Portale di gestione

24.02

Manuale dell'amministratore della società

REVISIONE: 11/03/2024

Sommario

Informazioni sul documento **5**
Informazioni sul portale di gestione **6**
Account e unità 6
Gestione delle quote 7
Visualizzazione delle quote dell'organizzazione 8
Definizione delle quote per gli utenti 13
Browser Web supportati 15
Istruzioni passo a passo **16**
Attivazione di un account amministratore 16
Requisiti per la password 16
Accesso al portale di gestione e ai servizi 16
Passaggio dal portale di gestione alle console dei servizi e viceversa 17
Navigazione nel portale di gestione 17
Creazione di unità 17
Creazione di un account utente 18
Ruoli utente disponibili per ogni servizio 20
Ruolo Amministratore di sola lettura 22
Ruolo di operatore di ripristino 23
Modifica delle impostazioni di notifica per un utente 23
Notifiche ricevute in base al ruolo dell'utente 25
Disabilitazione e abilitazione di un account utente 25
Eliminazione di un account utente 25
Trasferimento della titolarità di un account utente 26
Configurazione dell'autenticazione a due fattori 27
Come funziona 27
Propagazione delle impostazioni dell'autenticazione a due fattori a tutti i livelli dei tenant 29
Configurazione dell'autenticazione a due fattori per il tenant 30
Gestione dell'autenticazione a due fattori per gli utenti 30
Ripristinare l'autenticazione a due fattori in caso di perdita del dispositivo di secondo fattore 32
Protezione da attacchi di forza bruta 32
Aggiornamento automatico degli agenti 33
Per aggiornare gli agenti automaticamente 34
Per monitorare gli aggiornamenti degli agenti 35
Configurazione dell'archivio immutabile 35
Storage e agenti supportati 37

Gestione attività **38**
Visualizzazione dei ticket del Service Desk 38
Creazione di un ticket del Service Desk 39
Aggiornamento dei ticket del Service Desk 40
Monitoraggio **42**
Utilizzo 42
Dashboard Operazioni 42
Stato protezione 43
#CyberFit Score per sistema 44
Widget di Endpoint Detection and Response (EDR) 45
Monitoraggio integrità del disco 48
Mappa di protezione dati 52
Widget di valutazione delle vulnerabilità 53
Widget di installazione patch 54
Informazioni sulla scansione del backup 56
Recentemente interessato 56
URL bloccati 57
Widget Inventario software 58
Widget Inventario hardware 59
Cronologia della sessione 60
Registro di audit 60
Campi del registro di audit 61
Filtri e ricerca 62
Elaborazione di rapporti **63**
Report utilizzo 63
Tipo di rapporto 63
Ambito del report 63
Metriche con utilizzo pari a zero 63
Configurazione di Report di utilizzo pianificati 64
Configurazione di Report di utilizzo personalizzati 64
Dati nei report di utilizzo 65
Report Operazioni 65
Azioni con i report 66
Riepilogo esecutivo 69
Widget del report Riepilogo esecutivo 69
Configurazione delle impostazioni del report Riepilogo esecutivo 77
Creazione di un report Riepilogo esecutivo 78

Personalizzazione del report Riepilogo esecutivo 78
Invio dei report Riepilogo esecutivo 80
Fusi orari nei report 80
Dati inseriti nel report in base al tipo di widget 81
Integrazioni **84**
Catalogo delle integrazioni 84
Tutte le integrazioni 84
Integrazioni in uso 85
Limitazione dell'accesso all'interfaccia Web 85
Limiti di accesso alla società 86
Gestione dei clienti API 86
Cosa è un client API? 86
Procedura di integrazione tipica 87
Creazione di un client API 87
Reimpostazione del valore segreto di un client API 88
Disabilitazione di un client API 88
Abilitazione di un client API disabilitato 88
Eliminazione di un client API 89
Indice **90**

Informazioni sul documento

Questo documento è destinato agli amministratori di clienti che desiderano utilizzare il portale di gestione cloud per creare e gestire account utente, unità e quote, per configurare e controllare l'accesso e per monitorare l'utilizzo e le operazioni nella propria organizzazione cloud.

Informazioni sul portale di gestione

Il portale di gestione costituisce l'interfaccia Web con la piattaforma cloud, che fornisce servizi di protezione dati.

Sebbene ogni servizio sia dotato di una propria interfaccia Web chiamata console del servizio, il portale di gestione consente agli amministratori di controllare l'utilizzo del servizio, creare account utente e unità, generare report e altro ancora.

Account e unità

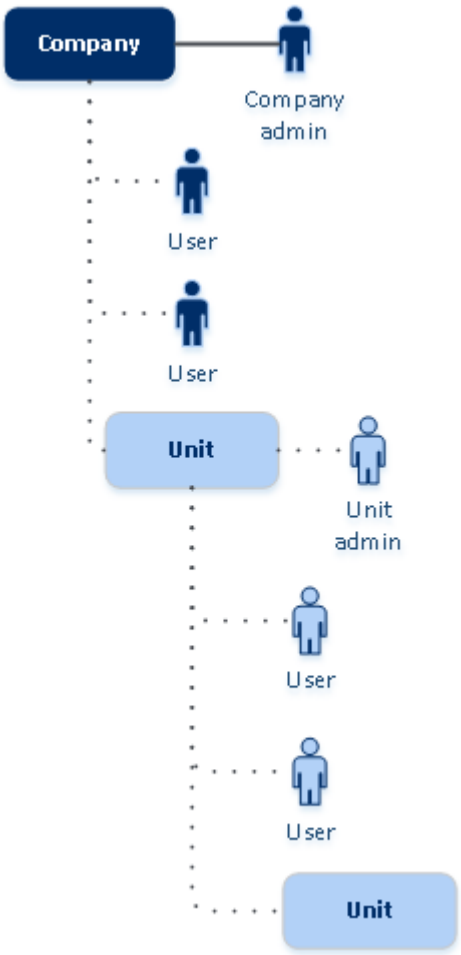
Esistono due tipi di account utente: account amministratore e account utente.

- Gli **amministratori** possono accedere al portale di gestione. Dispongono del ruolo di amministratore in tutti i servizi.
- Gli **utenti** non possono accedere al portale di gestione. Il loro accesso ai servizi e il loro ruolo nei servizi viene definito da un amministratore.

Gli amministratori possono creare le unità, che generalmente corrispondono alle unità o ai reparti dell'azienda. Ogni account esiste o a livello di società o in un'unità.

Un amministratore può gestire unità, account di amministratore e account utente nel proprio livello di gerarchia o a un livello inferiore.

La figura seguente illustra tre livelli gerarchici: la società e due unità. Le unità e gli account facoltativi sono indicati da una linea tratteggiata.



La seguente tabella riassume le operazioni che possono essere eseguite dagli amministratori e dagli utenti.

Operazione	Utenti	Amministratori
Creazione di unità	No	Sì
Creazione di account	No	Sì
Download e installazione del software	Sì	Sì
Utilizzo dei servizi	Sì	Sì
Creazione di report sull'utilizzo del servizio	No	Sì

Gestione delle quote

Le **quote** limitano la capacità del tenant di utilizzare il servizio.

Nel portale di gestione vengono visualizzate le quote dei servizi allocate all'organizzazione dal service provider, che tuttavia non possono essere gestite.

È invece possibile gestire le quote dei servizi degli utenti dell'organizzazione.

Visualizzazione delle quote dell'organizzazione

Nel portale di gestione passare a **Panoramica** > **Utilizzo**. Viene mostrato un pannello di controllo che visualizza le quote allocate all'organizzazione. Le quote di ogni servizio vengono mostrate in una scheda distinta.

Quote del servizio Backup

È possibile specificare la quota di archiviazione nel cloud, la quota per il backup locale e il numero massimo di sistemi/dispositivi/siti web che un utente è autorizzato a proteggere. Sono disponibili le quote seguenti:

Quote per dispositivi

- **Workstation**
- **Server**
- **Macchine virtuali**
- **Dispositivi mobili**
- **Server di web hosting** (server virtuali e fisici Linux che eseguono i pannelli di controllo di Plesk, cPanel, DirectAdmin, VirtualMin o ISPManager)
- **Siti Web**

Un sistema/dispositivo/sito web è considerato protetto finché risulta associato ad almeno un piano di protezione. Un dispositivo mobile diventa protetto dopo il primo backup.

Quando il surplus della quota viene superato per più dispositivi, l'utente non può applicare il piano di protezione ad altri dispositivi.

Quote per origini dati nel cloud

- **Utenze di Microsoft 365**
  Questa quota è applicata dal service provider per l'intera azienda. Gli amministratori dell'azienda possono visualizzare la quota e l'utilizzo nel portale di gestione.
  Il licensing delle utenze di Microsoft 365 dipende dalla modalità di fatturazione selezionata per Cyber Protection.

Importante
L'agente locale e l'agente cloud consumano quote distinte. Se si esegue il backup degli stessi workload utilizzando entrambi gli agenti, l'addebito avviene due volte. Per esempio:

- Se si esegue il backup delle caselle di posta di 120 utenti tramite l'agente locale e si esegue il backup dei file di OneDrive degli stessi utenti tramite l'agente cloud, verranno addebitate 240 utenze di Microsoft 365.
- Se si esegue il backup delle caselle di posta di 120 utenti tramite l'agente locale e si esegue il backup delle stesse caselle di posta anche tramite l'agente cloud, verranno addebitate 240 utenze di Microsoft 365.

Nella modalità di fatturazione **Per workload**, la quota delle **utenze di Microsoft 365** viene conteggiata per i singoli utenti. È considerato singolo utente un utente che ha almeno:

- Casella di posta protetta
- OneDrive protetto
- Accesso ad almeno una risorsa protetta a livello aziendale: Sito di Microsoft 365 SharePoint Online o Microsoft 365 Teams.
  Per maggiori informazioni su come controllare il numero di membri di un sito di Microsoft 365 SharePoint o Teams, fare riferimento a questo articolo della Knowledge Base.

Nota
Gli utenti bloccati di Microsoft 365 che non dispongono di una casella di posta personale protetta o di OneDrive, e possono accedere solo alle risorse condivise (caselle di posta condivise, siti SharePoint e Microsoft Teams), non riceveranno alcun addebito.
Per utente bloccato si intende l'utente che non dispone di credenziali valide e che non può accedere ai servizi di Microsoft 365. Per informazioni su come bloccare tutti gli utenti senza licenza in un'organizzazione di Microsoft 365, fare riferimento a "Impedire l'accesso agli utenti di Microsoft 365 senza licenza" (pag. 11).

Le utenze di Microsoft 365 seguenti non vengono addebitate e non richiedono una licenza per utenza:

- Caselle di posta condivise
- Sale e attrezzatura
- Utenti esterni con accesso ai siti SharePoint e/o Microsoft Teams oggetto di backup

Per ulteriori informazioni sulle opzioni di licenza disponibili con la modalità di fatturazione per gigabyte, fare riferimento alla documentazione di Cyber Protect Cloud relativa al licensing per GB di Microsoft 365.
Per ulteriori informazioni sulle opzioni di licenza disponibili con la modalità di fatturazione per workload, fare riferimento alla documentazione di Cyber Protect Cloud relativa alle modifiche di pricing e licensing per Microsoft 365.

- **Microsoft 365 Teams**

Questa quota è applicata dal service provider per l'intera azienda. Questa quota abilita o disabilita la possibilità di proteggere Microsoft 365 Teams e definisce il numero massimo di team che è possibile proteggere. Per la protezione di un team, indipendentemente dal numero di membri o di canali che lo costituiscono, è necessaria una quota. Gli amministratori dell'azienda possono visualizzare la quota e l'utilizzo nel portale di gestione.

- **Microsoft 365 SharePoint Online**

  Questa quota è applicata dal service provider per l'intera azienda. Questa quota abilita o disabilita la possibilità di proteggere i siti di SharePoint Online e definisce il numero massimo di raccolte dei siti e siti di gruppo che è possibile proteggere.

  Gli amministratori dell'azienda possono visualizzare la quota nel portale di gestione. La quota può inoltre essere visualizzata, insieme alla quantità di archivio occupato dai backup di SharePoint Online nei report di utilizzo.
- **Utenze di Google Workspace**

  Questa quota è applicata dal service provider per l'intera azienda. L'azienda può proteggere caselle di posta di **Gmail** (incluso calendario e contatti), file di **Google Drive** o entrambi. Gli amministratori dell'azienda possono visualizzare la quota e l'utilizzo nel portale di gestione.
- **Google Workspace Shared Drive**

  Questa quota è applicata dal service provider per l'intera azienda. Questa quota abilita o disabilita la possibilità di proteggere le unità condivise di Google Workspace Shared Drive. Se la quota è abilitata, è possibile proteggere un numero illimitato di unità condivise. Gli amministratori dell'azienda non possono visualizzare la quota nel portale di gestione, ma possono visualizzare la quantità di archivio occupato dai backup delle unità condivise nei report di utilizzo.

  Il backup delle unità condivise di Google Workspace è disponibile solo ai clienti che dispongono di almeno una quota di utenze di Google Workspace aggiuntiva. Tale quota viene solo verificata e non sarà utilizzata.

Un'utenza di Microsoft 365 è considerata protetta finché almeno un piano di protezione è applicato alla casella di posta o al OneDrive dell'utente. Un'utenza di Google Workspace è considerata protetta finché almeno un piano di protezione è applicato alla casella di posta o al Google Drive dell'utente.

Quando il surplus della quota viene superato per più utenze, l'amministratore dell'azienda non può applicare il piano di protezione ad altre utenze.

Quote per archivio

- **Backup locale**

  La quota **Backup locale** limita la dimensione totale dei backup locali creati utilizzando l'infrastruttura cloud. Non è possibile definire un surplus per questa quota.
- **Risorse cloud**

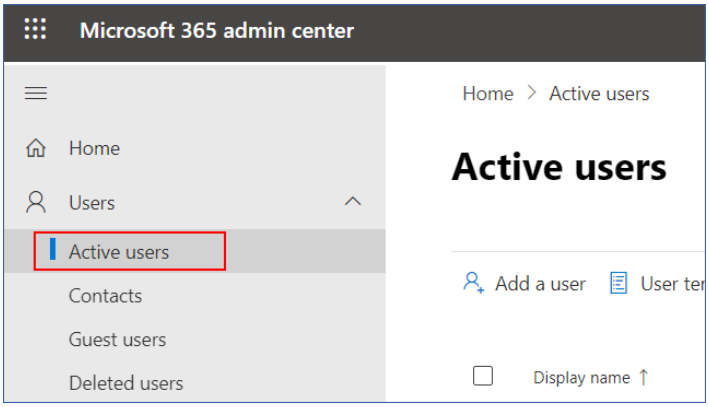
  La quota **Risorse cloud** combina la quota per l'archivio di backup e le quote per il disaster recovery. La quota di archiviazione di backup limita la dimensione totale dei backup posizionati nell'archivio cloud. Quando si supera il surplus della quota, i backup non vanno a buon fine.

Impedire l'accesso agli utenti di Microsoft 365 senza licenza

È possibile impedire di accedere a tutti gli utenti senza licenza presenti nell'organizzazione Microsoft 365 modificando il relativo stato di accesso.

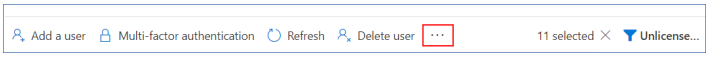
Per impedire l'accesso agli utenti senza licenza

1. Accedere al centro di amministrazione di Microsoft 365 (https://admin.microsoft.com) con un ruolo di amministratore globale.
2. Nel menu di navigazione, passare a **Utenti** > **Utenti attivi**.



3. Fare clic su **Filtro** e quindi selezionare **Utenti senza licenza**.

4. Selezionare le caselle di controllo accanto ai nomi degli utenti, quindi fare clic sull'icona dei puntini di sospensione (...).



5. Nel menu, selezionare **Modifica stato di accesso**.
6. Selezionare la casella di controllo **Blocca l'accesso degli utenti** e fare clic su **Salva**.

Quote del servizio Disaster Recovery

Nota
Gli elementi dell'offerta Disaster Recovery sono disponibili solo con il componente aggiuntivo Disaster Recovery.

Queste quote sono applicate dal service provider per l'intera azienda. Gli amministratori dell'azienda possono visualizzare le quote e l'utilizzo nel portale di gestione, ma non possono definire le quote per un utente.

- **Archivio di disaster recovery**

  Lo storage Disaster Recovery mostra la dimensione dello storage di backup dei server protetti con Disaster Recovery. L'uso dello storage di disaster recovery equivale all'uso dello storage di backup dei workload protetti con i server di disaster recovery. Tale storage è calcolato a partire

dal momento in cui viene creato un server di ripristino, a prescindere dal fatto che il server sia attualmente in esecuzione. Se il surplus per questa quota viene raggiunto, non sarà possibile creare server primari e di ripristino o aggiungere/estendere dischi ai server primari esistenti. Se il surplus per questa quota viene superato, non sarà possibile avviare un failover o avviare un server arrestato. I server in esecuzione non verranno arrestati.

- **Punti di calcolo**

  Questa quota limita le risorse di CPU e RAM che vengono consumate dai server primari e di ripristino nell'arco di un periodo di fatturazione. Se il surplus per questa quota viene raggiunto, tutti i server primari e di ripristino verranno spenti. Non sarà possibile utilizzare questi server fino all'inizio del successivo periodo di fatturazione. Per impostazione predefinita, il periodo di fatturazione corrisponde a un mese di calendario.

  Se la quota è disabilitata, non è possibile utilizzare i server, indipendentemente dal periodo di fatturazione.
- **Indirizzi IP pubblici**

  Questa quota limita il numero di indirizzi IP pubblici che è possibile assegnare ai server primari e di ripristino. Se il surplus per questa quota viene raggiunto, non sarà possibile abilitare indirizzi IP pubblici per altri server. È possibile impedire a un server di utilizzare un indirizzo IP pubblico deselezionando la casella di controllo **Indirizzo IP pubblico** nelle impostazioni del server. Successivamente, è possibile consentire a un altro server di utilizzare un indirizzo IP pubblico, che in genere non sarà lo stesso.

  Quando la quota è disabilitata, nessun server utilizza gli indirizzi IP pubblici e pertanto non sarà raggiungibile da Internet.
- **Server cloud**

  Questa quota limita il numero totale di server primari e di ripristino. Se il surplus per questa quota viene raggiunto, non sarà possibile creare server primari o di ripristino.

  Se la quota è disabilitata, i server sono visibili nella console di Cyber Protect, ma l'unica operazione disponibile è **Elimina**.
- **Accesso Internet**

  Questa quota abilita o disabilita l'accesso a Internet dai server primari o di ripristino.

  Se la quota è disabilitata, i server primari e di ripristino non saranno in grado di connettersi a Internet.

Quote del servizio File Sync & Share

Queste quote sono applicate dal service provider per l'intera azienda. Gli amministratori dell'azienda possono visualizzare le quote e l'utilizzo nel portale di gestione.

- **Utenti**

  Questa quota consente di configurare il numero di utenti che possono accedere al servizio.

  Gli account Amministratore non vengono conteggiati come parte della quota.
- **Archiviazione nel cloud**

  Un archivio nel cloud nel quale archiviare i file degli utenti. Questa quota definisce lo spazio allocato per un tenant nell'archiviazione nel cloud.

Quote del servizio Consegna fisica dei dati

Il consumo delle quote del servizio Consegna fisica dei dati viene considerato per unità. È possibile salvare i backup iniziali di più macchine su un solo disco rigido.

Queste quote sono applicate dal service provider per l'intera azienda. Gli amministratori dell'azienda possono visualizzare le quote e l'utilizzo nel portale di gestione, ma non possono definire le quote per un utente.

- **Nel cloud**
  Consente di inviare un backup iniziale al datacenter cloud utilizzando un'unità disco rigido. Questa quota definisce il numero massimo di unità che possono essere trasferite al datacenter cloud.

Quote del servizio Notary

Queste quote sono applicate dal service provider per l'intera azienda. Gli amministratori dell'azienda possono visualizzare le quote e l'utilizzo nel portale di gestione.

- **Archivio Notary**
  Definisce lo spazio massimo di storage nel cloud per i file autenticati, i file firmati e i file di cui è in corso il processo di autenticazione o di firma.
  Per diminuire l'utilizzo di questa quota, è possibile eliminare dallo storage i file già autenticati o firmati.
- **Autenticazioni**
  Definisce il numero massimo di file autenticabili tramite il servizio di autenticazione.
  Un file viene considerato autenticato non appena viene caricato nello storage di autenticazione e il relativo stato di autenticazione cambia in **In corso**.
  Se lo stesso file viene autenticato più volte, ogni autenticazione vale come una nuova.
- **eSignature**
  Definisce il numero massimo di firme elettroniche.

Definizione delle quote per gli utenti

Le **quote** consentono di limitare la capacità di un utente di utilizzare il servizio. Per impostare le quote per un utente, selezionare l'utente nella scheda **Utenti** in **Gestione azienda**, quindi fare clic sull'icona a forma di matita nella sezione **Quote**.

Quando la quota viene superata, viene inviata una notifica all'indirizzo e-mail dell'utente. Se non viene impostato un surplus della quota, la quota viene considerata "**flessibile.**" Ciò significa che non vengono applicati limiti relativi all'utilizzo del servizio Cyber Protection.

Se viene specificato il surplus della quota, la quota è considerata "**rigida.**" Il **surplus della quota** consente all'utente di superare la quota del valore specificato. Quando si supera surplus della quota, vengono applicati i limiti definiti per l'uso del servizio.

Esempio

Quota flessibile: È stata impostata una quota per workstation pari a 20. Quando il numero delle workstation protette dell'utente raggiunge 20, l'utente riceve una notifica via e-mail, ma il servizio Cyber Protection rimane disponibile.

Quota rigida: Se è stata impostata una quota per workstation pari a 20 e un surplus della quota di 5, l'utente riceve una notifica via e-mail quando il numero delle workstation protette raggiunge 20 e il servizio Cyber Protection viene disabilitato quando il numero raggiunge 25.

Quote del servizio Backup

È possibile specificare la quota di storage di backup e il numero massimo di sistemi/dispositivi/siti web che un utente è autorizzato a proteggere. Sono disponibili le quote seguenti:

Quote per dispositivi

- **Workstation**
- **Server**
- **Macchine virtuali**
- **Dispositivi mobili**
- **Server di web hosting** (server virtuali e fisici Linux che eseguono i pannelli di controllo di Plesk, cPanel, DirectAdmin, VirtualMin o ISPManager)
- **Siti Web**

Un sistema/dispositivo/sito web è considerato protetto finché risulta associato ad almeno un piano di protezione. Un dispositivo mobile diventa protetto dopo il primo backup.

Quando il surplus della quota viene superato per più dispositivi, l'utente non può applicare il piano di protezione ad altri dispositivi.

Quota per il servizio di Archiviazione

- **Archivio di backup**

La quota di storage di backup limita la dimensione totale dei backup posizionati nel cloud storage. Quando si supera il surplus della quota di storage di backup, i backup non hanno esito positivo.

Importante
L'agente locale e l'agente cloud consumano quote distinte. Se si esegue il backup degli stessi workload utilizzando entrambi gli agenti, l'addebito avviene due volte. Per esempio:

- Se si esegue il backup delle caselle di posta di 120 utenti tramite l'agente locale e si esegue il backup dei file di OneDrive degli stessi utenti tramite l'agente cloud, verranno addebitate 240 utenze di Microsoft 365.
- Se si esegue il backup delle caselle di posta di 120 utenti tramite l'agente locale e si esegue il backup delle stesse caselle di posta anche tramite l'agente cloud, verranno addebitate 240 utenze di Microsoft 365.

Quote del servizio File Sync & Share

È possibile definire le seguenti quote del servizio File Sync & Share per un utente:

- **Spazio di archiviazione personale**
  Definisce lo spazio di cloud storage allocato per i file dell'utente.

Quote del servizio Notary

È possibile definire le seguenti quote del servizio Notary per un utente:

- **Archivio Notary**
  Definisce lo spazio massimo di storage nel cloud per i file autenticati, i file firmati e i file di cui è in corso il processo di autenticazione o di firma.
  Per diminuire l'utilizzo di questa quota, è possibile eliminare dallo storage i file già autenticati o firmati.
- **Autenticazioni**
  Definisce il numero massimo di file autenticabili tramite il servizio di autenticazione.
  Un file viene considerato autenticato non appena viene caricato nello storage di autenticazione e il relativo stato di autenticazione cambia in **In corso**.
  Se lo stesso file viene autenticato più volte, ogni autenticazione vale come una nuova.
- **eSignature**
  Definisce il numero massimo di firme elettroniche.

Browser Web supportati

L'interfaccia Web supporta i seguenti browser:

- Google Chrome 29 o versione successiva
- Mozilla Firefox 23 o versione successiva
- Opera 16 o versione successiva
- Microsoft Edge 25 o versioni successive
- Safari 8 o versioni successive in esecuzione nei sistemi operativi macOS e iOS

In altri browser Web (inclusi browser Safari eseguiti in altri sistemi operativi), l'interfaccia utente potrebbe essere visualizzata in modo non corretto o alcune funzioni potrebbero non essere disponibili.

Istruzioni passo a passo

I seguenti passaggi guideranno l'utente nelle attività di base del portale di gestione. I passaggi illustrano la procedura da eseguire per:

- Attivare l'account amministratore
- Accedere al portale di gestione e ai servizi
- Creare un'unità
- Creare un account utente

Attivazione di un account amministratore

Dopo aver eseguito la registrazione per un servizio, l'utente riceverà un messaggio e-mail contenente le seguenti informazioni:

- **Dati di login.** Il nome utente utilizzato per accedere. I dati di login vengono visualizzati anche nella pagina di attivazione dell'account.
- Pulsante **Attiva account**. Fare clic sul pulsante e impostare la password per l'account. Verificare che la password sia lunga almeno nove caratteri. Per ulteriori informazioni sulla password, fare riferimento a "Requisiti per la password" (pag. 16).

Requisiti per la password

La password di un account utente deve essere lunga almeno 9 caratteri. Viene inoltre effettuato un controllo sulla complessità delle password, dopo il quale le password vengono collocate in una delle seguenti categorie:

- Vulnerabile
- Medio
- Complessa

Non è possibile salvare una password vulnerabile, anche se contiene 9 caratteri o più. Le password che ripetono il nome utente, il login, l'e-mail dell'utente o il nome del tenant al quale appartiene l'account utente sono considerate vulnerabili. Anche le password più comuni sono considerate vulnerabili.

Per rafforzare una password, aggiungere più caratteri. L'uso di più caratteri, come numeri, lettere maiuscole e minuscole e caratteri speciali non è obbligatorio, ma consente di creare password più complesse e anche più corte.

Accesso al portale di gestione e ai servizi

1. Aprire la pagina di accesso della console del servizio.
2. Digitare il login e quindi fare clic su **Avanti**.

3. Digitare la password e quindi fare clic su **Avanti**.
4. Eseguire una delle seguenti operazioni:
   - Per accedere al portale di gestione, fare clic su **Portale di gestione**.
   - Per accedere a un servizio, fare clic sul nome del servizio.

Il periodo di timeout per il portale di gestione è di 24 ore per le sessioni attive e di un'ora per le sessioni inattive.

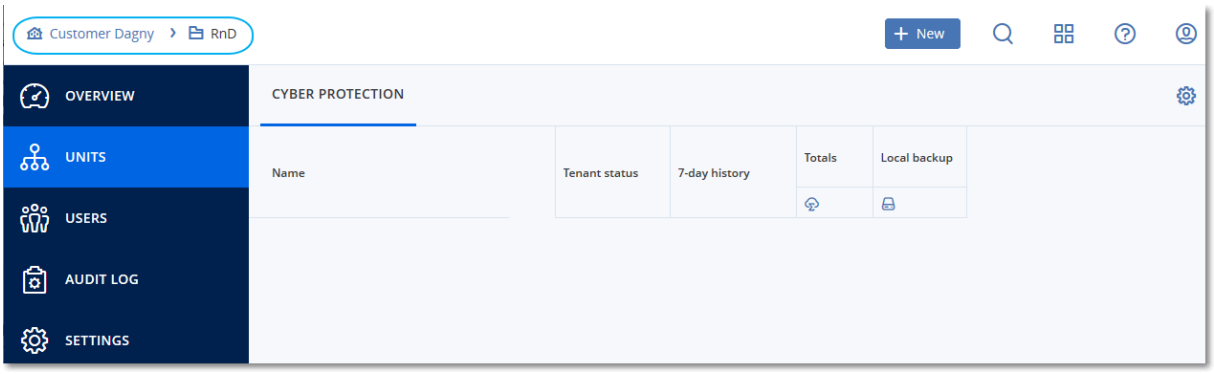
Passaggio dal portale di gestione alle console dei servizi e viceversa

Per passare dal portale di gestione alle console dei servizi e viceversa, fare clic sull'icona nell'angolo in alto a destra e selezionare il **portale di gestione** o il servizio da aprire.

Navigazione nel portale di gestione

Quando si usa il portale di gestione, in qualsiasi momento si lavora con una società o una unità. Ciò viene indicato nell'angolo in alto a sinistra.

Per impostazione predefinita, è selezionato il livello gerarchico più elevato disponibile all'utente. Fare clic sul nome dell'unità per esaminare in dettaglio la gerarchia. Per tornare a un livello superiore, fare clic sul nome del livello nell'angolo in alto a sinistra.



Vengono visualizzate tutte le sezioni dell'interfaccia utente, relative solo alla società o all'unità nella quale si sta lavorando. Per esempio:

- Il pulsante **Nuovo** consente di creare un'unità o un account utente solo in questa unità o società.
- La scheda **Unità** visualizza solo le unità che sono figli diretti della società o unità in questione.
- La scheda **Utenti** visualizza solo gli account utente esistenti nella società o unità in questione.

Creazione di unità

Ignorare questo passaggio se non si desidera organizzare gli account in unità.

Se si pianifica di creare le unità in un secondo momento, tenere presente che non è possibile spostare gli account esistenti tra unità o tra società e unità. È quindi necessario innanzitutto creare un'unità che verrà poi popolata con gli account.

Per creare un'unità

1. Accedere al portale di gestione.
2. Passare all'unità nella quale si desidera creare una nuova unità.
3. Nell'angolo in alto a destra fare clic su **Nuova** > **Unità**.
4. In **Nome**, specificare un nome per la nuova unità.
5. [Facoltativo] In **Lingua**, modificare la lingua predefinita che verrà utilizzata in questa unità per le notifiche, i report e il software.
6. Eseguire una delle seguenti operazioni:
   - Per creare un amministratore per l'unità, fare clic su **Avanti**, e quindi seguire la procedura descritta in "Creazione di un account utente" a partire dal passaggio 4.
   - Per creare un'unità senza un amministratore, fare clic su **Salva e chiudi**. È possibile aggiungere amministratori e utenti all'unità in un secondo momento.

L'unità appena creata viene visualizzata nella scheda **Unità**.

Per modificare le impostazioni dell'unità o specificare le informazioni di contatto, selezionare l'unità nella scheda **Unità**, quindi fare clic sull'icona a forma di matita nella sezione che si desidera modificare.

Creazione di un account utente

Ignorare questo passaggio se non si desidera creare ulteriori account utente.

È possibile creare account aggiuntivi nei casi seguenti:

- Account amministratore società — per condividere le attività di gestione con altre persone.
- Account amministratore unità — per delegare la gestione ad altre persone, le cui autorizzazioni di accesso saranno strettamente limitate all'unità corrispondente.
- Account utente — per consentire agli utenti di accedere esclusivamente a un sottoinsieme dei servizi.

Per creare un account utente

1. Accedere al portale di gestione.
2. Passare all'unità nella quale si desidera creare un nuovo account utente.
3. Nell'angolo in alto a destra fare clic su **Nuovo** > **Utente**.
4. Specificare le seguenti informazioni per l'account:

- **Accedi**

  Importante
  Ciascun account deve disporre di un unico login

- **E-mail**

  Importante
  Se l'utente è registrato nel servizio File Sync & Share, fornire l'e-mail che è stata utilizzata per la registrazione di File Sync & Share.

  Tenere presente che ciascun account utente del cliente deve disporre di un indirizzo e-mail esclusivo.

- [Facoltativo] **Nome**
- [Facoltativo] **Cognome**
- In **Lingua**, modificare la lingua predefinita che verrà utilizzata per questo account per le notifiche, i report e il software.

5. Selezionare i servizi ai quali l'utente potrà accedere e i ruoli in ciascun servizio.
   - Se la casella di controllo **Amministratore società** è selezionata, l'utente potrà accedere al portale di gestione e al ruolo di amministratore in tutti i servizi.
   - Se la casella di controllo **Amministratore unità** è selezionata, l'utente potrà accedere al portale di gestione, ma potrà disporre o meno del ruolo di amministratore del servizio a seconda del servizio.
   - Altrimenti, l'utente potrà disporre dei ruoli selezionati nei servizi selezionati.
6. Fare clic su **Crea**.

L'account utente appena creato viene visualizzato nella scheda **Utenti**.

Per modificare le impostazioni dell'utente o specificare le impostazioni di notifica e le quote per l'utente, selezionare l'utente nella scheda **Utenti**, quindi fare clic sull'icona a forma di matita nella sezione che si desidera modificare.

Per reimpostare la password di un utente

1. Nel portale di gestione, passare a **Gestione azienda** > **Utenti**.
2. Selezionare l'utente di cui si desidera reimpostare la password, quindi fare clic sull'icona dei puntini di sospensione > **Reimposta password**.
3. Confermare l'operazione facendo clic su **Reimposta**.

L'utente può completare il processo di reimpostazione seguendo le istruzioni nell'e-mail ricevuta.

Per i servizi che non supportano l'autenticazione a due fattori (ad esempio la registrazione a Cyber Infrastructure), potrebbe essere necessario convertire un account utente in un *Account di servizio*, ovvero un account che non richiede l'autenticazione a due fattori.

Per convertire un account utente nel tipo di account di servizio

1. Nel portale di gestione, passare a **Gestione azienda** > **Utenti**.
2. Selezionare l'utente il cui account si desidera convertire nel tipo di account di servizio, quindi fare clic sull'icona dei puntini di sospensione > **Contrassegna come account di servizio**.
3. Nella finestra di conferma, immettere il codice di autenticazione a due fattori e confermare l'azione.

Ora l'account può essere utilizzato per i servizi che non supportano l'autenticazione a due fattori.

Ruoli utente disponibili per ogni servizio

Un utente può disporre di diversi ruoli, ma di un solo ruolo per ogni servizio.

Per ogni servizio è possibile definire quale ruolo verrà assegnato a un utente.

Servizio	Ruolo	Descrizione
n/d	Amministratore società	Questo ruolo concede diritti di amministratore completi per tutti i servizi. Questo ruolo consente l'accesso alla whitelist aziendale. Se per l'azienda è abilitata la funzionalità Disaster Recovery del servizio Protezione, questo ruolo consente anche l'accesso alla funzionalità Disaster Recovery.
Portale di gestione	Amministratore	Questo ruolo consente l'accesso al portale di gestione dal quale l'amministratore può gestire gli utenti dell'intera organizzazione. Il ruolo garantisce, ad esempio, autorizzazioni complete per le schermate della funzionalità Endpoint Detection and Response, inclusi i widget.
	Amministratore di sola lettura Livello del partner	Questo ruolo fornisce l'accesso di sola lettura a tutti gli oggetti nel portale di gestione del Partner e nei portali di gestione di tutti i clienti di questo Partner. Tali utenti possono accedere ai dati di altri utenti dell'organizzazione in modalità di sola lettura. Possono modificare i piani di protezione, ma non possono salvare le modifiche apportate ai piani di scripting, ai piani di monitoraggio o ai piani agente.
	Amministratore di sola lettura Livello del cliente	Questo ruolo consente l'accesso di sola lettura a tutti gli oggetti nel portale di gestione dell'intera azienda. Gli utenti con questo ruolo possono accedere ai dati di altri utenti dell'organizzazione in modalità di sola lettura.
	Amministratore di sola	Questo ruolo consente l'accesso di sola lettura a tutti gli

	lettura Livello dell'unità	oggetti nel portale di gestione dell'unità e delle sotto unità dell'azienda. Gli utenti con questo ruolo possono accedere ai dati di altri utenti dell'organizzazione in modalità di sola lettura.
Protezione	Amministratore Cyber	Oltre ai diritti del ruolo Amministratore, questo ruolo consente la configurazione e la gestione del servizio Cyber Protection e l'approvazione delle azioni in Cyber Scripting. Il ruolo di Amministratore Cyber è disponibile solo nei tenant in cui è abilitato il pacchetto Advanced Management.
	Amministratore	Questo ruolo consente la configurazione e la gestione di Protezione per i clienti. Il ruolo è necessario, ad esempio, per configurare e gestire la funzionalità Disaster Recovery, la funzionalità Endpoint Detection and Response e la whitelist aziendale.
	Amministratore di sola lettura	Il ruolo consente l'accesso di sola lettura a tutti gli oggetti del servizio Protezione. Gli utenti con questo ruolo possono accedere ai dati di altri utenti dell'organizzazione in modalità di sola lettura. L'amministratore di sola lettura non può configurare né gestire la funzionalità Disaster Recovery, la funzionalità Endpoint Detection and Response o la whitelist aziendale.
	Ripristina operatore	Il ruolo consente di accedere ai backup delle organizzazioni Microsoft 365 e Google Workspace e ne permette il ripristino, limitando l'accesso ai contenuti riservati.
	Utente	Questo ruolo abilita l'utilizzo del servizio Protezione senza i privilegi di amministrazione. È consentito l'accesso a funzionalità quali Endpoint Detection and Response, ma gli utenti a cui questo ruolo è assegnato non possono accedere ai dati di altri utenti dell'organizzazione.
File Sync & Share	Amministratore	Questo ruolo consente la configurazione e la gestione di File Sync & Share per gli utenti. Un account con questo ruolo non viene conteggiato come parte della quota **Utenti** in quanto non prevede l'accesso alla funzionalità File Sync & Share.
	Utente	Questo ruolo consente l'utilizzo del servizio File Sync & Share. Gli utenti possono accedere solo ai propri dati e ai dati che vengono condivisi con loro.
	Guest	Un account con questo ruolo viene creato quando un utente di File Sync & Share condivide contenuti o con un

		utente di Cyber Protect Cloud a cui non è consentito l'utilizzo del servizio File Sync & Share o con una persona che non è un utente di Cyber Protect Cloud. Il ruolo Guest non dispone di una cartella di sincronizzazione, non può consumare cloud storage e non viene conteggiato come parte della quota **Utenti** in quanto il ruolo non concede l'accesso alla funzionalità File Sync & Share. Un ruolo Guest può essere 'promosso' a un ruolo Utente o Amministratore.
Servizio Notary	Amministratore	Questo ruolo consente la configurazione e la gestione del Servizio Notary per gli utenti.
	Utente	Questo ruolo consente l'utilizzo del Servizio Notary senza i privilegi di amministrazione. Gli utenti con questo ruolo non possono accedere ai dati di altri utenti dell'organizzazione.

Ruolo Amministratore di sola lettura

Un account con questo ruolo dispone dell'accesso di sola lettura alla console di Cyber Protect ed è in grado di:

- Acquisire dati di diagnostica, come i report di sistema.
- Visualizzare i punti di ripristino di un backup; non può invece esplorare i dettagli del contenuto di backup e non può visualizzare file, cartelle o messaggi e-mail.

Un amministratore di sola lettura non può:

- Avviare o arrestare attività.

  Ad esempio, un amministratore di sola lettura non può avviare un ripristino o arrestare un backup in esecuzione.
- Accedere al file system su sistemi di origine o destinazione.

  Ad esempio, un amministratore di sola lettura non può visualizzare file, cartelle o messaggi e-mail di un sistema oggetto di backup.
- Modificare le impostazioni.

  Ad esempio, un amministratore di sola lettura non può creare un piano di protezione o modificarne le impostazioni.
- Creare, aggiornare o eliminare dati.

  Ad esempio, un amministratore di sola lettura non può eliminare i backup.

Tutti gli elementi dell'interfaccia utente che non sono accessibili a un amministratore di sola lettura sono nascosti, ad eccezione delle impostazioni predefinite del piano di protezione. Queste impostazioni sono visibili, ma il pulsante **Salva** non è attivo.

Qualsiasi modifica relativa agli account e ai ruoli viene visualizzata nella scheda **Attività** con le informazioni seguenti:

- Elementi modificati
- Esecutore delle modifiche
- Data e ora di esecuzione delle modifiche

Ruolo di operatore di ripristino

Questo ruolo è disponibile solo nel servizio Cyber Protection ed è limitato ai backup di Microsoft 365 e Google Workspace.

Un operatore di ripristino può eseguire le seguenti operazioni:

- Visualizzare avvisi e attività.
- Scorrere e aggiornare l'elenco dei backup.
- Sfogliare i backup senza accedere al loro contenuto. L'operatore di ripristino può visualizzare i nomi dei file e gli oggetti e i mittenti delle e-mail di cui è stato eseguito il backup.
- Ricerca nei backup (non è supportata la ricerca full text).
- Ripristinare backup cloud-to-cloud nella posizione originale nell'organizzazione Microsoft 365 o Google Workspace di origine.

Un operatore di ripristino non può eseguire le seguenti operazioni:

- Eliminare avvisi.
- Aggiungere o eliminare organizzazioni Microsoft 365 o Google Workspace.
- Aggiungere, eliminare o rinominare posizioni di backup.
- Eliminare o rinominare i backup.
- Creare, eliminare o rinominare le cartelle quando si ripristina un backup in una posizione personalizzata.
- Applicare un piano di backup o eseguire un backup.
- Accedere ai file o al contenuto delle e-mail di cui è stato eseguito il backup.
- Eseguire il download di file di cui è stato eseguito il backup o di allegati e-mail.
- Inviare come e-mail risorse cloud di cui è stato eseguito il backup, come e-mail o elementi del calendario.
- Visualizzare o ripristinare le conversazioni di Microsoft 365 Teams.
- Ripristino di backup cloud-to-cloud su posizioni non originali quali una casella di posta differente, OneDrive, Google Drive o Microsoft 365 Team.

Modifica delle impostazioni di notifica per un utente

Per modificare le impostazioni di notifica per un utente, passare a **Gestione azienda** > **Utenti**. Selezionare l'utente per il quale configurare le notifiche, quindi fare clic sull'icona a forma di matita nella sezione **Impostazioni**. Le seguenti impostazioni di notifica sono disponibili se il servizio Cyber Protection è stato attivato per il tenant nel quale è stato creato l'utente:

- **Notifiche relative al superamento delle quote** (abilitata per impostazione predefinita)
  Notifiche relative al superamento delle quote.
- **Report di utilizzo pianificati** (abilitata per impostazione predefinita)
  I report di utilizzo che vengono inviati il primo giorno di ogni mese.
- **Notifiche sul branding dell'URL** (disabilitate per impostazione predefinita)
  Notifiche sull'imminente scadenza del certificato utilizzato per l'URL personalizzato dei servizi Cyber Protect Cloud. Le notifiche vengono inviate a tutti gli amministratori del tenant selezionato 30, 15, 7, 3 e 1 giorno prima della scadenza del certificato.
- **Notifiche di errore**, **Notifiche di attenzione** e **Notifiche di esito positivo** (disabilitate per impostazione predefinita)
  Notifiche relative ai risultati dell'esecuzione dei piani di protezione e ai risultati delle operazioni di ripristino per ogni dispositivo.
- **Riepilogo giornaliero degli avvisi attivi** (abilitata per impostazione predefinita)
  Il riepilogo giornaliero viene generato in base all'elenco degli avvisi attivi presenti nella console di Cyber Protect al momento della creazione del riepilogo. Il riepilogo viene generato e inviato una volta al giorno, tra le 10:00 e le 23:59 del fuso UTC. L'orario di generazione e invio del report dipende dal carico di lavoro nel data center. Se non sono presenti avvisi attivi entro tale ora, il riepilogo non viene inviato. Il riepilogo non include informazioni relative agli avvisi passati non più attivi. Se, ad esempio, un utente individua un backup non riuscito ed elimina l'avviso, oppure se un backup viene eseguito di nuovo con esito positivo prima della generazione del riepilogo, l'avviso non sarà più presente nella console e quindi non verrà inserito nel riepilogo.
- **Notifiche di controllo dispositivo** (disabilitate per impostazione predefinita)
  Notifiche sui tentativi di utilizzo delle porte e dei dispositivi periferici a cui sono associate restrizioni nei piani di protezione con il modulo Controllo dispositivo abilitato.
- **Notifiche relative al ripristino** (disabilitate per impostazione predefinita)
  Notifiche relative alle azioni di ripristino delle risorse seguenti: messaggi e-mail e intera casella di posta dell'utente, cartelle pubbliche, OneDrive/GoogleDrive: OneDrive completo e file o cartelle, file di SharePoint, Teams: Canali, intero Team, messaggi e-mail, sito del Team.
  Nell'ambito di queste notifiche, le azioni seguenti sono considerate azioni di ripristino: invio come e-mail, download, o avvio di un'operazione di ripristino.
- **Notifiche di prevenzione della perdita di dati** (disabilitate per impostazione predefinita)
  Notifiche sugli avvisi di Prevenzione della perdita di dati relative all'attività di questo utente sulla rete.
- **Notifiche relative ai problemi di sicurezza** (disabilitate per impostazione predefinita)
  Notifiche relative al malware rilevato durante l'accesso, l'esecuzione e le scansioni su richiesta e ai rilevamenti provenienti dal motore comportamentale e dal motore di filtro degli URL.
  Sono disponibili due opzioni: **Mitigato** e **Non mitigato**. Queste opzioni si riferiscono agli avvisi relativi ai problemi di Endpoint Detection and Response (EDR), agli avvisi EDR dai feed delle minacce e a singoli avvisi (per i workload sui quali non è attivata la funzionalità EDR).
  Simultaneamente alla creazione di un avviso EDR, viene inviata un'e-mail all'utente interessato. Se lo stato della minaccia relativa al problema cambia, viene inviata una nuova e-mail. Le e-mail

includono pulsanti di azione che consentono all'utente di visualizzare i dettagli del problema (se è stato mitigato) oppure di indagare e correggere quanto accaduto (se non è stato mitigato).

- **Notifiche relative all'infrastruttura** (disabilitate per impostazione predefinita)
  Notifiche relative all'infrastruttura di Disaster Recovery: quando questa non è disponibile o quando non sono disponibili i tunnel VPN.

Tutte le notifiche vengono inviate all'indirizzo e-mail dell'utente.

Notifiche ricevute in base al ruolo dell'utente

Le notifiche inviate da Cyber Protection dipendono dal ruolo dell'utente.

Tipo di notifica\Ruolo utente	Utente	Amministratore di clienti
Notifiche relative ai propri dispositivi	Sì	Sì
Notifiche relative a tutti i dispositivi dell'organizzazione	n/d	Sì (ad eccezione di **Notifiche relative ai problemi di sicurezza**)
Notifiche relative ai backup di Microsoft 365, Google Workspace e altri backup basati su cloud	n/d	Sì

Disabilitazione e abilitazione di un account utente

Potrebbe essere necessario disabilitare un account utente per limitare temporaneamente il suo accesso alla piattaforma cloud.

Per disabilitare un account utente

1. Nel portale di gestione passare a **Utenti**.
2. Selezionare l'account utente da disabilitare, quindi fare clic sull'icona dei puntini di sospensione > **Disabilita**.
3. Confermare l'operazione facendo clic su **Disabilita**.

L'utente non sarà in grado di utilizzare la piattaforma cloud né di ricevere alcuna notifica.

Per abilitare un account utente disabilitato, selezionarlo dall'elenco degli utenti e fare clic sull'icona dei puntini di sospensione > **Abilita**.

Eliminazione di un account utente

Potrebbe essere necessario eliminare permanentemente un account utente per liberare le risorse che utilizza, ad esempio spazio di archiviazione o licenza. Le statistiche di utilizzo verranno aggiornate entro un giorno dall'eliminazione. Se l'account contiene più dati, potrebbe richiedere più tempo.

Prima di eliminare un account utente, è necessario disabilitarlo. Per ulteriori informazioni su come eseguire questa operazione, fare riferimento a "Disabilitazione e abilitazione di un account utente".

Per eliminare un account utente

1. Nel portale di gestione passare a **Utenti**.
2. Selezionare l'account utente disabilitato, quindi fare clic sull'icona dei puntini di sospensione > **Elimina**.
3. Per confermare l'azione, immettere il login e fare clic su **Elimina**.

Di conseguenza:

- Tutte le notifiche configurate per questo account verranno disabilitate.
- Tutti i dati che appartengono a questo account utente verranno eliminati.
- L'amministratore non potrà accedere al portale di gestione.
- Tutti i backup dei workload associati a questo utente verranno eliminati.
- Verrà annullata la registrazione di tutti i sistemi associati a questo account utente.
- Tutti i piani di protezione verranno revocati da tutti i workload associati a questo utente.
- Tutti i dati di File Sync & Share che appartengono a questo utente (ad esempio file e cartelle) verranno eliminati.
- I dati Notary che appartengono a questo utente (ad esempio file autenticati, file firmati elettronicamente) verranno eliminati.
- Lo **Stato dell'utente** viene visualizzato come **Eliminato**. Passando il mouse sullo stato **Eliminato** viene visualizzata la data di eliminazione dell'utente e una nota che indica la possibilità di recuperare tutti i dati e le impostazioni pertinenti entro 30 giorni dalla data di eliminazione indicata.

Trasferimento della titolarità di un account utente

Potrebbe essere necessario trasferire la titolarità a un account utente se si desidera mantenere l'accesso ai dati di un utente con privilegi limitati.

Importante
Non è possibile riassegnare il contenuto di un account eliminato.

Per trasferire la titolarità di un account utente:

1. Nel portale di gestione passare a **Utenti**.
2. Selezionare l'account utente di cui si desidera trasferire la titolarità, quindi fare clic sull'icona a forma di matita nella sezione **Informazioni generali**.
3. Sostituire l'e-mail esistente con l'e-mail del futuro proprietario dell'account, quindi fare clic su **Fine**.
4. Confermare l'operazione facendo clic su **Sì**.

5. Il futuro proprietario dell'account dovrà verificare il proprio indirizzo e-mail seguendo le istruzioni che gli verranno inviate.
6. Selezionare l'account utente di cui si sta trasferendo la titolarità, quindi fare clic sull'icona dei puntini di sospensione > **Reimposta password**.
7. Confermare l'operazione facendo clic su **Reimposta**.
8. Il futuro proprietario dell'account dovrà reimpostare la password seguendo le istruzioni che verranno inviate al suo indirizzo e-mail.

A questo punto il nuovo proprietario potrà accedere all'account.

Configurazione dell'autenticazione a due fattori

L'**autenticazione a due fattori (2FA)** è una tipologia di autenticazione multifattoriale che verifica l'identità di un utente combinando due fattori differenti:

- Un elemento noto all'utente (PIN o password)
- Un elemento a disposizione dell'utente (token)
- Un elemento che consente di riconoscere fisicamente l'utente (biometria)

L'autenticazione a due fattori fornisce una protezione aggiuntiva contro l'accesso non autorizzato all'account.

La piattaforma supporta l'autenticazione **TOTP (Time-based One-Time Password)**. Quando è abilitata l'autenticazione TOTP, per accedere al sistema gli utenti devono immettere la password tradizionale e un codice TOTP temporaneo. In altre parole, l'utente immette la password (il primo fattore) e il codice TOTP (il secondo fattore). Il codice TOTP viene generato dall'applicazione di autenticazione installata nel dispositivo di secondo fattore dell'utente, in base all'orario attuale e al segreto (codice QR o codice alfanumerico) fornito dalla piattaforma.

Come funziona

1. L'autenticazione a due fattori viene abilitata a livello di organizzazione.
2. Tutti gli utenti dell'organizzazione devono installare l'applicazione di autenticazione sui propri dispositivi di secondo fattore (smartphone, laptop, desktop o tablet). Tale applicazione viene utilizzata per generare codici TOTP temporanei. Sono consigliati gli autenticatori seguenti:
   - Google Authenticator
     Versione app iOS (https://apps.apple.com/app/google-authenticator/id388497605)
     Versione Android (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2)
   - Microsoft Authenticator
     Versione app iOS (https://apps.apple.com/app/microsoft-authenticator/id983156458)
     Versione Android (https://play.google.com/store/apps/details?id=com.azure.authenticator)

Importante
Gli utenti devono accertarsi che l'orario sul dispositivo nel quale è installata l'applicazione di autenticazione sia impostato in modo corretto e corrisponda all'orario corrente.

3. Gli utenti dell'organizzazione devono accedere nuovamente al sistema.
4. Dopo aver inserito login e password, verrà loro richiesto di configurare l'autenticazione a due fattori per i propri account utente.
5. A tal fine dovranno scansionare il codice QR utilizzando l'applicazione di autenticazione. Se non è possibile scansionare il codice QR, è possibile utilizzare codice a 32 cifre visualizzato al di sotto del codice QR e aggiungerlo manualmente all'applicazione di autenticazione.

Importante
È consigliabile salvare queste informazioni: stampare il codice QR, annotare il segreto TOTP (password temporanea), utilizzare un'applicazione che supporti il backup dei codici in un cloud. Il codice TOTP della password temporanea è necessario per ripristinare l'autenticazione a due fattori in caso di perdita del dispositivo di secondo fattore.

6. Il codice TOTP della password temporanea viene generato nell'applicazione di autenticazione. Viene automaticamente rigenerato ogni 30 secondi.
7. L'utente deve inserire il codice TOTP nella finestra **Configura autenticazione a due fattori** visualizzata dopo aver immesso la password.
8. Viene così configurata l'autenticazione a due fattori per gli utenti.

Quando gli utenti accedono al sistema verrà richiesto loro di fornire login, password e il codice TOTP temporaneo generato nell'applicazione di autenticazione. Gli utenti possono contrassegnare il browser come attendibile quando accedono al sistema, evitando così che il codice TOTP venga richiesto nei login successivi eseguiti con lo stesso browser.

Per ripristinare l'autenticazione a due fattori su un nuovo dispositivo

Se è possibile accedere all'app di autenticazione mobile precedentemente installata:

1. Installare un'app di autenticazione sul nuovo dispositivo.
2. Utilizzare il file PDF salvato al momento dell'impostazione dell'autenticazione 2FA nel dispositivo. Questo file contiene il codice a 32 cifre che deve essere inserito nell'app di autenticazione per collegarla di nuovo all'account Acronis.

Importante
Se il codice è corretto ma non funziona, accertarsi di aver sincronizzato l'orario nell'app di autenticazione mobile.

3. Se al momento dell'impostazione non è stato salvato il file PDF:

a. *Fare clic su **Reimposta l'autenticazione 2FA** e inserire la password temporanea mostrata nell'app di autenticazione mobile precedentemente installata.*

b. Seguire le istruzioni a video.

Se non è possibile accedere all'app di autenticazione mobile precedentemente installata:

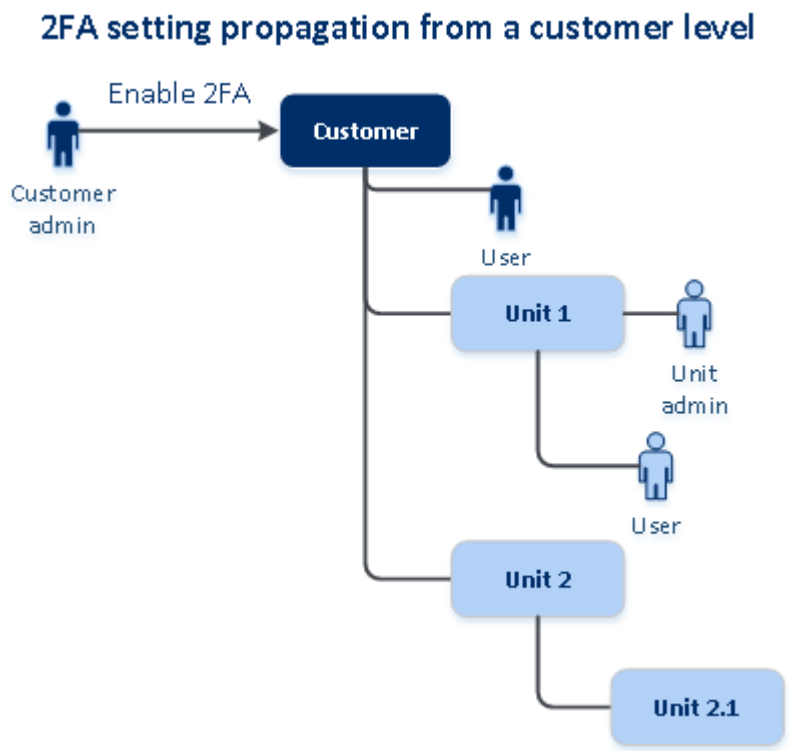
1. Prendere un nuovo dispositivo mobile.
2. Utilizzare il file PDF archiviato per collegare un nuovo dispositivo (il nome predefinito del file è `cyberprotect-2fa-backupcode.pdf`).
3. Ripristinare l'accesso all'account dal backup. Verificare che l'app mobile supporti i backup.
4. Aprire l'app con lo stesso account da un altro dispositivo mobile se è supportato dall'app.

Propagazione delle impostazioni dell'autenticazione a due fattori a tutti i livelli dei tenant

L'autenticazione a due fattori viene configurata a livello di **organizzazione**. Può essere impostata solo per la propria organizzazione.

Le impostazioni dell'autenticazione a due fattori vengono propagate ai livelli dei tenant come indicato di seguito.

- Le unità ereditano automaticamente le impostazioni dell'autenticazione a due fattori dall'organizzazione cliente.



Nota

1. Non è possibile configurare l'autenticazione a due fattori a livello di unità.
2. È possibile gestire le impostazioni dell'autenticazione a due fattori delle organizzazioni (unità) figlio.

Configurazione dell'autenticazione a due fattori per il tenant

L'amministratore può abilitare l'autenticazione a due fattori per l'organizzazione.

Per configurare l'autenticazione a due fattori per il tenant

1. Nel Portale di Gestione passare a **Impostazioni** > **Sicurezza**.
2. Far scorrere l'interruttore **Autenticazione a due fattori,** quindi fare clic su **Abilita**.

A questo punto, tutti gli utenti dell'organizzazione devono configurare l'autenticazione a due fattori per i propri account. Riceveranno un messaggio che indica loro di procedere alla configurazione al prossimo accesso o alla scadenza della sessione corrente.

La barra di stato al di sotto dell'interruttore mostra il numero di utenti che hanno configurato l'autenticazione a due fattori per i propri account. Per controllare quali utenti hanno configurato i propri account, passare alla scheda **Gestione azienda** > **Utenti** e controllare la colonna **Stato 2FA**. Lo stato 2FA degli utenti che non hanno ancora configurato l'autenticazione a due fattori per i propri account è **Impostazione richiesta**.

Dopo aver eseguito la configurazione dell'autenticazione a due fattori, gli utenti dovranno inserire il login, la password e un codice TOTP ogni volta che accedono alla console del servizio.

Per disabilitare l'autenticazione a due fattori per il tenant

1. Nel Portale di Gestione passare a **Impostazioni** > **Sicurezza**.
2. Per disabilitare l'autenticazione a due fattori, disattivare l'indicatore scorrevole e quindi fare clic su **Disabilita**.
3. [Se almeno un utente ha configurato l'autenticazione a due fattori all'interno dell'organizzazione] Immettere il codice TOTP generato nell'applicazione di autenticazione del dispositivo mobile.

L'autenticazione a due fattori viene disabilitata per l'organizzazione, tutti i segreti vengono cancellati e tutti i browser attendibili vengono dimenticati. Tutti gli utenti accederanno al sistema utilizzando solo il login e la password personale. Nella scheda **Gestione azienda** > **Utenti** la colonna **Stato 2FA** viene nascosta.

Gestione dell'autenticazione a due fattori per gli utenti

È possibile monitorare le impostazioni dell'autenticazione a due fattori per tutti gli utenti e ripristinare le impostazioni nella scheda **Gestione azienda** > **Utenti** del portale di gestione.

Monitoraggio

Nel portale di gestione, in **Gestione azienda** > **Utenti**, viene visualizzato un elenco di tutti gli utenti dell'organizzazione. Lo **Stato 2FA** indica se l'autenticazione a due fattori è impostata per un utente.

Per ripristinare l'autenticazione a due fattori per un utente

1. Nel portale di gestione, passare a **Gestione azienda** > **Utenti**.
2. Nella scheda **Utenti**, individuare l'utente per il quale modificare le impostazioni e quindi fare clic sull'icona con i puntini di sospensione.
3. Fare clic su **Ripristina autenticazione a due fattori**.
4. Immettere il codice TOTP generato nell'applicazione di autenticazione del dispositivo di secondo fattore e quindi fare clic su **Ripristina**.

L'utente potrà di nuovo configurare l'autenticazione a due fattori.

Per ripristinare il browser attendibile per un utente

1. Nel portale di gestione, passare a **Gestione azienda** > **Utenti**.
2. Nella scheda **Utenti**, individuare l'utente per il quale modificare le impostazioni e quindi fare clic sull'icona con i puntini di sospensione.
3. Fare clic su **Ripristina tutti i browser attendibili**.
4. Immettere il codice TOTP generato nell'applicazione di autenticazione del dispositivo di secondo fattore e quindi fare clic su **Ripristina**.

Al prossimo accesso, l'utente per il quale sono stati ripristinati tutti i browser attendibili dovrà fornire il codice TOTP.

Gli utenti possono resettare da sé tutti i browser attendibili e le impostazioni di autenticazione a due fattori. Per farlo, effettuare il login nel sistema, fare clic sul link corrispondente, quindi inserire il codice TOTP per confermare l'operazione.

Per disabilitare l'autenticazione a due fattori per un utente

Non è consigliabile disabilitare l'autenticazione a due fattori perché ciò può generare potenziali vulnerabilità nella sicurezza del tenant.

Come eccezione, è possibile disabilitare l'autenticazione a due fattori per un utente e mantenere la funzionalità per tutti gli altri utenti del tenant. Questa soluzione alternativa può rivelarsi funzionale quando l'autenticazione a due fattori è abilitata in un tenant nel quale è configurata l'integrazione cloud e tale integrazione autorizza l'accesso alla piattaforma tramite l'account utente (password di accesso). Per continuare a utilizzare l'integrazione, come soluzione temporanea, è possibile convertire l'utente in un account di servizio per il quale l'autenticazione a due fattori non è applicabile.

Importante
La conversione regolare degli utenti in account di servizio, finalizzata a disabilitare l'autenticazione a due fattori, non è consigliabile perché genera rischi per la sicurezza del tenant.

La soluzione consigliata per utilizzare le integrazioni cloud senza disabilitare l'autenticazione a due fattori per i tenant è di creare i client API e configurare le integrazioni cloud in modo che lavorino con questi.

1. Nel portale di gestione, passare a **Gestione azienda** > **Utenti**.
2. Nella scheda **Utenti**, individuare l'utente per il quale modificare le impostazioni e quindi fare clic sull'icona con i puntini di sospensione.
3. Fare clic su **Contrassegna come account di servizio**. Un utente ottiene uno stato speciale di autenticazione a due fattori definito **Account di servizio.**
4. [Se per almeno un utente di un tenant è stata configurata l'autenticazione a due fattori] Immettere il codice TOTP generato nell'applicazione di autenticazione del dispositivo di secondo fattore per confermare la disabilitazione.

Per abilitare l'autenticazione a due fattori per un utente

In alcuni casi è necessario abilitare l'autenticazione a due fattori per un utente per il quale l'impostazione è stata precedentemente disabilitata.

1. Nel portale di gestione, passare a **Gestione azienda** > **Utenti**.
2. Nella scheda **Utenti**, individuare l'utente per il quale modificare le impostazioni e quindi fare clic sull'icona con i puntini di sospensione.
3. Fare clic su **Contrassegna come account normale**. L'utente deve configurare l'autenticazione a due fattori o fornire il codice TOTP quando accede al sistema.

Ripristinare l'autenticazione a due fattori in caso di perdita del dispositivo di secondo fattore

Per ripristinare l'accesso all'account in caso di perdita del dispositivo di secondo fattore, procedere come indicato in uno degli approcci suggeriti:

- Ripristinare il segreto TOTP (codice QR o codice alfanumerico) da un backup.
  Utilizzare un dispositivo di secondo fattore e aggiungere il segreto TOTP nell'applicazione di autenticazione installata nel dispositivo.
- Chiedere all'amministratore di ripristinare l'autenticazione a due fattori.

Protezione da attacchi di forza bruta

Si definisce attacco di forza bruta quando un intruso tenta di accedere al sistema inserendo una molteplicità di password nella speranza di individuare quella corretta.

Il meccanismo di protezione da attacchi di forza bruta della piattaforma si basa sui cookie di dispositivo.

Le impostazioni per la protezione da attacchi di forza bruta utilizzate dalla piattaforma sono predefinite:

Parametro	Inserire la password	Inserire il codice TOTP
Limite di tentativi	10	5
Tempo limite per tentativi (il limite si resetta dopo ogni timeout)	15 min (900 sec)	15 min (900 sec)
Il blocco sarà attivato fra	Limite di tentativi + 1 (11° tentativo)	Limite di tentativi
Tempo di blocco	5 min (300 sec)	5 min (300 sec)

Se l'autenticazione a due fattori è abilitata, viene emesso un cookie di dispositivo verso un client (browser) solo dopo che l'autenticazione avviene con successo utilizzando entrambi i fattori (password e codice TOTP).

Per i browser attendibili, il cookie di dispositivo viene emesso dopo l'avvenuta autenticazione con un solo fattore (password).

I tentativi di inserimento del codice TOTP vengono registrati per utente, non per dispositivo. Questo significa che, anche qualora un utente tenti di inserire il codice TOTP usando dispositivi diversi, verrà comunque bloccato.

Aggiornamento automatico degli agenti

Importante
Al momento, è possibile accedere alla funzionalità di gestione dell'aggiornamento dell'agente soltanto se è abilitato Protezione.

Cyber Protect dispone di tre tipi di agenti che possono essere installati nei sistemi protetti: Agente per Windows, Agente per Linux e Agente per Mac.

Cyber Files Cloud è disponibile in una versione per Windows e in una per MacOS dell'Agente Desktop per File Sync & Share, che consente la sincronizzazione di file e cartelle tra un sistema e un'area di cloud storage dell'utente di File Sync & Share per incentivare il lavoro offline e le procedure lavorative WFH (Work From Home) e BYOD (Bring Your Own Device).

Per semplificare la gestione di più workload, è possibile configurare (e disabilitare) gli aggiornamenti automatici e senza intervento dell'utente di tutti gli agenti su tutti i sistemi.

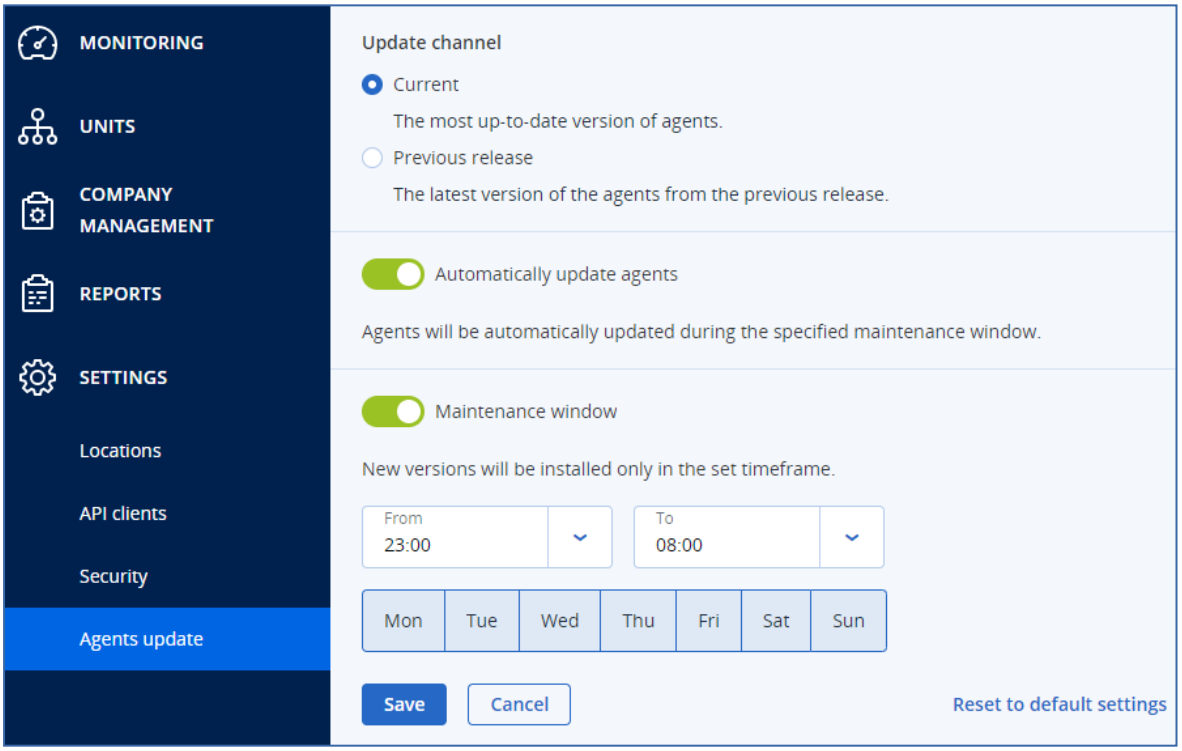
Nota
Per gestire gli agenti sui singoli sistemi e personalizzare le impostazioni di aggiornamento automatico, consultare la sezione della Guida per l'utente di Cyber Protect su come aggiornare gli agenti.

Per aggiornare gli agenti automaticamente

Nota
Se non è stata abilitata alcuna protezione, le impostazioni per l'aggiornamento automatico dell'Agente per File Sync & Share sono ereditate dal Service Provider.

Per mostrare l'aggiornamento automatico degli agenti dalla pagina iniziale del portale di gestione

1. Selezionare **Impostazioni > Aggiornamento agenti**.



2. Selezionare quale versione individuare per gli aggiornamenti automatici: **Attuale** o **Release precedente**.
   (L'impostazione predefinita è **Attuale**.)
3. Attivare l'opzione **Aggiorna automaticamente gli agenti**.
   (L'impostazione predefinita è **On**.)
4. Impostare l'intervallo di manutenzione.
   (L'impostazione predefinita è 23:00 - 08:00.)

Nota
Benché i processi di aggiornamento degli agenti siano progettati per essere rapidi e semplici, consigliamo sempre di scegliere un intervallo che causi un'interruzione operativa minima agli utenti, perché questi non possono prevenire o posticipare gli aggiornamenti automatici.

5. [Facoltativo] Selezionare i giorni specifici in cui eseguire gli aggiornamenti automatici.
6. Selezionare **Salva.**

Nota
Gli aggiornamenti automatici sono disponibili solo per:

- Agenti Cyber Protect, versione 15.0.26986 (rilasciata a maggio 2021) o successive.
- Agente Desktop per File Sync & Share, versione 15.0.30370 o successive.

Prima che possano avere effetto gli aggiornamenti automatici, gli agenti meno recenti devono essere aggiornati manualmente alla versione più recente.

Per monitorare gli aggiornamenti degli agenti

Importante
Gli aggiornamenti degli agenti possono essere monitorati solo se il modulo di protezione è stato abilitato.

Per monitorare gli aggiornamenti degli agenti, consultare le sezioni relative agli avvisi e alle attività della Guida per l'utente di Cyber Protect.

Configurazione dell'archivio immutabile

Lo storage immutabile consente di accedere ai backup eliminati durante un periodo di conservazione specificato. Sarà possibile ripristinare il contenuto da questi backup, ma non sarà possibile modificarli, spostarli o eliminarli. Al termine del periodo di conservazione, i backup eliminati verranno eliminati definitivamente.

Lo storage immutabile contiene i backup seguenti:

- Backup eliminati manualmente.
- Backup eliminati automaticamente in base alle impostazioni indicate nella sezione **Tempo di conservazione** di un piano di protezione o della sezione **Regole di conservazione** di un piano di pulizia.

I backup eliminati nello storage immutabile utilizzano comunque uno spazio di storage il cui consumo viene addebitato.

Lo spazio di storage utilizzato dai tenant eliminati, incluso quello per lo storage immutabile, non viene addebitato.

Per i tenant cliente, l'archivio immutabile è disponibile nelle modalità seguenti:

- **Modalità Governance**
  Questa modalità consente di disabilitare e abilitare di nuovo l'archivio immutabile, modificare il periodo di conservazione o passare alla modalità Compliance.
- **Modalità Conformità**

  Attenzione!
  La selezione della modalità Compliance è irreversibile.

  Non è possibile disabilitare l'archivio immutabile né modificare il periodo di conservazione e non è possibile tornare alla modalità Governance.

Per la configurazione delle impostazioni dello storage immutabile è necessario aver abilitato l'autenticazione a due fattori per il tenant al quale appartiene l'account amministratore.

Nota
Per consentire l'accesso ai backup eliminati, la porta 40440 dello storage di backup deve essere abilitata per le connessioni in entrata.

Per abilitare l'archivio immutabile

1. Accedere al portale di gestione come amministratore, quindi passare a **Impostazioni** > **Sicurezza**.
2. Abilitare l'opzione **Archivio immutabile**.
3. Specificare un periodo di conservazione in un intervallo compreso tra 14 e 3650 giorni.
   Il periodo di conservazione predefinito è di 14 giorni. Un periodo di conservazione più lungo implica un maggiore utilizzo dello storage.
4. Selezionare la modalità Archivio immutabile, quindi confermare la scelta se richiesto.
5. Fare clic su **Salva**.

   Attenzione!
   La selezione della **Modalità Conformità** è irreversibile. Dopo aver selezionato questa modalità, non sarà più possibile disabilitare l'archivio immutabile, modificarne la modalità o il periodo di conservazione.

6. Per far sì che un archivio esistente supporti lo storage immutabile, creare un nuovo backup in tale archivio.
   Per creare un nuovo backup, eseguire il piano di protezione in modo manuale o in base alla pianificazione.

   Attenzione!
   Se si elimina un backup prima che l'archivio supporti lo storage immutabile, tale backup verrà cancellato definitivamente.

Per disabilitare l'archivio immutabile

1. Accedere al portale di gestione come amministratore, quindi passare a **Impostazioni** > **Sicurezza**.
2. Disabilitare l'opzione **Archivio immutabile**.

   Nota
   È possibile disabilitare l'archivio immutabile solo in Modalità Governance.

   Attenzione!
   La disabilitazione dello storage immutabile non ha effetto immediato. Durante il grace period di 14 giorni, lo storage immutabile è ancora attivo e sarà possibile accedere ai backup eliminati in base al loro periodo di conservazione originale. Al termine del grace period, tutti i backup contenuti nello storage immutabile verranno eliminati definitivamente.

3. Confermare la selezione facendo clic su **Disabilita**.

Storage e agenti supportati

- Lo storage immutabile è supportato solo nel cloud storage.

  Lo storage immutabile è disponibile per i cloud storage su hosting di Acronis e dei partner che utilizzano Cyber Infrastructure versione 4.7.1 o successiva.

  Sono supportati tutti gli storage che possono essere utilizzati con Cyber Infrastructure Backup Gateway, ad esempio lo storage Cyber Infrastructure, lo storage Amazon S3 ed EC2 e lo storage Microsoft Azure.

  Lo storage immutabile richiede che la porta TCP 40440 sia aperta per il servizio Backup Gateway in Cyber Infrastructure. Nella versione 4.7.1 e successive, la porta TCP 40440 è aperta automaticamente in presenza del tipo di traffico **Backup (ABGW) public**. Per ulteriori informazioni sui tipi di traffico, consultare la documentazione di Acronis Cyber Infrastructure.
- L'archivio immutabile richiede un agente di protezione versione 21.12 (build 15.0.28532) o successive.
- Sono supportati solo i backup TIBX (Versione 12).

Gestione attività

Se l'account include l'accesso al servizio Advanced Automation, fare clic su **Gestione attività** per visualizzare e gestire i ticket del Service Desk.

Nota
Gli utenti a cui è assegnato il ruolo di Responsabile clienti in Advanced Automation possono visualizzare e gestire tutti i ticket del Service Desk dell'organizzazione; gli utenti a cui è assegnato il ruolo Cliente possono visualizzare e aggiornare solo i propri ticket.

Visualizzazione dei ticket del Service Desk

Per visualizzare i ticket del Service Desk esistenti, nel portale di gestione passare a **Gestione attività > Service Desk**. Vengono visualizzate informazioni su ogni ticket, incluso:

- Un collegamento al ticket.
- Lo stato corrente del ticket.
- Il tempo totale dedicato al ticket.
- L'utente che ha richiesto il ticket.
- Il cliente.
- La priorità del ticket.
- L'agente di supporto assegnato.
- Il contratto SLA assegnato, il termine ultimo entro il quale lo SLA deve essere rispettato per non incorrere in violazioni, quando è previsto il nuovo aggiornamento da parte di un tecnico responsabile dei ticket.
- L'ultima data di aggiornamento del ticket.

Per esportare i dati dei ticket, fare clic su **Esporta**. Un file con estensione XSL e denominato **Ticket** verrà scaricato nel workload.

È inoltre possibile filtrare e ordinare l'elenco visualizzato per individuare uno specifico ticket; per applicare filtri più avanzati, utilizzare lo strumento **Filtra** per definire quali ticket dovranno essere visualizzati.

Creazione di un ticket del Service Desk

Per creare un nuovo ticket

1. Passare a **Gestione attività > Service Desk**. Viene visualizzato un elenco di tutti i ticket aperti.

   Nota
   Gli utenti a cui è assegnato il ruolo di Responsabile clienti in Advanced Automation possono visualizzare tutti i ticket del Service Desk dell'organizzazione; gli utenti a cui è assegnato il ruolo Cliente possono visualizzare solo i propri ticket.

2. Fare clic su **+ Nuovo**. Viene visualizzata la schermata Crea nuovo ticket.
3. Definire quanto segue:
   - Nel campo **Titolo del ticket**, aggiungere il titolo del ticket.
   - Nel campo **Richiedente** (abilitato solo per gli utenti con il ruolo di Responsabile clienti), selezionare l'utente desiderato dall'elenco degli utenti e contatti attivi del cliente. Il campo **Nome cliente** è disabilitato per gli utenti con il ruolo di Responsabile clienti e Cliente.
   - [Facoltativo] Nel campo **Numero di telefono**, aggiungere il numero di telefono pertinente. Se si aggiorna il numero predefinito visualizzato, il nuovo numero viene archiviato come numero di telefono predefinito dell'utente.
   - Nel campo **Superiore**, selezionare l'utente desiderato dall'elenco degli utenti del cliente attivo (ad esempio, gli utenti a cui è assegnato il ruolo di Responsabile clienti).
   - Nella sezione **Articolo o servizio di configurazione**, selezionare una tra le opzioni **Servizio gestito** o **Servizio IT**.
     - **Servizio gestito**: questa opzione viene selezionata e precompilata con i dettagli corrispondenti se nel contratto pertinente è disponibile il tipo di prodotto Servizio gestito. L'opzione è disabilitata se nel contratto non è presente il tipo di prodotto Servizio gestito.
     - **Servizio IT**: questa opzione viene selezionata e precompilata con i dettagli corrispondenti se nel contratto pertinente è disponibile il tipo di prodotto Servizio IT. L'opzione è disabilitata se nel contratto non è presente il tipo di prodotto Servizio IT.
     - Il campo **Articolo di configurazione** mostra i dispositivi collegati al servizio IT o al servizio gestito selezionato (viene visualizzata la voce **Articolo di configurazione sconosciuto** se il dispositivo è sconosciuto); è facoltativo selezionare un dispositivo dopo aver selezionato un servizio (quando si seleziona un dispositivo in questo scenario, lo SLA non cambia e resta quello appartenente al servizio).

       Nota
       I dispositivi in elenco includono quelli forniti da Cyber Protect. Se Cyber Protection offre un'opzione di controllo remoto per uno dei dispositivi in elenco, è possibile connettersi da remoto direttamente dal ticket utilizzando il protocollo RDP o il client HTML5.

- È inoltre possibile selezionare una categoria nel campo **Categoria** e definire una priorità nel campo **Priorità**. Il campo **SLA** indica il contratto SLA sottoscritto con il managed service provider di riferimento.

- Nella sezione **Aggiornamento ticket**, è possibile aggiungere alla casella di testo visualizzata descrizioni e commenti formattati, incluse immagini e altri file multimediali per un massimo di 25 MB; i tipi e i formati supportati sono elencati nella sezione **Allegati** della casella di testo visualizzata. Lo stato del ticket viene impostato su **Nuovo** per impostazione predefinita e non può essere modificato.
- Abilitare l'interruttore **Invia e-mail al richiedente** per garantire che tutti gli aggiornamenti ai ticket siano inviati al richiedente.
- Nella sezione **Allegati**, fare clic (oppure trascinare e rilasciare) per aggiungere ogni allegato necessario.

  È possibile allegare uno qualsiasi dei seguenti formati e tipi di file, per un massimo di 25 MB.
  - File multimediali: .avi, .mp4, .mp3
  - E-mail: .eml, .msg
  - Immagini: .png, .gif, .jpeg, .jpg, .heic, .bmp, .tiff, .svg
  - Documenti e file di registro: .doc, .docx, .xls, .xlsx, .ppt, .pptx, .txt, .log, .pdf
  - Archivi: .zip, .rar

4. Fare clic su **Fine**. Una volta generato, il ticket viene aggiunto all'elenco dei ticket aperti.

Aggiornamento dei ticket del Service Desk

Per aggiornare un ticket

1. Passare a **Gestione attività > Service Desk**. Viene visualizzato un elenco di tutti i ticket attualmente aperti.

   Nota
   Gli utenti a cui è assegnato il ruolo di Responsabile clienti in Advanced Automation possono visualizzare tutti i ticket del Service Desk dell'organizzazione; gli utenti a cui è assegnato il ruolo Cliente possono visualizzare solo i propri ticket.

2. (Facoltativo) In presenza di un numero elevato di ticket, utilizzare il filtro per individuare i ticket a cui si è interessati.

   Fare clic su **Filtro** (o su **Filtri salvati** se è stato precedentemente definito un filtro) e selezionare i valori pertinenti dai campi visualizzati. È possibile fare clic sull'opzione **Aggiungi a filtri salvati** per salvare il filtro definito e utilizzarlo successivamente.

   In alternativa, utilizzare la barra **Cerca** per individuare i ticket pertinenti.
3. Fare clic sul collegamento alla riga del ticket pertinente e apportare le modifiche necessarie nelle schede visualizzate.

- **Attività**: visualizza le attività recenti effettuate sul ticket, incluso lo stato corrente e i commenti aggiunti al ticket.

  Nota
  Se lo stato di un ticket generato da un avviso nella console di Cyber Protect viene impostato su **Chiuso**, viene chiuso anche l'avviso nella console di Cyber Protect.

- **Panoramica**: visualizza le impostazioni generali del ticket, che possono essere modificate come necessario; per ulteriori informazioni, consultare "Creazione di un ticket del Service Desk" (pag. 39).

  In questa scheda è possibile modificare lo stato del ticket; ad esempio, impostare lo stato del ticket su **In corso** quando si inizia a lavorare sul ticket o modificarlo in **Chiuso** quando è possibile chiuderlo. È anche possibile modificare i dispositivi collegati un ticket; ad esempio, se è stato creato un ticket che non include il dispositivo corretto, è possibile fare clic sull'elenco a discesa **Articolo di configurazione** per selezionare il dispositivo pertinente.

Per ulteriori informazioni sui vari campi disponibili quando si modifica un ticket, consultare "Creazione di un ticket del Service Desk" (pag. 39).

4. Fare clic su **Salva modifiche**.

   Tenere presente che se l'interruttore **Invia e-mail al richiedente** è abilitato, all'utente corrispondente viene inviata un'e-mail.

Monitoraggio

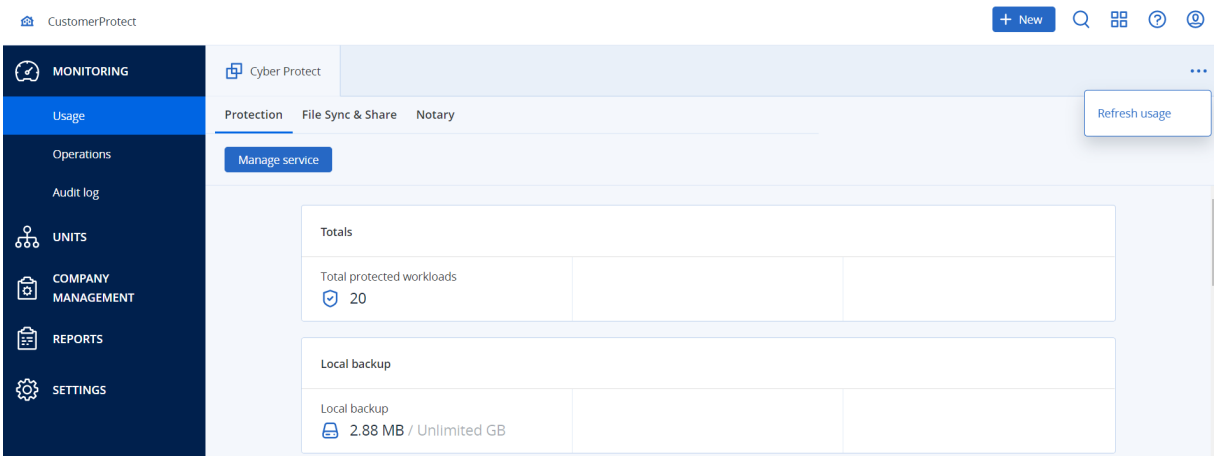
Per accedere alle informazioni sull'utilizzo dei servizi e sulle operazioni, fare clic su **Monitoraggio**.

Utilizzo

La scheda **Utilizzo** fornisce una panoramica dell'utilizzo dei servizi, incluse le quote se presenti, e consente di accedere alle console dei servizi.

Per aggiornare i dati di utilizzo visualizzati sulla scheda, fare clic sui puntini di sospensione nell'angolo in alto a destra dello schermo e selezionare **Aggiorna utilizzo**.

Nota
Il recupero dei dati può richiedere fino a 10 minuti. Ricaricare la pagina per visualizzare i dati aggiornati.



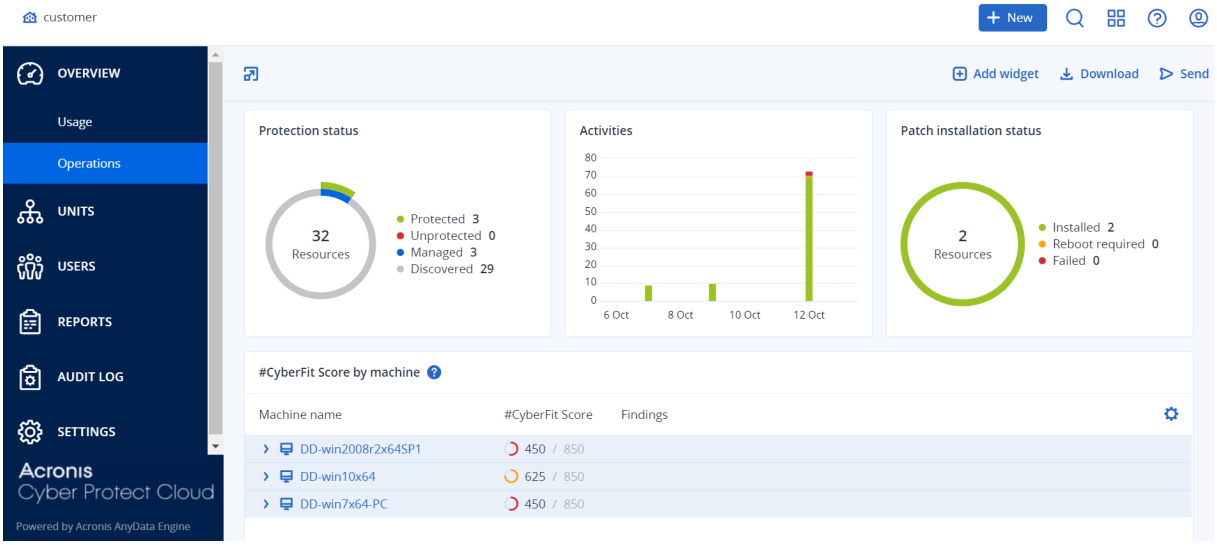
Dashboard Operazioni

Il pannello di controllo **Operazioni** è disponibile soltanto agli amministratori dell'azienda che operano a livello aziendale.

Il pannello di controllo **Operazioni** fornisce una serie di widget personalizzabili che offrono un'anteprima delle operazioni relative al servizio Cyber Protection.

I widget sono aggiornati ogni due minuti. I widget presentano elementi cliccabili che consentono di indagare e risolvere i problemi. È possibile scaricare lo stato corrente del pannello di controllo in formato .pdf e/o .xlsx, oppure inviarlo tramite e-mail.

È possibile scegliere tra numerosi widget, presentati come tabelle, grafici a torta, a barre e mappe ad albero. È inoltre possibile aggiungere numerosi widget dello stesso tipo con filtri diversi.



Per riorganizzare i widget nel pannello di controllo

Trascinare e rilasciare i widget facendo clic sui rispettivi nomi.

Per modificare un widget

Fare clic sull'icona a forma di matita accanto al nome del widget. La modifica del widget consente all'utente di rinominarlo, modificarne l'intervallo temporale e impostare i filtri.

Per aggiungere un widget

Fare clic su **Aggiungi widget** e quindi eseguire una delle seguenti operazioni:

- Fare clic sul widget che si desidera aggiungere. Il widget verrà aggiunto con le impostazioni predefinite.
- Per modificare il widget prima di aggiungerlo, fare clic sull'icona a forma di matita visualizzata quando il widget è selezionato. Dopo aver modificato il widget, fare clic su **Fine**.

Per rimuovere un widget

Fare clic sul simbolo X accanto al nome del widget.

Stato protezione

Stato protezione

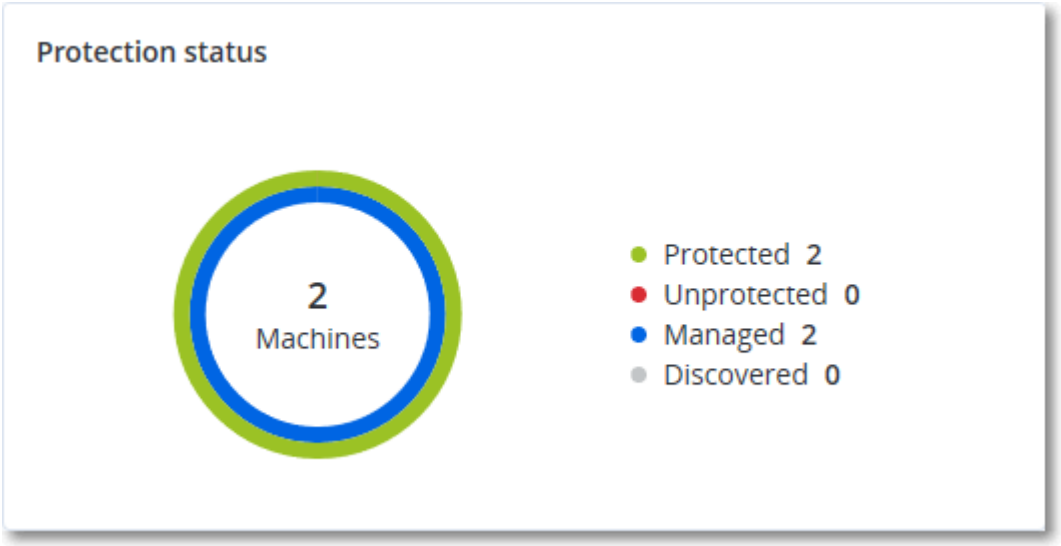
Questo widget mostra lo stato della protezione corrente di tutti i sistemi.

Un sistema può trovarsi in uno dei seguenti stati:

- **Protetto**: per tutti i sistemi con un piano di protezione applicato.
- **Non protetto**: per tutti i sistemi senza un piano di protezione applicato. Sono inclusi i sistemi individuati e quelli gestiti ai quali non è applicato un piano di protezione.

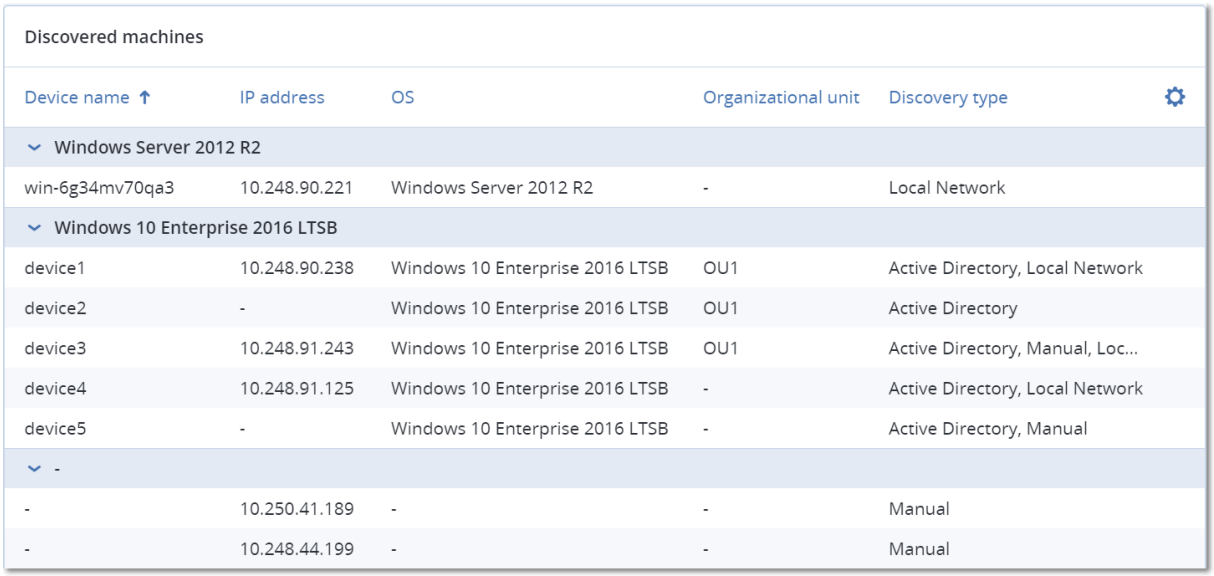
- **Gestito**: per tutti i sistemi con l'agente di protezione installato.
- **Individuato** : per tutti i sistemi senza l'agente di protezione installato.

Facendo clic sullo stato, si verrà reindirizzati all'elenco dei sistemi che presentano tale stato, per maggiori informazioni.



Macchine individuate

Questo widget mostra l'elenco dei sistemi rilevati durante l'intervallo di tempo specificato.



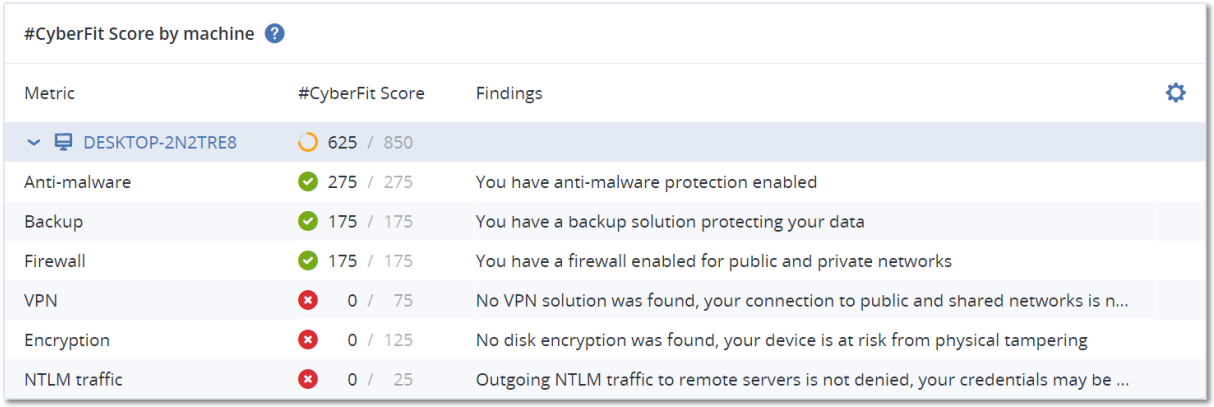
#CyberFit Score per sistema

Questo widget mostra, per ogni sistema, il #CyberFit Score totale, i punteggi che lo compongono e i risultati ottenuti per ogni metrica valutata:

- Anti-malware
- Backup
- Firewall
- VPN
- Crittografia
- Traffico NTLM

Per migliorare il punteggio di ogni metrica è possibile visualizzare le raccomandazioni disponibili nel report.

Per ulteriori informazioni sul #CyberFit Score, consultare "#CyberFit Score dei sistemi".



Widget di Endpoint Detection and Response (EDR)

Importante
Si tratta di una versione con Accesso prioritario alla documentazione EDR. Alcune delle funzionalità e delle descrizioni potrebbero essere incomplete.

Endpoint Detection and Response (EDR) include una serie di widget a cui è possibile accedere dalla dashboard **Operazioni**.

I widget disponibili sono:

- Distribuzione dei principali problemi per workload
- MTTR del problema
- Burndown dei problemi di sicurezza
- Stato della rete dei workload

Distribuzione dei principali problemi per workload

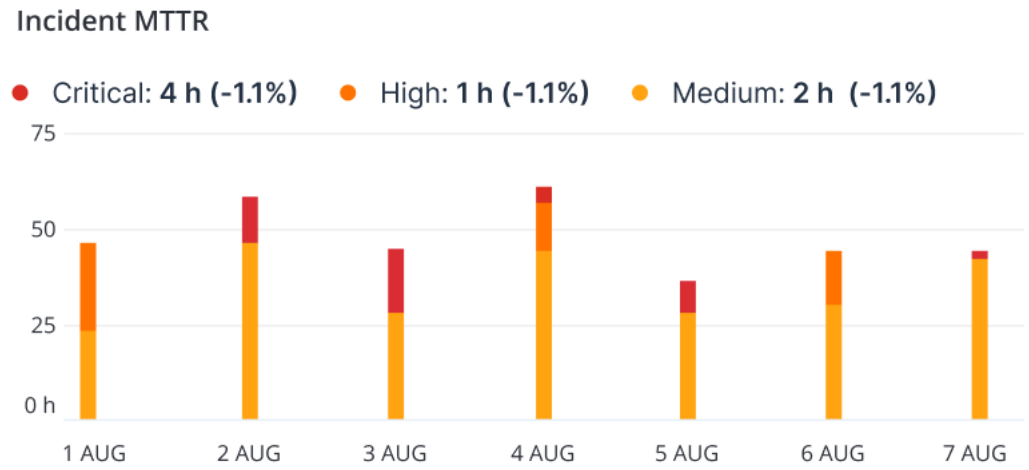
Questo widget mostra i primi cinque workload con il maggior numero di problemi (fare clic su **Mostra tutto** per essere reindirizzati all'elenco dei problemi filtrato in base alle impostazioni del widget).

Passare il mouse su una riga del workload per visualizzare i dettagli dello stato corrente delle indagini sui problemi; i possibili stati dell'indagine sono **Non avviata**, **Indagine in corso**, **Chiusa** e **Falso positivo**. Fare quindi clic sul workload che si desidera analizzare ulteriormente e selezionare il cliente di interesse nella finestra popup visualizzata; l'elenco dei problemi viene aggiornato in base alle impostazioni del widget.

MTTR del problema

Questo widget mostra il tempo medio di risoluzione dei problemi di sicurezza. Indica la rapidità con la quale i problemi vengono analizzati e risolti.

Fare clic su una colonna per visualizzare in dettaglio i problemi in base al livello di gravità (**Critico**, **Alto** e **Medio**) e un'indicazione del tempo impiegato per risolverli in base ai diversi livelli di gravità. Il valore in percentuale (%) mostrato tra parentesi indica l'aumento o la diminuzione rispetto al periodo di tempo precedente.

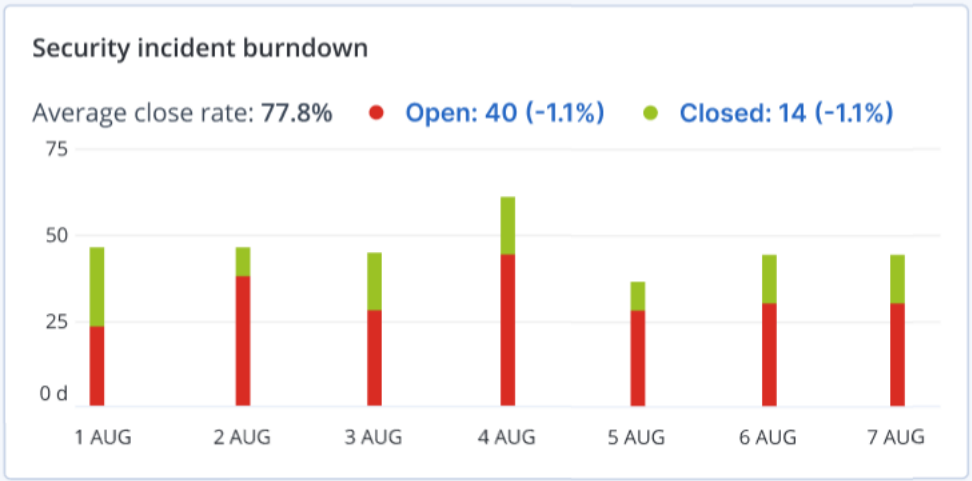


Burndown dei problemi di sicurezza

Questo widget indica il tasso di efficienza nella risoluzione dei problemi; il numero di problemi aperti viene misurato a fronte del numero di problemi chiusi in un determinato periodo di tempo.

Passare il mouse su una colonna per visualizzare in dettaglio i problemi chiusi o aperti per il giorno selezionato. Se si fa clic sul valore Aperto, viene visualizzata una finestra popup nella quale è possibile selezionare il tenant di interesse; viene visualizzato l'elenco dei problemi filtrati relativi al tenant, dal quale è possibile osservare i problemi attualmente aperti (con lo stato **Indagine in corso** o **Non avviata**). Se si fa clic sul valore Chiuso, viene visualizzato l'elenco dei problemi per il tenant selezionato, filtrato per visualizzare i problemi non più aperti (con lo stato **Chiuso** o **Falso positivo**).

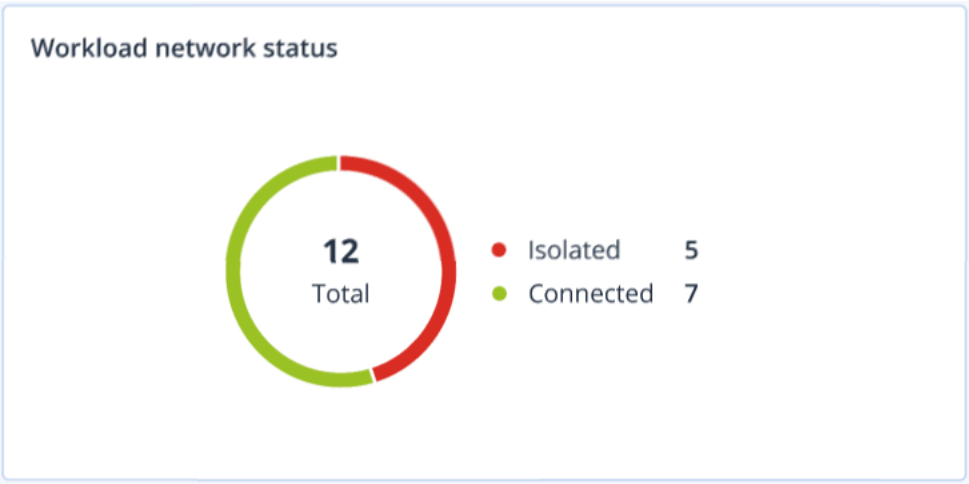
Il valore in percentuale (%) mostrato tra parentesi indica l'aumento o la diminuzione rispetto al periodo di tempo precedente.



Stato della rete dei workload

Questo widget mostra lo stato corrente della rete dei workload e indica il numero di workload isolati e connessi.

Fare clic sul valore Isolato; viene visualizzata una finestra popup nella quale selezionare il tenant di interesse. La vista del workload visualizzata viene filtrata per mostrare i workload isolati. Fare clic sul valore Connesso per visualizzare l'elenco Workload con agenti filtrato per mostrare i workload connessi (per il tenant selezionato).



Monitoraggio integrità del disco

Il monitoraggio dell'integrità del disco fornisce informazioni sullo stato corrente del disco e su quello prevedibile, così da prevenire perdite di dati che potrebbero essere correlate a un guasto del disco. La funzione supporta dischi HDD e SSD.

Limitazioni

- La previsione dell'integrità del disco è supportata solo per i sistemi che eseguono Windows.
- È possibile monitorare solo i dischi dei sistemi fisici. Non è possibile monitorare e mostrare nel widget dell'integrità del disco i dischi delle virtual machine.
- Non sono supportate le configurazioni RAID. I widget di integrità del disco non includono informazioni sui sistemi in cui è implementato RAID.
- Le unità SSD NVMe non sono supportate.

L'integrità del disco è rappresentata da uno dei seguenti stati:

- **OK**
  L'integrità del disco è compresa tra il 70 e il 100%.
- **Attenzione**
  L'integrità del disco è compresa tra il 30 e il 70%.
- **Critico**
  L'integrità del disco è compresa tra lo 0 e il 30%.
- **Calcolo dei dati del disco in corso**
  È in corso il calcolo dello stato corrente del disco e delle previsioni.

Come funziona

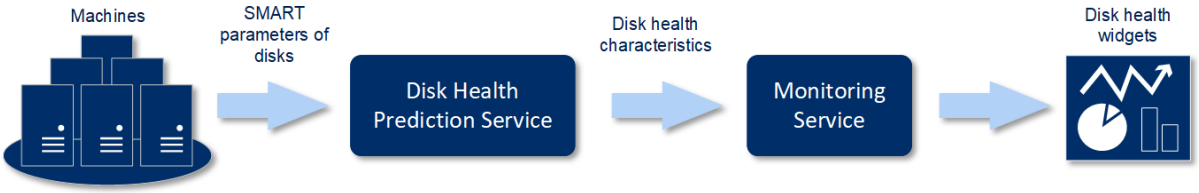
Il servizio Previsione dell'integrità del disco utilizza un modello di previsione basato su intelligenza artificiale.

1. L'agente di protezione acquisisce i parametri SMART dei dischi e invia i dati raccolti al servizio Previsione dell'integrità del disco:
   - SMART 5 – Conteggio dei settori riallocati.
   - SMART 9 – Ore di attività.
   - SMART 187 – Errori non correggibili segnalati.
   - SMART 188 – Timeout comando.
   - SMART 197 – Conteggio settori attualmente in sospeso.
   - SMART 198 – Conteggio settori non correggibili offline.
   - SMART 200 – Frequenza errori di scrittura.
2. Il servizio Previsione dell'integrità del disco elabora i parametri SMART ricevuti, effettua le previsioni e fornisce quindi le informazioni seguenti sull'integrità del disco:

- Stato corrente di integrità del disco: OK, Attenzione, Critico.
- Previsione dell'integrità del disco: negativa, stabile, positiva.
- Probabilità della previsione dell'integrità del disco in percentuale.

Il periodo di previsione è un mese.

3. Il Servizio di monitoraggio riceve queste caratteristiche e quindi mostra le informazioni pertinenti nei widget di integrità del disco nella console di Cyber Protect.



Widget di integrità del disco

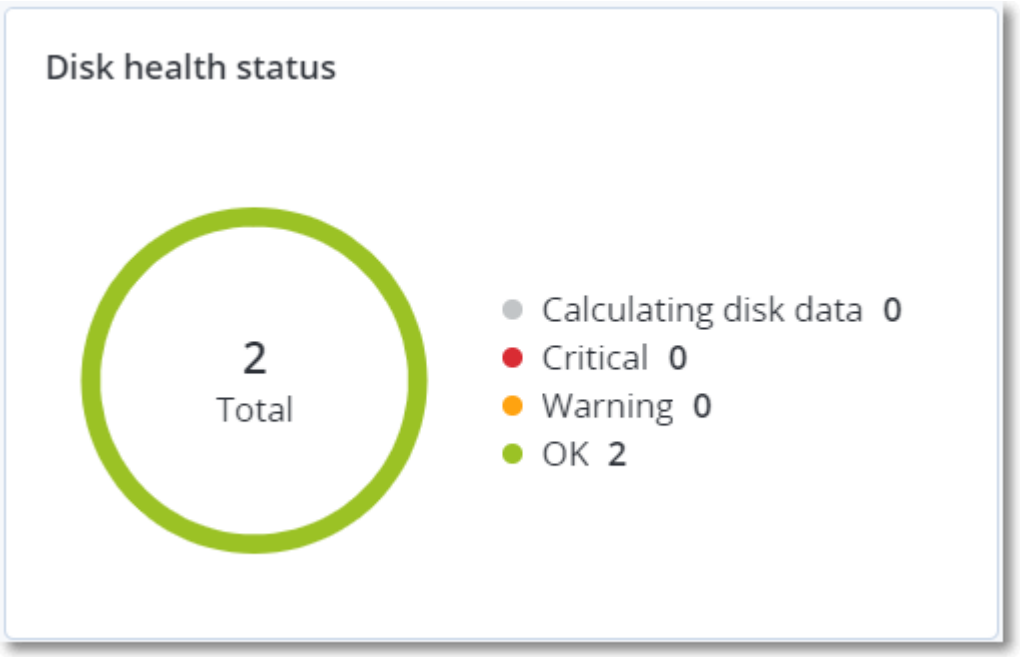
I risultati del monitoraggio dell'integrità del disco vengono presentati nei widget seguenti, disponibili nella console di Cyber Protect.

- **Panoramica dell'integrità del disco** è un widget con struttura ad albero dotata di due livelli di dettaglio, visualizzabili eseguendo il drill down:
  - Livello del sistema
    Mostra informazioni di riepilogo sullo stato dell'integrità del disco di sistemi selezionati del cliente. Vengono mostrati solo gli stati del disco critici. Gli altri stati vengono mostrati nei suggerimenti visualizzati quando si passa il mouse su uno specifico blocco. La dimensione del blocco del sistema dipende dalla dimensione totale di tutti i dischi del sistema. Il colore del blocco del sistema dipende dallo stato del disco con maggiore criticità individuato.

- Livello del disco
  Mostra lo stato corrente dell'integrità del disco di tutti i dischi del sistema selezionato. Ogni blocco disco mostra una delle seguenti previsioni di integrità del disco e la sua probabilità, espressa in percentuale:
  - Verrà danneggiato
  - Resterà stabile

- Verrà migliorato

- **Stato di integrità del disco** è un widget con grafico a torta che mostra il numero di dischi per ogni stato.



Avvisi di stato dell'integrità del disco

Il controllo dell'integrità del disco viene eseguito ogni 30 minuti, mentre l'avviso corrispondente viene generato una volta al giorno. Viene sempre generato un avviso quando lo stato di integrità del disco passa da **Attenzione** a **Critico**.

Nome avviso	Gravità	Stato integrità del disco	Descrizione
È possibile che il disco sia stato danneggiato	Attenzione	(30 – 70)	Il disco <nome disco> di questo sistema potrebbe subire un guasto nel prossimo futuro. Eseguire il backup dell'immagine completa del disco il più presto possibile, sostituirlo e quindi ripristinare l'immagine sul nuovo disco.
Il guasto del disco è imminente	Critico	(0 – 30)	Il disco <nome disco> in questo sistema è in condizioni critiche e potrebbe subire un danno nell'immediato futuro. Con queste condizioni il backup dell'immagine del disco non è consigliato, perché il lavoro aggiuntivo richiesto potrebbe causare il guasto del disco. Eseguire immediatamente il backup dei file più importanti presenti sul disco, e sostituirlo.

Mappa di protezione dati

La funzione Mappa di protezione dati consente di individuare tutti i dati ritenuti importanti e di ottenere informazioni dettagliate su numero, dimensione, posizione, stato della protezione di tutti i file rilevanti, in una vista scalabile con mappa ad albero.

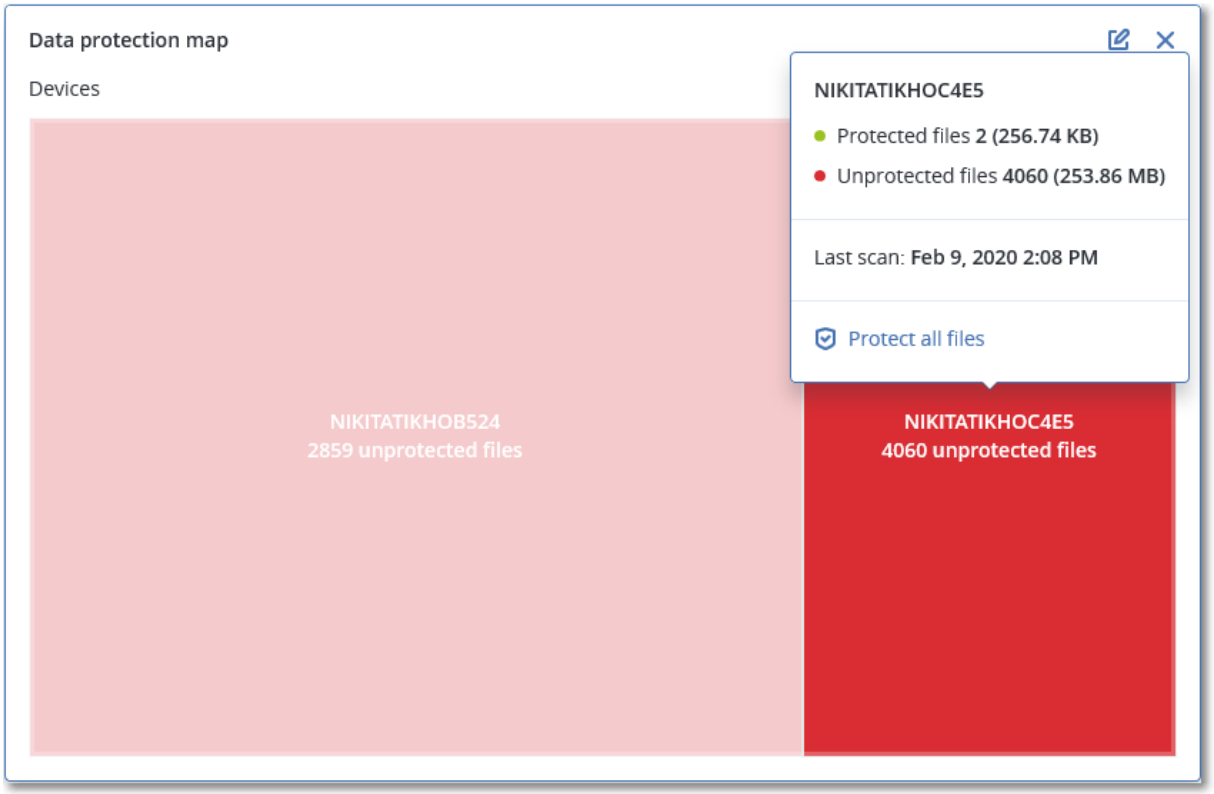
Ogni dimensione del blocco dipende dal numero/dimensione totale di tutti i file importanti che appartengono a un cliente/sistema.

I file possono presentare uno dei seguenti stati di protezione:

- **Critico** – è presente una percentuale compresa tra il 51 e il 100% di file non protetti con le estensioni specificate dall'utente di cui non viene eseguito il backup e di cui il backup non verrà eseguito con le impostazioni di backup esistenti per il sistema/la a posizione selezionati.
- **Basso** – è presente una percentuale compresa tra il 21 e il 50% di file non protetti con le estensioni specificate dall'utente di cui non viene eseguito il backup e di cui il backup non verrà eseguito con le impostazioni di backup esistenti per il sistema/la posizione selezionati.
- **Medio** – è presente una percentuale compresa tra l'1 e il 20% di file non protetti con le estensioni specificate dall'utente di cui non viene eseguito il backup e di cui il backup non verrà eseguito con le impostazioni di backup esistenti per il sistema/la posizione selezionati.
- **Alto** – tutti i file con le estensioni specificate dall'utente sono protetti (viene eseguito il backup) per il sistema/la posizione selezionati.

I risultati dell'analisi della protezione dati sono disponibili nel pannello di controllo del widget Mappa di protezione dati, una mappa ad albero che mostra i dettagli a livello di sistema:

- Livello del sistema – mostra informazioni di riepilogo sullo stato di protezione dei file importanti dei clienti selezionati.



Per proteggere file che non sono protetti, passare il mouse sul blocco e fare clic su **Proteggi tutti i file**. Nella finestra di dialogo sono reperibili informazioni sul numero di file non protetti e sulla loro posizione. Per proteggerli, fare clic su **Proteggi tutti i file**.

È inoltre possibile scaricare un rapporto dettagliato in formato CSV.

Widget di valutazione delle vulnerabilità

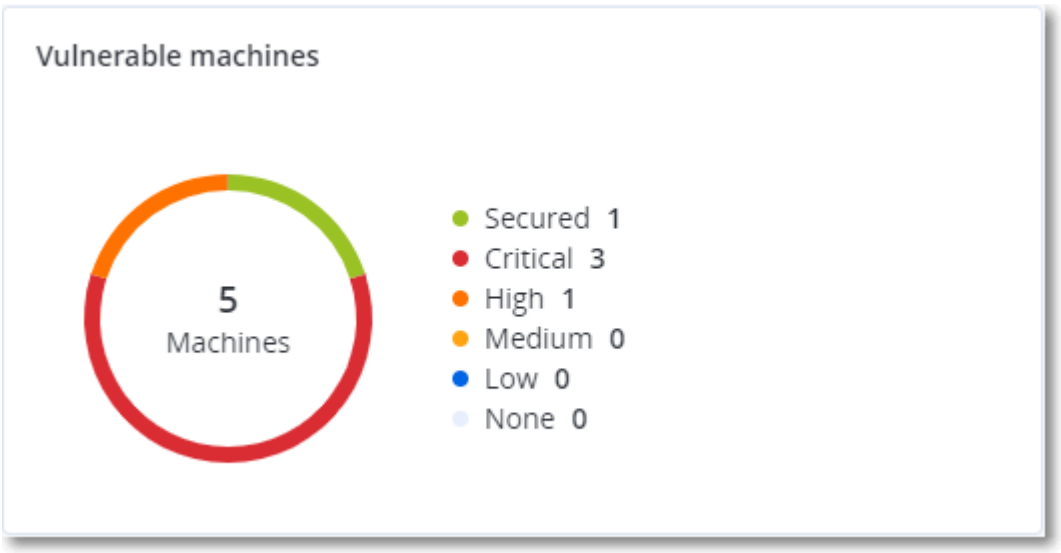
Sistemi vulnerabili

Questo widget mostra i sistemi vulnerabili ordinati in base alla gravità della vulnerabilità.

Conformemente al sistema CVSS (Common Vulnerability Scoring System) v3.0, la vulnerabilità individuata può presentare uno dei seguenti livelli di gravità:

- Protetto: non sono state individuate vulnerabilità
- Critico: 9.0 - 10.0 CVSS
- Alto: 7.0 - 8.9 CVSS
- Medio: 4.0 - 6.9 CVSS

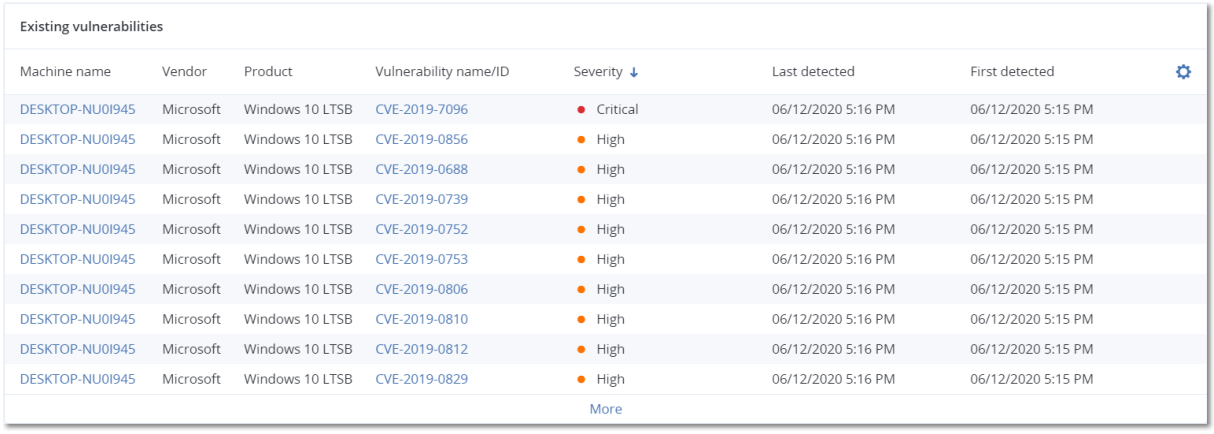
- Basso: 0.1 - 3.9 CVSS
- Nessuno: 0.0 CVSS



Vulnerabilità esistenti

Questo widget mostra le vulnerabilità attualmente esistenti sui sistemi. Nel widget **Vulnerabilità esistenti** sono presenti due colonne che mostrano gli indicatori data e ora:

- **Individuata per la prima volta** – la data e l'ora della prima individuazione della vulnerabilità nel sistema.
- **Individuata l'ultima volta** – la data e l'ora dell'ultima individuazione della vulnerabilità nel sistema.



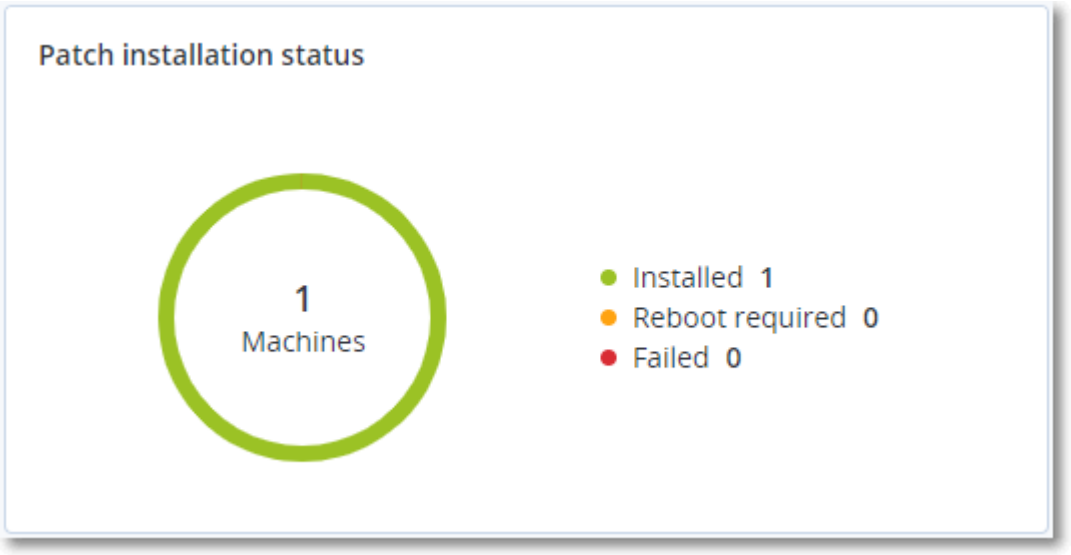
Widget di installazione patch

Sono disponibili quattro widget correlati alla funzionalità di gestione delle patch.

Stato di installazione patch

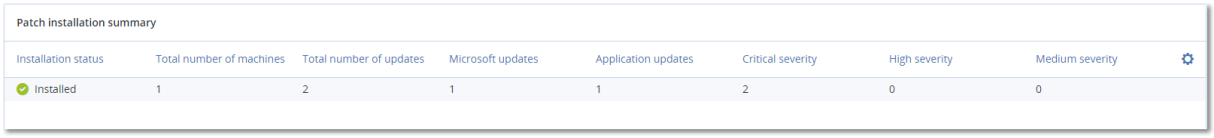
Questo widget mostra il numero di sistemi raggruppati in base allo stato di installazione delle patch.

- **Installate** – tutte le patch disponibili sono installate in un sistema
- **Riavvio necessario** – dopo l'installazione della patch, è richiesto il riavvio di un sistema
- **Non riuscita** – l'installazione di una patch non è riuscita in un sistema



Riepilogo di installazione patch

Questo widget mostra il riepilogo delle patch presenti nei sistemi, in base allo stato di installazione delle patch.



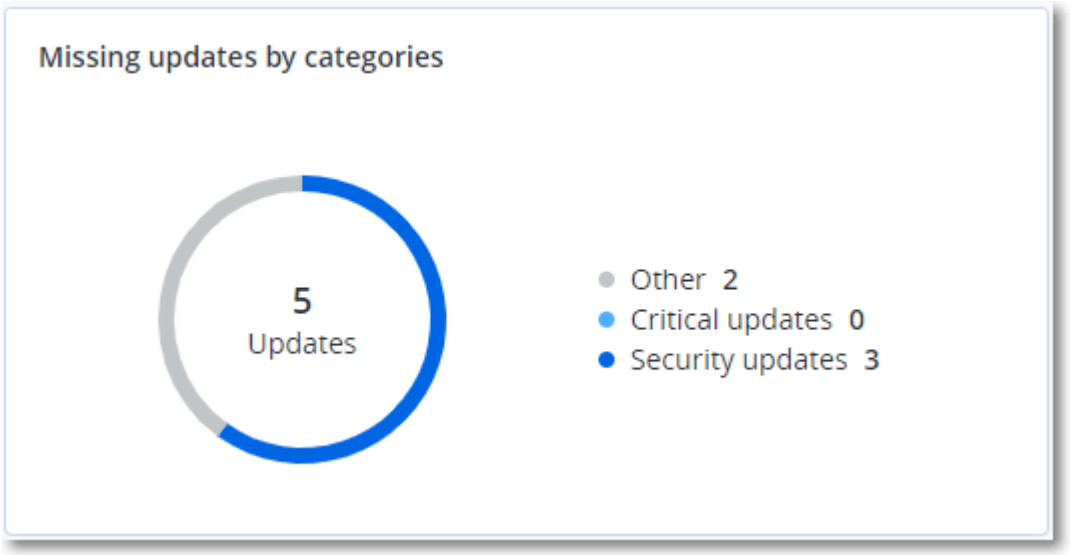
Cronologia di installazione patch

Questo widget mostra informazioni dettagliate sulle patch installate nei sistemi.

Aggiornamenti non effettuati per categorie

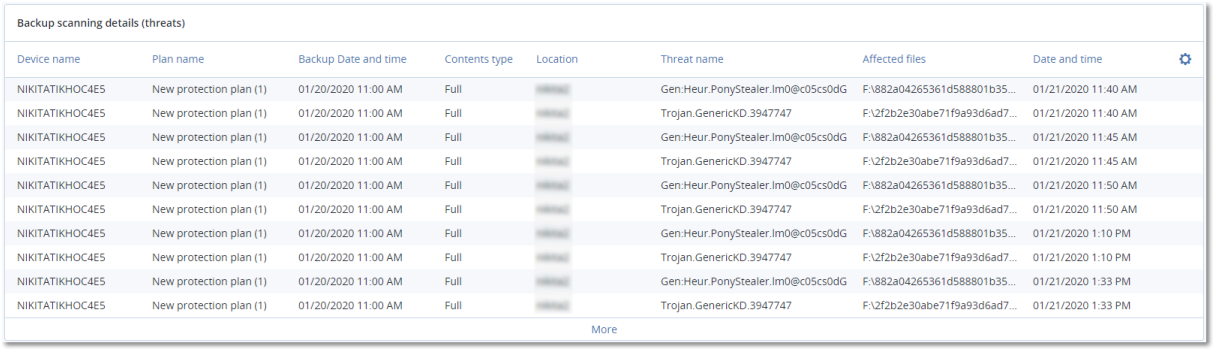
Questo widget mostra il numero di aggiornamenti non effettuati, per categoria. Vengono mostrate le seguenti categorie:

- Aggiornamenti di sicurezza
- Aggiornamenti critici
- Altro



Informazioni sulla scansione del backup

Questo widget mostra informazioni dettagliate sulle minacce individuate nei backup.



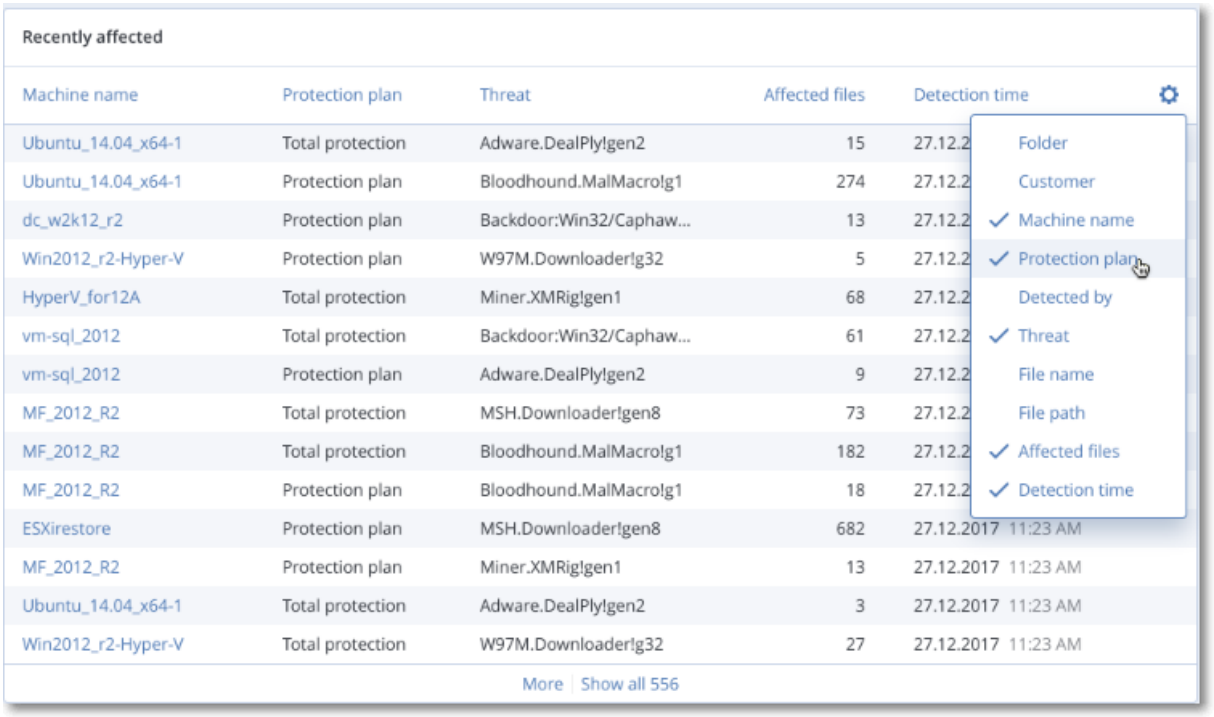
Backup scanning details (threats)

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

Recentemente interessato

Questo widget mostra informazioni dettagliate sui workload recentemente interessati da minacce quali virus, malware e ramsomware. Lo strumento rende disponibili informazioni sulle minacce individuate, l'orario di individuazione e il numero di file infettati.



Download dei dati relativi ai workload recentemente interessati

È possibile scaricare i dati relativi ai workload recentemente interessati, generare un file CSV e inviarlo ai destinatari specificati.

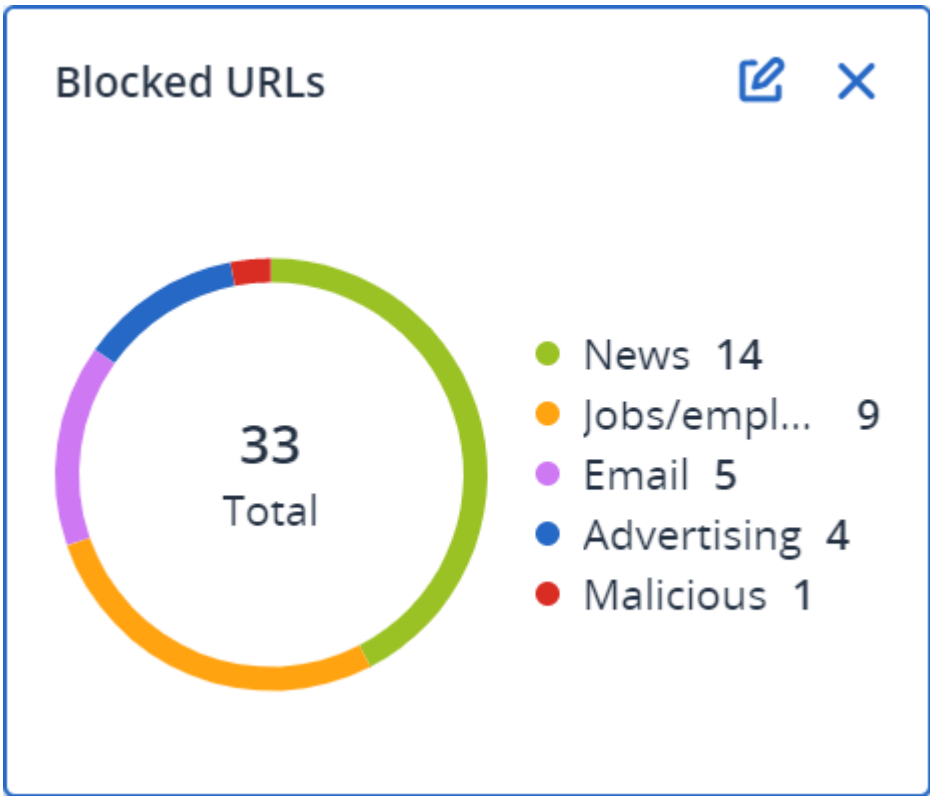
Per scaricare i dati relativi ai workload recentemente interessati

1. Nel widget **Recentemente interessati** fare clic su **Scarica dati**.
2. Nel campo **Periodo di tempo**, inserire il numero di giorni per i quali scaricare i dati. Il numero massimo di giorni che è possibile inserire è 200.
3. Nel campo **Destinatari**, immettere gli indirizzi e-mail di tutte le persone che riceveranno un'e-mail con il link per scaricare il file CSV.
4. Fare clic su **Download**.

   Il sistema avvia la generazione del file CSV contenente i dati relativi ai workload interessati per il periodo di tempo specificato. Una volta completato il file CSV, il sistema invia un'e-mail ai destinatari. Ogni destinatario potrà quindi scaricare il file CSV.

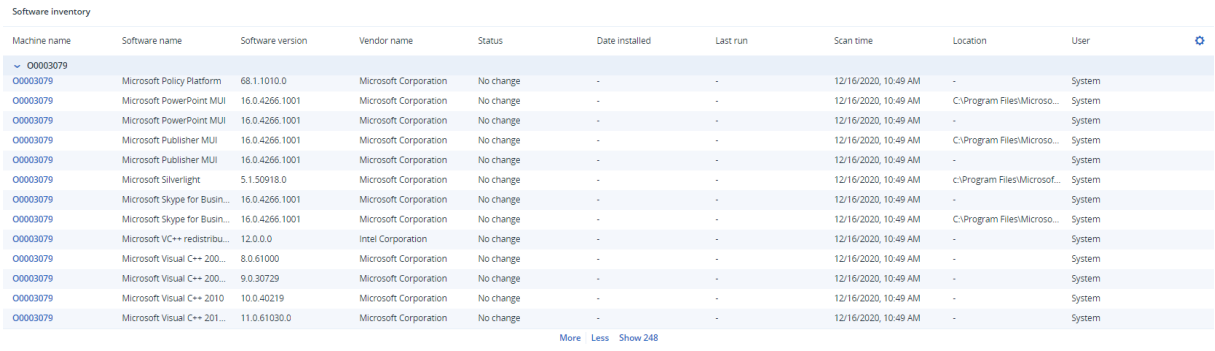
URL bloccati

Il widget mostra le statistiche degli URL bloccati per categoria. Per ulteriori informazioni sui filtri URL e la divisione in categorie, consultare il manuale utente del servizio Cyber Protection.

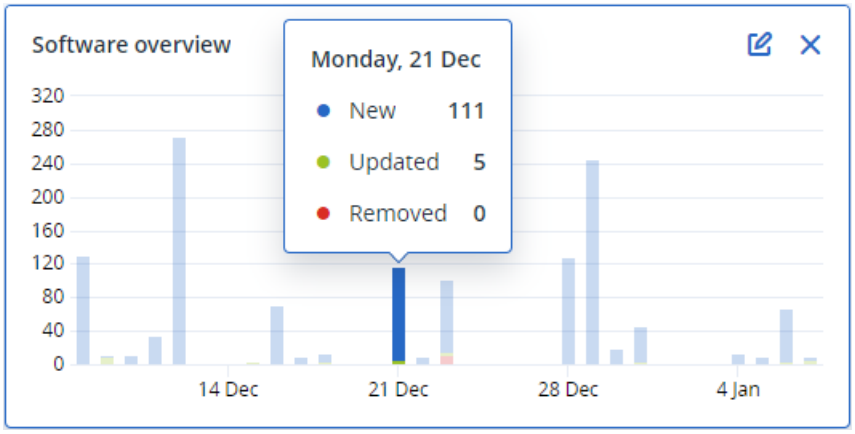


Widget Inventario software

Il widget di tabella **Inventario software** mostra informazioni dettagliate su tutti i componenti software installati nei sistemi Windows e macOS dell'organizzazione.



Il widget **Panoramica software** mostra il numero di applicazioni nuove, aggiornate ed eliminate sui sistemi Windows e macOS dell'organizzazione per il periodo di tempo specificato (7 giorni, 30 giorni o mese corrente).



Quando si passa il mouse su una determinata barra del grafico, viene visualizzato un suggerimento che mostra le informazioni seguenti:

Nuove - il numero di nuove applicazioni installate.

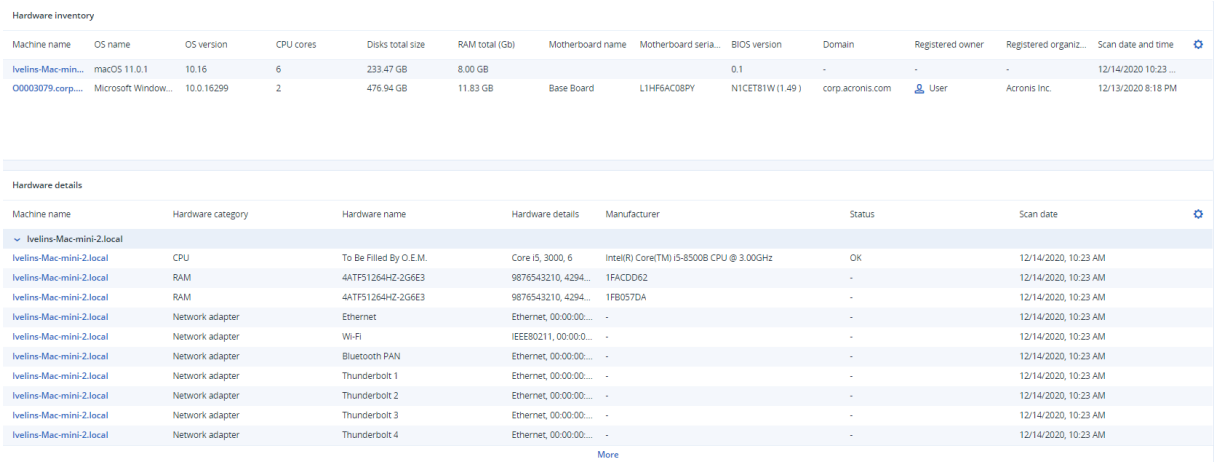
Aggiornate - il numero di applicazioni aggiornate.

Rimosse - il numero di applicazioni rimosse.

Facendo clic sulla parte di barra relativa a un determinato stato, l'utente viene reindirizzato alla pagina **Gestione software** -> **Inventario software**. Le informazioni presenti nella pagina sono filtrate in base alla data e allo stato corrispondenti.

Widget Inventario hardware

I widget di tabella **Inventario hardware** e **Dettagli hardware** mostrano informazioni su tutti i componenti hardware installati sui dispositivi Windows e macOS fisici e virtuali dell'organizzazione.



Il widget di tabella **Modifiche hardware** mostra informazioni su tutti i componenti hardware aggiunti, eliminati e modificati sui sistemi Windows e macOS fisici e virtuali dell'organizzazione per il periodo di tempo specificato (7 giorni, 30 giorni o mese corrente).

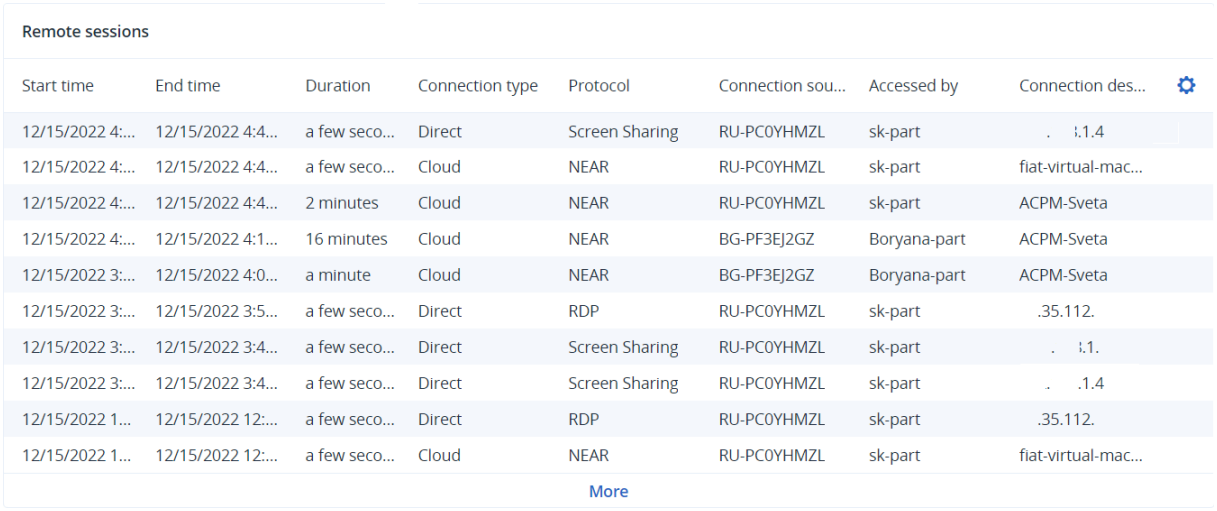
Hardware changes

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

More

Cronologia della sessione

Il widget mostra informazioni dettagliate sulle sessioni di desktop remoto e di trasferimento di file eseguite nell'organizzazione in un intervallo di tempo specificato.



Remote sessions

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

More

Registro di audit

Per visualizzare il registro di audit, fare clic su **Monitoraggio** > **Registro di audit**.

Il registro di audit contiene una registrazione cronologica degli eventi seguenti:

- Operazioni eseguite dagli utenti nel portale di gestione
- Operazioni con risorse cloud-to-cloud eseguite dagli utenti nella console di Cyber Protect
- Operazioni di Cyber Scripting eseguite dagli utenti nella console di Cyber Protect
- Messaggi di sistema relativi a consumo di quote e quote raggiunte

Il registro visualizza gli eventi dell'organizzazione o dell'unità che si sta utilizzando e le relative unità figlio. È possibile fare clic su un evento per visualizzare ulteriori informazioni.

I registri di audit sono archiviati nei data center e la loro disponibilità non può essere influenzata dai problemi sui sistemi degli utenti finali.

La pulizia del registro avviene giornalmente. Gli eventi vengono rimossi dopo 180 giorni.

Campi del registro di audit

Per ogni evento il registro visualizza i campi seguenti:

- **Evento**
  Breve descrizione dell'evento. Ad esempio: **Tenant creato**, **Tenant eliminato**, **Utente creato**, **Utente eliminato**, **Quota raggiunta**, **Contenuto di backup esaminato**, **Script modificato**.
- **Gravità**
  Una tra le seguenti:
  - **Errore**
    Indica un errore.
  - **Attenzione**
    Indica un'azione potenzialmente negativa. Ad esempio: **Tenant eliminato**, **Utente eliminato**, **Quota raggiunta**.
  - **Avviso**
    Indica un evento che potrebbe richiedere attenzione. Ad esempio: **Tenant aggiornato**, **Utente aggiornato**.
  - **Informativo**
    Indica una modifica o un'azione informativa neutrale. Ad esempio: **Tenant creato**, **Utente creato**, **Quota aggiornata**, **Piano di scripting eliminato**.
- **Data**
  Data e ora in cui si è verificato l'evento.
- **Nome oggetto**
  L'oggetto sul quale è stata eseguita l'operazione. Ad esempio, l'oggetto dell'evento **Utente aggiornato** è l'utente di cui sono state modificate le proprietà. Per gli eventi correlati a una quota, l'oggetto è la quota.
- **Tenant**
  Il nome dell'unità a cui appartiene l'oggetto. Ad esempio, il tenant dell'evento **Utente aggiornato** è l'unità in cui si trova l'utente. Il tenant dell'evento **Quota raggiunta** è l'utente la cui quota è stata raggiunta.
- **Iniziatore**
  Il login dell'utente che ha avviato l'evento. Per i messaggi di sistema e gli eventi avviati da amministratori di livello superiore, l'iniziatore viene visualizzato come **Sistema**.
- **Tenant dell'iniziatore**
  Il nome dell'unità a cui appartiene l'iniziatore. Per i messaggi di sistema e gli eventi avviati da amministratori di livello superiore, il campo è vuoto.
- **Metodo**
  Mostra se l'evento è stato avviato tramite l'interfaccia Web o tramite l'API.
- **IP**
  L'indirizzo IP della macchina dalla quale è stato avviato l'evento.

Filtri e ricerca

È possibile filtrare gli eventi in base a tipo, gravità o data. È inoltre possibile eseguire una ricerca tra gli eventi in base a nome, oggetto, tenant, iniziatore e tenant dell'iniziatore.

Elaborazione di rapporti

Per accedere ai report sull'utilizzo dei servizi e sulle operazioni, fare clic su **Report**.

Nota
Questa funzionalità non è disponibile nelle edizioni Standard del servizio Cyber Protection.

Report utilizzo

I report sull'utilizzo forniscono dati cronologici relativi all'utilizzo dei servizi. I report di utilizzo sono disponibili nei formati CSV e HTML.

Tipo di rapporto

È possibile selezionare uno dei seguenti tipi di report:

- **Utilizzo corrente**
  Il rapporto contiene le metriche di utilizzo correnti del servizio.
- **Riepilogo per il periodo**
  Il rapporto contiene le metriche di utilizzo del servizio relative al termine del periodo specificato e la differenza tra le metriche all'inizio e alla fine del periodo specificato.
- **Giorno per giorno per il periodo**
  Il rapporto contiene le metriche di utilizzo correnti del servizio e le relative modifiche per ogni giorno del periodo specificato.

Ambito del report

È possibile selezionare l'ambito del report tra i seguenti valori:

- **Clienti e partner diretti**
  Il report conterrà le statistiche di utilizzo del servizio relative solo alle unità figlio immediate della società o dell'unità nella quale si sta lavorando.
- **Tutti i clienti e i partner**
  Il report conterrà le statistiche di utilizzo del servizio relative a tutte le unità figlio della società o dell'unità nella quale si sta lavorando.
- **Tutti i clienti e i partner (includendo i dettagli utente)**
  Il report conterrà le statistiche di utilizzo del servizio relative a tutte le unità figlio della società o dell'unità nella quale si sta lavorando, e di tutti gli utenti dell'unità.

Metriche con utilizzo pari a zero

È possibile ridurre il numero di righe contenute nel report mostrando informazioni sulle metriche che hanno un utilizzo diverso da zero e nascondendo quelle con un utilizzo pari a zero.

Configurazione di Report di utilizzo pianificati

Un report pianificato fornisce le statistiche di utilizzo del servizio per l'ultimo mese di calendario. I report sono generati alle ore 23:59:59 del fuso orario UTC il primo giorno del mese e vengono inviati il secondo giorno dello stesso mese. I report vengono inviati a tutti gli amministratori dell'azienda che hanno selezionato la casella **Report di utilizzo pianificati** nelle impostazioni utente.

Per abilitare o disabilitare un report pianificato

1. Accedere al portale di gestione.
2. Assicurarsi di operare nella prima società o unità di livello superiore disponibile.
3. Fare clic su **Report** > **Utilizzo**.
4. Fare clic su **Pianificati**.
5. Selezionare o deselezionare la casella di controllo **Invia un report di riepilogo mensile** del report.
6. In **Livello di dettaglio**, selezionare l'ambito del report.
7. [Facoltativo] Selezionare **Nascondi metriche con utilizzo pari a zero** per escludere dal report le metriche con utilizzo pari a zero.

Configurazione di Report di utilizzo personalizzati

Un report personalizzato viene generato su richiesta e non può essere pianificato. Il report verrà inviato all'indirizzo e-mail dell'utente.

Per generare un report personalizzato

1. Accedere al portale di gestione.
2. Passare all'unità per la quale si desidera creare un report.
3. Fare clic su **Report** > **Utilizzo**.
4. Fare clic su **Personalizzato**.
5. In **Tipo**, selezionare il tipo di report.
6. [Non disponibile per il tipo di report **Utilizzo corrente**] In **Periodo**, selezionare il periodo di report:
   - **Mese di calendario corrente**
   - **Mese di calendario precedente**
   - **Personalizzato**
7. [Non disponibile per il tipo di report **Utilizzo corrente**] Se si desidera specificare un periodo di report personalizzato, selezionare le date di inizio e di fine. Altrimenti, ignorare questo passaggio.
8. In **Livello di dettaglio**, selezionare l'ambito del report.

9. [Facoltativo] Selezionare **Nascondi metriche con utilizzo pari a zero** per escludere dal report le metriche con utilizzo pari a zero.
10. Per generare il report, fare clic su **Genera e invia**.

Dati nei report di utilizzo

Il report sull'utilizzo del servizio Cyber Protection contiene i seguenti dati relativi all'azienda o a un'unità:

- Dimensione dei backup per unità, per utente e per tipo di dispositivo.
- Numero di dispositivi protetti per unità, per utente e per tipo di dispositivo.
- Valore prezzo per unità, per utente e per tipo di dispositivo.
- La dimensione totale dei backup.
- Quantità totale di dispositivi protetti.
- Valore prezzo totale.

Nota
Se il servizio Cyber Protection non riesce a individuare un tipo di dispositivo, questo viene visualizzato come **non tipizzato** nel report.

Report Operazioni

I report **Operazioni** sono disponibili soltanto agli amministratori dell'azienda che operano a livello aziendale.

Un report relativo alle operazioni può includere qualsiasi insieme di widget del pannello di controllo **Operazioni**. Tutti i widget mostrano le informazioni di riepilogo per l'intera azienda.
A seconda del tipo di widget, il report include i dati relativi a un intervallo di tempo o al momento in cui il report è stato esplorato o generato. Vedere "Dati inseriti nel report in base al tipo di widget" (pag. 81).

Tutti i widget cronologici mostrano i dati per lo stesso intervallo di tempo. È possibile modificare questo intervallo nelle impostazioni del report.

È possibile utilizzare i report predefiniti o crearne uno personalizzato.

È possibile scaricare un report o inviarlo via e-mail in formato Excel (XLSX) o PDF.

I report predefiniti sono elencati di seguito:

Nome report	Descrizione
#CyberFit Score per sistema	Mostra il #CyberFit Score, basato sulla valutazione delle metriche di sicurezza e delle configurazioni per ogni sistema, nonché i miglioramenti consigliati.

Avvisi	Mostra gli avvisi generati durante un periodo di tempo specificato.
Informazioni sulla scansione del backup	Mostra informazioni dettagliate sulle minacce individuate nei backup.
Attività giornaliere	Mostra informazioni di riepilogo sulle attività eseguite durante un periodo di tempo specificato.
Mappa di protezione dati	Mostra informazioni dettagliate su numero, dimensione, posizione, stato della protezione di tutti i file importanti sui sistemi.
Minacce rilevate	Mostra informazioni relative ai sistemi interessati per numero di minacce bloccate e di sistemi integri e vulnerabili.
Macchine individuate	Mostra tutti i sistemi individuati nella rete dell'organizzazione.
Previsione dell'integrità del disco	Mostra le previsioni circa i guasti di HDD/SSD e lo stato attuale dei dischi.
Vulnerabilità esistenti	Mostra le vulnerabilità esistenti per i sistemi operativi e le applicazioni dell'organizzazione. Visualizza inoltre le informazioni sui sistemi interessati nella rete per ogni prodotto in elenco.
Riepilogo di gestione patch	Mostra il numero di patch mancanti, patch installate e patch applicabili. È possibile esplorare i report per ottenere le informazioni sulle patch installate e/o mancanti e ulteriori dettagli su tutti i sistemi.
Riepilogo	Mostra informazioni di riepilogo sui dispositivi protetti per un periodo di tempo specificato.
Attività settimanali	Mostra informazioni di riepilogo sulle attività eseguite durante un periodo di tempo specificato.
Inventario software	Mostra informazioni dettagliate su tutti i componenti software installati nei sistemi Windows e macOS dell'organizzazione.
Inventario hardware	Mostra informazioni dettagliate su tutti i componenti hardware disponibili nei sistemi Windows e macOS fisici e virtuali dell'organizzazione.
Sessioni remote	Mostra informazioni dettagliate sulle sessioni di desktop remoto e di trasferimento di file eseguite nell'organizzazione in un intervallo di tempo specificato.

Azioni con i report

Per visualizzare un report, fare clic sul relativo nome.

Per aggiungere un nuovo report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report disponibili, fare clic su **Aggiungi report**.
3. [Per aggiungere un report predefinito] Fare clic sul nome del report predefinito.
4. [Per aggiungere un report personalizzato] Fare clic su **Personalizzato** e quindi aggiungere i widget al report.
5. [Facoltativo] Trascinare e rilasciare i widget per riorganizzarli.

Per modificare un report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report da modificare.
   È possibile:
   - Rinominare il report.
   - Modificare l'intervallo di tempo di tutti i widget nel report.
   - Specificare i destinatari del report e la data in cui il report verrà inviato. Sono disponibili i formati PDF e XLSX.

Per eliminare un report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report da eliminare.
3. Fare clic sull'icona dei puntini di sospensione, quindi fare clic su **Elimina**.
4. Confermare la selezione facendo clic su **Elimina**.

Per programmare un report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report da pianificare, quindi fare clic su **Impostazioni**.
3. Attivare il commutatore **Pianificato**.
   - Specificare gli indirizzi e-mail dei destinatari.
   - Selezionare il formato del report.

     Nota
     È possibile esportare fino a 1.000 voci in un file PDF e fino a 10.000 voci in un file XLSX. I timestamp nei file PDF e XLSX utilizzano l'ora locale del sistema.

   - Selezionare la lingua del report.
   - Configurare la pianificazione.
4. Fare clic su **Salva**.

Per scaricare un report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report, quindi fare clic su **Scarica**.
3. Selezionare il formato del report.

Per inviare un report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report, quindi fare clic su **Invia**.
3. Specificare gli indirizzi e-mail dei destinatari.
4. Selezionare il formato del report.
5. Fare clic su **Invia**.

Per esportare la struttura del report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report.
3. Fare clic sull'icona dei puntini di sospensione, quindi fare clic su **Esporta**.

La struttura del report viene salvata nel sistema come file JSON.

Per effettuare il dumping dei dati del report

Utilizzando questa opzione, è possibile esportare tutti i dati per un intervallo temporale del cliente, senza filtrarli, in un file CSV e inviare il file a un destinatario e-mail.

Nota
È possibile esportare fino a 150.000 voci in un file CSV. I timestamp nel file CSV utilizzano l'orario UTC (Coordinated Universal Time).

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report con i dati di cui eseguire il dump.
3. Fare clic sull'icona dei puntini di sospensione, quindi fare clic su **Dump dati**.
4. Specificare gli indirizzi e-mail dei destinatari.
5. In **Intervallo di tempo**, specificare l'intervallo temporale del cliente per il quale eseguire il dump dei dati.

   Nota
   La preparazione dei file CSV relativi a periodi più lunghi richiede più tempo.

6. Fare clic su **Invia**.

Riepilogo esecutivo

Il report Riepilogo esecutivo offre una panoramica dello stato della protezione degli ambienti e dei dispositivi protetti dell'organizzazione, per un intervallo di date specificato.

Il report Riepilogo esecutivo include sezioni personalizzabili con widget dinamici che mostrano le metriche prestazionali chiave relative all'utilizzo dei seguenti servizi cloud: Backup, Protezione antimalware, Valutazione delle vulnerabilità, Gestione patch, Notary, Disaster Recovery, Files Sync & Share.

È possibile personalizzare il report in diversi modi.

- Aggiungere o eliminare sezioni.
- Modificare l'ordine delle sezioni.
- Rinominare le sezioni.
- Spostare i widget da una sezione a un'altra.
- Modificare l'ordine dei widget in ogni sezione.
- Aggiungere o rimuovere widget.
- Personalizzare i widget.

È possibile generare i report Riepilogo esecutivo in formato PDF ed Excel, e quindi inviarli alle parti interessate o ai titolari dell'organizzazione dei clienti, in modo che possano visualizzare con facilità il valore tecnico e aziendale dei servizi forniti.

Widget del report Riepilogo esecutivo

È possibile aggiungere o rimuovere sezioni e widget dal report Riepilogo esecutivo in modo da controllare le informazioni da includervi.

Widget Panoramica dei workload

La tabella seguente fornisce più informazioni sui widget presenti nella sezione **Panoramica dei workload**.

Widget	Descrizione
Stato della protezione dei workload cloud	Questo widget mostra il numero di workload cloud protetti e non protetti per tipo al momento della generazione del report. È considerato protetto un workload cloud al quale è applicato almeno un piano di backup. È considerato non protetto un workload cloud al quale non è applicato alcun piano di backup. Nel diagramma sono mostrati i tipi di workload cloud elencati di seguito (in ordine alfabetico dalla A alla Z): • Google Workspace Drive • Google Workspace Gmail

Widget	Descrizione
	• Google Workspace Shared Drive • Caselle di posta di Exchange ospitato • Caselle di posta di Microsoft 365 • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • Siti Web Per alcuni tipi di workload, vengono utilizzati i seguenti gruppi di workload: • Microsoft 365: Utenti, Gruppi, Cartelle pubbliche, Team e Raccolte di siti • Google Workspace: Utenti e unità condivise • Exchange ospitato: Utenti Se in un gruppo di workload sono presenti più di 10.000 workload, il widget non mostra alcun dato per i workload corrispondenti. Se, ad esempio, il cliente dispone di un account di Microsoft 365 con 10.000 caselle di posta e di un servizio OneDrive per 500 utenti, tutti appartengono al gruppo dei workload utente. La somma di questi workload è pari a 10.500, che supera il limite di 10.000 unità per un gruppo di workload. Pertanto, il widget nasconderà i tipi di workload corrispondenti: Caselle di posta di Microsoft 365 e Microsoft 365 OneDrive.
Riepilogo di Cyber Protection	Questo widget mostra le metriche principali delle prestazioni di Cyber Protection per il periodo di tempo specificato. **Data esecuzione backup** - Dimensione totale degli archivi creati negli storage cloud e locale. **Minacce mitigate** - Il numero totale di malware bloccati su tutti i dispositivi. **URL dannosi bloccati**- Il numero totale di URL bloccati su tutti i dispositivi. **Vulnerabilità con patch applicate** - Il numero totale di vulnerabilità corrette tramite l'installazione di patch software su tutti i dispositivi. **Patch installate**- Il numero totale di patch installate su tutti i dispositivi. **Server protetti da Disaster Recovery** - Il numero totale dei server protetti da Disaster Recovery. **Utenti di File Sync & Share** - Il numero totale di utenti e di utenti guest che utilizzano Cyber Files. **File autenticati** - Il numero totale di file autenticati. **Documenti con firma elettronica** - Il numero totale di documenti con firma elettronica. **Dispositivi periferici bloccati** - Il numero totale di dispositivi periferici bloccati.

Widget	Descrizione
Stato della rete dei workload	Questo widget mostra il numero di workload isolati e di quelli connessi (questo è lo stato normale dei workload). Selezionare il cliente di interesse; la vista del workload visualizzata viene filtrata per mostrare i workload isolati. Fare clic sul valore Connesso per visualizzare l'elenco Workload con agenti filtrato per mostrare i workload connessi (per il cliente selezionato).
Stato di protezione dei workload	Il widget mostra i workload protetti e non protetti per tipo al momento della generazione del report. È considerato protetto un workload al quale è applicato almeno un piano di backup o di protezione. Un workload non protetto è un workload al quale non è applicato alcun piano di backup o di protezione. Vengono calcolati i seguenti workload: **Server** - Server fisici e server Controller di dominio. **Workstation** - Workstation fisiche. **Macchina virtuale** - Macchina virtuale con e senza agente. **Server di web hosting** - Server virtuali o fisici sui quali è installato cPanel o Plesk. **Dispositivi mobili** - Dispositivi mobile fisici. Un workload può appartenere a più di una categoria. Ad esempio, un server di web hosting viene conteggiato in due categorie - **Server** e **Server di web hosting**.

Widget di Protezione antimalware

La tabella seguente fornisce più informazioni sui widget presenti nella sezione **Difesa dalle minacce**.

Widget	Descrizione
Scansione antimalware dei file	Il widget mostra i risultati della scansione antimalware su richiesta effettuata sui dispositivi, per l'intervallo di date specificato. **File** - Il numero totale di file scansionati **Pulito** - Il numero totale di file puliti **Rilevato, in quarantena** - Il numero totale di file infetti messi in quarantena **Rilevato, non in quarantena** - Il numero totale di file infetti non messi in quarantena **Dispositivi protetti** - Il numero totale di dispositivi ai quali è applicata una policy di protezione antimalware **Numero totale di dispositivi registrati** - Il numero totale di dispositivi registrati al momento della generazione del report

Widget	Descrizione
Scansione anti-malware dei backup	Il widget mostra i risultati della scansione antimalware effettuata sui backup, per l'intervallo di date specificato, utilizzando le metriche seguenti: • Numero totale di punti di ripristino scansionati • Numero di punti di ripristino puliti • Numero di punti di ripristino puliti con partizioni non supportate • Numero di punti di ripristino infetti. Questa metrica include il numero di punti di ripristino infetti con partizioni non supportate.
URL bloccati	Il widget mostra il numero di URL bloccati, raggruppati per categoria di sito web, per l'intervallo di date specificato. Il widget elenca le sette categorie di siti web che presentano il numero più elevato di URL bloccati, e combina le categorie di siti web rimanenti nella voce **Altro**. Per ulteriori informazioni sulle categorie di siti web, consultare l'argomento relativo al filtraggio degli URL in Cyber Protection.
Burndown dei problemi di sicurezza	Questo widget indica il tasso di efficienza nella risoluzione dei problemi di sicurezza per l'azienda selezionata; il numero di problemi aperti viene misurato a fronte del numero di problemi chiusi in un determinato periodo di tempo. Passare il mouse su una colonna per visualizzare in dettaglio i problemi chiusi o aperti per il giorno selezionato. Il valore in percentuale (%) mostrato tra parentesi indica l'aumento o la diminuzione rispetto al periodo di tempo precedente.
MTTR del problema	Questo widget mostra il tempo medio di risoluzione dei problemi di sicurezza. Indica la rapidità con la quale i problemi vengono analizzati e risolti. Fare clic su una colonna per visualizzare in dettaglio i problemi in base al livello di gravità (**Critico**, **Alto** e **Medio**) e un'indicazione del tempo impiegato per risolverli in base ai diversi livelli di gravità. Il valore in percentuale (%) mostrato tra parentesi indica l'aumento o la diminuzione rispetto al periodo di tempo precedente.
Stato minaccia	Questo widget mostra lo stato corrente della minaccia per i workload dell'azienda (indipendentemente dal numero dei workload); evidenzia il numero attuale di problemi non mitigati che devono essere analizzati. Il widget indica anche il numero di problemi mitigati (manualmente e/o automaticamente dal sistema).
Minacce rilevate per tecnologia di protezione	Per l'intervallo di date specificato, il widget mostra il numero di minacce rilevate, raggruppate in base alle tecnologie di protezione seguenti: • Scansione antimalware • Motore comportamentale • Protezione dal mining di criptovalute

Widget	Descrizione
	• Prevenzione degli exploit • Protezione attiva contro il ransomware • Protezione in tempo reale • Filtro URL

Widget di Backup

La tabella seguente fornisce più informazioni sui widget presenti nella sezione **Backup**.

Widget	Descrizione
Workload con backup eseguito	Il widget mostra il numero totale dei workload registrati per stato di backup. **Backup eseguito** - Numero di workload di cui è stato eseguito il backup (con almeno un backup riuscito) durante l'intervallo di date del report. **Backup non eseguito** - Numero di workload di cui non è stato eseguito il backup (senza alcun backup riuscito) durante l'intervallo di date del report.
Stato integrità del disco per dispositivo fisici	Il widget mostra lo stato di integrità complessivo dei dispositivi fisici in base agli stati di integrità dei rispettivi dischi. **OK** - Questo stato di integrità del disco è correlato ai valori [70-100]. Lo stato del dispositivo corrisponde a **OK** quando tutti i relativi dischi sono nello stato **OK**. **Attenzione** - Questo stato di integrità del disco è correlato ai valori [30-70]. Lo stato del dispositivo corrisponde a **Attenzione** quando lo stato di almeno uno dei suoi dispositivi corrisponde a **Attenzione** e quando non sono presenti dischi nello stato **Errore**. **Errore** - Questo stato di integrità del disco è correlato ai valori [0-30]. Lo stato del dispositivo corrisponde a **Errore** quando lo stato di almeno uno dei suoi dispositivi corrisponde a **Errore**. **Calcolo dei dati del disco in corso** - Lo stato del dispositivo corrisponde a **Calcolo dei dati del disco** quando gli stati dei relativi dischi non sono ancora stati calcolati.
Utilizzo dell'archivio di backup	Per l'intervallo di date specificato, il widget mostra il numero totale e la dimensione totale dei backup archiviati nel cloud e in locale.

Widget Valutazione della vulnerabilità e gestione patch

La tabella seguente fornisce più informazioni sui widget presenti nella sezione **Valutazione della vulnerabilità e gestione patch**.

Widget	Descrizione
Vulnerabilità con patch applicate	Il widget mostra i risultati delle prestazioni di valutazione delle vulnerabilità per l'intervallo di date specificato. **Totale**- Il numero totale di vulnerabilità con patch applicate. **Vulnerabilità del software Microsoft** - Il numero totale di vulnerabilità di Microsoft corrette su tutti i dispositivi Windows. **Vulnerabilità del software Windows di terze parti** - Il numero totale di vulnerabilità del software Windows di terze parti corrette, su tutti i dispositivi Windows. **Workload scansionati** - Il numero totale di dispositivi analizzati alla ricerca di vulnerabilità almeno una volta durante l'intervallo di date specificato.
Patch installate	Il widget mostra i risultati delle prestazioni della gestione delle patch per l'intervallo di date specificato. **Installate**- Il numero totale di patch applicate installate su tutti i dispositivi. **Patch del software Microsoft**- Il numero totale di patch del software Microsoft installate su tutti i dispositivi Windows. **Patch del software Windows di terze parti**- Il numero totale di patch del software Windows di terze parti installate su tutti i dispositivi Windows. **Workload con patch applicata** - Il numero totale di dispositivi con patch applicata (almeno una patch installata durante l'intervallo di date specificato).

Widget di Disaster Recovery

La tabella seguente fornisce più informazioni sui widget presenti nella sezione **Disaster Recovery**.

Widget	Descrizione
Statistiche di Disaster Recovery	Il widget mostra le metriche KPI di Disaster Recovery per l'intervallo di date specificato. **Failover di produzione** - Il numero di operazioni di failover di produzione per l'intervallo di tempo specificato. **Failover di prova** - Il numero di operazioni di failover di prova eseguite durante l'intervallo di tempo specificato. **Server primari** - Il numero totale di server primari al momento della generazione del report. **Server di ripristino** - Il numero totale di server di ripristino al momento della generazione del report. **IP pubblici** - Il numero totale di indirizzi IP pubblici al momento della generazione del report.

Widget	Descrizione
	Punti di calcolo totali consumati - Il numero totale di punti di calcolo consumati durante l'intervallo di tempo specificato.
Server di Disaster Recovery testati	Il widget mostra informazioni sui server protetti da Disaster Recovery e testati tramite failover di prova. Il widget mostra le metriche seguenti: **Server di ripristino** - Il numero totale di server protetti da Disaster Recovery (server dotati di almeno un server di ripristino) al momento della generazione del report. **Testati** - Il numero di server protetti da Disaster Recovery che sono stati testati usando il failover di prova durante l'intervallo di tempo selezionato, sul totale dei server protetti da Disaster Recovery. **Non testati** - Il numero di server protetti da Disaster Recovery che non sono stati testati usando il failover di prova durante l'intervallo di tempo selezionato, sul totale dei server protetti da Disaster Recovery. Il widget mostra anche la dimensione dello storage di Disaster Recovery (in GB) al momento della generazione del report. È la somma delle dimensioni di backup dei server cloud.
Server protetti con Disaster Recovery	Il widget mostra informazioni sui server protetti da Disaster Recovery e sui server non protetti. Il widget mostra le metriche seguenti: Il numero totale di server registrati nel tenant cliente al momento della generazione del report. **Protetti** - Il numero di server protetti da Disaster Recovery (server dotati di almeno un server di ripristino e di un backup del server completo), sul totale di tutti i server registrati al momento della generazione del report. **Non protetti** - Il numero totale di server non protetti, sul totale di tutti i server registrati al momento della generazione del report.

Widget Prevenzione della perdita di dati

L'argomento seguente fornisce maggiori informazioni sulle periferiche bloccate nella sezione **Prevenzione della perdita di dati**.

Il widget mostra il numero totale di dispositivi bloccati e il numero totale di dispositivi bloccati per tipo di dispositivo e per l'intervallo di date specificato.

- Archivio rimovibile
- Rimovibile crittografato
- Stampanti

- Appunti - Include i tipi di dispositivo per gli appunti e l'acquisizione di screenshot.
- Dispositivi mobili
- Bluetooth
- Unità ottiche
- Unità floppy
- USB - Include i tipi di dispositivo Porta USB e Porta USB reindirizzata.
- FireWire
- Unità mappate
- Appunti reindirizzati - Include i tipi di dispositivi Appunti reindirizzati in entrata e Appunti reindirizzati in uscita.

Il widget mostra i primi sette tipi di dispositivo che presentano il numero più alto di dispositivi bloccati e combina i tipi di dispositivo rimanenti nel tipo di dispositivo **Altro**.

Widget di File Sync & Share

La tabella seguente fornisce più informazioni sui widget presenti nella sezione **File Sync & Share**.

Widget	Descrizione
Statistiche di File Sync & Share	Il widget mostra le metriche seguenti: **Archiviazione totale nel cloud utilizzata** - L'utilizzo dello storage totale di tutti gli utenti. **Utenti finali** - Il numero totale di utenti finali. **Spazio di archiviazione utilizzato in media per utente** - lo spazio di storage medio utilizzato da ogni utente finale. **Utenti guest** - Il numero totale di utenti guest.
Utilizzo dell'archivio di File Sync & Share per utente finale	Il widget mostra il numero totale di utenti finali del servizio File Sync & Share con un utilizzo dello storage compreso negli intervalli seguenti: • 0 – 1 GB • 1 – 5 GB • 5 – 10 GB • 10 – 50 GB • 50 – 100 GB • 100 – 500 GB • 500 – 1 TB • 1+ TB

Widget del servizio Notary

La tabella seguente fornisce più informazioni sui widget presenti nella sezione **Notary**.

Widget	Descrizione
Statistiche di Cyber Notary	Il widget mostra le metriche seguenti del servizio Notary: **Archivio cloud Notary utilizzato** - La dimensione totale dello storage utilizzato per i servizi Notary. **File autenticati** - Il numero totale di file autenticati. **Documenti con firma elettronica** - Il numero totale di documenti e file con firma elettronica.
File autenticati dagli utenti finali	Mostra il numero totale dei file autenticati per tutti gli utenti finali. Gli utenti vengono raggruppati in base al numero di file autenticati di cui dispongono. • Fino a 10 file • 11 - 100 file • 101 - 500 file • 501 - 1000 file • 1000+ file
Documenti con firma elettronica degli utenti finali	Il widget mostra il numero totale di documenti e file con firma elettronica per tutti gli utenti finali. Gli utenti vengono raggruppati in base al numero di file e documenti con firma elettronica di cui dispongono. • Fino a 10 file • 11 - 100 file • 101 - 500 file • 501 - 1000 file • 1000+ file

Configurazione delle impostazioni del report Riepilogo esecutivo

È possibile aggiornare le impostazioni del report Riepilogo esecutivo che sono state configurate durante la creazione del report.

Per aggiornare le impostazioni del report Riepilogo esecutivo

1. Nella console di gestione, passare a **Report**>**Riepilogo esecutivo**.
2. Fare clic sul nome del report Riepilogo esecutivo da aggiornare.
3. Fare clic su **Impostazioni**.
4. Modificare i valori nei campi come necessario.
5. Fare clic su **Salva**.

Creazione di un report Riepilogo esecutivo

È possibile creare un report Riepilogo esecutivo, visualizzare un'anteprima del contenuto, configurare i destinatari del report e pianificarne l'invio automatico.

Per creare un report Riepilogo esecutivo

1. Nella console di gestione, passare a **Report**>**Riepilogo esecutivo**.
2. Fare clic su **Crea report Riepilogo esecutivo**.
3. In **Nome report**, immettere il nome del report.
4. Selezionare i destinatari del report.
   - Per inviare il report a tutti i contatti e gli utenti, selezionare **Invia a tutti i contatti e utenti**.
   - Per inviare il report a contatti e utenti specifici
     a. Deselezionare l'opzione **Invia a tutti i contatti e utenti**.
     b. Fare clic su **Seleziona contatti**.
     c. Selezionare i contatti e gli utenti specifici. Per individuare con facilità un contatto specifico, è possibile utilizzare la funzione Cerca.
     d. Fare clic su **Seleziona**.
5. Selezionare l'intervallo: **30 giorni** o **Questo mese**
6. Selezionare il formato del file: **PDF**, **Excel** oppure **Excel e PDF**.
7. Configurare le impostazioni di pianificazione.
   - Per inviare il report ai destinatari in una data e ora specifica:
     a. Abilitare l'opzione **Pianificato**.
     b. Fare clic sul campo **Giorno del mese**, cancellare il contenuto del campo Ultimo giorno e fare clic sulla data da impostare.
     c. Nel campo **Ora** inserire l'ora da impostare.
     d. Fare clic su **Applica**.
   - Per creare il report senza inviarlo ai destinatari, disabilitare l'opzione **Pianificato**.
8. Fare clic su **Salva**.

Personalizzazione del report Riepilogo esecutivo

È possibile definire le informazioni da includere nel report Riepilogo esecutivo. È possibile aggiungere o eliminare sezioni, aggiungere o eliminare widget, rinominare sezioni, personalizzare widget e trascinare e rilasciare widget e sezioni per modificare l'ordine con cui le informazioni vengono visualizzate nel report stesso.

Per aggiungere una sezione

1. Fare clic su **Aggiungi elemento** > **Aggiungi sezione**.
2. Nella finestra **Aggiungi sezione**, digitare un nome per la sezione o utilizzare quello predefinito.
3. Fare clic su **Aggiungi al report**.

Per rinominare una sezione

1. Nella sezione che si desidera rinominare, fare clic su **Modifica**.
2. Nella finestra **Modifica sezione**, digitare il nuovo nome.
3. Fare clic su **Salva**.

Per eliminare una sezione

1. Nella sezione che si desidera eliminare, fare clic su **Elimina sezione**.
2. Nella finestra di conferma **Elimina sezione**, fare clic su **Elimina**.

Per aggiungere un widget con impostazioni predefinite a una sezione

1. Nella sezione alla quale si desidera aggiungere il widget, fare clic su **Aggiungi widget**.
2. Nella finestra **Aggiungi widget** fare clic sul widget da aggiungere.

Per aggiungere un widget personalizzato a una sezione

1. Nella sezione alla quale si desidera aggiungere il widget, fare clic su **Aggiungi widget**.
2. Nella finestra **Aggiungi widget** fare clic sul widget da aggiungere e quindi su **Personalizza**.
3. Configurare i campi come necessario.
4. Fare clic su **Aggiungi widget**.

Per aggiungere un widget con impostazioni predefinite al report

1. Fare clic su **Aggiungi elemento** > **Aggiungi widget**.
2. Nella finestra **Aggiungi widget** fare clic sul widget da aggiungere.

Per aggiungere un widget personalizzato al report

1. Fare clic su **Aggiungi widget**.
2. Nella finestra **Aggiungi widget** fare clic sul widget da aggiungere e quindi su **Personalizza**.
3. Configurare i campi come necessario.
4. Fare clic su **Aggiungi widget**.

Per ripristinare le impostazioni predefinite di un widget

1. Nel widget che si desidera personalizzare, fare clic su **Modifica**.
2. Fare clic su **Ripristina allo stato predefinito**.
3. Fare clic su **Fine**.

Per personalizzare un widget

1. Nel widget che si desidera personalizzare, fare clic su **Modifica**.
2. Modificare i campi come necessario.
3. Fare clic su **Fine**.

Invio dei report Riepilogo esecutivo

È possibile inviare un report Riepilogo esecutivo su richiesta. In questo caso, l'impostazione **Pianificato** viene ignorata e il report è inviato immediatamente. Per l'invio del report, il sistema utilizza i valori relativi a Destinatari, Intervallo e Formato file configurati nelle **Impostazioni**. Prima di inviare il report è possibile modificare manualmente tali impostazioni. Per ulteriori informazioni, consultare "Configurazione delle impostazioni del report Riepilogo esecutivo" (pag. 77).

Per inviare un report Riepilogo esecutivo

1. Nel portale di gestione, passare a **Report**>**Riepilogo esecutivo**.
2. Fare clic sul nome del report Riepilogo esecutivo da inviare.
3. Fare clic su **Invia ora**.
   Il sistema invia il report Riepilogo esecutivo ai destinatari selezionati.

Fusi orari nei report

I fusi orari utilizzati nei report variano in funzione del tipo di report. La tabella seguente contiene informazioni da utilizzare come riferimento.

Tipo e posizione del report	Fuso orario utilizzato nel report
Portale di gestione > Panoramica > Operazioni (widget)	L'orario di generazione del report è indicato con il fuso orario del sistema in cui viene eseguito il browser.
Portale di gestione > Panoramica > Operazioni (esportato in PDF o xslx)	• L'indicatore data e ora del report esportato è indicato nel fuso orario del sistema utilizzato per esportare il report. • Il fuso orario delle attività visualizzate nel report è il fuso UTC.
Portale di gestione > Report > Utilizzo > Report pianificati	• Il report è generato alle ore 23:59:59 del fuso orario UTC il primo giorno del mese. • Viene inviato il secondo giorno del mese.
Portale di gestione > Report > Utilizzo > Report personalizzati	La data e il fuso orario del report sono indicati con il fuso UTC.
Portale di gestione > Report > Operazioni (widget)	• L'orario di generazione del report è indicato con il fuso orario del sistema in cui viene eseguito il browser. • Il fuso orario delle attività visualizzate nel report è il fuso UTC.
Portale di gestione > Report >	• L'indicatore data e ora del report esportato è indicato nel fuso

Operazioni (esportato in PDF o xslx)	orario del sistema utilizzato per esportare il report. • Il fuso orario delle attività visualizzate nel report è il fuso UTC.
Portale di gestione > Report > Operazioni (distribuzione pianificata)	• Il fuso orario della distribuzione del report è il fuso UTC. • Il fuso orario delle attività visualizzate nel report è il fuso UTC.
Portale di gestione > Utenti > Riepilogo giornaliero degli avvisi attivi	• Il report viene inviato una volta al giorno tra le 10:00 e le 23:59 del fuso UTC. L'orario di invio del report dipende dal carico di lavoro nel data center. • Il fuso orario delle attività visualizzate nel report è il fuso UTC.
Portale di gestione > Utenti > Notifiche sullo stato del servizio Cyber Protection	• Il report viene inviato al completamento di un'attività. **Nota** A seconda del carico di lavoro del data center, l'invio di alcuni report potrebbe subire ritardi. • Il fuso orario dell'attività visualizzata nel report è il fuso UTC.

Dati inseriti nel report in base al tipo di widget

In base all'intervallo di dati che visualizzano, i widget nella dashboard sono di due tipi:

- Widget che visualizzano i dati correnti nel momento in cui il report viene sfogliato o generato.
- Widget che visualizzano dati cronologici.

Quando si configura un intervallo di dati nelle impostazioni del report, per eseguire il dump relativo a un determinato periodo, l'intervallo di tempo selezionato verrà applicato solo ai widget che visualizzano dati cronologici. Il parametro dell'intervallo di tempo non è applicabile ai widget che visualizzano i dati correnti nel momento in cui il report viene sfogliato.

La tabella seguente elenca i widget disponibili e i relativi intervalli di dati.

Nome widget	Dati visualizzati nel widget e nei report
#CyberFit Score per sistema	Correnti
5 avvisi più recenti	Correnti
Dettagli sugli avvisi attivi	Correnti
Riepilogo avvisi attivi	Correnti
Attività	Cronologici
Elenco attività	Cronologici
Cronologia avvisi	Cronologici

Scansione anti-malware dei backup	Cronologici
Scansione anti-malware dei file	Cronologici
Informazioni sulla scansione del backup (minacce)	Cronologici
Stato backup	Cronologici - nelle colonne **Esecuzioni totali** e **Numero di esecuzioni riuscite** Correnti - in tutte le altre colonne
Utilizzo dell'archivio di backup	Cronologici
Dispositivi periferici bloccati	Cronologici
URL bloccati	Correnti
Applicazioni cloud	Correnti
Stato della protezione dei workload cloud	Correnti
Cyber protection	Correnti
Riepilogo di Cyber Protection	Cronologici
Mappa di protezione dati	Cronologici
Dispositivi	Correnti
Server di Disaster Recovery testate	Cronologici
Statistiche di Disaster Recovery	Cronologici
Macchine individuate	Correnti
Panoramica dell'integrità del disco	Correnti
Stato integrità del disco	Correnti
Stato integrità del disco per dispositivi fisici	Correnti
Documenti con firma elettronica degli utenti finali	Correnti
Vulnerabilità esistenti	Cronologici
Statistiche di File Sync & Share	Correnti
Utilizzo dell'archivio di File Sync & Share per utente finale	Correnti
Modifiche hardware	Cronologici
Dettagli hardware	Correnti

Inventario hardware	Correnti
Riepilogo avvisi cronologici	Cronologici
Riepilogo posizioni	Correnti
Aggiornamenti non effettuati per categorie	Correnti
Non protetto	Correnti
File autenticati dagli utenti finali	Correnti
Statistiche Notary	Correnti
Cronologia di installazione patch	Cronologici
Stato di installazione patch	Cronologici
Riepilogo di installazione patch	Cronologici
Vulnerabilità con patch applicate	Cronologici
Patch installate	Cronologici
Stato protezione	Correnti
Recentemente interessato	Cronologici
Sessioni remote	Cronologici
Burndown dei problemi di sicurezza	Cronologici
MTTR dei problemi di sicurezza	Cronologici
Server protetti con Disaster Recovery	Correnti
Inventario software	Correnti
Panoramica software	Cronologici
Stato minaccia	Correnti
Minacce rilevate per tecnologia di protezione	Cronologici
Distribuzione dei principali problemi per workload	Correnti
Sistemi vulnerabili	Correnti
Stato della rete dei workload	Correnti
Workload con backup eseguito	Cronologici
Stato di protezione dei workload	Correnti

Integrazioni

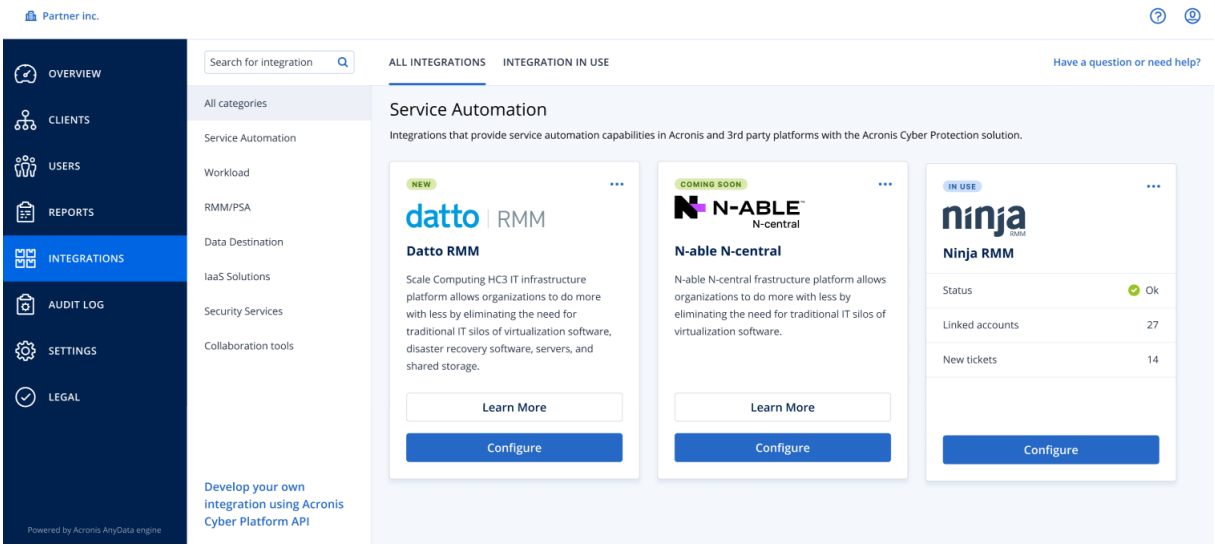
Catalogo delle integrazioni

Questa pagina funge da posizione globale centrale per la registrazione e l'aggiornamento di tutte le applicazioni integrate.
Da qui è possibile aggiungere nuove integrazioni o modificare quelle esistenti.

Nota
Solo gli utenti con un ruolo di **Amministratore dell'azienda** hanno il permesso di modificare la configurazione dell'integrazione.

Tutte le integrazioni

La scheda **Tutte le integrazioni** visualizza un elenco di tutte le integrazioni attualmente disponibili, ordinate come riquadri uno accanto all'altro.



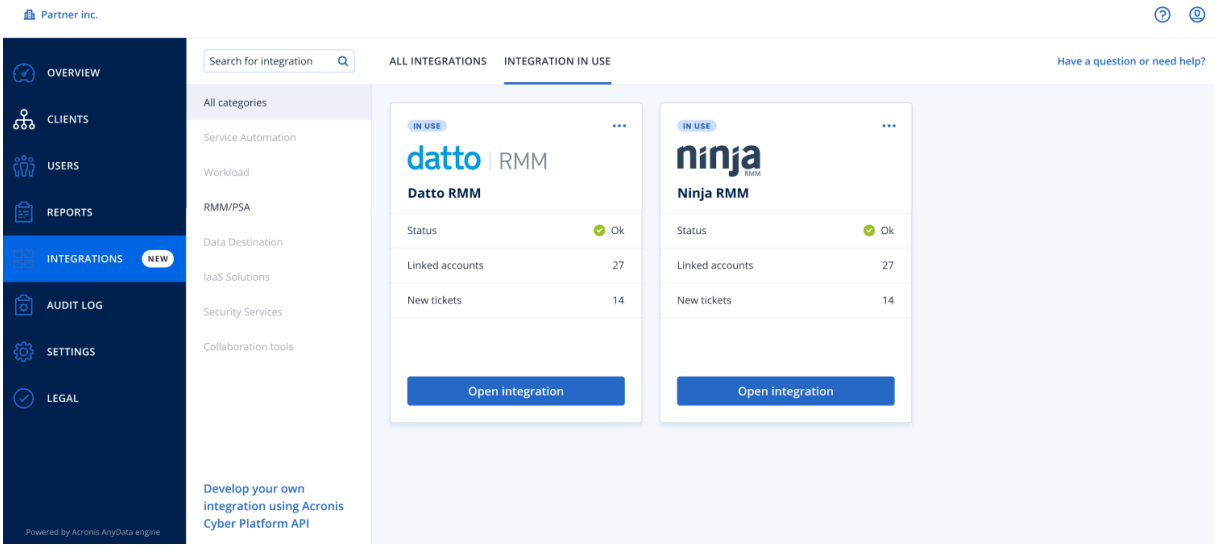
Ogni riquadro visualizza una breve descrizione del prodotto e due opzioni aggiuntive:

- **Per saperne di più**: fare clic su questo pulsante per ulteriori informazioni su una specifica integrazione:
  - **Funzionalità di integrazione**
  - **Collegamenti alla documentazione**
  - **Contatti di assistenza**
- **Configura**: utilizzare questa opzione per modificare alcune delle impostazioni di integrazione.

I riquadri che rappresentano le integrazioni inattive sono grigi e disattivati, e possono presentare l'etichetta "**In arrivo**".

Integrazioni in uso

La scheda **Integrazioni in uso** mostra un elenco di tutte le integrazioni attualmente nello stato attivo, ognuna accompagnata da informazioni generiche.



Fare clic su **Apri integrazione** per accedere direttamente alle applicazioni corrispondenti.

A sinistra si trova un elenco delle categorie di integrazione in cui tutte le applicazioni esistenti sono classificate in determinati gruppi: automazione dei servizi, workload, RMM/PSA, ecc. Facendo clic su ogni singola categoria vengono visualizzate le integrazioni che appartengono al gruppo specificato. La categoria attualmente visualizzata è evidenziata.

Utilizzare l'opzione **Cerca** per fare query e cercare le integrazioni scelte.

È possibile filtrare la lista delle integrazioni per categoria ed etichetta. Le etichette sono in ordine alfabetico. Se non ci sono risultati, ampliare la ricerca e includere più categorie.

Per disabilitare l'applicazione, fare clic sull'icona dei puntini di sospensione nell'angolo in alto a destra, quindi fare clic su **Disattiva**.

È disponibile anche un link alla Documentazione delle API Acronis, se si è interessati a sviluppare una propria integrazione.

Limitazione dell'accesso all'interfaccia Web

È possibile limitare l'accesso all'interfaccia Web specificando un elenco di indirizzi IP da cui gli utenti possono eseguire l'accesso.

Questa limitazione si applica anche all'accesso al portale di gestione tramite l'API.

Questa limitazione è valida solo per il livello in cui è impostata. *Non* si applica ai membri delle unità figlio.

Per limitare l'accesso all'interfaccia Web

1. Accedere al portale di gestione.
2. Passare all'unità per la quale si desidera limitare l'accesso.
3. Fare clic su **Impostazioni** > **Sicurezza**.
4. Selezionare la casella di controllo **Abilita il controllo di accesso**.
5. In **Indirizzi IP consentiti**, specificare gli indirizzi IP consentiti.
   È possibile immettere i seguenti parametri, separati da un punto e virgola.
   - Indirizzi IP, ad esempio: 192.0.2.0
   - Intervalli IP, ad esempio: 192.0.2.0-192.0.2.255
   - Sottoreti, ad esempio: 192.0.2.0/24
6. Fare clic su **Salva**.

Limiti di accesso alla società

Gli amministratori a livello di società possono limitare l'accesso alla società agli amministratori di livello superiore.

Se l'accesso alla società è limitato, gli amministratori di livello superiore possono solo modificare le proprietà della società. Non saranno in grado di vedere gli account utente e le unità figlio.

Per limitare l'accesso alla società

1. Accedere al portale di gestione.
2. Fare clic su **Impostazioni** > **Sicurezza**.
3. Disabilitare l'opzione **Accesso al supporto**.
4. Fare clic su **Salva**.

Gestione dei clienti API

È possibile integrare sistemi di terze parti in Cyber Protect Cloud usando le relative interfacce di programmazione API. L'accesso a queste API è abilitato tramite i client API, parte integrante della struttura di autorizzazione OAuth 2.0 della piattaforma.

Cosa è un client API?

Un client API è uno speciale account di piattaforma che rappresenta un sistema di terze parti che deve essere autenticato e autorizzato per accedere ai dati nelle API della piattaforma e ai suoi servizi.

L'accesso al client è limitato a un tenant, nel quale un amministratore crea il client e i relativi tenant secondari.

Quando viene creato, il client eredita i ruoli di servizio dell'account di amministrazione, ruoli che non possono essere modificati in un secondo momento. La modifica o la disabilitazione dei ruoli dell'account amministratore non ha effetto sul client.

Le credenziali del client sono costituite dall'identificatore univoco e dal valore segreto. Le credenziali non hanno scadenza e non possono essere utilizzate per accedere al portale di gestione o a qualsiasi console del servizio. Il valore del segreto può essere ripristinato.

Non è possibile abilitare l'autenticazione a due fattori per il client.

Procedura di integrazione tipica

1. Un amministratore crea un client API in un tenant che viene gestito da un sistema di terze parti.
2. L'amministratore abilita il flusso di credenziali del client OAuth 2.0 nel sistema di terzi.
   In base a questo flusso, prima di accedere al tenant e ai relativi servizi tramite l'API, il sistema deve inviare le credenziali del client creato alla piattaforma, utilizzando l'autorizzazione API. La piattaforma genera e restituisce un token di sicurezza, una stringa crittografata univoca assegnata a questo client specifico. Il sistema deve aggiungere questo token a tutte le richieste API.
   Un token di sicurezza evita di dover passare le credenziali del client tramite le richieste API. Per ulteriore sicurezza, il token scade dopo due ore. Al termine delle due ore, tutte le richieste API con il token scaduto non avranno esito positivo e il sistema dovrà richiedere un nuovo token alla piattaforma.

Per ulteriori informazioni sull'uso delle API di autorizzazione e di piattaforma, fare riferimento alla guida dello sviluppatore all'indirizzo https://developer.acronis.com/doc/account-management/v2/guide/index.

Creazione di un client API

1. Accedere al portale di gestione.
2. Fare clic su **Impostazioni** > **Client API** > **Crea client API**.
3. Inserire un nome per il client API.
4. Fare clic su **Avanti**.
   Al momento della creazione, per il client API è impostato lo stato predefinito **Attivo**.
5. Copiare e salvare l'ID e il valore del segreto del client e l'URL del data center. Saranno necessari durante l'abilitazione del flusso di credenziali del client OAuth 2.0 in un sistema di terzi.

   Importante
   Per ragioni di sicurezza, il valore segreto viene visualizzato solo una volta. In caso di perdita, non sarà possibile recuperare questo valore ma solo eseguirne il ripristino.

6. Fare clic su **Fine**.

Reimpostazione del valore segreto di un client API

1. Accedere al portale di gestione.
2. Fare clic su **Impostazioni** > **Client API**.
3. Individuare il client richiesto nell'elenco.
4. Fare clic su e quindi su **Reimposta segreto**.
5. Confermare la decisione facendo clic su **Avanti**.
   Viene generato un nuovo valore del segreto. L'ID del client e l'URL del data center non vengono modificati.
   Tutti i token di sicurezza assegnati a questo client scadranno immediatamente e le richieste API con tali token non avranno esito positivo.
6. Copiare e salvare il nuovo valore del segreto del client.

   Importante
   Per ragioni di sicurezza, il valore segreto viene visualizzato solo una volta. In caso di perdita, non sarà possibile recuperare questo valore ma solo eseguirne il ripristino.

7. Fare clic su **Fine**.

Disabilitazione di un client API

1. Accedere al portale di gestione.
2. Fare clic su **Impostazioni** > **Client API**.
3. Individuare il client richiesto nell'elenco.
4. Fare clic su , quindi su **Disabilita**.
5. Confermare la propria decisione.
   Lo stato del client cambia in **Disabilitato**.
   Le richieste API con token di sicurezza assegnate a questo client non avranno esito positivo, ma i token non scadranno immediatamente. La disabilitazione del client non ha effetto sulla scadenza dei token.
   Sarà possibile riabilitare il client in qualsiasi momento.

Abilitazione di un client API disabilitato

1. Accedere al portale di gestione.
2. Fare clic su **Impostazioni** > **Client API**.
3. Individuare il client richiesto nell'elenco.
4. Fare clic su , quindi su **Abilita**.

Lo stato del client cambia in **Attivo**.

Le richieste API con token di sicurezza assegnate a questo client avranno esito positivo se i token non sono ancora scaduti.

Eliminazione di un client API

1. Accedere al portale di gestione.
2. Fare clic su **Impostazioni** > **Client API**.
3. Individuare il client richiesto nell'elenco.
4. Fare clic su , quindi su **Elimina**.
5. Confermare la propria decisione.

   Tutti i token di sicurezza assegnati a questo client scadranno immediatamente e le richieste API con tali token non avranno esito positivo.

Importante

Non è possibile recuperare un client eliminato.

Indice

#

#CyberFit Score per sistema 44

A

Abilitazione di un client API disabilitato 88

Accesso al portale di gestione e ai servizi 16

Account e unità 6

Aggiornamenti non effettuati per categorie 55

Aggiornamento automatico degli agenti 33

Aggiornamento dei ticket del Service Desk 40

Ambito del report 63

Attivazione di un account amministratore 16

Avvisi di stato dell'integrità del disco 52

B

Browser Web supportati 15

Burndown dei problemi di sicurezza 46

C

Campi del registro di audit 61

Catalogo delle integrazioni 84

Come funziona 27, 48

Configurazione dell'archivio immutabile 35

Configurazione dell'autenticazione a due fattori 27

Configurazione dell'autenticazione a due fattori per il tenant 30

Configurazione delle impostazioni del report Riepilogo esecutivo 77

Configurazione di Report di utilizzo personalizzati 64

Configurazione di Report di utilizzo pianificati 64

Cosa è un client API? 86

Creazione di un account utente 18

Creazione di un client API 87

Creazione di un report Riepilogo esecutivo 78

Creazione di un ticket del Service Desk 39

Creazione di unità 17

Cronologia della sessione 60

Cronologia di installazione patch 55

D

Dashboard Operazioni 42

Dati inseriti nel report in base al tipo di widget 81

Dati nei report di utilizzo 65

Definizione delle quote per gli utenti 13

Disabilitazione di un client API 88

Disabilitazione e abilitazione di un account utente 25

Distribuzione dei principali problemi per workload 45

Download dei dati relativi ai workload recentemente interessati 57

E

Elaborazione di rapporti 63

Eliminazione di un account utente 25

Eliminazione di un client API 89

F

Filtri e ricerca 62

Fusi orari nei report 80

G

Gestione attività 38

Gestione dei clienti API 86

Gestione dell'autenticazione a due fattori per gli utenti 30

Gestione delle quote 7

I

Impedire l'accesso agli utenti di Microsoft 365 senza licenza 11

Informazioni sul documento 5

Informazioni sul portale di gestione 6

Informazioni sulla scansione del backup 56

Integrazioni 84

Integrazioni in uso 85

Invio dei report Riepilogo esecutivo 80

Istruzioni passo a passo 16

L

Limitazione dell'accesso all'interfaccia Web 85

Limitazioni 48

Limiti di accesso alla società 86

M

Macchine individuate 44

Mappa di protezione dati 52

Metriche con utilizzo pari a zero 63

Modifica delle impostazioni di notifica per un utente 23

Monitoraggio 31, 42

Monitoraggio integrità del disco 48

MTTR del problema 46

N

Navigazione nel portale di gestione 17

Notifiche ricevute in base al ruolo dell'utente 25

P

Passaggio dal portale di gestione alle console dei servizi e viceversa 17

Per abilitare l'autenticazione a due fattori per un utente 32

Per aggiornare gli agenti automaticamente 34

Per configurare l'autenticazione a due fattori per il tenant 30

Per disabilitare l'autenticazione a due fattori per il tenant 30

Per disabilitare l'autenticazione a due fattori per un utente 31

Per monitorare gli aggiornamenti degli agenti 35

Per ripristinare il browser attendibile per un utente 31

Per ripristinare l'autenticazione a due fattori per un utente 31

Personalizzazione del report Riepilogo esecutivo 78

Procedura di integrazione tipica 87

Propagazione delle impostazioni dell'autenticazione a due fattori a tutti i livelli dei tenant 29

Protezione da attacchi di forza bruta 32

Q

Quota per il servizio di Archiviazione 14

Quote del servizio Backup 8, 14

Quote del servizio Consegna fisica dei dati 13

Quote del servizio Disaster Recovery 11

Quote del servizio File Sync & Share 12, 15

Quote del servizio Notary 13, 15

Quote per archivio 10

Quote per origini dati nel cloud 8

R

Recentemente interessato 56

Registro di audit 60

Reimpostazione del valore segreto di un client API 88

Report Operazioni 65

Report utilizzo 63

Requisiti per la password 16

Riepilogo di installazione patch 55

Riepilogo esecutivo 69

Ripristinare l'autenticazione a due fattori in caso di perdita del dispositivo di secondo fattore 32

Ruoli utente disponibili per ogni servizio 20

S

Sistemi vulnerabili 53

Stato della rete dei workload 47

Stato di installazione patch 54

Stato protezione 43

T

Tipo di rapporto 63

Trasferimento della titolarità di un account utente 26

Tutte le integrazioni 84

U

URL bloccati 57

Utilizzo 42

V

Visualizzazione dei ticket del Service Desk 38

Visualizzazione delle quote dell'organizzazione 8

Vulnerabilità esistenti 54

W

Widget del report Riepilogo esecutivo 69

Widget del servizio Notary 76

Widget di Backup 73

Widget di Disaster Recovery 74

Widget di Endpoint Detection and Response (EDR) 45

Widget di File Sync & Share 76

Widget di installazione patch 54

Widget di integrità del disco 49

Widget di Protezione antimalware 71

Widget di valutazione delle vulnerabilità 53

Widget Inventario hardware 59

Widget Inventario software 58

Widget Panoramica dei workload 69

Widget Prevenzione della perdita di dati 75

Widget Valutazione della vulnerabilità e gestione patch 73