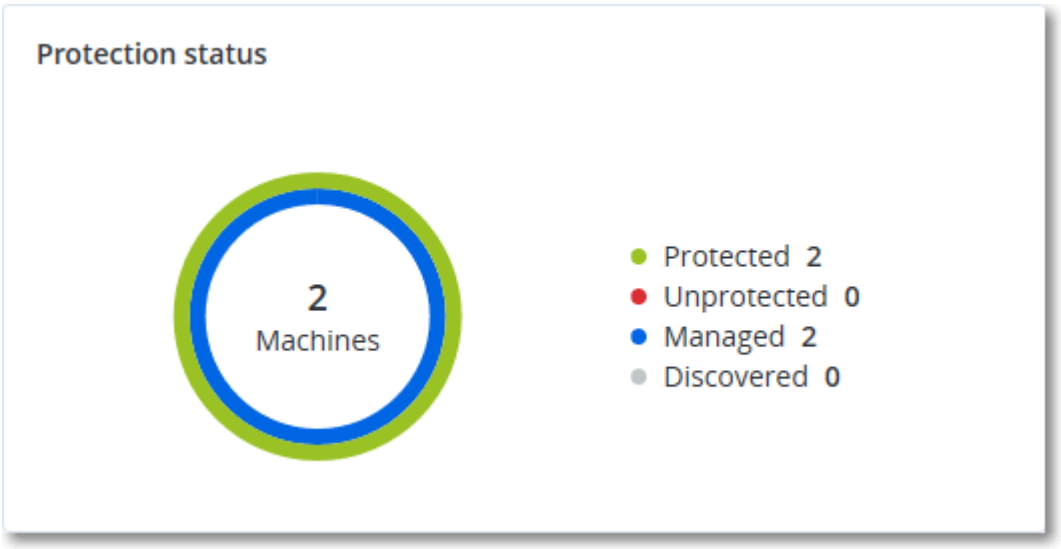
Status ochrony

Ten widżet umożliwia wyświetlenie aktualnego statusu ochrony wszystkich komputerów.

Komputer może mieć jeden z następujących statusów:

- **Chronione** — komputery z zastosowanym planem ochrony.
- **Niechronione** — komputery bez zastosowanego planu ochrony. Są to zarówno wykryte, jak i zarządzane komputery, do których nie zastosowano planu ochrony.
- **Zarządzane** — komputery z zainstalowanym agentem ochrony.
- **Wykryto** — komputery bez zainstalowanego agenta ochrony.

Kliknięcie statusu komputera spowoduje przejście do listy komputerów o danym statusie, gdzie można znaleźć dodatkowe informacje.



Wykryte komputery

Ten widżet przedstawia listę komputerów wykrytych we wskazanym okresie.

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

Wynik #CyberFit według komputerów

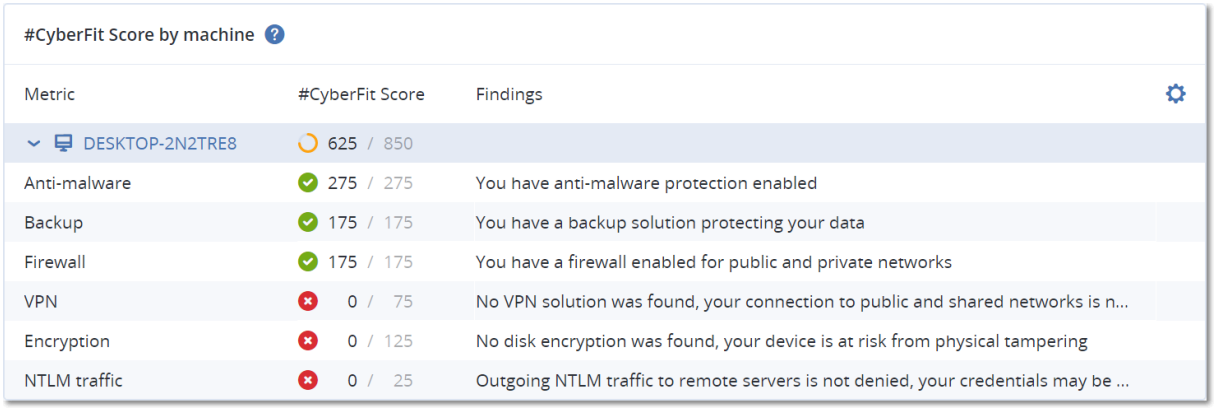
W przypadku tego widżetu jest pokazywany łączny wynik #CyberFit, jego wyniki składowe oraz diagnozy z badań poszczególnych wskaźników:

- Ochrona antywirusowa
- Kopia zapasowa
- Zapora

- VPN
- Szyfrowanie
- Ruch NTLM

Aby poprawić wartości poszczególnych wskaźników, zapoznaj się z zaleceniami przedstawionymi w raporcie.

Więcej informacji na temat wyniku #CyberFit można znaleźć w sekcji „Wyniki #CyberFit komputerów”.



Widżety pakietu Endpoint Detection and Response (EDR)

Ważne
Niniejsza wersja dokumentacji pakietu EDR jest udostępniana w ramach Programu wczesnego dostępu. Niektóre zestawienia funkcji i opisy mogą być niekompletne.

Endpoint Detection and Response (EDR) obejmuje szereg widżetów dostępnych z pulpitu nawigacyjnego **Operacje**.

Dostępne są następujące widżety:

- Podział najliczniejszych incydentów według obciążeń
- Średni czas rozwiązywania problemu incydentu
- Wykres spalania dotyczący incydentów bezpieczeństwa
- Status sieciowy obciążeń

Podział najliczniejszych incydentów według obciążeń

Ten widżet przedstawia pięć obciążeń z największą liczbą incydentów (kliknij **Pokaż wszystko**, aby przejść do listy incydentów przefiltrowanej zgodnie z ustawieniami widżetu).

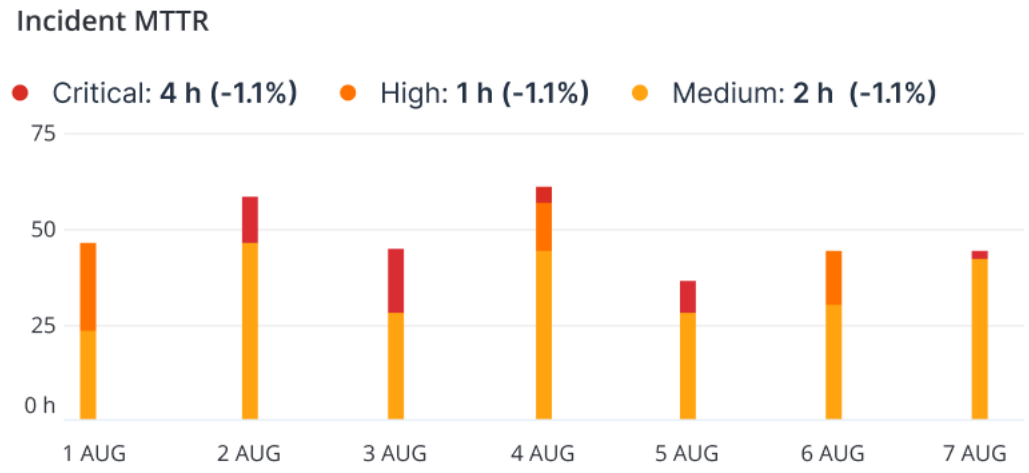
Zatrzymaj wskaźnik myszy na wierszu z obciążeniem, aby wyświetlić podział bieżącego stanu dochodzenia poszczególnych incydentów. Stany dochodzenia to **Nie uruchomiono**, **Trwa dochodzenie**, **Zamknięto** i **Fałszywe zgłoszenie**. Następnie kliknij obciążenie, które chcesz poddać

dalszym analizom, i w wyświetlonym wyskakującym okienku wybierz odpowiedniego klienta. Lista incydentów jest odświeżana zgodnie z ustawieniami widżetu.

Średni czas rozwiązywania problemu incydentu

Na tym widżecie jest przedstawiany średni czas rozwiązywania problemu związanego z incydentem bezpieczeństwa. Wskazuje on, jak szybko problemy incydentów są badane w ramach dochodzenia i rozwiązywane.

Kliknij kolumnę, aby wyświetlić podział incydentów według ich ważności (**Krytyczne**, **Wysoki** i **Średni**) oraz wskazanie, ile czasu zajęło rozwiązanie problemu o różnym poziomie ważności. Wartość % podana w nawiasie oznacza wzrost lub spadek w porównaniu z poprzednim okresem.



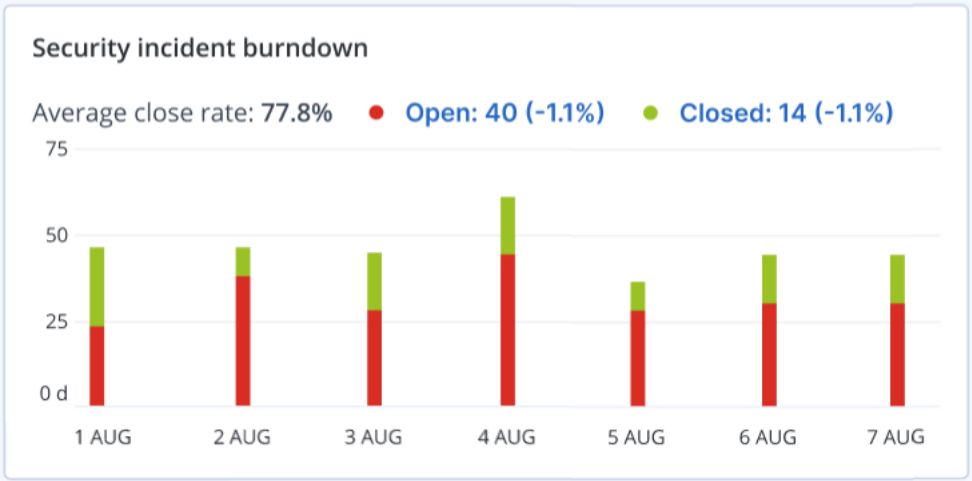
Wykres spalania dotyczący incydentów bezpieczeństwa

Ten widżet przedstawia wskaźnik efektywności zamykania incydentów. Liczba otwartych incydentów jest ujmowana w stosunku do liczby zamkniętych incydentów w danym okresie.

Zatrzymaj wskaźnik myszy na dowolnej kolumnie, aby wyświetlić podział zamkniętych i otwartych incydentów z wybranego dnia. Kliknięcie wartości Otwarte powoduje wyświetlenie wyskakującego

okienka, w którym należy wybrać odpowiedniego dzierżawcę. W celu wyświetlenia aktualnie otwartych incydentów (mających stan **Trwa dochodzenie** lub **Nie uruchomiono**) zostanie wyświetlona przefiltrowana lista incydentów dotyczących wybranego dzierżawcy. Jeśli klikniesz wartość Zamknięto, zostanie wyświetlona lista incydentów dotyczących wybranego dzierżawcy i przefiltrowana w celu wyświetlenia incydentów, które nie są już otwarte (mających stan **Zamknięto** lub **Fałszywe zgłoszenie**).

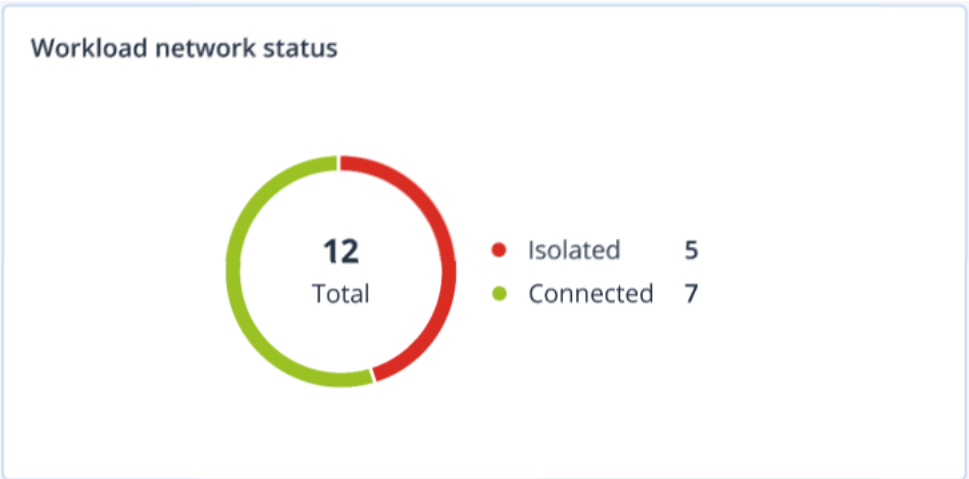
Wartość % podana w nawiasie oznacza wzrost lub spadek w porównaniu z poprzednim okresem.



Status sieciowy obciążeń

Ten widżet przedstawia bieżący status sieciowy obciążeń oraz wskazuje, ile obciążeń jest odizolowanych i ile połączonych.

Kliknięcie wartości Izolowano powoduje wyświetlenie wyskakującego okienka, w którym należy wybrać odpowiedniego dzierżawcę. Wyświetlony widok obciążeń zostanie przefiltrowany w celu wyświetlenia odizolowanych obciążeń. Kliknij wartość Podłączono, aby wyświetlić listę obciążeń z agentami przefiltrowaną w celu wyświetlenia połączonych obciążeń (w kontekście wybranego dzierżawcy).



Monitorowanie kondycji dysków

Monitorowanie kondycji dysków dostarcza informacji o bieżącej kondycji dysku i prognozach na jej temat, dzięki czemu można zapobiec utracie danych, do której mogłoby dojść wskutek awarii dysku. Obsługiwane są zarówno dyski HDD, jak i dyski SSD.

Ograniczenia

- Prognoza kondycji dysków jest obsługiwana tylko w przypadku komputerów z systemem Windows.
- Monitorowane są tylko dyski komputerów fizycznych. Dyski maszyn wirtualnych nie mogą być monitorowane ani pokazywane na widżetach kondycji dysków.
- Konfiguracje macierzy RAID nie są obsługiwane. Widżety kondycji dysków nie zawierają żadnych informacji o komputerach z implementacją macierzy RAID.
- Dyski NVMe SSD nie są obsługiwane.

Kondycja dysku może być odzwierciedlana przez jeden z następujących statusów:

- **OK**
  Kondycja dysku w zakresie 70–100%.
- **Ostrzeżenie**
  Kondycja dysku w zakresie 30–70%.
- **Krytyczne**
  Kondycja dysku w zakresie 0–30%.
- **Obliczanie danych dysku**
  Trwa obliczanie aktualnego statusu dysku i generowanie prognozy.

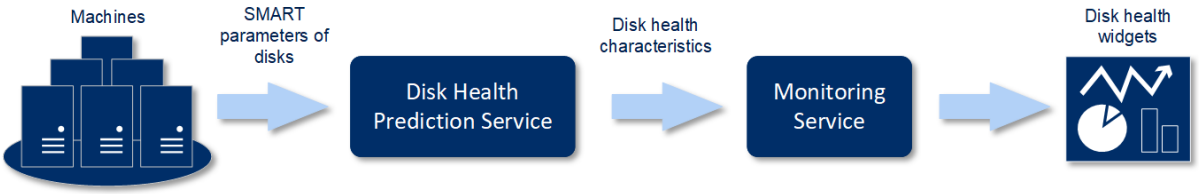
Sposób działania

Usługa Prognoza kondycji dysków korzysta z modelu predykcyjnego opartego na sztucznej inteligencji.

1. Agent ochrony zbiera parametry SMART dysków i przekazuje te dane do usługi Prognoza kondycji dysków:
   - SMART 5 — liczba ponownie alokowanych sektorów.
   - SMART 9 — liczba godzin w stanie zasilania.
   - SMART 187 — zgłoszone nienaprawialne błędy.
   - SMART 188 — przekroczony limit czasu wykonywania polecenia.
   - SMART 197 — liczba oczekujących sektorów.
   - SMART 198 — liczba nienaprawialnych sektorów w trybie offline.
   - SMART 200 — wskaźnik błędów zapisu.

2. Usługa Prognoza kondycji dysków przetwarza uzyskane parametry SMART, sporządza prognozy i udostępnia następujące charakterystyki kondycji dysków:
   - Bieżący stan dysku: OK, Ostrzeżenie, Krytyczne.
   - Prognoza kondycji dysków: negatywna, stabilna, pozytywna.
   - Prawdopodobieństwo prognozy kondycji dysku w procentach.

   Prognoza obejmuje okres najbliższego miesiąca.
3. Usługa monitorowania odbiera te właściwości, a następnie wyświetla odpowiednie informacje na widżetach kondycji dysków w konsoli Cyber Protect.



Widżety kondycji dysków

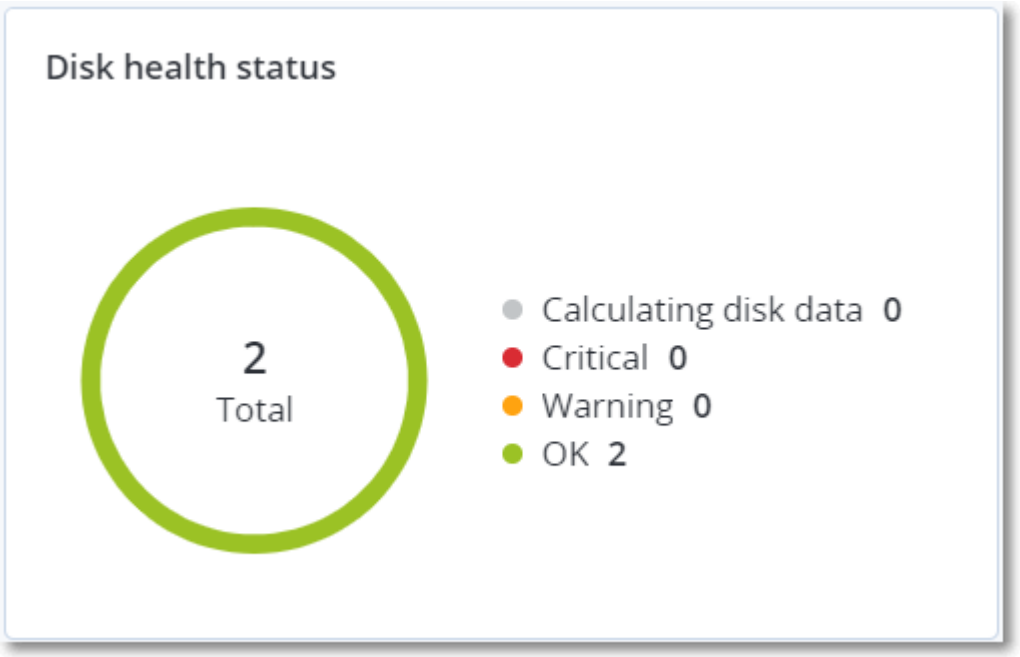
Wyniki monitorowania kondycji dysków są prezentowane na następujących widżetach dostępnych w konsoli Cyber Protect.

- **Przegląd kondycji dysków** — widżet w formie mapy drzewa obejmującej dwa poziomy szczegółów, które można zmieniać przez pogłębianie analizy.
  - Poziom komputera
    Zawiera podsumowanie statusów kondycji dysków wybranych komputerów klientów. Widoczny jest tylko najbardziej krytyczny status dysku. Pozostałe statusy są pokazywane na etykietce wyświetlanej po wskazaniu danego bloku myszą. Rozmiar bloku komputera zależy od łącznego rozmiaru dysków tego komputera. Kolor bloku komputera zależy od najbardziej krytycznego wykrytego statusu dysku.

- Poziom dysku
  Zawiera aktualne statusy kondycji wszystkich dysków wybranego komputera. Każdy blok dysków zawiera jedną z następujących prognoz kondycji dysków wraz z jej prawdopodobieństwem wyrażonym w procentach:
  - Ulegnie pogorszeniu
  - Pozostanie stabilne

- Ulegnie poprawie

- **Status kondycji dysków** — widżet w postaci wykresu kołowego przedstawiający liczby dysków według poszczególnych statusów.



Alerty dotyczące statusów kondycji dysków

Kondycja dysku jest sprawdzana co 30 minut, a raz dziennie jest generowany odpowiedni alert. Gdy kondycja dysku zmieni się z **Ostrzeżenie** na **Krytyczne**, zawsze zostanie wygenerowany alert.

Nazwa alertu	Ważność	Status kondycji dysków	Opis
Możliwość awarii dysku	Ostrzeżenie	(30 – 70)	Dysk <nazwa dysku> komputera prawdopodobnie ulegnie awarii. Jak najszybciej utwórz pełną kopię zapasową obrazu dysku, wymień go, a następnie odzyskaj obraz na nowy dysk.
Bliska awaria dysku	Krytyczne	(0 – 30)	Dysk <nazwa dysku> komputera jest w stanie krytycznym i najprawdopodobniej bardzo szybko ulegnie awarii. Odradzamy tworzenie kopii zapasowej obrazu tego dysku, ponieważ dodatkowe obciążenie może spowodować jego awarię. Niezwłocznie utwórz kopię zapasową wszystkich najważniejszych plików z tego dysku i go wymień.

Mapa ochrony danych

Funkcja mapy ochrony danych pozwala na wykrycie wszystkich ważnych danych i uzyskanie szczegółowych informacji o liczbie, rozmiarze, lokalizacji, statusach ochrony wszystkich ważnych plików w skalowalnym widoku mapy drzewa.

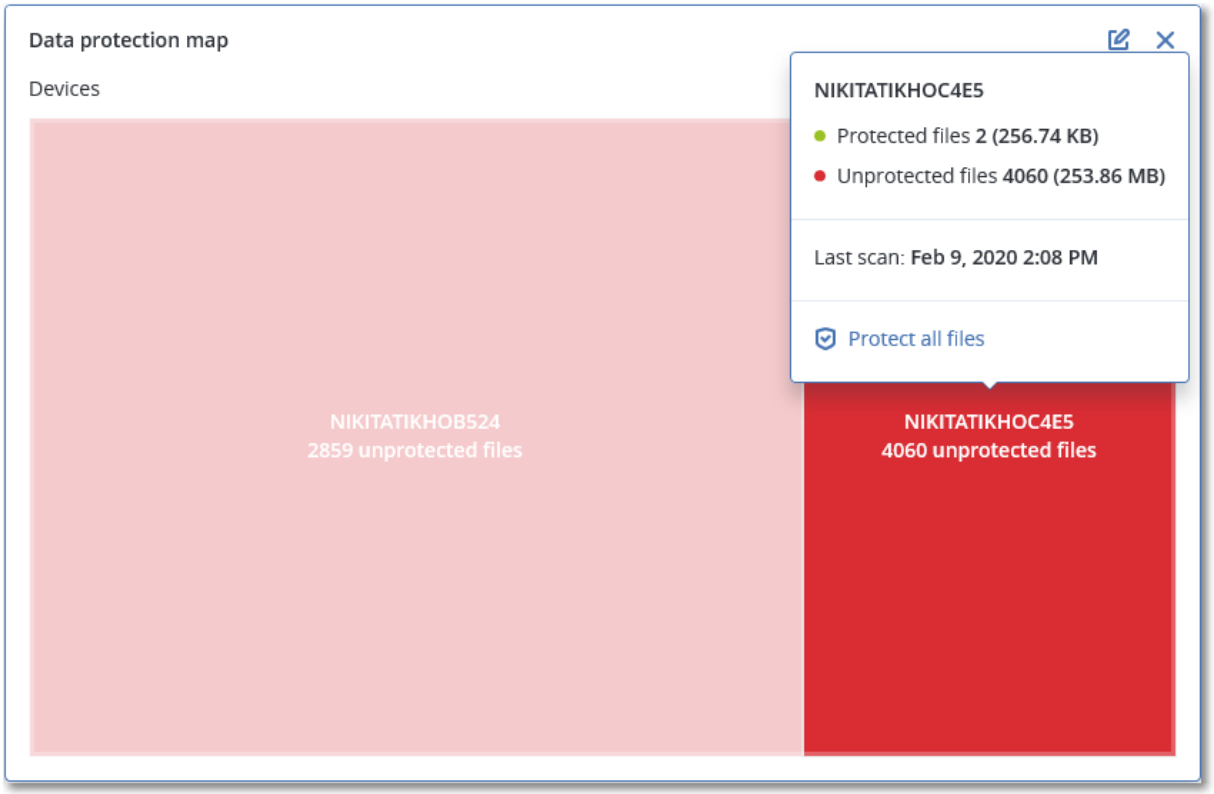
Każdy rozmiar bloku zależy od łącznej liczby lub łącznego rozmiaru wszystkich ważnych plików klienta bądź komputera.

Pliki mogą mieć jeden z następujących statusów ochrony:

- **Krytyczny** — 51–100% niechronionych plików z podanymi rozszerzeniami, które nie są uwzględniane w kopiach zapasowych i nie będą uwzględniane w kopiach zapasowych przy obecnych ustawieniach tworzenia kopii zapasowych wybranego komputera lub wybranej lokalizacji.
- **Niski** — 21–50% niechronionych plików z podanymi rozszerzeniami, czyli plików, które nie są uwzględniane w kopiach zapasowych i nie będą uwzględniane w kopiach zapasowych przy obecnych ustawieniach tworzenia kopii zapasowych wybranego komputera lub wybranej lokalizacji.
- **Średni** — 1–20% niechronionych plików z podanymi rozszerzeniami, czyli plików, które nie są uwzględniane w kopiach zapasowych i nie będą uwzględniane w kopiach zapasowych przy obecnych ustawieniach tworzenia kopii zapasowych wybranego komputera lub wybranej lokalizacji.
- **Wysoki** — wszystkie pliki z podanymi rozszerzeniami są chronione (uwzględniane w kopiach zapasowych) w przypadku wybranego komputera lub wybranej lokalizacji.

Wyniki kontroli ochrony danych można znaleźć na pulpicie nawigacyjnym w widżecie Mapa ochrony danych — jest to mapa drzewa ze szczegółowymi informacjami na poziomie komputera:

- Poziom komputera — zawiera informacje o statusach ochrony ważnych plików na poszczególnych komputerach wybranego klienta.



Aby zacząć chronić niechronione pliki, zatrzymaj wskaźnik myszy na bloku i kliknij **Chroń wszystkie pliki**. W tym oknie dialogowym znajdziesz informacje o liczbie niechronionych plików i ich lokalizacjach. Aby objąć te pliki ochroną, kliknij **Chroń wszystkie pliki**.

Możesz też pobrać szczegółowy raport w formacie CSV.

Widżety dotyczące oceny luk w zabezpieczeniach

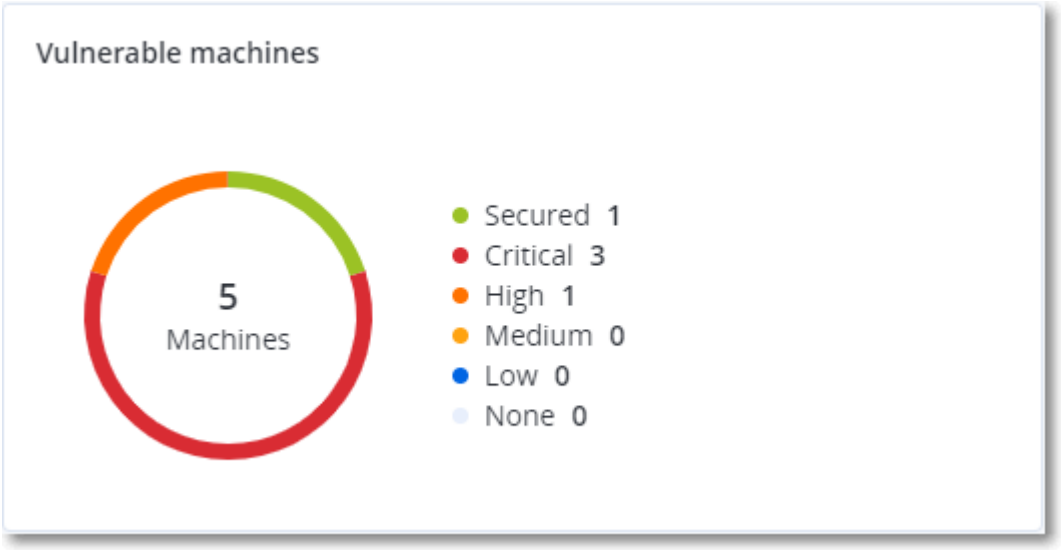
Komputery z lukami w zabezpieczeniach

Ten widżet przedstawia komputery z lukami w zabezpieczeniach uporządkowane według ważności luk.

Znaleziona luka może mieć jeden z następujących poziomów ważności określony zgodnie z systemem Common Vulnerability Scoring System (CVSS) w wersji 3.0:

- Bezpieczny: nie znaleziono luk w zabezpieczeniach
- Krytyczny: 9,0–10,0 w skali CVSS
- Wysoki: 7,0–8,9 w skali CVSS

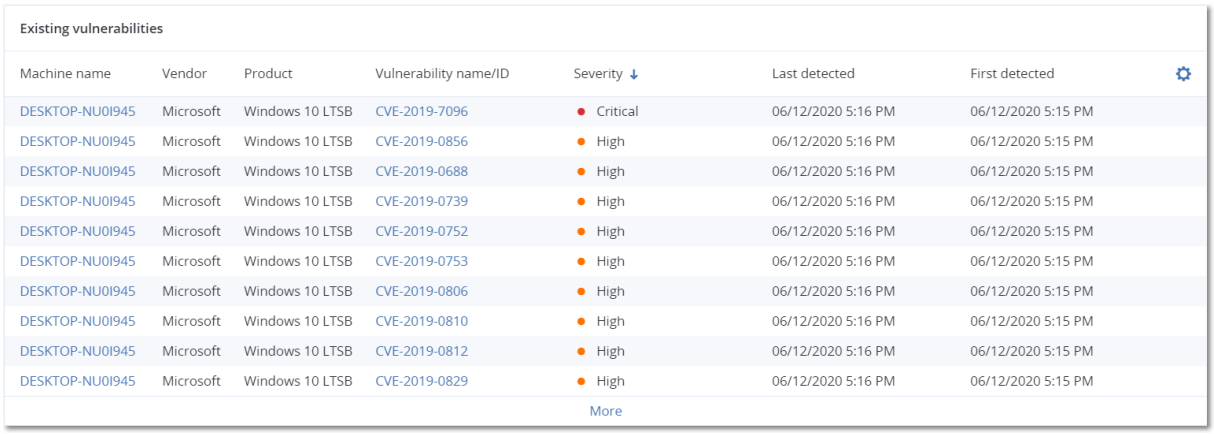
- Średni: 4,0–6,9 w skali CVSS
- Niski: 0,1–3,9 w skali CVSS
- Brak: 0,0 w skali CVSS



Występujące luki w zabezpieczeniach

Ten widżet przedstawia obecnie występujące luki w zabezpieczeniach na komputerach. W widżecie **Istniejące luki w zabezpieczeniach** są dostępne dwie kolumny z sygnaturami czasowymi:

- **Pierwsze wykrycie** — data i godzina pierwszego wykrycia luki na komputerze.
- **Ostatnie wykrycie** — data i godzina ostatniego wykrycia luki na komputerze.


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

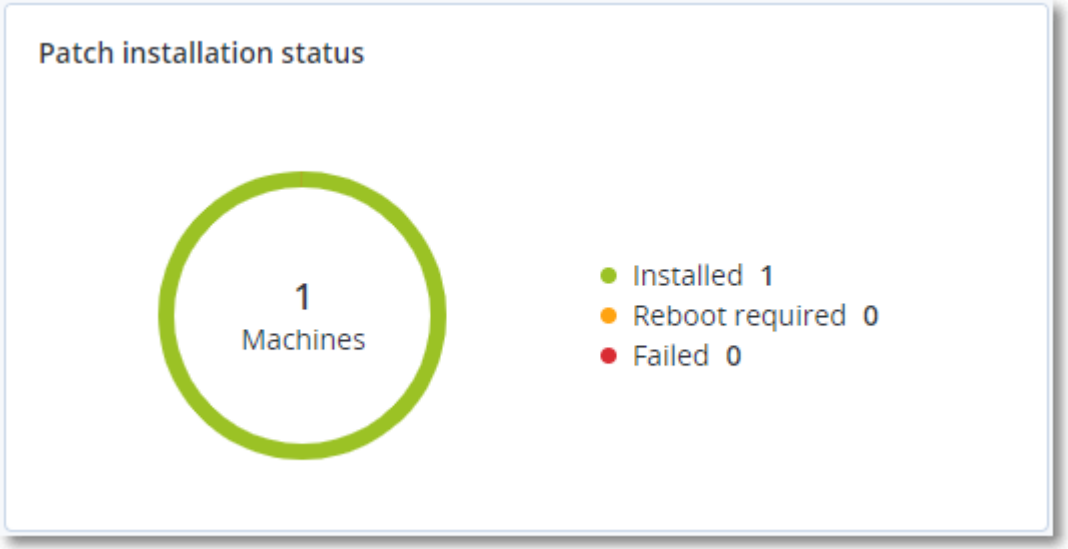
Widżety dotyczące instalacji poprawek

Występują cztery widżety związane z funkcjami zarządzania poprawkami.

Status instalacji poprawek

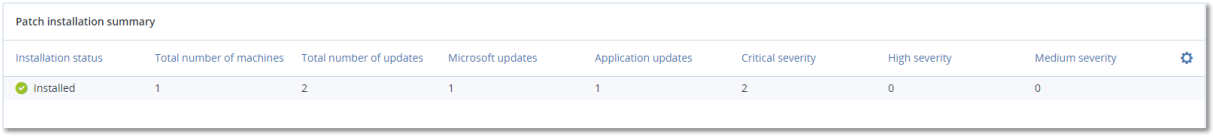
Ten widżet przedstawia liczbę komputerów pogrupowanych według statusów instalacji poprawek.

- **Zainstalowane** — na komputerze zainstalowano wszystkie dostępne poprawki
- **Wymagane ponowne uruchomienie** — po zainstalowaniu poprawki wymagane jest ponowne uruchomienie komputera
- **Niepowodzenie** — instalacja poprawki zakończyła się niepowodzeniem



Podsumowanie instalacji poprawek

Ten widżet przedstawia podsumowanie poprawek na komputerach według statusów ich instalacji.


Patch installation summary

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

Historia instalacji poprawek

Ten widżet przedstawia szczegółowe informacje o poprawkach na komputerach.


Patch installation history

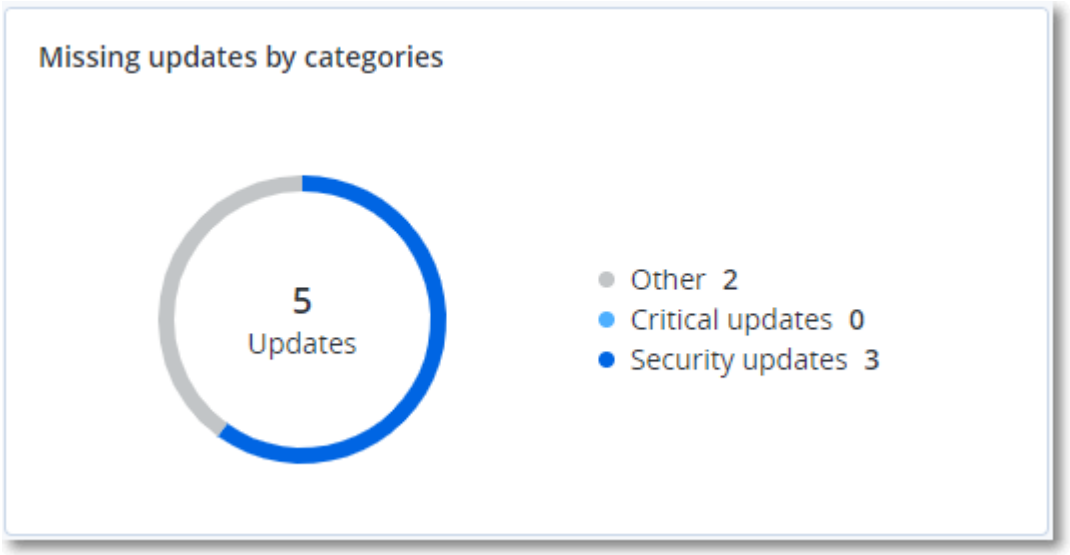
Machine name	Update name	Version	Severity	Approval status	Installation status	Installation date
NIKITATIKHOC4E5	FastStone Soft FastStone I...	5.9	Medium	New	Installed	02/05/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical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

More

Brakujące aktualizacje według kategorii

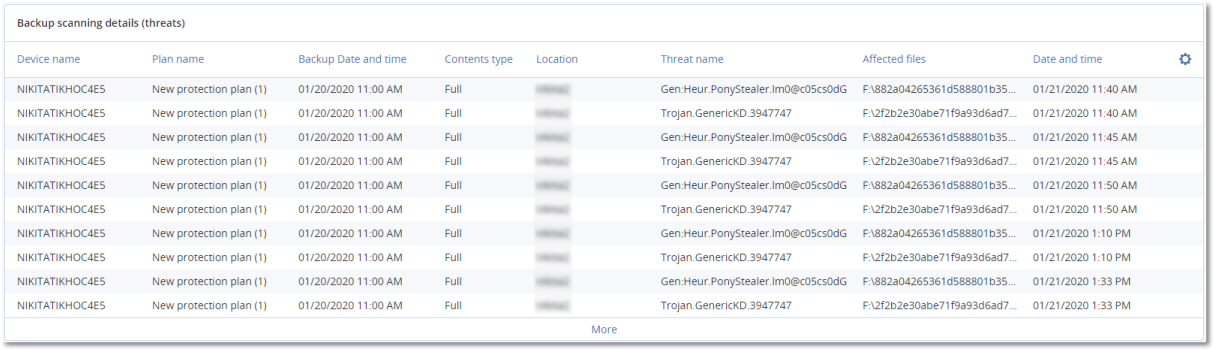
Ten widżet przedstawia liczbę brakujących aktualizacji według kategorii. Pokazywane są następujące kategorie:

- Aktualizacje zabezpieczeń
- Aktualizacje krytyczne
- Inne



Szczegóły skanowania kopii zapasowej

Ten widżet przedstawia szczegółowe informacje o wykrytych zagrożeniach w kopiach zapasowych.

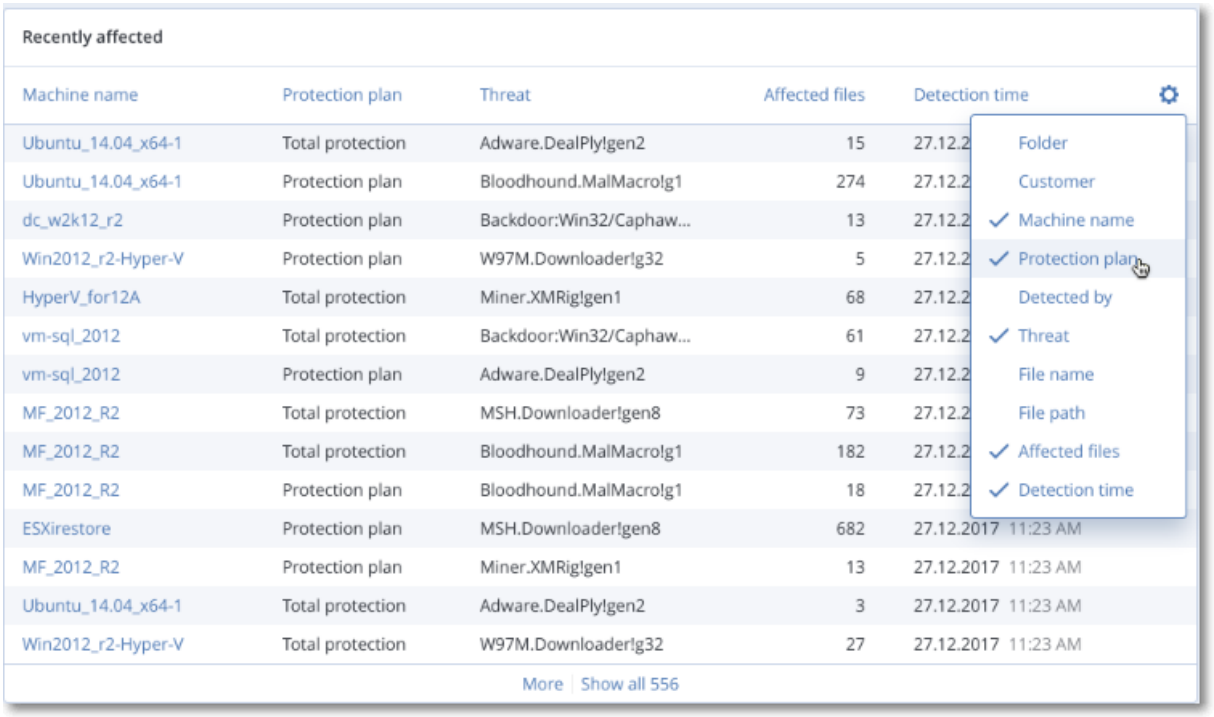

Backup scanning details (threats)

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

Ostatnio dotknięte problemem

Ten widżet przedstawia szczegółowe informacje o obciążeniach, które ucierpiały wskutek zagrożeń, takich jak wirusy, złośliwe oprogramowanie czy ramsomware. Dostępne są informacje o wykrytych zagrożeniach, czasie ich wykrycia oraz liczbie plików, na które miały one wpływ.



Pobieranie danych dotyczących ostatnio dotkniętych problemem obciążeń

Można pobrać dane dotyczące ostatnio dotkniętych problemem obciążeń, wygenerować plik CSV i wysłać go do wskazanych odbiorców.

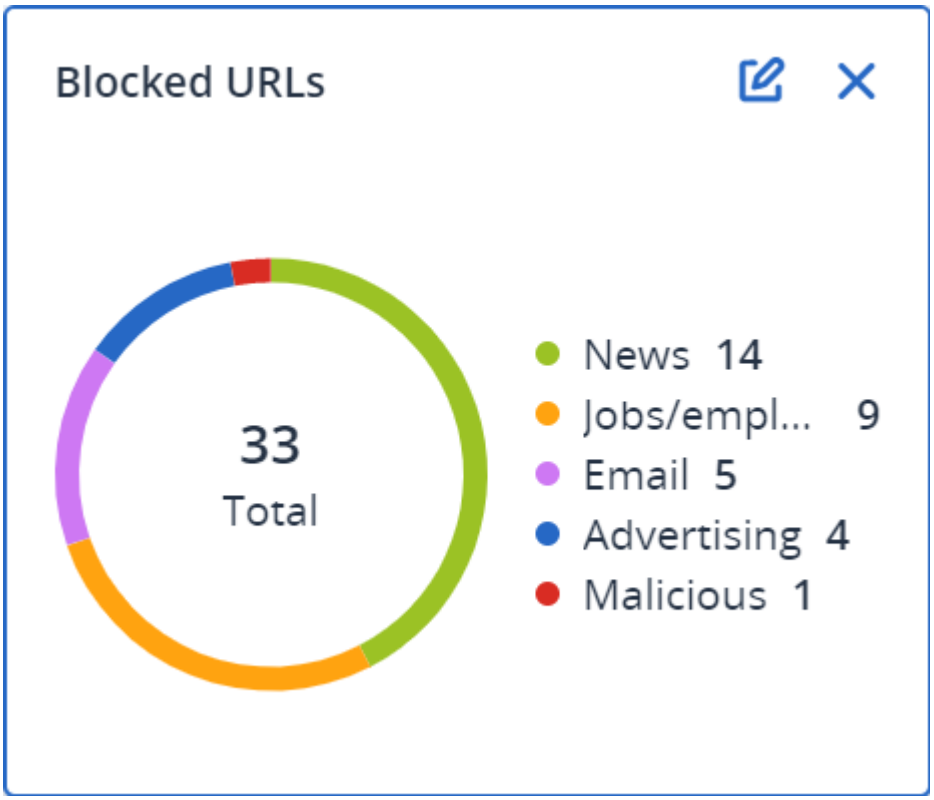
Aby pobrać dane dotyczące ostatnio dotkniętych problemem obciążeń

1. W widżecie **Ostatnio dotknięte problemem** kliknij **Pobierz dane**.
2. W polu **Okres** wprowadź liczbę dni, których mają dotyczyć pobierane dane. Można wprowadzić maksymalnie 200 dni.
3. W polu **Odbiorcy** wprowadź adresy e-mail wszystkich osób, które otrzymają wiadomość e-mail z łączem umożliwiającym pobranie pliku CSV.
4. Kliknij **Pobierz**.

   System zacznie generować plik CSV z danymi dotyczącymi obciążeń, które zostały dotknięte problemem we wskazanym okresie. Gdy plik CSV będzie gotowy, system wyśle wiadomość e-mail do odbiorców. Każdy odbiorca będzie mógł pobrać ten plik CSV.

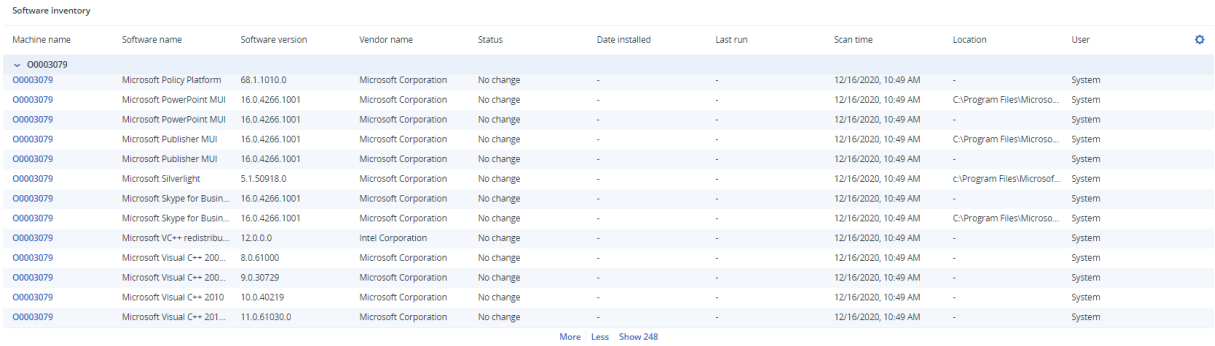
Zablokowane adresy URL

Ten widżet przedstawia dane statystyczne dotyczące zablokowanych adresów URL według kategorii. Więcej informacji na temat filtrowania i określania kategorii adresów URL można znaleźć w podręczniku użytkownika rozwiązania Cyber Protection.



Widżet inwentaryzacji oprogramowania

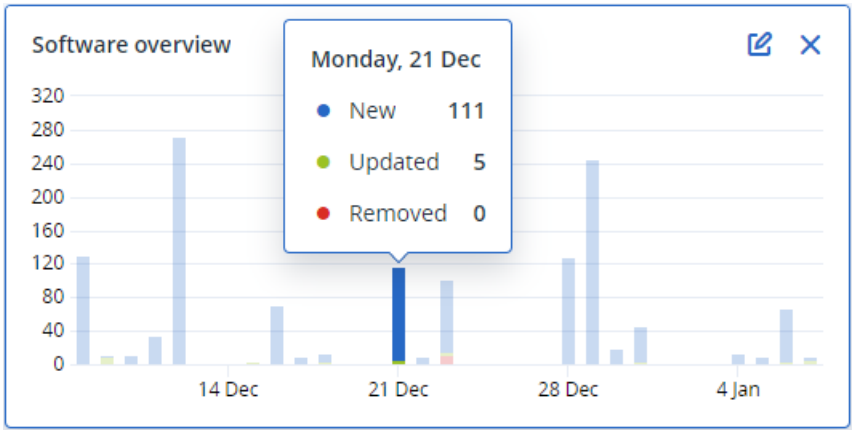
W widżecie tabeli **Inwentaryzacja oprogramowania** są wyświetlane szczegółowe informacje na temat wszystkich programów zainstalowanych na urządzeniach organizacji z systemem Windows lub macOS.


Software inventory

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

More | Less | Show 248

W widżecie tabeli **Przegląd oprogramowania** są wyświetlane liczby nowych, zaktualizowanych i usuniętych we wskazanym okresie (7 dni, 30 dni lub bieżący miesiąc) aplikacji na urządzeniach organizacji z systemem Windows lub macOS.



Po wskazaniu myszą określonego słupka wykresu pojawia się etykieta z następującymi informacjami:

Nowe — liczba nowo zainstalowanych aplikacji.

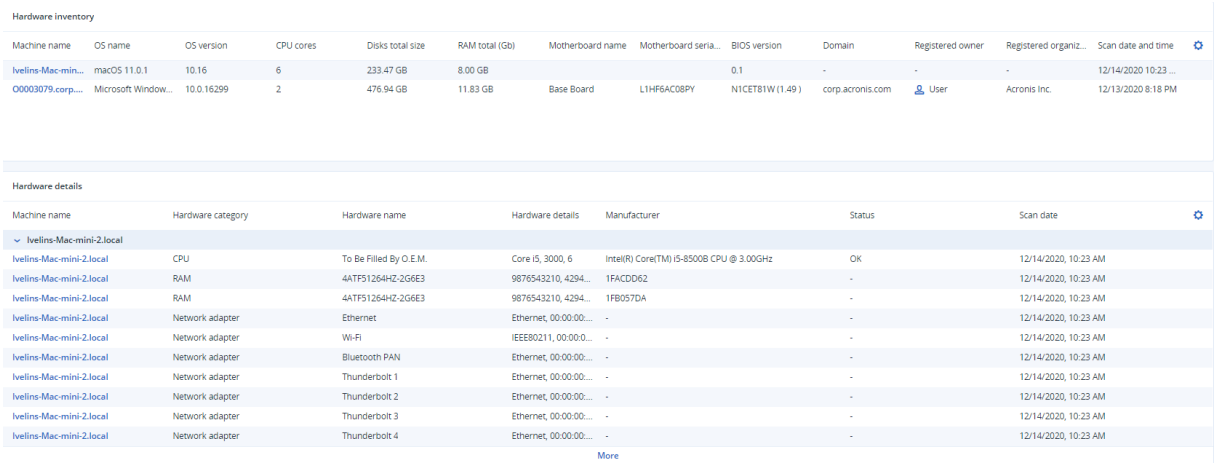
Zaktualizowano — liczba zaktualizowanych aplikacji.

Usunięto — liczba usuniętych aplikacji.

Po kliknięciu części słupka odpowiadającej danemu statusowi nastąpi przekierowanie do strony **Zarządzanie oprogramowaniem** -> **Inwentaryzacja oprogramowania**. Informacje dostępne na tej stronie są filtrowane według odpowiedniej daty i statusu.

Widżety inwentaryzacji sprzętu

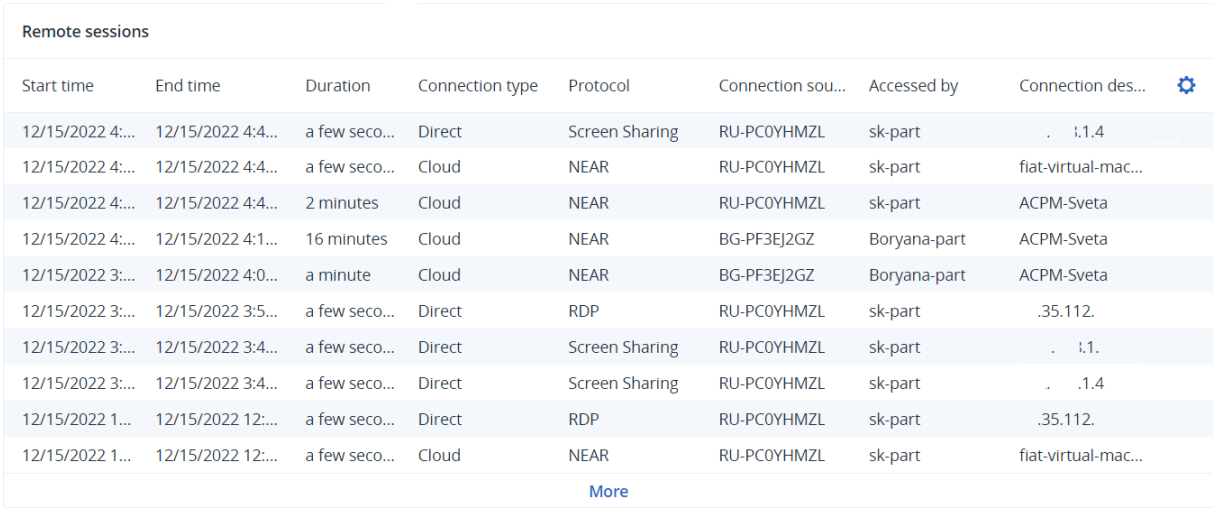
W widżetach tabeli **Inwentaryzacja sprzętu** i **Szczegóły sprzętu** są pokazywane informacje na temat wszystkich elementów sprzętowych zainstalowanych w fizycznych i wirtualnych urządzeniach z systemem Windows lub macOS należących do Twojej organizacji.



W widżecie tabeli **Zmiany sprzętowe** są wyświetlane informacje na temat sprzętu w należących do Twojej organizacji fizycznych i wirtualnych urządzeniach z systemem Windows lub macOS, który dodano, usunięto i zmieniono we wskazanym okresie (7 dni, 30 dni lub bieżący miesiąc).

Historia sesji

Ten widżet umożliwia wyświetlenie szczegółowych informacji o sesjach pulpitu zdalnego i przesyłania plików zrealizowanych w ramach organizacji we wskazanym okresie.



Dziennik inspekcji

Aby przejrzeć dziennik inspekcji, kliknij **Monitorowanie** > **Dziennik inspekcji**.

Dziennik inspekcji udostępnia chronologiczny zapis następujących zdarzeń:

- Operacje wykonywane przez użytkowników w portalu zarządzania
- Operacje dotyczące zasobów obsługiwanych między chmurami wykonywane przez użytkowników w konsoli Cyber Protect
- Operacje skryptów cybernetycznych wykonywane przez użytkowników w konsoli Cyber Protect
- Komunikaty systemowe o osiągnięciu i stopniu wykorzystania limitów

W dzienniku widoczne są zdarzenia występujące w ramach organizacji lub jednostki, w której aktualnie pracujesz, oraz jej jednostek podrzędnych. Kliknięcie zdarzenia umożliwia wyświetlenie dodatkowych informacji na jego temat.

Dzienniki inspekcji są przechowywane w centrum danych i problemy na komputerach użytkowników nie ograniczają ich dostępności.

Dziennik jest codziennie oczyszczany. Zdarzenia są usuwane po 180 dniach.

Pola dziennika inspekcji

W przypadku każdego zdarzenia w dzienniku są dostępne następujące informacje:

- **Zdarzenie**

  Krótki opis zdarzenia. Na przykład **Dzierżawca został utworzony**, **Dzierżawca został usunięty**, **Użytkownik został utworzony**, **Użytkownik został usunięty**, **Limit został osiągnięty**, **Przeglądano zawartość kopii zapasowej**, **Skrypt został zmieniony**.
- **Ważność**

  Może być jedna z następujących:
  - **Błąd**

    Oznacza błąd.
  - **Ostrzeżenie**

    Oznacza potencjalnie negatywną czynność. Na przykład **Dzierżawca został usunięty**, **Użytkownik został usunięty**, **Limit został osiągnięty**.
  - **Powiadomienie**

    Oznacza, że zdarzenie może wymagać uwagi. Na przykład **Dzierżawca został zaktualizowany**, **Użytkownik został zaktualizowany**.
  - **Informacja**

    Oznacza informację o neutralnej w skutkach zmianie lub czynności. Na przykład **Dzierżawca został utworzony**, **Użytkownik został utworzony**, **Limit został zaktualizowany**, **Plan skryptów został usunięty**.
- **Data**

  Data i godzina wystąpienia zdarzenia.
- **Nazwa obiektu**

  Obiekt, na którym została wykonana operacja. Na przykład obiektem zdarzenia **Użytkownik został zaktualizowany** jest użytkownik, którego właściwości zostały zmienione. W przypadku zdarzeń dotyczących limitu obiektem jest limit.
- **Dzierżawca**

  Nazwa jednostki, do której należy obiekt. Na przykład dzierżawcą zdarzenia **Użytkownik został zaktualizowany** jest jednostka, w której znajduje się użytkownik. Dzierżawcą zdarzenia **Limit został osiągnięty** jest użytkownik, którego limit został osiągnięty.
- **Inicjator**

  Nazwa logowania użytkownika inicjującego zdarzenie. W przypadku komunikatów systemowych i zdarzeń inicjowanych przez administratorów wyższego poziomu inicjator jest pokazywany jako **System**.
- **Dzierżawca inicjatora**

Nazwa jednostki, do której należy inicjator. W przypadku komunikatów systemowych i zdarzeń inicjowanych przez administratorów wyższego poziomu to pole pozostaje puste.

- **Metoda**

  Pokazuje, czy zdarzenie zostało zainicjowane za pomocą interfejsu internetowego czy za pośrednictwem interfejsu API.
- **Adres IP**

  Adres IP urządzenia, z którego zainicjowano zdarzenie.

Filtrowanie i wyszukiwanie

Zdarzenia można filtrować według typu, ważności lub daty. Można też je przeszukiwać według nazwy, obiektu, dzierżawcy, inicjatora i dzierżawcy inicjatora.

Raportowanie

Aby uzyskać dostęp do raportów z wykorzystania usług i operacji, kliknij **Raporty**.

Uwaga
Ta funkcja jest niedostępna w wersjach Standard usługi Cyber Protection.

Raporty z użytkowania

Raporty dotyczące wykorzystania zawierają dane historyczne o korzystaniu z usług. Raporty dotyczące wykorzystania są dostępne zarówno w formacie CSV, jak i HTML.

Typ raportu

Możesz wybrać jeden z następujących typów raportów:

- **Obecne wykorzystanie**
  Raport zawiera aktualne wskaźniki wykorzystania usługi.
- **Podsumowanie okresu**
  Raport zawiera wskaźniki wykorzystania usługi z końca wskazanego okresu oraz różnice między wskaźnikami z początku i końca tego okresu.
- **Dzień po dniu w podanym okresie**
  Raport zawiera wskaźniki wykorzystania usługi i ich zmiany w poszczególnych dniach wskazanego okresu.

Zakres raportu

W razie potrzeby można wskazać zakres raportu, wybierając jedną z poniższych wartości:

- **Bezpośredni klienci i partnerzy**
  Raport będzie zawierać wskaźniki wykorzystania usług dotyczące tylko bezpośrednich jednostek podrzędnych firmy lub jednostki, w ramach której działasz.
- **Wszyscy klienci i partnerzy**
  Raport będzie zawierać wskaźniki wykorzystania usług dotyczące wszystkich jednostek podrzędnych firmy lub jednostki, w ramach której działasz.
- **Wszyscy klienci i partnerzy (w tym szczegółowe dane użytkownika)**
  Raport będzie zawierać wskaźniki wykorzystania usług dotyczące wszystkich jednostek podrzędnych firmy lub jednostki, w ramach której działasz, a także wszystkich użytkowników w tych jednostkach.

Wskaźniki wskazujące zerowy stan wykorzystania

Można zmniejszyć liczbę wierszy w raporcie, ograniczając wyświetlanie informacji wyłącznie do wskaźników wskazujących niezerowy poziom wykorzystania przez ukrycie informacji o wskaźnikach wskazujących poziom zerowy.

Konfigurowanie zaplanowanych raportów z wykorzystania

Zaplanowany raport obejmuje wskaźniki wykorzystania usług z ostatniego pełnego miesiąca kalendarzowego. Raporty są generowane pierwszego dnia miesiąca o godzinie 23:59:59 czasu UTC i wysyłane drugiego dnia tego samego miesiąca. Raporty są wysyłane do wszystkich administratorów Twojej firmy lub jednostki, którzy zaznaczyli pole wyboru **Zaplanowane raporty z użytkowania** w swoich ustawieniach użytkownika.

Aby włączyć lub wyłączyć zaplanowany raport

1. Zaloguj się do portalu zarządzania.
2. Upewnij się, że działasz na poziomie firmy lub jednostki znajdującej się najwyżej w hierarchii spośród wszystkich, które są dla Ciebie dostępne.
3. Kliknij **Raporty** > **Wykorzystanie**.
4. Kliknij **Zaplanowane**.
5. Zaznacz lub wyczyść pole wyboru **Wysyłaj miesięczny raport podsumowujący**.
6. W polu **Poziom szczegółów** wybierz zakres raportu.
7. [Opcjonalnie] Wybierz **Ukryj wskaźniki wskazujące zerowy stan wykorzystania**, jeśli chcesz wykluczyć z raportu wskaźniki wskazujące zerowy poziom wykorzystania.

Konfigurowanie niestandardowych raportów z wykorzystania

Raport niestandardowy jest generowany na żądanie — nie można go zaplanować. Raport zostanie wysłany na Twój adres e-mail.

Aby wygenerować raport niestandardowy

1. Zaloguj się do portalu zarządzania.
2. Przejdź do jednostki, w której przypadku chcesz utworzyć raport.
3. Kliknij **Raporty** > **Wykorzystanie**.
4. Kliknij **Niestandardowe**.
5. W polu **Typ** wybierz typ raportu.
6. [Opcja niedostępna w przypadku typu raportu **Obecne wykorzystanie**] W polu **Okres** wybierz okres raportowania:
   - **Obecny miesiąc kalendarzowy**
   - **Poprzedni miesiąc kalendarzowy**
   - **Niestandardowe**
7. [Opcja niedostępna w przypadku typu raportu **Obecne wykorzystanie**] Jeśli chcesz wskazać niestandardowy okres raportowania, wybierz datę początkową i końcową. W przeciwnym razie pomiń ten krok.
8. W polu **Poziom szczegółów** wybierz zakres raportu.

9. [Opcjonalnie] Wybierz **Ukryj wskaźniki wskazujące zerowy stan wykorzystania**, jeśli chcesz wykluczyć z raportu wskaźniki wskazujące zerowy poziom wykorzystania.
10. Aby wygenerować raport, kliknij **Wygeneruj i wyślij**.

Dane w raportach z wykorzystania

Raport dotyczący korzystania z usługi Cyber Protection obejmuje następujące dane o firmie lub jednostce:

- Rozmiar kopii zapasowych według jednostki, użytkownika i typu urządzenia.
- Liczba chronionych urządzeń według jednostki, użytkownika i typu urządzenia.
- Cena według jednostki, użytkownika i typu urządzenia.
- Łączny rozmiar kopii zapasowych.
- Łączna liczba chronionych urządzeń.
- Łączna wartość cenowa.

Uwaga
Jeśli usługa Cyber Protection nie może wykryć typu urządzenia, urządzenie to jest oznaczane w raporcie jako **bez określonego typu**.

Raporty z operacji

Raporty z **operacji** są dostępne tylko dla administratorów firm podczas wykonywania operacji na poziomie firmy.

Raport z operacji może zawierać dowolny zestaw widżetów pulpitu nawigacyjnego dla **operacji**. Wszystkie widżety przedstawiają skrócone informacje dotyczące całej firmy.
W zależności od typu widżetu raport zawiera dane ze wskazanego zakresu czasu lub z chwili przeglądania bądź generowania raportu. Zobacz "Raportowane dane zależnie od typu widżetu" (s. 80).

Wszystkie widżety historyczne przedstawiają dane z tego samego zakresu czasu. Zakres ten można zmienić w ustawieniach raportów.

Można korzystać z raportów domyślnych lub utworzyć raport niestandardowy.

Możesz raport pobrać lub wysłać pocztą e-mail w formacie XLSX (Excel) bądź PDF.

Raporty domyślne wymieniono poniżej:

Nazwa raportu	Opis
Wynik #CyberFit według komputerów	Pokazuje wynik #CyberFit oszacowany na podstawie oceny wskaźników zabezpieczeń i konfiguracji poszczególnych komputerów oraz zalecenia dotyczące możliwych udoskonaleń.

Alerty	Zawiera alerty zgłoszone w podanym okresie.
Szczegóły skanowania kopii zapasowej	Zawiera szczegółowe informacje o wykrytych zagrożeniach w kopiach zapasowych.
Codzienne działania	Zawiera zestawienie informacji o działaniach wykonanych w podanym okresie.
Mapa ochrony danych	Zawiera szczegółowe informacje o liczbie, rozmiarze, lokalizacji i statusach ochrony wszystkich ważnych plików na komputerach.
Wykryte zagrożenia	Zawiera szczegółowe informacje o zagrożonych komputerach według liczby zablokowanych zagrożeń oraz o komputerach będących w dobrej kondycji i mających luki w zabezpieczeniach.
Wykryte komputery	Zawiera listę wszystkich komputerów znalezionych w sieci organizacji.
Prognoza kondycji dysków	Zawiera prognozowane terminy awarii dysków HDD/SSD oraz aktualne statusy dysków.
Występujące luki w zabezpieczeniach	Zawiera listę istniejących luk w zabezpieczeniach systemów operacyjnych i aplikacji organizacji. Raport obejmuje również szczegółowe informacje dotyczące zagrożonych komputerów w sieci w przypadku każdego produktu z listy.
Podsumowanie zarządzania poprawkami	Zawiera liczbę brakujących, zainstalowanych i możliwych poprawek. W ramach raportów można wyświetlać bardziej szczegółowe informacje, aby sprawdzać brakujące bądź zainstalowane poprawki oraz informacje na temat wszystkich systemów.
Podsumowanie	Zawiera podsumowanie informacji o chronionych urządzeniach w podanym okresie.
Działania w tygodniu	Zawiera zestawienie informacji o działaniach wykonanych w podanym okresie.
Inwentaryzacja oprogramowania	Zawiera szczegółowe informacje na temat wszystkich programów zainstalowanych na komputerach organizacji z systemem Windows lub macOS.
Inwentaryzacja sprzętu	Zawiera szczegółowe informacje na temat wszystkich elementów sprzętowych dostępnych w komputerach fizycznych i maszynach wirtualnych z systemem Windows lub macOS należących do Twojej organizacji.
Sesje zdalne	Umożliwia wyświetlenie szczegółowych informacji o sesjach pulpitu zdalnego i przesyłania plików zrealizowanych w ramach organizacji we wskazanym okresie.

Czynności dotyczące raportów

Aby zobaczyć raport, kliknij jego nazwę.

Aby dodać nowy raport

1. W konsoli Cyber Protect przejdź do sekcji **Raporty**.
2. Pod listą dostępnych raportów kliknij **Dodaj raport**.
3. [Aby dodać predefiniowany raport] Kliknij nazwę predefiniowanego raportu.
4. [Aby dodać raport niestandardowy] Kliknij **Niestandardowe**, a następnie dodaj widżety do raportu.
5. [Opcjonalnie] Możesz przeciągać widżety, aby zmienić ich rozmieszczenie.

Aby edytować raport

1. W konsoli Cyber Protect przejdź do sekcji **Raporty**.
2. Na liście raportów wybierz raport do edycji.
   Możesz wykonać następujące czynności:
   - Zmiana nazwy raportu.
   - Zmiana zakresu czasu wszystkich widżetów w raporcie.
   - Określenie odbiorców raportu i czasu wysłania do nich raportu. Dostępne formaty to PDF i XLSX.

Aby usunąć raport

1. W konsoli Cyber Protect przejdź do sekcji **Raporty**.
2. Na liście raportów wybierz raport do usunięcia.
3. Kliknij ikonę wielokropka (...), a następnie kliknij **Usuń**.
4. Potwierdź wybór, klikając **Usuń**.

Aby zaplanować raport

1. W konsoli Cyber Protect przejdź do sekcji **Raporty**.
2. Na liście raportów wybierz raport do zaplanowania, a następnie kliknij **Ustawienia**.
3. Włącz przełącznik **Zaplanowane**.
   - Podaj adresy e-mail odbiorców.
   - Wybierz format raportu.

Uwaga
Można wyeksportować do 1000 pozycji w formacie PDF i do 10 000 pozycji w formacie XLSX. Sygnatury czasowe w plikach PDF i XLSX są oparte na lokalnym czasie urządzenia.

- Wybierz język raportu.
- Skonfiguruj harmonogram.

4. Kliknij **Zapisz**.

Aby pobrać raport

1. W konsoli Cyber Protect przejdź do sekcji **Raporty**.
2. Na liście raportów wybierz raport, a następnie kliknij **Pobierz**.
3. Wybierz format raportu.

Aby wysłać raport

1. W konsoli Cyber Protect przejdź do sekcji **Raporty**.
2. Na liście raportów wybierz raport, a następnie kliknij **Wyślij**.
3. Podaj adresy e-mail odbiorców.
4. Wybierz format raportu.
5. Kliknij **Wyślij**.

Aby wyeksportować strukturę raportu

1. W konsoli Cyber Protect przejdź do sekcji **Raporty**.
2. Na liście raportów wybierz raport.
3. Kliknij ikonę wielokropka (...), a następnie kliknij **Eksportuj**.

W wyniku tych działań struktura raportu zostanie zapisana na komputerze jako plik JSON.

Aby składować dane raportu

Korzystając z tej opcji, można wyeksportować wszystkie dane z niestandardowego okresu — bez ich filtrowania — do pliku CSV i wysłać plik CSV do odbiorcy wiadomości e-mail.

Uwaga
Można wyeksportować do 150 000 pozycji w formacie CSV. Sygnatury czasowe w pliku CSV są oparte na uniwersalnym czasie koordynowanym (UTC).

1. W konsoli Cyber Protect przejdź do sekcji **Raporty**.
2. Na liście raportów wybierz raport, z którego danymi chcesz wykonać zrzut.
3. Kliknij ikonę wielokropka (...), a następnie kliknij **Dane zrzutu**.
4. Podaj adresy e-mail odbiorców.
5. W polu **Zakres czasu** wskaż niestandardowy okres, który chcesz uwzględnić w zrzucie danych.

   Uwaga
   W przypadku dłuższych okresów przygotowywanie plików CSV zajmuje więcej czasu.

6. Kliknij **Wyślij**.

Podsumowanie

Raport podsumowujący stanowi ogólny przegląd statusu ochrony środowiska organizacji i chronionych urządzeń we wskazanym okresie.

Raport podsumowujący zawiera dostosowywane sekcje z widżetami dynamicznymi, na których są wyświetlane kluczowe wskaźniki wydajności związane z korzystaniem z następujących usług chmurowych: Kopia zapasowa, Ochrona przed złośliwym oprogramowaniem, Ocena luk w zabezpieczeniach, Zarządzanie poprawkami, Notary, Odzyskiwanie po awarii oraz File Sync & Share.

Raport można dostosowywać na kilka sposobów, takich jak:

- Dodanie lub usunięcie sekcji.
- Zmiana kolejności sekcji.
- Zmiana nazwy sekcji.
- Przeniesienie widżetów do innej sekcji.
- Zmiana kolejności widżetów w poszczególnych sekcjach.
- Dodanie lub usunięcie widżetów.
- Dostosowanie widżetów.

Raporty podsumowujące można generować w formacie PDF i Excel, a następnie przesyłać odpowiednim zainteresowanym lub właścicielom organizacji, aby mogli w przystępnej formie zobaczyć techniczną i biznesową wartość świadczonych usług.

Widżety usługi Podsumowanie

Możesz dodawać lub usuwać sekcje oraz widżety w ramach raportu podsumowującego i w ten sposób określać, jakie informacje mają być w nim zawarte.

Widżety usługi Przegląd obciążeń

Poniższa tabela zawiera dodatkowe informacje na temat widżetów dostępnych w sekcji **Przegląd obciążeń**.

Widżet	Opis
Status ochrony obciążeń w chmurze	Ten widżet przedstawia liczbę chronionych i niechronionych obciążeń w chmurze według typów w chwili wygenerowania raportu. Chronione obciążenia w chmurze to obciążenia, do których zastosowano co najmniej jeden plan tworzenia kopii zapasowych. Niechronione obciążenia w chmurze to obciążenia, do których nie zastosowano żadnego planu tworzenia kopii zapasowych. Na wykresie przedstawiono następujące typy obciążeń w chmurze (w kolejności alfabetycznej od A do Z):

Widżet	Opis
	• Dysk Google Workspace • Gmail Google Workspace • Dysk współdzielony Google Workspace • Skrzynki pocztowe usługi Hosted Exchange • Skrzynki pocztowe Microsoft 365 • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • Witryny internetowe W przypadku niektórych typów obciążeń są stosowane następujące grupy obciążeń: • Microsoft 365: Użytkownicy, Grupy, Foldery publiczne, Zespoły i Kolekcje witryn • Google Workspace: Użytkownicy i Dyski współdzielone • Hosted Exchange: Użytkownicy Jeśli w jednej grupie obciążeń znajduje się więcej niż 10 000 obciążeń, widżet nie wyświetla żadnych danych na temat poszczególnych obciążeń. Jeśli więc na przykład klient ma konto Microsoft 365 z 10 000 skrzynek pocztowych oraz usługę OneDrive dla 500 użytkowników, to wszystkie one należą do grupy obciążeń Użytkownicy. Łącznie jest to 10 500 obciążeń, co oznacza przekroczenie limitu 10 000 obciążeń w grupie. W związku z tym widżet będzie ukrywać odpowiadające im typy obciążeń: Skrzynki pocztowe Microsoft 365 i Microsoft 365 OneDrive.
Podsumowanie ochrony cybernetycznej	Ten widżet przedstawia kluczowe wskaźniki wydajności ochrony cybernetycznej we wskazanym okresie. **Dane uwzględnione w kopii zapasowej** — łączny rozmiar archiwów utworzonych w chmurze i magazynach lokalnych. **Ograniczone zagrożenia** — całkowita liczba złośliwych programów zablokowanych na wszystkich urządzeniach. **Zablokowane złośliwe adresy URL** — łączna liczba adresów URL zablokowanych na wszystkich urządzeniach. **Luki w zabezpieczeniach, do których zastosowano poprawki** — łączna liczba luk w zabezpieczeniach wyeliminowanych przez zainstalowanie poprawek oprogramowania na wszystkich urządzeniach. **Zainstalowane poprawki** — łączna liczba zainstalowanych poprawek na wszystkich urządzeniach. **Serwery chronione przez usługę Odzyskiwanie po awarii** — łączna liczba serwerów chronionych przy użyciu usługi Odzyskiwanie po awarii.

Widżet	Opis
	Użytkownicy usługi File Sync & Share — łączna liczba użytkowników i gości korzystających z rozwiązania Cyber Files. **Notaryzowane pliki** — łączna liczba notaryzowanych plików. **Dokumenty podpisane elektronicznie** — łączna liczba dokumentów podpisanych elektronicznie. **Zablokowane urządzenia peryferyjne** — łączna liczba zablokowanych urządzeń peryferyjnych.
Status sieciowy obciążeń	Ten widżet wskazuje, ile obciążeń jest odizolowanych i ile połączonych (jest to normalny stan obciążenia). Wybierz odpowiedniego klienta. Wyświetlony widok obciążeń zostanie przefiltrowany w celu wyświetlenia odizolowanych obciążeń. Kliknij wartość Podłączono, aby wyświetlić listę obciążeń z agentami przefiltrowaną w celu wyświetlenia połączonych obciążeń (w kontekście wybranego klienta).
Status ochrony obciążeń	Ten widżet przedstawia chronione i niechronione obciążenia według typów w chwili wygenerowania raportu. Obciążenia chronione to obciążenia, do których zastosowano co najmniej jeden plan ochrony lub plan tworzenia kopii zapasowych. Obciążenia niechronione to obciążenia, do których nie zastosowano żadnego planu ochrony ani planu tworzenia kopii zapasowych. Wliczane są następujące obciążenia: **Serwery** — serwery fizyczne i serwery będące kontrolerami domen. **Stacje robocze** — fizyczne stacje robocze. **Maszyny wirtualne** — maszyny wirtualne z agentami i bez agentów. **Serwery hostingu witryn internetowych** — serwery wirtualne lub fizyczne z zainstalowanymi panelami sterowania cPanel lub Plesk. **Urządzenia mobilne** — fizyczne urządzenia mobilne. Jedno obciążenie może należeć do więcej niż jednej kategorii. Na przykład serwer hostingu witryn internetowych jest wliczany do dwóch kategorii: **Serwery** i **Serwery hostingu witryn internetowych**.

Widżety usługi Ochrona przed złośliwym oprogramowaniem

Poniższa tabela zawiera dodatkowe informacje na temat widżetów dostępnych w sekcji **Obrona przed zagrożeniami**.

Widżet	Opis
Skanowanie antywirusowe plików	Ten widżet przedstawia wyniki wykonywanego na żądanie skanowania antywirusowego urządzeń we wskazanym okresie. **Pliki** — łączna liczba przeskanowanych plików.

Widżet	Opis
	Czyste — łączna liczba czystych plików. **Wykryto, zastosowano kwarantannę** — łączna liczba zainfekowanych plików poddanych kwarantannie. **Wykryto, nie zastosowano kwarantanny** — łączna liczba zainfekowanych plików, których nie poddano kwarantannie. **Chronione urządzenia** — łączna liczba urządzeń z zastosowanymi zasadami ochrony przed złośliwym oprogramowaniem. **Łączna liczba zarejestrowanych urządzeń** — łączna liczba zarejestrowanych urządzeń w czasie generowania raportu.
Skanowanie antywirusowe kopii zapasowych	Ten widżet przedstawia wyniki skanowania antywirusowego kopii zapasowych we wskazanym okresie według następujących wskaźników: • Łączna liczba przeskanowanych punktów odzyskiwania • Liczba czystych punktów odzyskiwania • Liczba czystych punktów odzyskiwania z nieobsługiwanymi partycjami • Liczba zainfekowanych punktów odzyskiwania — ten wskaźnik obejmuje liczbę zainfekowanych punktów odzyskiwania z nieobsługiwanymi partycjami.
Zablokowane adresy URL	Ten widżet przedstawia liczbę zablokowanych adresów URL we wskazanym okresie pogrupowanych według kategorii witryn. W widżecie jest wymienionych siedem kategorii witryn internetowych, w których przypadku odnotowano największą liczbę zablokowanych adresów URL. Pozostałe kategorie witryn są wyświetlane łącznie i oznaczone jako **Inne**. Więcej informacji na temat kategorii witryn można znaleźć w temacie Filtrowanie adresów URL w sekcji Cyber Protection.
Wykres spalania dotyczący incydentów bezpieczeństwa	Ten widżet przedstawia wskaźnik efektywności zamykania incydentów w ramach wybranej firmy. Liczba otwartych incydentów jest ujmowana w stosunku do liczby zamkniętych incydentów w danym okresie. Zatrzymaj wskaźnik myszy na dowolnej kolumnie, aby wyświetlić podział zamkniętych i otwartych incydentów z wybranego dnia. Wartość % podana w nawiasie oznacza wzrost lub spadek w porównaniu z poprzednim okresem.
Średni czas rozwiązywania problemu incydentu	Na tym widżecie jest przedstawiany średni czas rozwiązywania problemu związanego z incydentem bezpieczeństwa. Wskazuje on, jak szybko problemy incydentów są badane w ramach dochodzenia i rozwiązywane. Kliknij kolumnę, aby wyświetlić podział incydentów według ich ważności (**Krytyczne**, **Wysoki** i **Średni**) oraz wskazanie, ile czasu zajęło rozwiązanie problemu o różnym poziomie ważności. Wartość % podana w nawiasie oznacza wzrost lub spadek w porównaniu z poprzednim okresem.

Widżet	Opis
Status zagrożeń	Ten widżet przedstawia aktualny status zagrożeń w przypadku obciążeń w firmie (niezależnie od liczby obciążeń) z wyraźnym zaznaczeniem bieżącej liczby incydentów, których skutki nie zostały zniwelowane i które wymagają dochodzeń. Widżet wskazuje również liczbę incydentów, których skutki zostały zniwelowane (ręcznie i/lub automatycznie przez system).
Wykryte zagrożenia według technologii ochrony	Ten widżet przedstawia liczbę wykrytych zagrożeń we wskazanym okresie pogrupowanych według następujących technologii ochrony: • Skanowanie antywirusowe • Mechanizm zachowań • Ochrona przed cryptominingiem • Ochrona przed exploitami • Aktywna ochrona przed ransomware • Ochrona w czasie rzeczywistym • Filtrowanie adresów URL

Widżety usługi Kopia zapasowa

Poniższa tabela zawiera dodatkowe informacje na temat widżetów dostępnych w sekcji **Kopia zapasowa**.

Widżet	Opis
Obciążenia uwzględnione w kopii zapasowej	Ten widżet przedstawia łączną liczbę zarejestrowanych obciążeń według statusów kopii zapasowych. **Utworzono kopię zapasową** — liczba obciążeń uwzględnionych w kopii zapasowej (wykonano co najmniej jedną udaną kopię zapasową) w okresie ujętym w raporcie. **Nie utworzono kopii zapasowej** — liczba obciążeń, które nieuwzględnionych w kopii zapasowej (nie wykonano żadnej udanej kopii zapasowej) w okresie ujętym w raporcie.
Status kondycji dysków według urządzeń fizycznych	Ten widżet przedstawia zagregowany status kondycji urządzeń fizycznych oceniony na podstawie statusów kondycji ich dysków. **OK** — ten status kondycji dysków dotyczy wartości [70–100]. Urządzenie ma status **OK**, gdy wszystkie jego dyski mają status **OK**. **Ostrzeżenie** — ten status kondycji dysków dotyczy wartości [30–70]. Urządzenie ma status **Ostrzeżenie**, gdy status choćby jednego z jego dysków ma status **Ostrzeżenie** i żaden z pozostałych dysków nie ma statusu **Błąd**. **Błąd** — ten status kondycji dysków dotyczy wartości [0–30]. Urządzenie ma status **Błąd**, gdy status choćby jednego z jego dysków ma status **Błąd**.

Widżet	Opis
	Obliczanie danych dysku — urządzenie ma status **Obliczanie danych dysku**, gdy jeszcze nie obliczono statusów jego dysków.
Wykorzystanie magazynu kopii zapasowych	Ten widżet przedstawia łączną liczbę i łączny rozmiar kopii zapasowych w chmurze oraz magazynie lokalnym we wskazanym okresie.

Widżety usługi Ocena luk w zabezpieczeniach i zarządzanie poprawkami

Poniższa tabela zawiera dodatkowe informacje na temat widżetów dostępnych w sekcji **Ocena luk w zabezpieczeniach i zarządzanie poprawkami**.

Widżet	Opis
Luki w zabezpieczeniach, do których zastosowano poprawki	Ten widżet przedstawia wyniki wykonania oceny luk w zabezpieczeniach we wskazanym okresie. **Łącznie** — łączna liczba luk w zabezpieczeniach, do których zastosowano poprawki. **Luki w zabezpieczeniach oprogramowania firmy Microsoft** — łączna liczba usuniętych luk w zabezpieczeniach oprogramowania Microsoft na wszystkich urządzeniach z systemem Windows. **Luki w zabezpieczeniach oprogramowania innych firm przeznaczonego do systemu Windows** — łączna liczba usuniętych luk w zabezpieczeniach oprogramowania innych firm przeznaczonego do systemu Windows na wszystkich urządzeniach z systemem Windows. **Przeskanowane obciążenia** — łączna liczba urządzeń, które zostały pomyślnie przeskanowane pod kątem luk w zabezpieczeniach co najmniej raz we wskazanym okresie.
Zainstalowane poprawki	Ten widżet przedstawia wyniki zarządzania poprawkami we wskazanym okresie. **Zainstalowane** — łączna liczba poprawek pomyślnie zainstalowanych na wszystkich urządzeniach. **Poprawki do oprogramowania firmy Microsoft** — łączna liczba poprawek do oprogramowania firmy Microsoft pomyślnie zainstalowanych na wszystkich urządzeniach z systemem Windows. **Poprawki do oprogramowania innych firm przeznaczonego do systemu Windows** — łączna liczba poprawek do oprogramowania innych firm przeznaczonego do systemu Windows pomyślnie zainstalowanych na wszystkich urządzeniach z systemem Windows. **Obciążenia z zastosowanymi poprawkami** — łączna liczba urządzeń, do których pomyślnie zastosowano poprawki (co najmniej jedna poprawka pomyślnie zainstalowana we wskazanym okresie).

Widżety usługi Odzyskiwanie po awarii

Poniższa tabela zawiera dodatkowe informacje na temat widżetów dostępnych w sekcji **Odzyskiwanie po awarii**.

Widżet	Opis
Statystyki usługi Odzyskiwanie po awarii	Ten widżet przedstawia kluczowe wskaźniki wydajności odzyskiwania po awarii we wskazanym okresie. **Produkcyjne przełączenia awaryjne** — liczba operacji produkcyjnego przełączania awaryjnego we wskazanym okresie. **Testowe przełączenia awaryjne** — liczba operacji testowego przełączania awaryjnego wykonanych we wskazanym okresie. **Serwery podstawowe** — łączna liczba serwerów podstawowych w chwili wygenerowania raportu. **Serwery odzyskiwania** — łączna liczba serwerów odzyskiwania w chwili wygenerowania raportu. **Publiczne adresy IP** — łączna liczba publicznych adresów IP w chwili wygenerowania raportu. **Wykorzystane punkty obliczeniowe łącznie** — łączna liczba punktów obliczeniowych wykorzystanych we wskazanym okresie.
Przetestowane serwery odzyskiwania po awarii	Ten widżet przedstawia informacje o serwerach chronionych przez usługę Odzyskiwanie po awarii i przetestowanych przez wykonanie testowego przełączenia awaryjnego. Ten widżet przedstawia następujące wskaźniki: **Chronione serwery** — liczba serwerów chronionych przez usługę Odzyskiwanie po awarii (serwerów mających co najmniej jeden serwer odzyskiwania) w chwili wygenerowania raportu. **Przetestowane** — liczba serwerów chronionych przez usługę Odzyskiwanie po awarii przetestowanych przy użyciu testowego przełączania awaryjnego we wskazanym okresie spośród wszystkich serwerów chronionych przez usługę Odzyskiwanie po awarii. **Nieprzetestowane** — liczba serwerów chronionych przez usługę Odzyskiwanie po awarii nieprzetestowanych przy użyciu testowego przełączania awaryjnego we wskazanym okresie spośród wszystkich serwerów chronionych przez usługę Odzyskiwanie po awarii. Ten widżet przedstawia również rozmiar magazynu odzyskiwania po awarii (w GB) w chwili wygenerowania raportu. Jest to suma rozmiarów kopii zapasowych serwerów chmurowych.
Serwery	Ten widżet przedstawia informacje o serwerach chronionych przez usługę

Widżet	Opis
chronione przy użyciu usługi Odzyskiwanie po awarii	Odzyskiwanie po awarii i serwerach niechronionych. Ten widżet przedstawia następujące wskaźniki: Łączna liczba serwerów zarejestrowanych w ramach dzierżawcy-klienta w chwili wygenerowania raportu. **Chronione** — liczba serwerów chronionych przez usługę Odzyskiwanie po awarii (mających co najmniej jeden serwer odzyskiwania i kopię zapasową całego serwera) spośród wszystkich zarejestrowanych serwerów w chwili wygenerowania raportu. **Niechronione** — łączna liczba niechronionych serwerów spośród wszystkich zarejestrowanych serwerów w chwili wygenerowania raportu.

Widżet usługi Zapobieganie utracie danych

Poniższy temat zawiera dodatkowe informacje na temat zablokowanych urządzeń peryferyjnych w sekcji **Zapobieganie utracie danych**.

Ten widżet przedstawia łączną liczbę zablokowanych urządzeń we wskazanym okresie i łączną liczbę zablokowanych urządzeń według ich typów.

- Magazyn wymienny
- Zaszyfrowane urządzenie wymienne
- Drukarki
- Schowek — obejmuje typy urządzeń powiązane ze schowkiem i do rejestrowania zrzutów ekranu.
- Urządzenia mobilne
- Bluetooth
- Dyski optyczne
- Dyskietki
- USB — obejmuje typy urządzeń do portów USB i przekierowywanych portów USB.
- FireWire
- Zamapowane dyski
- Przekierowane dane schowka — obejmuje typy urządzeń powiązane z przychodzącymi i wychodzącymi przekierowanymi danymi schowka.

Ten widżet przedstawia pierwsze siedem typów urządzeń, w których przypadku odnotowano najwyższą liczbę zablokowanych urządzeń, a pozostałe typy urządzeń są wyświetlane łącznie i oznaczone jako **Inne**.

Widżety usługi File Sync & Share

Poniższa tabela zawiera dodatkowe informacje na temat widżetów dostępnych w sekcji **File Sync & Share**.

Widżet	Opis
Statystyki usługi File Sync & Share	Ten widżet przedstawia następujące wskaźniki: **Łączne wykorzystanie pamięci w chmurze** — łączne wykorzystanie magazynu przez wszystkich użytkowników. **Użytkownicy** — łączna liczba użytkowników. **Średnie wykorzystanie magazynu na użytkownika** — średnie wykorzystanie magazynu na użytkownika. **Użytkownicy-goście** — łączna liczba użytkowników-gości.
Wykorzystanie magazynu usługi File Sync & Share przez użytkowników	Ten widżet przedstawia łączne liczby użytkowników usługi File Sync & Share korzystających z magazynu w następujących zakresach: • 0–1 GB • 1–5 GB • 5–10 GB • 10–50 GB • 50–100 GB • 100–500 GB • 500 GB–1 TB • 1+ TB

Widżety usługi Notary

Poniższa tabela zawiera dodatkowe informacje na temat widżetów dostępnych w sekcji **Notary**.

Widżet	Opis
Statystyki usługi Cyber Notary	Ten widżet przedstawia następujące wskaźniki dotyczące usługi Notary: **Wykorzystanie pamięci w chmurze usługi Notary** — łączny rozmiar magazynu wykorzystywany na potrzeby usługi Notary. **Notaryzowane pliki** — łączna liczba notaryzowanych plików. **Dokumenty podpisane elektronicznie** — łączna liczba dokumentów i plików podpisanych elektronicznie.
Notaryzowane pliki użytkowników	Przedstawia łączną liczbę notaryzowanych plików wszystkich użytkowników. Użytkownicy są pogrupowani według liczb swoich notaryzowanych plików.

Widżet	Opis
	• Do 10 plików • 11–100 plików • 101–500 plików • 501–1000 plików • 1000+ plików
Podpisane elektronicznie dokumenty użytkowników	Ten widżet przedstawia łączną liczbę podpisanych elektronicznie dokumentów i plików wszystkich użytkowników. Użytkownicy są pogrupowani według liczb swoich dokumentów i plików podpisanych elektronicznie. • Do 10 plików • 11–100 plików • 101–500 plików • 501–1000 plików • 1000+ plików

Konfigurowanie ustawień raportu podsumowującego

Ustawienia raportu skonfigurowane podczas tworzenia raportu podsumowującego można zaktualizować.

Aby zaktualizować ustawienia raportu podsumowującego

1. W konsoli zarządzania przejdź do sekcji **Raporty** > **Podsumowanie**.
2. Kliknij nazwę raportu podsumowującego, który chcesz zaktualizować.
3. Kliknij **Ustawienia**.
4. Zmień wartości pól stosownie do potrzeb.
5. Kliknij **Zapisz**.

Tworzenie raportu podsumowującego

Można utworzyć raport podsumowujący, wyświetlić podgląd jego zawartości, skonfigurować odbiorców raportu i zaplanować jego automatyczne wysłanie.

Aby utworzyć raport podsumowujący

1. W konsoli zarządzania przejdź do sekcji **Raporty** > **Podsumowanie**.
2. Kliknij **Utwórz raport podsumowujący**.
3. W polu **Nazwa raportu** wpisz nazwę raportu.
4. Wybierz odbiorców raportu.

- Jeśli chcesz wysłać raport do wszystkich kontaktów i użytkowników, wybierz **Wyślij do wszystkich kontaktów i użytkowników**.
- Jeśli chcesz wysłać raport do wybranych kontaktów i użytkowników
  a. Wyczyść pole wyboru **Wyślij do wszystkich kontaktów i użytkowników**.
  b. Kliknij **Wybierz kontakty**.
  c. Wybierz kontakty i użytkowników. Aby łatwo znaleźć określony kontakt, możesz skorzystać z pola Szukaj.
  d. Kliknij **Wybierz**.

5. Wybierz zakres: **30 dni** lub **Ten miesiąc**
6. Wybierz format pliku: **PDF**, **Excel** lub **Excel i PDF**.
7. Skonfiguruj ustawienia harmonogramu.
   - Jeśli chcesz wysłać raport do wybranych odbiorców w określonym dniu o określonej godzinie:
     a. Włącz opcję **Zaplanowane**.
     b. Kliknij **Dzień miesiąca**, wyczyść pole Ostatni dzień i kliknij odpowiednią datę.
     c. W polu **Godzina** wprowadź odpowiednią godzinę.
     d. Kliknij **Zastosuj**.
   - Jeśli chcesz utworzyć raport bez wysyłania go do odbiorców, wyłącz opcję **Zaplanowane**.
8. Kliknij **Zapisz**.

Dostosowywanie raportu podsumowującego

Można określać, jakie informacje mają być zawarte w raporcie podsumowującym. Można dodawać lub usuwać sekcje, dodawać lub usuwać widżety, zmieniać nazwy sekcji, dostosowywać widżety oraz przeciągać widżety i sekcje, aby zmienić kolejność wyświetlania informacji w raporcie.

Aby dodać sekcję

1. Kliknij **Dodaj element** > **Dodaj sekcję**.
2. W oknie **Dodaj sekcję** wpisz nazwę sekcji lub użyj nazwy domyślnej.
3. Kliknij **Dodaj do raportu**.

Aby zmienić nazwę sekcji

1. W sekcji, której nazwę chcesz zmienić, kliknij **Edytuj**.
2. W oknie **Edytuj sekcję** wpisz nową nazwę.
3. Kliknij **Zapisz**.

Aby usunąć sekcję

1. W sekcji, którą chcesz usunąć, kliknij **Usuń sekcję**.
2. W oknie potwierdzenia operacji **Usuń sekcję** kliknij **Usuń**.

Aby dodać do sekcji widżet z ustawieniami domyślnymi

1. W sekcji, do której chcesz dodać widżet, kliknij **Dodaj widżet**.
2. W oknie **Dodaj widżet** kliknij widżet, który chcesz dodać.

Aby dodać do sekcji dostosowany widżet

1. W sekcji, do której chcesz dodać widżet, kliknij **Dodaj widżet**.
2. W oknie **Dodaj widżet** znajdź widżet, który chcesz dodać, i kliknij **Dostosuj**.
3. Skonfiguruj pola stosownie do potrzeb.
4. Kliknij **Dodaj widżet**.

Aby dodać do raportu widżet z ustawieniami domyślnymi

1. Kliknij **Dodaj element** > **Dodaj widżet**.
2. W oknie **Dodaj widżet** kliknij widżet, który chcesz dodać.

Aby dodać do raportu dostosowany widżet

1. Kliknij **Dodaj widżet**.
2. W oknie **Dodaj widżet** znajdź widżet, który chcesz dodać, i kliknij **Dostosuj**.
3. Skonfiguruj pola stosownie do potrzeb.
4. Kliknij **Dodaj widżet**.

Aby zresetować ustawienia domyślne widżetu

1. W widżecie, który chcesz dostosować, kliknij **Edytuj**.
2. Kliknij **Przywróć domyślne**.
3. Kliknij **Gotowe**.

Aby dostosować widżet

1. W widżecie, który chcesz dostosować, kliknij **Edytuj**.
2. Edytuj pola stosownie do potrzeb.
3. Kliknij **Gotowe**.

Wysyłanie raportów podsumowujących

Raport podsumowujący można wysłać na żądanie. W takim przypadku ustawienie **Zaplanowane** jest ignorowane i raport zostaje niezwłocznie wysłany. W przypadku wysyłania raportu system korzysta z ustawień Odbiorcy, Zakres i Format pliku skonfigurowanych w sekcji **Ustawienia**.

Ustawienia te można ręcznie zmienić przed wysłaniem raportu. Aby uzyskać więcej informacji, zobacz "Konfigurowanie ustawień raportu podsumowującego" (s. 76).

Aby wysłać raport podsumowujący

1. W portalu zarządzania przejdź do sekcji **Raporty** > **Podsumowanie**.
2. Kliknij nazwę raportu podsumowującego, który chcesz wysłać.
3. Kliknij **Wyślij teraz**.
   System wyśle raport podsumowujący do wybranych odbiorców.

Strefy czasowe w raportach

Strefy czasowe stosowane w raportach różnią się w zależności od typu raportu. Poniższa tabela zawiera odpowiednie informacje referencyjne.

Lokalizacja i typ raportu	Strefa czasowa w raporcie
Portal zarządzenia > Przegląd > Operacje (widżety)	Czas wygenerowania raportu jest zgodny ze strefą czasową komputera, na którym działa przeglądarka.
Portal zarządzenia > Przegląd > Operacje (eksportowany jako PDF lub xslx)	• Sygnatura czasowa wyeksportowanego raportu jest zgodna ze strefą czasową komputera użytego do wyeksportowania raportu. • Strefą czasową działań widocznych w raporcie jest UTC.
Portal zarządzania > Raporty > Użytkowanie > Zaplanowane raporty	• Raport jest generowany pierwszego dnia miesiąca o godzinie 23:59:59 czasu UTC. • Jest wysyłany drugiego dnia miesiąca.
Portal zarządzania > Raporty > Użytkowanie > Raporty niestandardowe	Strefą czasową i datą raportu jest UTC.
Portal zarządzenia > Raporty > Operacje (widżety)	• Czas wygenerowania raportu jest zgodny ze strefą czasową komputera, na którym działa przeglądarka. • Strefą czasową działań widocznych w raporcie jest UTC.
Portal zarządzenia > Raporty > Operacje (eksportowany jako PDF lub xslx)	• Sygnatura czasowa wyeksportowanego raportu jest zgodna ze strefą czasową komputera użytego do wyeksportowania raportu. • Strefą czasową działań widocznych w raporcie jest UTC.
Portal zarządzenia > Raporty > Operacje (zaplanowane dostarczenie)	• Strefą czasową dostarczenia raportu jest UTC. • Strefą czasową działań widocznych w raporcie jest UTC.
Portal zarządzania > Użytkownicy >	• Ten raport jest wysyłany raz dziennie między 10:00 a 23:59

Codzienne zestawienie aktywnych alertów	czasu UTC. Godzina wysłania raportu zależy od obciążenia centrum danych. • Strefą czasową działań widocznych w raporcie jest UTC.
Portal zarządzania > Użytkownicy > Powiadomienia o statusie cyberochrony	• Ten raport jest wysyłany po zakończeniu działania. **Uwaga** Niektóre raporty mogą być wysyłane z opóźnieniem — w zależności od obciążenia centrum danych. • Strefą czasową działania w raporcie jest UTC.

Raportowane dane zależnie od typu widżetu

Ze względu na wyświetlany zakres danych można wyróżnić dwa rodzaje widżetów na pulpicie nawigacyjnym:

- Widżety wyświetlające dane aktualne w chwili przeglądania lub generowania raportu.
- Widżety wyświetlające dane historyczne.

W przypadku skonfigurowania zakresu dat w ustawieniach raportu w celu utworzenia zrzutu danych z pewnego okresu, wybrany zakres czasu będzie miał zastosowanie tylko do widżetów wyświetlających dane historyczne. W przypadku widżetów wyświetlających dane aktualne w chwili przeglądania lub generowania raportu parametr zakresu czasu nie ma zastosowania.

W poniższej tabeli zamieszczono listę dostępnych widżetów i ich zakresów dat.

Nazwa widżetu	Dane wyświetlane w widżetach i raportach
Wynik #CyberFit według komputerów	Aktualne
5 ostatnich alertów	Aktualne
Szczegóły aktywnych alertów	Aktualne
Podsumowanie aktywnych alertów	Aktualne
Działania	Historyczne
Lista działań	Historyczne
Historia alertów	Historyczne
Skanowanie antywirusowe kopii zapasowych	Historyczne
Skanowanie antywirusowe plików	Historyczne
Szczegóły skanowania kopii zapasowej (zagrożenia)	Historyczne
Status kopii zapasowej	Historyczne — w kolumnach **Operacje łącznie** i

	Liczba pomyślnych operacji Aktualne — w pozostałych kolumnach
Wykorzystanie magazynu kopii zapasowych	Historyczne
Zablokowane urządzenia peryferyjne	Historyczne
Zablokowane adresy URL	Aktualne
Aplikacje w chmurze	Aktualne
Status ochrony obciążeń w chmurze	Aktualne
Cyber protection	Aktualne
Podsumowanie ochrony cybernetycznej	Historyczne
Mapa ochrony danych	Historyczne
Urządzenia	Aktualne
Przetestowane serwery odzyskiwania po awarii	Historyczne
Statystyki odzyskiwania po awarii	Historyczne
Wykryte komputery	Aktualne
Przegląd kondycji dysków	Aktualne
Status kondycji dysków	Aktualne
Status kondycji dysków według urządzeń fizycznych	Aktualne
Podpisane elektronicznie dokumenty użytkowników	Aktualne
Występujące luki w zabezpieczeniach	Historyczne
Statystyki usługi File Sync & Share	Aktualne
Wykorzystanie magazynu usługi File Sync & Share przez użytkowników	Aktualne
Zmiany sprzętowe	Historyczne
Szczegóły sprzętu	Aktualne
Inwentaryzacja sprzętu	Aktualne
Historyczne zestawienie alertów	Historyczne
Podsumowanie lokalizacji	Aktualne
Brakujące aktualizacje według kategorii	Aktualne

Niechroniony	Aktualne
Notaryzowane pliki użytkowników	Aktualne
Statystyki usługi Notary	Aktualne
Historia instalacji poprawek	Historyczne
Status instalacji poprawek	Historyczne
Podsumowanie instalacji poprawek	Historyczne
Luki w zabezpieczeniach, do których zastosowano poprawki	Historyczne
Zainstalowane poprawki	Historyczne
Status ochrony	Aktualne
Ostatnie objęte wpływem	Historyczne
Sesje zdalne	Historyczne
Wykres spalania dotyczący incydentów bezpieczeństwa	Historyczne
Średni czas rozwiązywania problemu incydentu bezpieczeństwa	Historyczne
Serwery chronione przez usługę Odzyskiwanie po awarii	Aktualne
Inwentaryzacja oprogramowania	Aktualne
Przegląd oprogramowania	Historyczne
Status zagrożeń	Aktualne
Wykryte zagrożenia według technologii ochrony	Historyczne
Podział najliczniejszych incydentów według obciążeń	Aktualne
Komputery z lukami w zabezpieczeniach	Aktualne
Status sieciowy obciążeń	Aktualne
Obciążenia uwzględnione w kopii zapasowej	Historyczne
Status ochrony obciążeń	Aktualne

Integracje

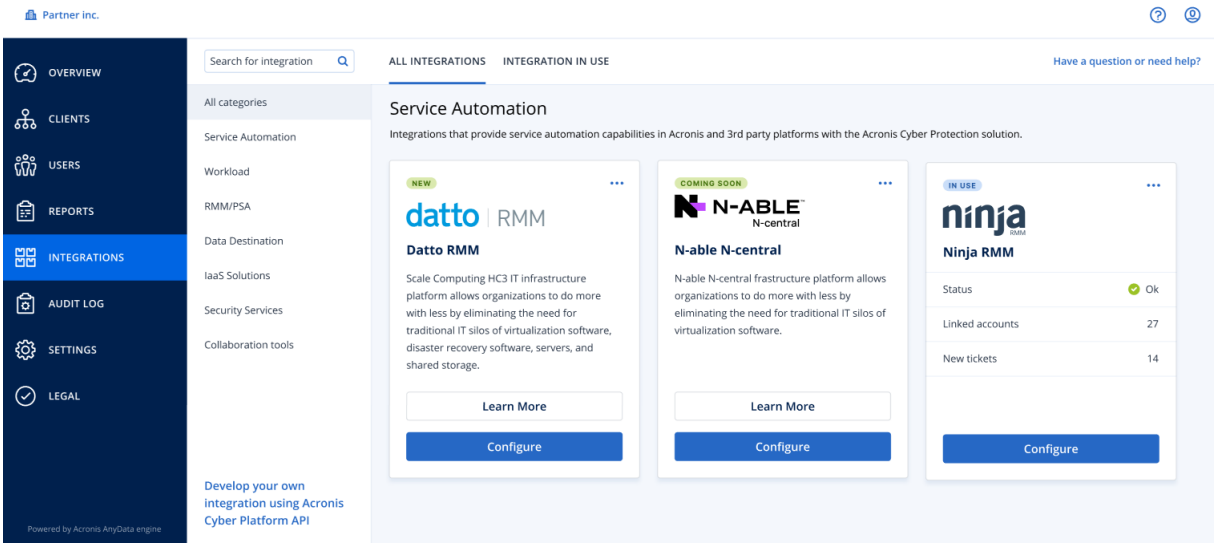
Katalog integracji

Ta strona to globalny punkt, w którym są rejestrowane i aktualizowane wszystkie aplikacje integracji. W tym miejscu można dodawać nowe integracje lub modyfikować istniejące.

Uwaga
Tylko użytkownicy z rolą **Administrator firmy** mają uprawnienia do zmiany konfiguracji integracji.

Wszystkie integracje

Na karcie **Wszystkie integracje** znajduje się lista wszystkich aktualnie dostępnych integracji, uporządkowanych obok siebie jako kafelki.



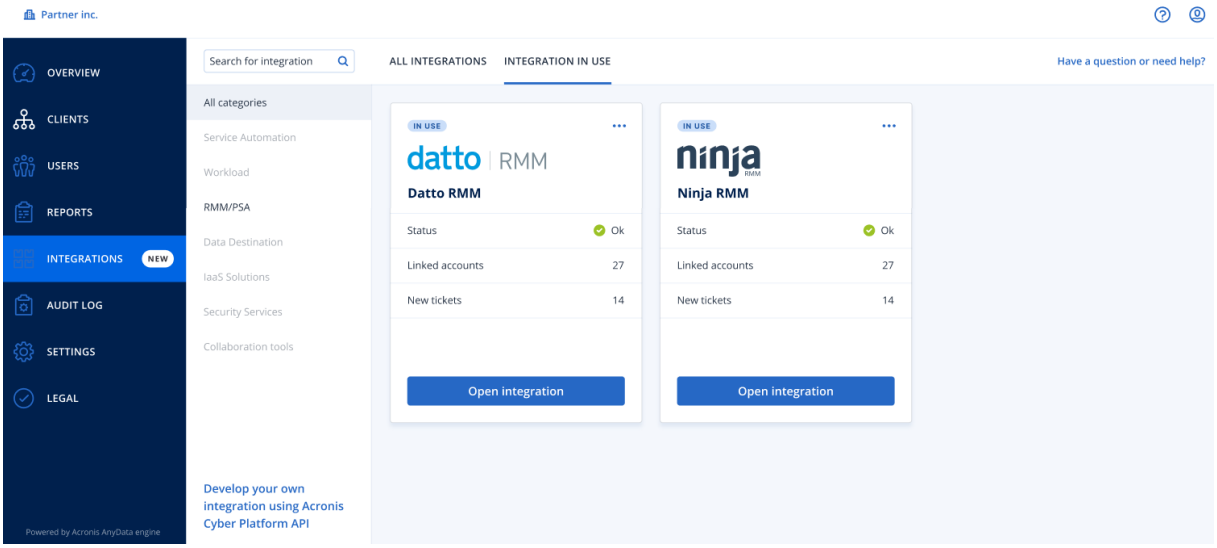
Na każdym kafelku znajduje się krótki opis produktu oraz dwie dodatkowe opcje:

- **Dowiedz się więcej** — kliknij ten przycisk, aby zobaczyć więcej szczegółów na temat konkretnej integracji:
  - **Funkcje integracji**
  - **Linki do dokumentacji**
  - **Dane kontaktowe pomocy technicznej**
- **Konfiguruj** — użyj tej opcji, aby edytować niektóre ustawienia integracji.

Kafelki reprezentujące nieaktywne integracje są wyszarzone i wyłączone. Mogą też mieć etykietę **„coming soon”**.

Używane integracje

Na karcie **Używane integracje** znajduje się lista wszystkich aktywnych integracji, a każdej z nich towarzyszą ogólne informacje.



Kliknij **Otwórz integrację**, aby uzyskać bezpośredni dostęp do odpowiedniej aplikacji.

Po lewej stronie znajduje się lista kategorii integracji, na której wszystkie istniejące aplikacje są sklasyfikowane w określonych grupach, takich jak automatyzacja usług, obciążenie, RMM/PSA itp. Kliknięcie jednej z kategorii spowoduje wyświetlenie integracji należących do tej konkretnej grupy. Aktualnie wyświetlana kategoria jest wyróżniona.

Za pomocą opcji **Szukaj** można tworzyć zapytania i szukać konkretnych integracji.

Listę integracji można filtrować według kategorii i etykiet. Etykiety są sortowane alfabetycznie. W przypadku braku wyników wyszukiwania poszerz kryteria wyszukiwania, aby objąć więcej kategorii.

Aby wyłączyć aplikację, kliknij ikonę wielokropka (...) w prawym górnym rogu kafelka i wybierz opcję **Dezaktywuj**.

Dostępny jest też link do dokumentacji interfejsu Acronis API dla osób zainteresowanych opracowywaniem własnych integracji.

Ograniczanie dostępu do interfejsu internetowego

Dostęp do interfejsu internetowego można ograniczyć, określając listę adresów IP, z których mogą się logować użytkownicy.

To ograniczenie dotyczy również dostępu do portalu zarządzania za pośrednictwem interfejsu API.

Ograniczenie to dotyczy tylko poziomu, na którym zostało ustawione. *Nie* jest ono stosowane w przypadku członków jednostek podrzędnych.

Aby ograniczyć dostęp do interfejsu internetowego

1. Zaloguj się do portalu zarządzania.
2. Przejdź do jednostki, w której przypadku chcesz ograniczyć dostęp.
3. Kliknij **Ustawienia** > **Zabezpieczenia**.
4. Zaznacz pole wyboru **Włącz kontrolę logowania**.
5. W polu **Dozwolone adresy IP** określ dozwolone adresy IP.
   Możesz wprowadzić dowolne z poniższych parametrów, oddzielając je średnikiem:
   - Adresy IP, na przykład: 192.0.2.0
   - Zakresy adresów IP, na przykład: 192.0.2.0–192.0.2.255
   - Podsieci, na przykład: 192.0.2.0/24
6. Kliknij **Zapisz**.

Ograniczanie dostępu do firmy

Administratorzy firmy mogą ograniczać do niej dostęp administratorom wyższych poziomów.

Jeśli dostęp do firmy jest ograniczony, administratorzy wyższych poziomów mogą tylko modyfikować właściwości firmy. Konta użytkowników ani jednostki podrzędne nie są dla nich widoczne.

Aby ograniczyć dostęp do firmy

1. Zaloguj się do portalu zarządzania.
2. Kliknij **Ustawienia** > **Zabezpieczenia**.
3. Wyłącz opcję **Dostęp do pomocy technicznej**.
4. Kliknij **Zapisz**.

Zarządzanie klientami API

Istnieje możliwość zintegrowania systemów innych firm z platformą Cyber Protect Cloud za pomocą jej interfejsów programowania aplikacji (application programming interface, API). Dostęp do interfejsów API można uzyskać za pośrednictwem klientów API, które stanowią integralną część środowiska autoryzacji OAuth 2.0 tej platformy.

Co to jest klient API?

Klient API to specjalne konto na platformie przeznaczone do reprezentowania systemu zewnętrznego, który musi się uwierzytelnić oraz uzyskać prawa dostępu do danych w interfejsach API platformy i jej usług.

Dostęp klienta jest ograniczony do dzierżawcy, w którego ramach administrator tworzy klienta, a także jego poddzierżawców.

Tworzony klient dziedziczy role usług konta administratora i ról tych nie można później zmienić. Zmiana lub wyłączenie ról konta administratora nie wpływa na klienta.

Poświadczenia klienta obejmują unikatowy identyfikator (ID) oraz wartość tajną. Te poświadczenia nie wygasają i nie można ich używać do logowania się do portalu zarządzania czy którejkolwiek konsoli usługi. Wartość tajną można zresetować.

Dla klienta nie można włączyć uwierzytelniania dwuskładnikowego.

Standardowa procedura integracji

1. Administrator tworzy klienta API w ramach dzierżawcy, którym będzie zarządzać system zewnętrzny.
2. Administrator włącza przepływ poświadczeń klienta OAuth 2.0 w systemie zewnętrznym.
   Zgodnie z tym przepływem przed uzyskaniem dostępu do dzierżawcy i jego usług za pośrednictwem interfejsu API system powinien najpierw wysłać do platformy poświadczenia utworzonego klienta za pośrednictwem autoryzacyjnego interfejsu API. Platforma generuje i wysyła systemowi token zabezpieczeń, czyli unikatowy ciąg kryptograficzny przypisany do tego konkretnego klienta. Potem system musi dodawać ten token do wszystkich żądań API.
   Token zabezpieczeń eliminuje konieczność przekazywania poświadczeń klienta razem z żądaniami API. Dla dodatkowego bezpieczeństwa token wygasa po dwóch godzinach. Gdy się to stanie, wszystkie żądania API z wygasłym tokenem zakończą się niepowodzeniem i system będzie zażądać od platformy nowego tokenu.

Więcej informacji na temat korzystania z autoryzacyjnego interfejsu API i interfejsów API platformy można znaleźć w podręczniku dewelopera pod adresem https://developer.acronis.com/doc/account-management/v2/guide/index.

Tworzenie klienta API

1. Zaloguj się do portalu zarządzania.
2. Kliknij **Ustawienia** > **Klienty API** > **Utwórz klienta API**.
3. Wprowadź nazwę klienta API.
4. Kliknij **Dalej**.
   Klient API jest domyślnie tworzony ze statusem **Aktywny**.
5. Skopiuj i zapisz identyfikator oraz wartość tajną klienta, a także adres URL centrum danych. Dane te będą potrzebne do włączenia przepływu poświadczeń klienta OAuth 2.0 w systemie zewnętrznym.

   Ważne
   Ze względów bezpieczeństwa wartość tajna jest wyświetlana tylko raz. W razie utraty tej wartości nie da się jej odzyskać — można ją tylko zresetować.

6. Kliknij **Gotowe**.

Resetowanie wartości tajnej klienta API

1. Zaloguj się do portalu zarządzania.
2. Kliknij **Ustawienia** > **Klienty API**.
3. Znajdź pożądanego klienta na liście.
4. Kliknij  , a następnie **Resetuj klucz tajny**.
5. Potwierdź decyzję, klikając **Dalej**.
   Zostanie wygenerowana nowa wartość tajna. Identyfikator klienta i adres URL centrum danych się nie zmienią.
   Wszystkie tokeny zabezpieczeń przypisane do tego klienta natychmiast wygasną, a żądania API z tymi tokenami zakończą się niepowodzeniem.
6. Skopiuj i zapisz nową wartość tajną klienta.

   Ważne
   Ze względów bezpieczeństwa wartość tajna jest wyświetlana tylko raz. W razie utraty tej wartości nie da się jej odzyskać — można ją tylko zresetować.

7. Kliknij **Gotowe**.

Wyłączanie klienta API

1. Zaloguj się do portalu zarządzania.
2. Kliknij **Ustawienia** > **Klienty API**.
3. Znajdź pożądanego klienta na liście.
4. Kliknij , a następnie kliknij **Wyłącz**.
5. Potwierdź decyzję.
   Status klienta zostanie zmieniony na **Wyłączono**.
   Żądania API z tokenami zabezpieczeń przypisanymi do tego klienta zakończą się niepowodzeniem, ale tokeny nie wygasną od razu. Wyłączenie klienta nie ma wpływu na czas ważności tokenów.
   W każdej chwili będzie można ponownie włączyć tego klienta.

Włączanie klienta API

1. Zaloguj się do portalu zarządzania.
2. Kliknij **Ustawienia** > **Klienty API**.
3. Znajdź pożądanego klienta na liście.
4. Kliknij  , a następnie kliknij **Włącz**.

Status klienta zostanie zmieniony na **Włączono**.

Jeśli tokeny jeszcze nie wygasły, żądania API z tokenami zabezpieczeń przypisanymi do tego klienta zakończą się powodzeniem.

Usuwanie klienta API

1. Zaloguj się do portalu zarządzania.
2. Kliknij **Ustawienia** > **Klienty API**.
3. Znajdź pożądanego klienta na liście.
4. Kliknij  , a następnie kliknij **Usuń**.
5. Potwierdź decyzję.

   Wszystkie tokeny zabezpieczeń przypisane do tego klienta natychmiast wygasną, a żądania API z tymi tokenami zakończą się niepowodzeniem.

Ważne

Usuniętego klienta nie da się odzyskać.

Indeks