Acronis

Microsoft 365 sotto attacco: minacce all’identità e al piano di controllo

E in che modo Acronis Security Posture Management le individua e le risolve

Introduzione

Microsoft 365 è diventato il piano di controllo delle moderne attività aziendali e gestisce identità, accessi, comunicazioni e dati all'interno delle organizzazioni. Con l'aumento della sua importanza, è cresciuto anche il suo valore come superficie di attacco primaria.

La natura degli attacchi però è cambiata in modo fondamentale.

Le minacce di oggi non si basano più su malware o compromissioni degli endpoint. Gli aggressori sfruttano invece identità, autorizzazioni ed eventuali configurazioni errate, operando interamente all'interno dei servizi legittimi di Microsoft 365. Basta un solo account amministratore compromesso, un'autorizzazione trascurata o una policy di accesso condizionale poco rigorosa per consentire agli hacker di ottenere un accesso persistente e di grande impatto senza far scattare i tradizionali avvisi di sicurezza.

Questo cambiamento crea una sfida critica per i managed service provider (MSP). Gli strumenti di sicurezza tradizionali spesso offrono poca visibilità su questi attacchi, mentre configurazioni errate e criteri incoerenti tra i tenant creano un'esposizione persistente.

I risultati: il rischio si accumula silenziosamente tra i tenant.

Questa guida offre una panoramica pratica e basata su scenari reali su come si svolgono i moderni attacchi a Microsoft 365 e su come Acronis Security Posture Management (SPM) aiuti gli MSP a individuare, prevenire e correggere questi rischi su larga scala.

La nuova realtà: sei già dentro l’attacco

Accedi a un tenant di un cliente. Non ci sono avvisi, né malware, né segnali evidenti di compromissione. Tutto appare normale in superficie, ma questo non significa che l’ambiente sia sicuro.

È possibile che un aggressore abbia già accesso al sistema. Potrebbe utilizzare credenziali valide o token persistenti ottenuti tramite phishing o abuso del consenso. Ancora più importante, potrebbe operare interamente all’interno di Microsoft 365, confondendosi con le attività legittime ed evitando i tradizionali meccanismi di rilevamento.

Gli attacchi moderni non si basano sull’accesso forzato: operano all’interno del piano di controllo.

Per gli MSP, questo cambia radicalmente il problema. Non si tratta più solo di rilevare le minacce attive: si tratta di identificare le vulnerabilità prima che vengano sfruttate, risolverle coerentemente in tutti i tenant e garantire che tali correzioni rimangano attive nel tempo, man mano che gli ambienti si evolvono.

Questa guida mostra come affrontare questa sfida nella pratica utilizzando Acronis Security Posture Management (SPM).

Scenario 1

Password spraying

“Non sembra esserci nulla che non va, ma un account ha appena effettuato l’accesso.”

Gli aggressori non hanno bisogno di entrare con la forza: basta che facciano il login. Testando password comuni su molti account, evitano i blocchi e alla fine ottengono accesso a uno di essi. Grazie alle credenziali valide, possono accedere a caselle di posta e a file e operare come un utente legittimo.

Di solito non vengono emessi avvisi, non c’è alcun malware e non ci sono segnali evidenti: solo attività che sembrano del tutto normali.

Acronis SPM sposta l’attenzione dal rilevamento all’esposizione. Evidenzia rischi come l’assenza di MFA, l’autenticazione legacy abilitata e configurazioni dell’identità che si discostano dalle best practice.

Da lì, valuti il tenant, imponi MFA, disabiliti l’autenticazione legacy e applichi questi controlli a tutti i tenant utilizzando modelli di base. Il monitoraggio continuo garantisce che eventuali deviazioni vengano rilevate e corrette.

Invece di inseguire un account compromesso, elimini le condizioni che hanno reso possibile l’attacco.

Cosa fai (nella piattaforma)

1 **Esegui un audit on-demand**

- Valuti istantaneamente il tenant rispetto alla base di sicurezza.
- Identifichi i punti deboli dell’autenticazione.

2 **Applichi la correzione di base**

- Applichi l’MFA a tutti gli utenti.
- Disabiliti l’autenticazione legacy.

3 **Lo automatizzi tra i tenant**

- Usi i modelli di base.
- Diffondi le policy a tutti i clienti.

4 **Abiliti un monitoraggio continuo**

- Acronis SPM rileva continuamente la deviazione dalla base.
- Lancia un avviso quando vengono creati nuovi utenti senza protezione.

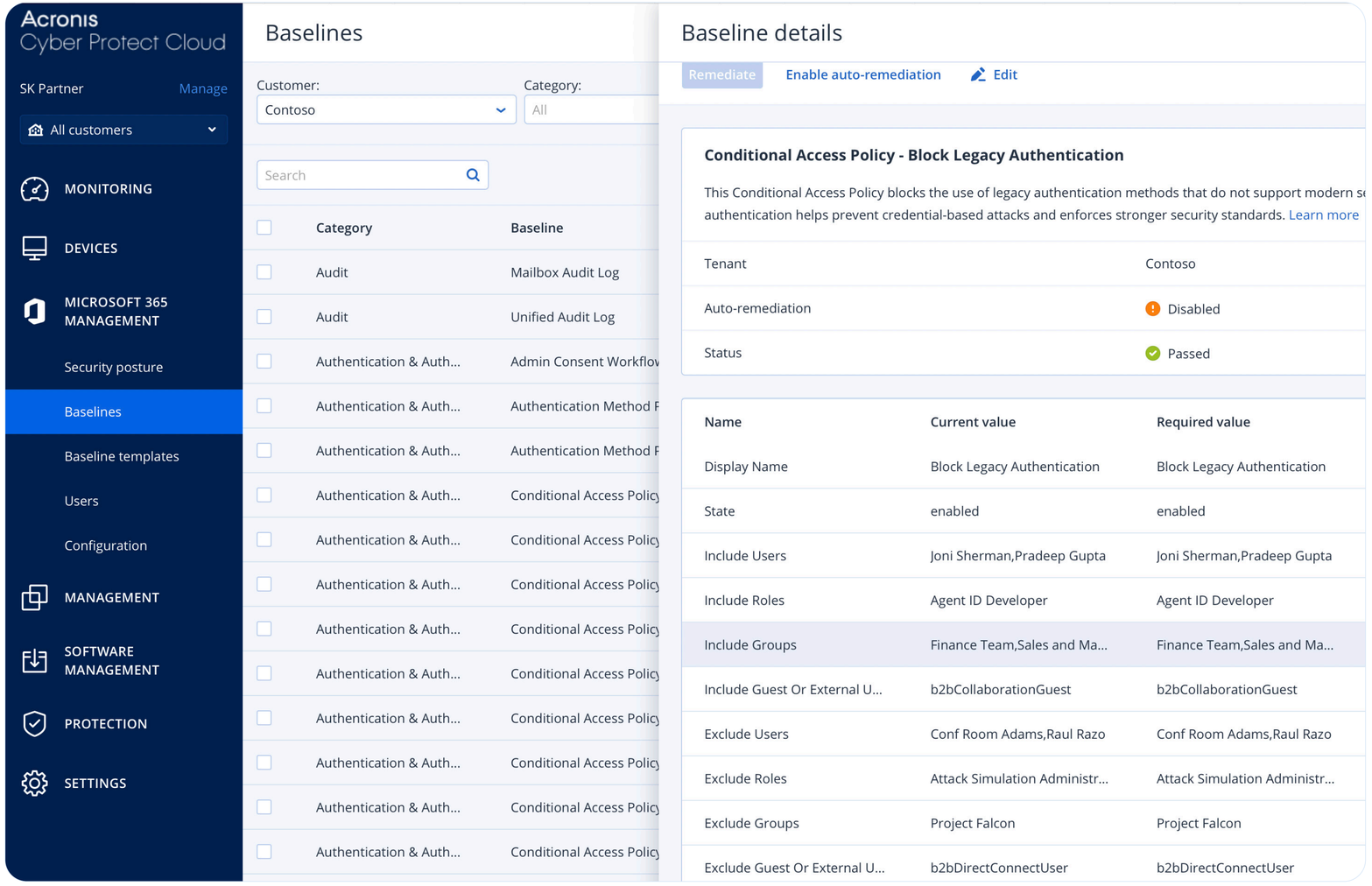
Cos'è appena successo?

Non hai inseguito un accesso.

Tu:

- Hai identificato lacune sistemiche a livello di identità.
- Le hai corrette una sola volta.
- Le hai applicate ovunque.
- Hai garantito che non si ripresentino.

Acronis SPM elimina le condizioni che rendono efficace il password spraying su larga scala.



Scenario 2

Abuso del consenso OAuth

“L’aggressore non ha più bisogno dell’utente.”

Un utente approva inconsapevolmente un’app OAuth malevola. Da quel momento, l’aggressore non ha più bisogno delle credenziali. Ottiene un accesso persistente a livello di API a e-mail e file tramite Microsoft Graph, spesso senza attivare alcun avviso.

Non c’è alcun accesso compromesso, nessuna attività di accesso sospetta e tutto sembra legittimo.

Acronis SPM mette in evidenza questo livello nascosto. Offre visibilità su tutte le app OAuth tra i tenant, sulle autorizzazioni concesse, come Mail.Read o Files.Read.All, e mette in evidenza le applicazioni rischiose o sconosciute.

Da lì, puoi identificare rapidamente le app ad alto privilegio o aggiunte di recente, revocarne le autorizzazioni e rimuovere gli accessi non autorizzati. Le policy possono quindi essere standardizzate, limitando il consenso degli utenti e richiedendo l’approvazione dell’amministratore, mentre l’automazione garantisce che questi controlli siano applicati a tutti i tenant.

Invece di inseguire le minacce basate sull’identità, individui ed elimini l’accesso persistente a livello di applicazione e ne impedisci il ripristino.

Cosa fai (nella piattaforma)

1 **Identifichi le applicazioni rischiose**

- Filtri le app con autorizzazioni elevate.
- Rilevi le app aggiunte di recente o sconosciute.

2 **Risolvi subito il problema**

- Revochi direttamente le autorizzazioni delle app.
- Rimuovi le integrazioni non autorizzate.

3 **Standardizzi la policy**

- Limiti il consenso degli utenti.
- Richiedi l’approvazione dell’amministratore.

4 **Automatizzi l’applicazione**

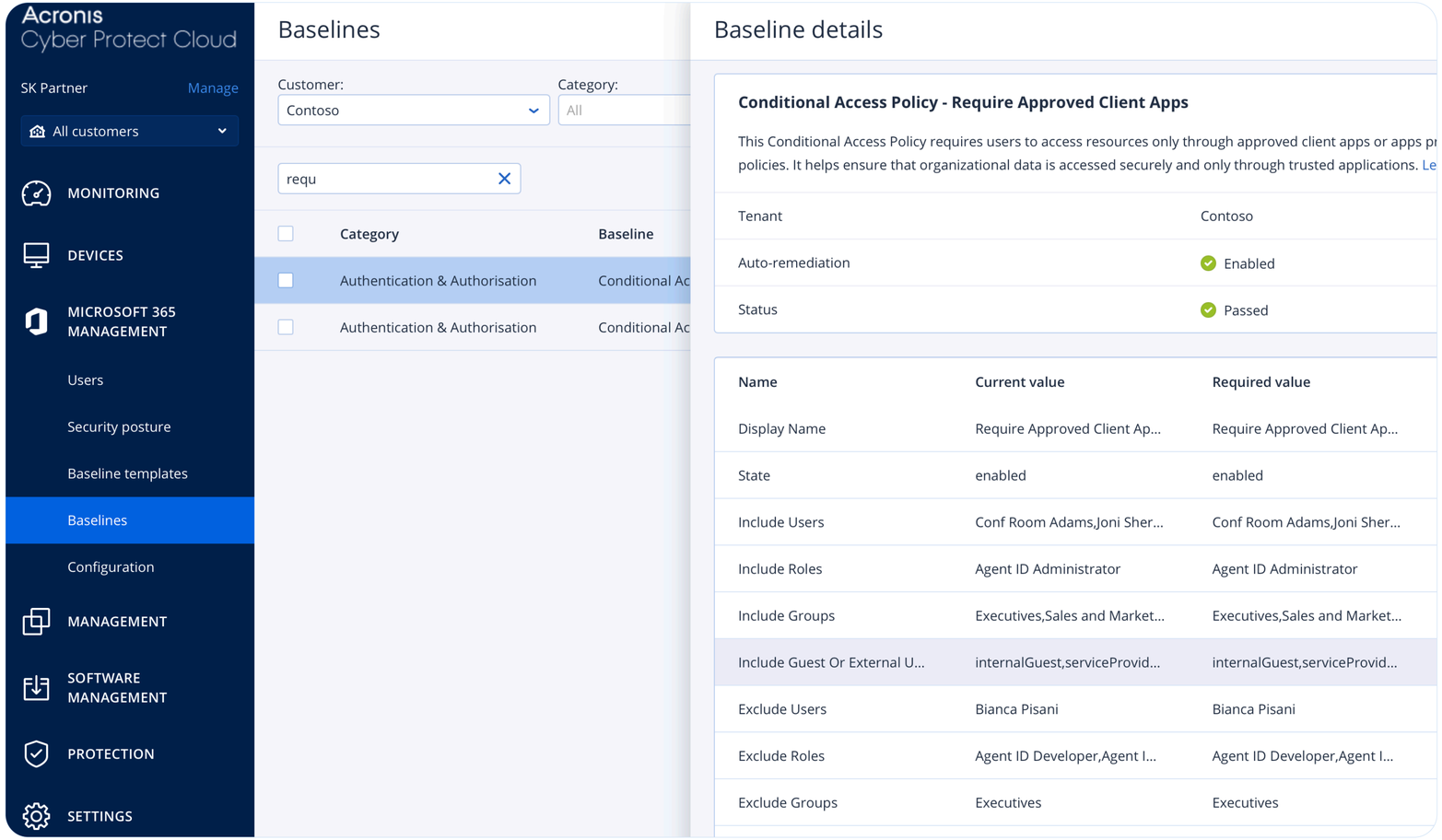
- Applichi le policy di governance delle app a tutti i tenant.
- Rilevi automaticamente le nuove app rischiose.

Cos’è appena successo?

Tu:

- Hai individuato una persistenza che aggirava l’identità.
- L’hai rimossa all’istante.
- Ne hai impedito la ricomparsa.

Acronis SPM offre visibilità e controllo sul livello applicativo su cui gli aggressori fanno affidamento per ottenere accesso a lungo termine.



Scenario 3

Phishing con codice dispositivo

“L’MFA ha funzionato ma l’aggressore ha comunque effettuato l’accesso.”

Un utente completa un accesso Microsoft legittimo e supera l’MFA, ma l’aggressore acquisisce il token di autenticazione. Con esso, ottiene un accesso persistente, legge le e-mail e crea regole della casella di posta, tutto senza attivare avvisi evidenti.

Non ci sono accessi falliti e l’MFA sembra aver funzionato come previsto.

Acronis SPM evidenzia il vero problema: le lacune nelle policy. Mette in evidenza policy di accesso condizionato carenti o assenti, la mancanza di controlli sulle sessioni e configurazioni delle identità che non rispettano gli standard delle best practice.

Da lì, applichi un accesso condizionale più rigoroso, imposti restrizioni di sessione e standardizzi questi controlli tra tutti i tenant. Il monitoraggio continuo garantisce che eventuali deviazioni vengano rilevate e corrette.

Anziché rilevare l’abuso di token, elimini le condizioni che lo consentono.

Cosa fai (nella piattaforma)

1. **Esegui il controllo di conformità di base**
   - Confronti le policy dei tenant con le best practice.
2. **Applichi i controlli dell’identità**
   - Rafforzi l’accesso condizionale.
   - Applichi le restrizioni di sessione.
3. **Automatizzi la correzione**
   - Applichi le policy a tutti i tenant.
   - Correggi automaticamente le deviazioni.
4. **Mantieni un’applicazione delle regole continua**
   - Acronis SPM monitora la deriva delle policy.
   - Evidenzia qualsiasi indebolimento dei controlli.

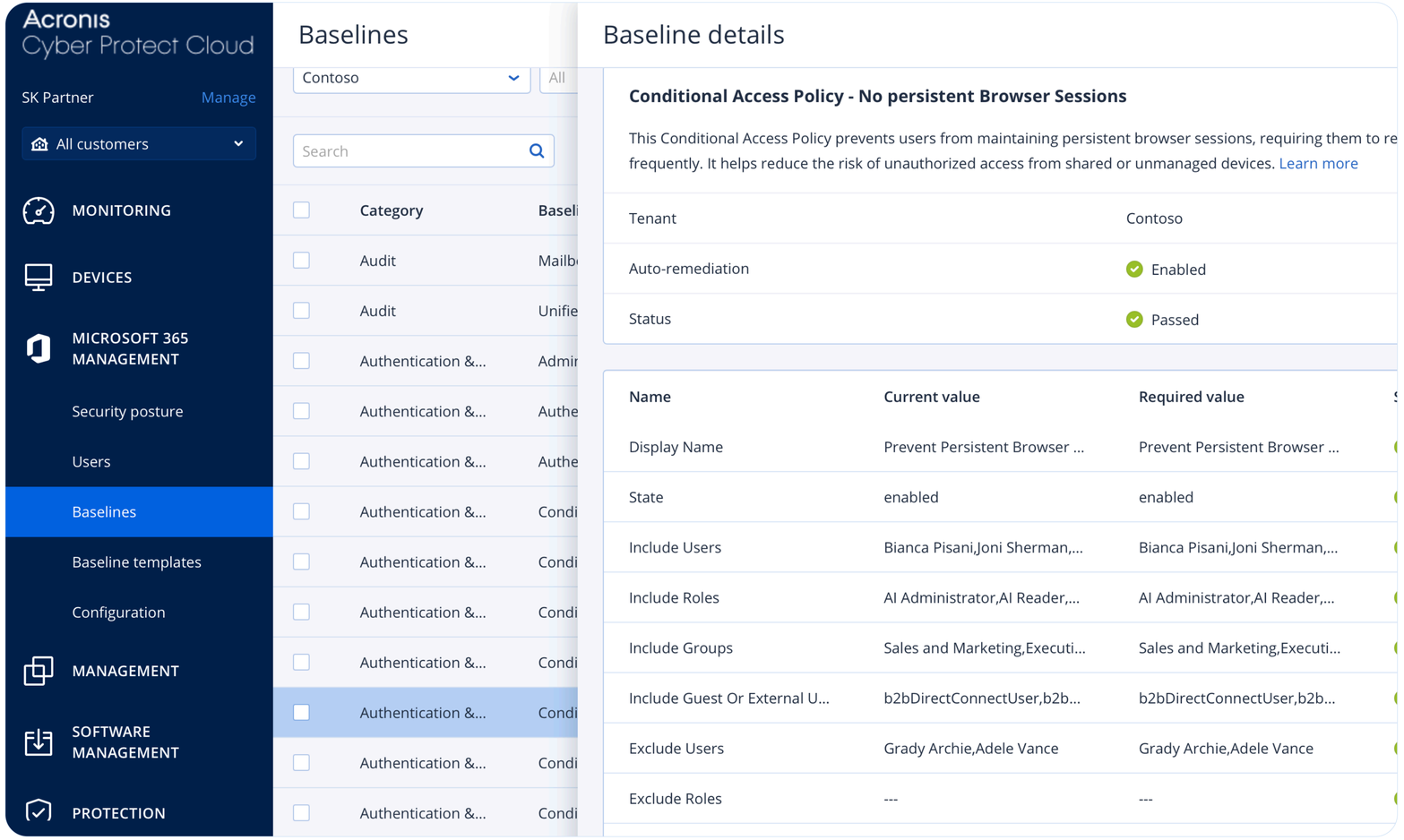
Cos'è appena successo?

Non hai rilevato il furto del token.

Tu:

- Hai chiuso le lacune nelle policy che lo consentivano.
- Hai standardizzato i controlli in tutti i tenant.
- Hai garantito un'applicazione delle regole a lungo termine.

Acronis SPM mette in sicurezza i flussi di autenticazione, non solo le identità.



Scenario 4

Escalation dei privilegi

“Un account diventa l’intero tenant.”

Un aggressore compromette un singolo account e inizia a esplorare. Trova privilegi eccessivi, più amministratori globali e una debole separazione dei ruoli. Da lì, l’escalation è semplice e porta al controllo completo del tenant.

Di solito non vengono emessi avvisi. La crescita eccessiva dei privilegi avviene gradualmente e, senza visibilità centralizzata, il rischio passa inosservato.

Acronis SPM lo mette chiaramente in evidenza, mostrando i ruoli amministrativi in tutti i tenant, identificando gli account con privilegi eccessivi e assegnando un livello di rischio in base all’esposizione.

Cosa fai (nella piattaforma)

1 **Verifichi i ruoli con privilegi**

- Identifichi gli account amministrativi eccessivi.

2 **Applichi il principio del privilegio minimo**

- Riduci gli amministratori globali.
- Standardizzi l’assegnazione dei ruoli.

3 **Automatizzi in tutti i tenant**

- Usi modelli di base per applicare le policy dei ruoli.

4 **Mantieni il controllo del ciclo di vita**

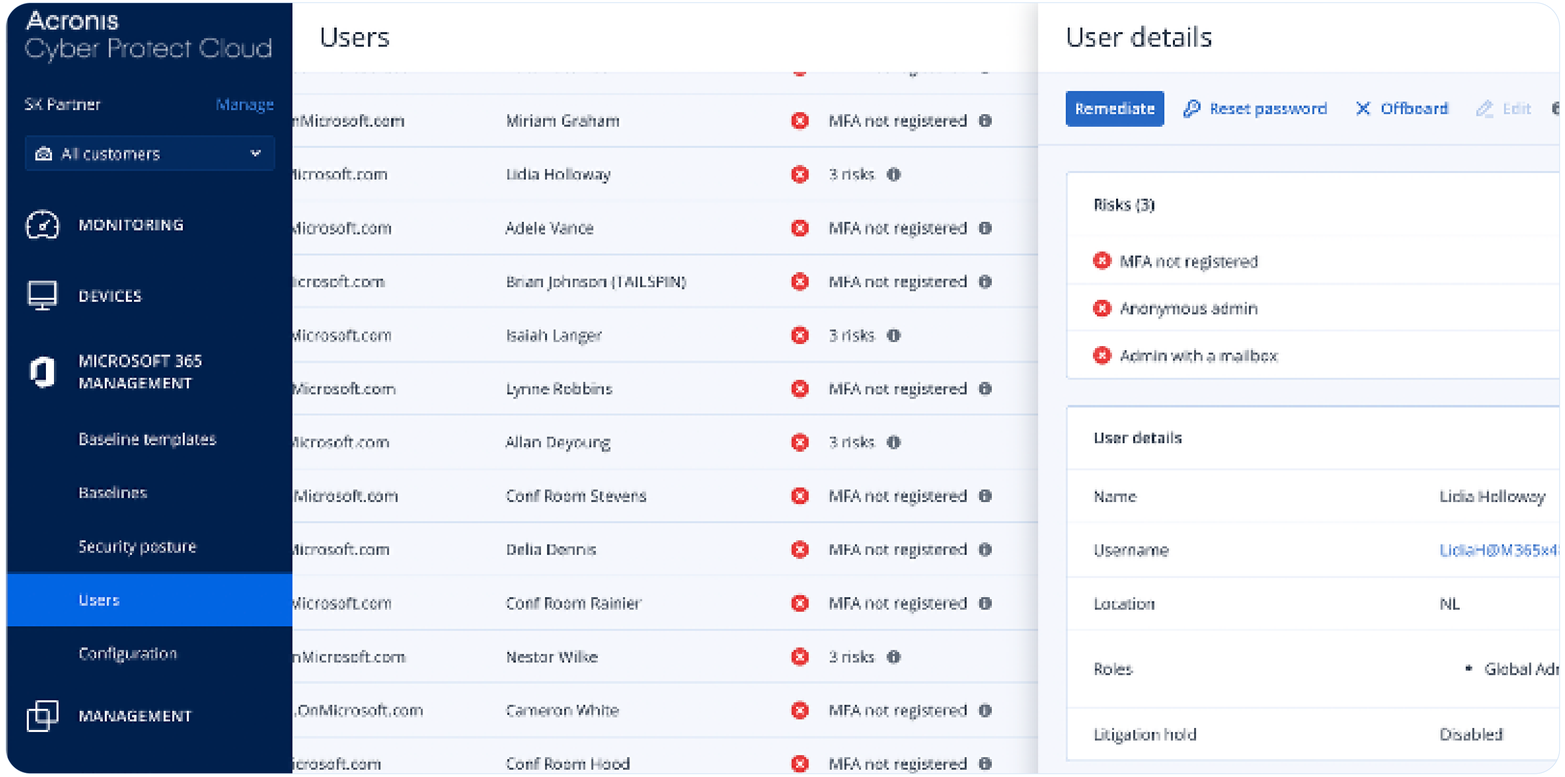
- Assegni i ruoli corretti durante l’onboarding.
- Revochi accessi, sessioni e licenze durante l’offboarding.

Cos’è appena successo?

Tu:

- Hai ridotto il raggio d’azione del danno.
- Hai standardizzato i privilegi in tutti gli ambienti.
- Hai garantito la sicurezza del ciclo di vita dell’identità.

Acronis SPM trasforma la proliferazione dei privilegi in una policy controllata e applicabile.



Puoi quindi verificare i ruoli privilegiati, ridurre il numero di amministratori globali e applicare policy di privilegio minimo su tutti i tenant utilizzando modelli di base. La gestione continua del ciclo di vita garantisce un accesso corretto durante l’onboarding e la revoca completa durante l’offboarding.

Invece di reagire all’escalation, limiti da subito il raggio d’impatto.

Cosa accomuna tutti questi attacchi

In ogni scenario:

Attacco	Causa principale
Password spraying	Controlli di identità deboli
Abuso di OAuth	Configurazioni errate dei permessi delle app
Phishing con codice dispositivo	Lacune nelle policy
Escalation dei privilegi	Permessi eccessivi

Il modello

Ingresso equivale a identità.

Persistenza equivale a configurazione.

L'impatto riguarda l'intero tenant.

La differenza di Acronis SPM

SPM non si limita a mostrare il rischio.

Consente agli MSP di gestire la sicurezza su larga scala.

Monitoraggio continuo

- Rilevamento 24 ore su 24, 7 giorni su 7, delle variazioni del livello di sicurezza.
- Identificazione in tempo reale di nuovi rischi.

Sicurezza basata su baseline

- Baseline predefinite basate sulle best practice.
- Modelli di baseline personalizzati.
- Standardizzazione su tutti i tenant.

Correzione automatica e manuale

- Correggi i problemi direttamente nella console.
- Automatizzl la risoluzione dei rischi ricorrenti.
- Elimini il lavoro manuale ripetitivo.

Gestione multitenant

- Controllo centralizzato su tutti i clienti.
- Propagazione delle policy su larga scala.

Controllo completo del ciclo di vita dell'identità

- Onboarding sicuro con ruoli e policy corretti.
- Offboarding sicuro con revoca delle sessioni e pulizia.

Integrazione operativa

- Integrazione con strumenti PSA.
- Workflow semplificati per i team MSP.

Riflessione conclusiva

I moderni attacchi a Microsoft 365 hanno successo perché:

- Nessuno vede l'esposizione.
- Nessuno la corregge in modo costante.
- Nessuno applica le regole in modo continuo.

Acronis SPM cambia tutto questo.

Dà agli MSP la possibilità di:

- Vedere il rischio in ogni tenant.
- Correggerlo istantaneamente.
- Applicare le regole automaticamente.
- Mantenerle corrette nel tempo.

Security Posture Management: un pilastro fondamentale di Protected 365

Security Posture Management (SPM) non è un componente aggiuntivo opzionale, ma una funzionalità fondamentale all'interno della soluzione Acronis Protected 365, che consente alla piattaforma di offrire la promessa di una protezione completa, potenziata dall'AI e 7-in-1 per Microsoft 365. SPM lavora in sinergia con backup, Email Security, Collaboration Security, XDR, archiviazione delle e-mail e Security Awareness Training per colmare completamente il divario della responsabilità condivisa di Microsoft in Exchange, Teams, SharePoint e OneDrive.

SPM svolge un ruolo critico nella fase "Colma le lacune con la protezione standard" del Protected 365 Maturity Model, accompagnando le organizzazioni dalla protezione di base a una resilienza proattiva. Mentre backup ed Email Security stabiliscono una protezione essenziale, SPM introduce una valutazione continua del rischio, l'applicazione delle policy e il rimedio automatizzato, garantendo che gli ambienti rimangano allineati alle best practice e conformi agli standard in evoluzione.

Monitorando continuamente le configurazioni, rilevando le deviazioni e consentendo un rimedio rapido, SPM affronta direttamente uno dei rischi più comuni e trascurati in Microsoft 365: la configurazione errata degli utenti e il deterioramento della sicurezza. Trasforma la sicurezza da un processo reattivo a una disciplina proattiva, guidata dalle policy, che riduce l'esposizione, rafforza la conformità e migliora la resilienza digitale complessiva.

Cosa fondamentale, SPM viene fornito all'interno della stessa piattaforma Acronis unica e multitenant, rafforzando così la proposta di valore fondamentale di Protected 365: un unico fornitore, un unico contratto, un'unica soluzione integrata Questo elimina la proliferazione di strumenti, riduce i costi operativi e consente a MSP e team IT di scalare in modo efficiente, migliorando al contempo la qualità del servizio e la redditività.

Agisci: colma subito le lacune

Le configurazioni errate non aspettano, e nemmeno tu dovresti farlo. Inizia oggi stesso la prova di Acronis Security Posture Management e individua immediatamente i rischi, applica le best practice e rafforza la sicurezza di Microsoft 365.

INIZIA LA PROVA GRATUITA

Acronis

Per ulteriori informazioni
acronis.com