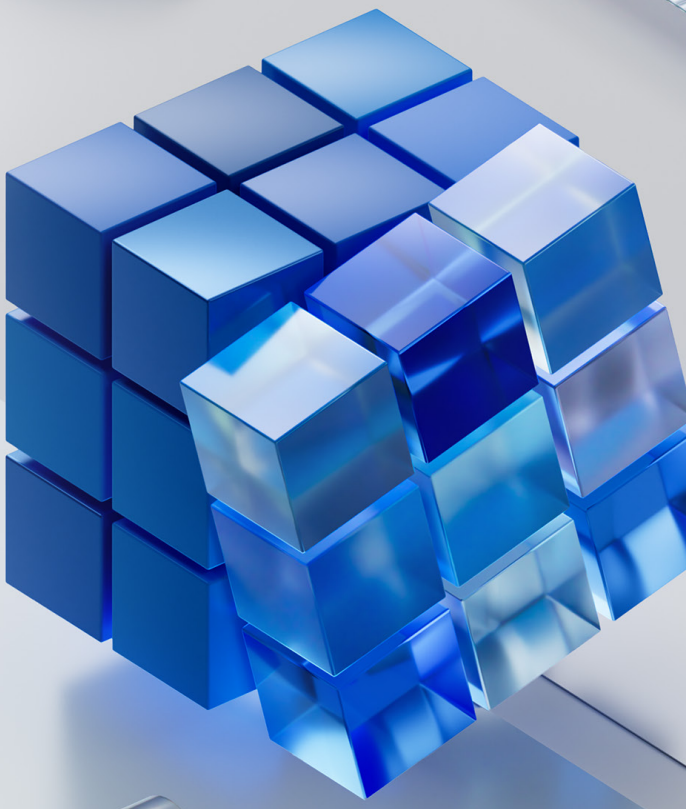
Acronis

Attacchi all'identità e al piano di controllo di Microsoft 365



9 minacce reali, quali vulnerabilità sfruttano e come gli MSP possono ridurre il rischio con Acronis SPM

I moderni attacchi a Microsoft 365 prendono sempre più di mira il piano di controllo – identità, applicazioni OAuth, autorizzazioni, sessioni e configurazioni – invece degli endpoint.

Negli ultimi incidenti reali, gli aggressori hanno sfruttato flussi di autenticazione legittimi, autorizzazioni eccessive, controlli di accesso deboli e configurazioni errate per ottenere un accesso persistente ai tenant di Microsoft 365.

Questa checklist riassume:

- Le tecniche di attacco utilizzate negli incidenti reali.
- Quali vulnerabilità hanno sfruttato gli aggressori.
- I controlli di Microsoft 365 consigliati per ridurre il rischio.
- In che modo Acronis SPM aiuta gli MSP a monitorare costantemente e garantire il livello di sicurezza di tutti i tenant.

1. Attacchi di password spraying

Incidente reale

Midnight Blizzard (2024).

Tecnica di attacco

Attacco di password spraying contro un account tenant legacy non di produzione.

Quali vulnerabilità sono state sfruttate

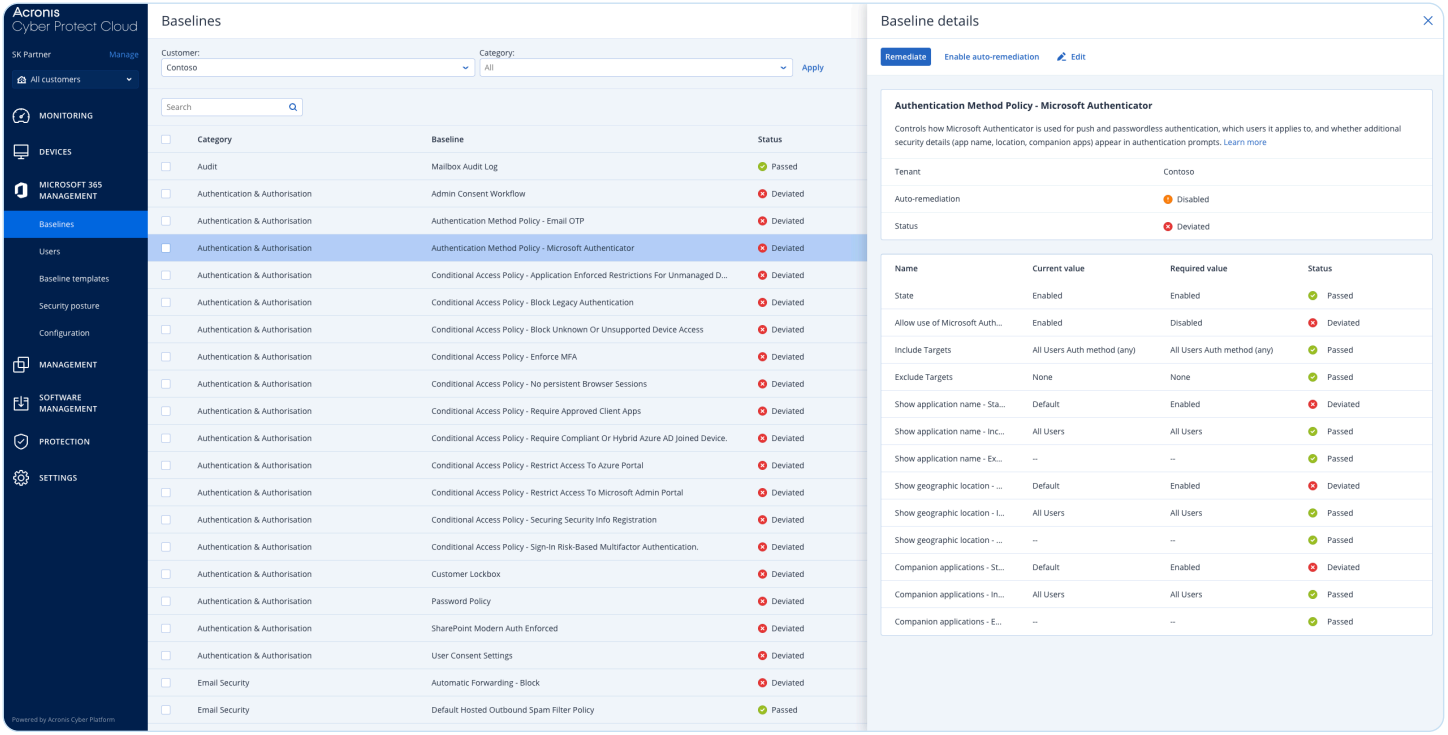
- Credenziali deboli.
- Assenza di MFA su un account legacy.

Controlli di sicurezza per ridurre il rischio

- Rinforzare l'applicazione dell'MFA.
- Eliminare le password deboli.
- Disabilitare i percorsi di autenticazione legacy.
- Monitorare le anomalie di accesso.

In che modo Acronis SPM può aiutarti

- Individua le lacune nell'MFA.
- Rileva le impostazioni di autenticazione non sicure.
- Monitora le deviazioni dalla baseline tra i tenant.
- Aiuta gli MSP a porre rimedio alle configurazioni deboli delle identità prima che diventino percorsi di attacco.



2. Falsificazione di token e abuso delle sessioni

Incidente reale

Storm-0558 (2023).

Tecnica di attacco

Token di autenticazione falsificati usati per accedere agli account e-mail nel cloud.

Quali vulnerabilità sono state sfruttate

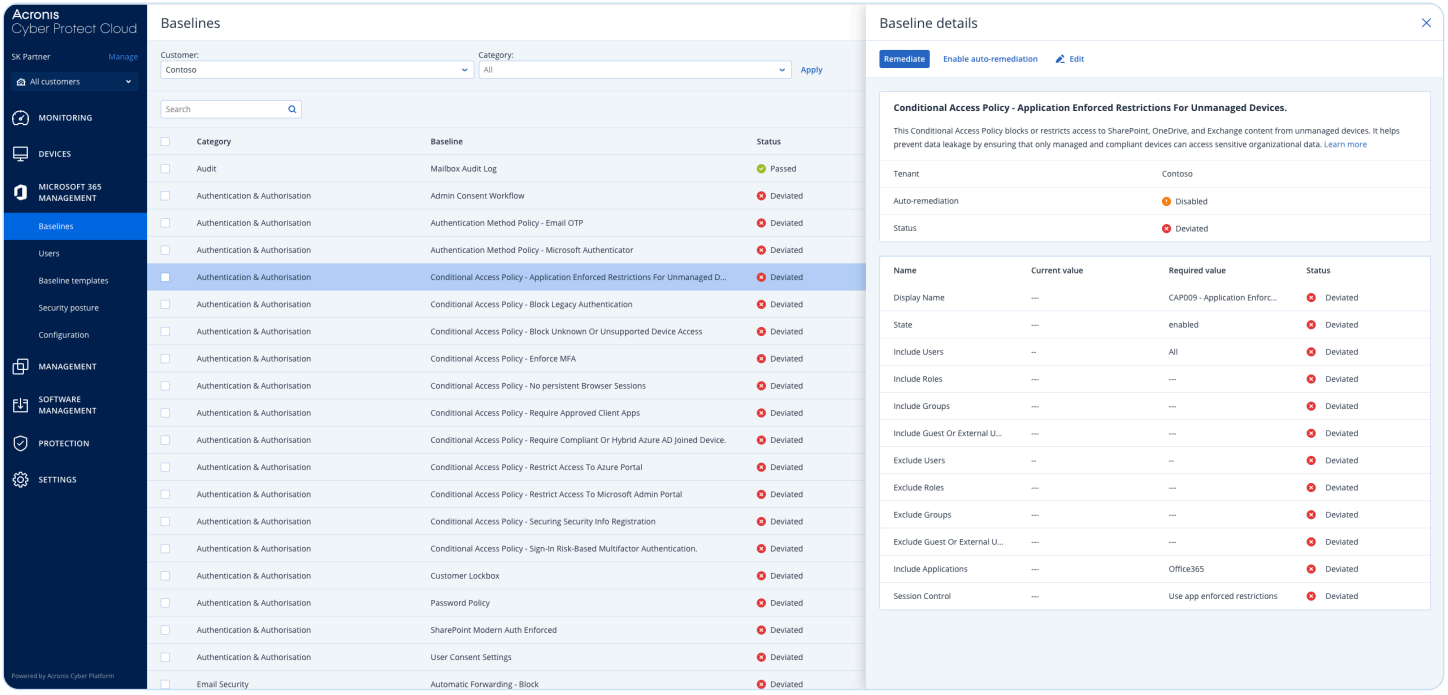
- Debolezze nella convalida dei token.
- Abuso delle chiavi di firma.
- Visibilità limitata sull'uso anomalo dei token.

Controlli di sicurezza per ridurre il rischio

- Rafforzare il livello di sicurezza dell'identità.
- Applicare l'MFA e l'accesso condizionale.
- Limitare le autorizzazioni alle app.
- Proteggere l'accesso privilegiato.
- Monitorare le anomalie di token e sessione.

In che modo Acronis SPM può aiutarti

- Aiuta a standardizzare il livello di sicurezza MFA e dell'accesso condizionale.
- Individua eventuali scostamenti nella configurazione delle identità.
- Supporta l'applicazione di baseline sicure per l'accesso amministrativo.
- Riduce l'esposizione dell'identità sul lato tenant adiacente.



3. Hijacking della sessione e phishing AiTM

Incidente reale

Più incidenti reali.

Tecnica di attacco

Furto dei cookie di sessione tramite phishing con reverse proxy.

Quali vulnerabilità sono state sfruttate

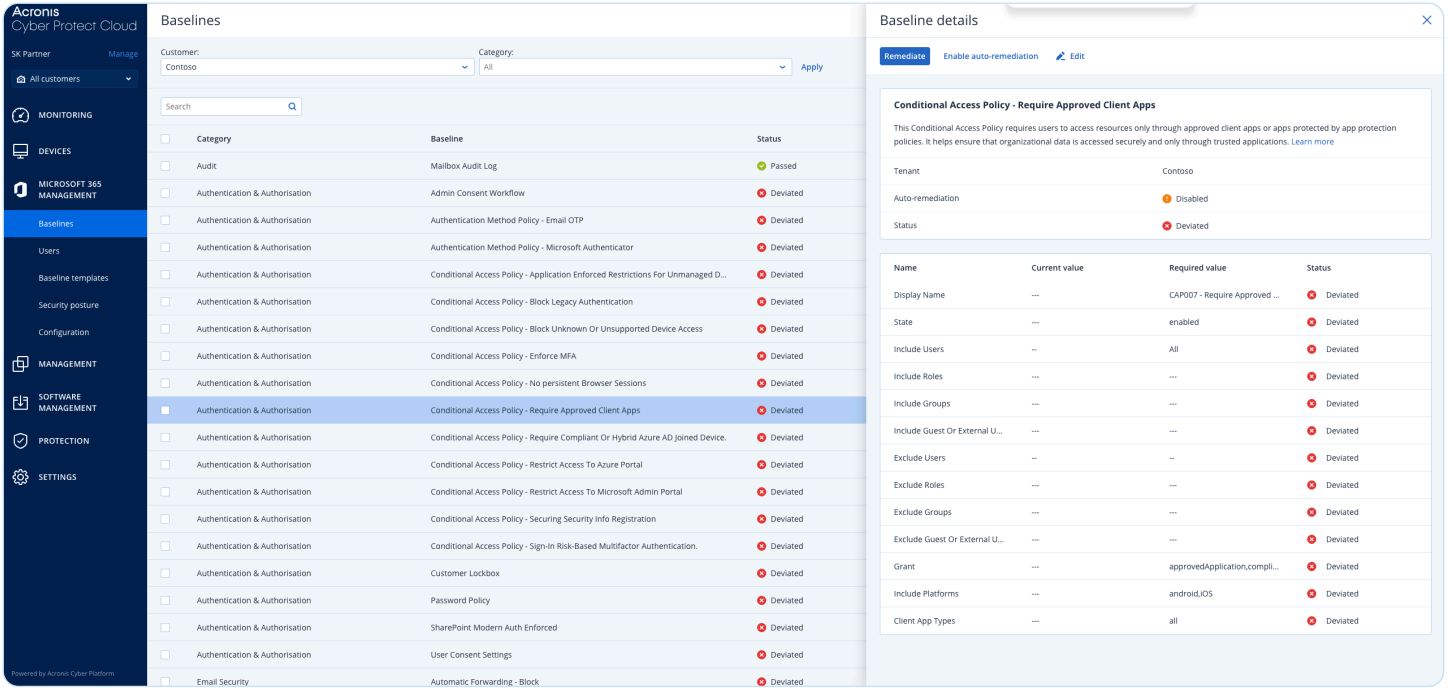
- Furto dei cookie di sessione autenticati.
- Applicazione poco rigorosa dell'accesso condizionale.
- Mancanza di restrizioni di accesso basate sul dispositivo.

Controlli di sicurezza per ridurre il rischio

- Richiedi dispositivi conformi o gestiti
- Applica l'accesso condizionale.
- Monitora i comportamenti anomali della sessione.
- Usa la valutazione continua dell'accesso, ove disponibile.

In che modo Acronis SPM può aiutarti

- Rileva eventuali scostamenti nel livello di sicurezza dell'accesso condizionale.
- Aiuta a mantenere baseline sicure per le policy di accesso.
- Supporta la standardizzazione dei controlli di identità e accesso ai dispositivi tra i tenant.



4. Attacchi di replay dei token

Incidente reale

Più incidenti reali.

Tecnica di attacco

Riutilizzo di token di aggiornamento primario rubati.

Quali vulnerabilità sono state sfruttate

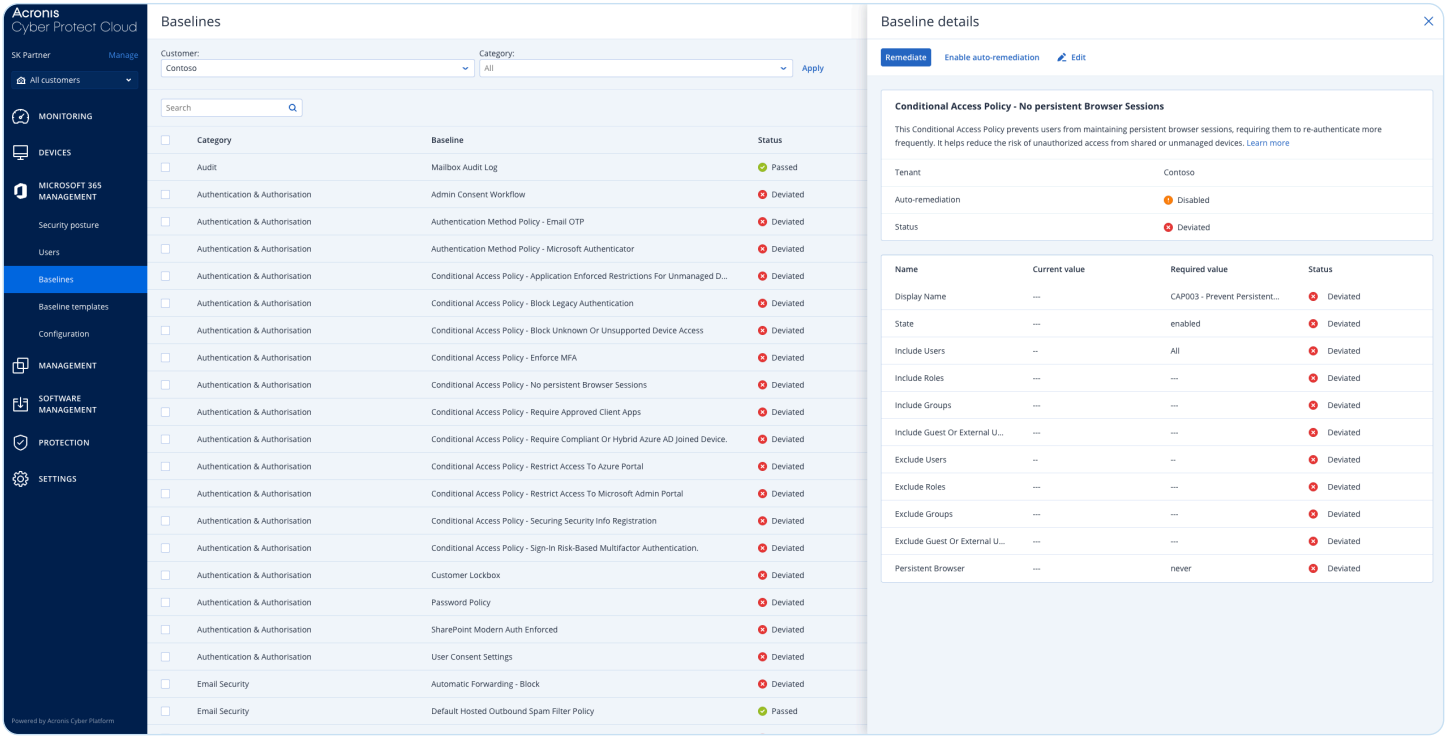
- Mancanza di protezione di token/sessione.
- Applicazione poco rigorosa della sessione.

Controlli di sicurezza per ridurre il rischio

- Attiva la protezione tramite token, se supportata.
- Utilizza i controlli di sessione di accesso condizionale.
- Limita l'accesso dai dispositivi non gestiti.

In che modo Acronis SPM può aiutarti

- Aiuta gli MSP a monitorare continuamente il livello di autenticazione.
- Rileva eventuali scostamenti della baseline in relazione ad accesso condizionale e a configurazione della sessione.
- Supporta l'applicazione di baseline sicure di identità e accesso.



5. Phishing dell'autorizzazione OAuth

Incidente reale

Più incidenti reali.

Tecnica di attacco

Autorizzazioni concesse da app dannose.

Quali vulnerabilità sono state sfruttate

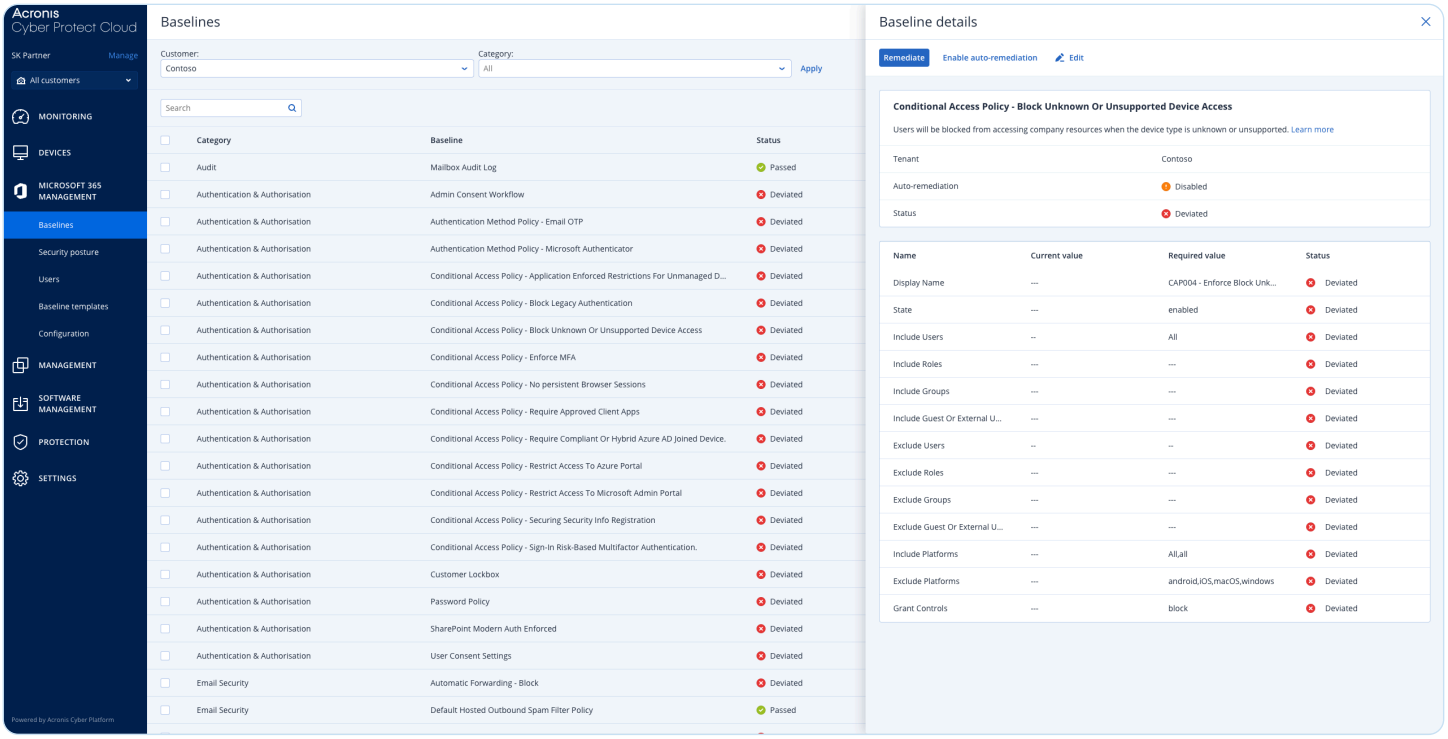
- Autorizzazione illimitata dell'utente.
- Governance delle applicazioni carente.

Controlli di sicurezza per ridurre il rischio

- Limita l'autorizzazione dell'utente.
- Richiedi l'approvazione dell'amministratore per le applicazioni.
- Consenti solo editori verificati e autorizzazioni a basso rischio.

In che modo Acronis SPM può aiutarti

- Standardizza i controlli relativi all'autorizzazione.
- Rileva eventuali scostamenti dalle policy di autorizzazione alle applicazioni approvate.
- Aiuta gli MSP a mantenere un livello di autorizzazione di Microsoft 365 sicuro tra i tenant.



6. Abuso di app OAuth ed esfiltrazione di dati tramite Graph API

Incidente reale

Più incidenti reali.

Tecnica di attacco

Accesso ai dati ed esfiltrazione tramite API attraverso applicazioni con autorizzazioni eccessive.

Quali vulnerabilità sono state sfruttate

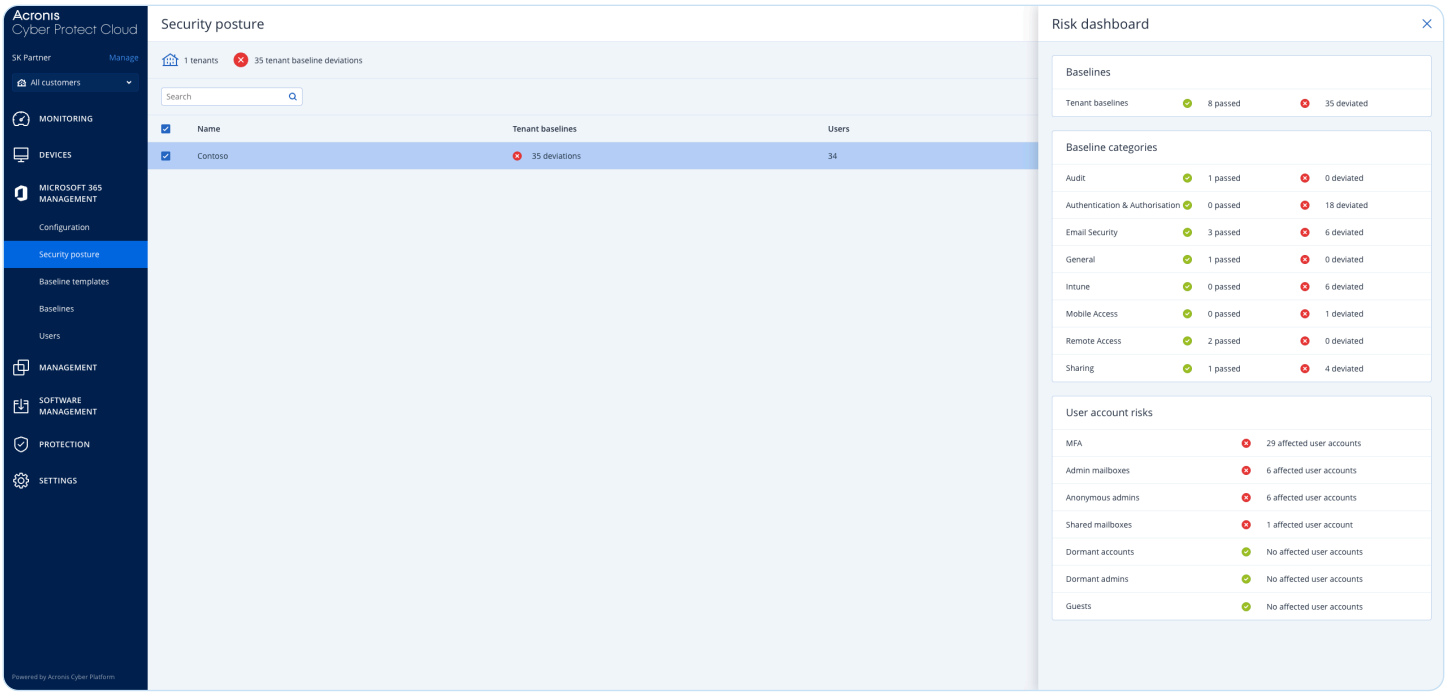
- Autorizzazioni Graph eccessive.
- Scarsa visibilità sul comportamento delle app.
- Accesso alle applicazioni non gestito.

Controlli di sicurezza per ridurre il rischio

- Verifica regolarmente le autorizzazioni delle applicazioni.
- Indaga sulle attività insolite di Graph.
- Controlla le app autorizzate da utenti esterni.

In che modo Acronis SPM può aiutarti

- Aiuta a mantenere il controllo sulle autorizzazioni delle app e sul livello di sicurezza delle autorizzazioni.
- Rileva eventuali scostamenti delle autorizzazioni e l'esposizione di app non gestite.
- Migliora la visibilità sul livello di sicurezza dell'accesso alle applicazioni di Microsoft 365.



7. Escalation dei privilegi e abuso eccessivo dei ruoli

Incidente reale

Molteplici escalation dei privilegi in Entra ID / Midnight Blizzard.

Tecnica di attacco

Escalation dei privilegi tramite privilegi amministrativi permanenti eccessivi.

Quali vulnerabilità sono state sfruttate

- Troppe Global Admin.
- Accumulo di privilegi.
- Governance dei ruoli carente.

Controlli di sicurezza per ridurre il rischio

- Applica il principio del privilegio minimo.
- Limita l'accesso amministrativo permanente.
- Controlla continuamente i ruoli con privilegi elevati.

In che modo Acronis SPM può aiutarti

- Identifica i ruoli amministrativi eccessivi e l'esposizione dei privilegi.
- Aiuta gli MSP a standardizzare un livello di sicurezza dei ruoli tra i tenant.
- Supporta l'applicazione dei criteri di base relativi all'identità e all'autorizzazione.

8. Esposizione di SharePoint e OneDrive

Incidente reale

Più incidenti reali.

Tecnica di attacco

Condivisione esterna eccessiva o accidentale.

Quali vulnerabilità sono state sfruttate

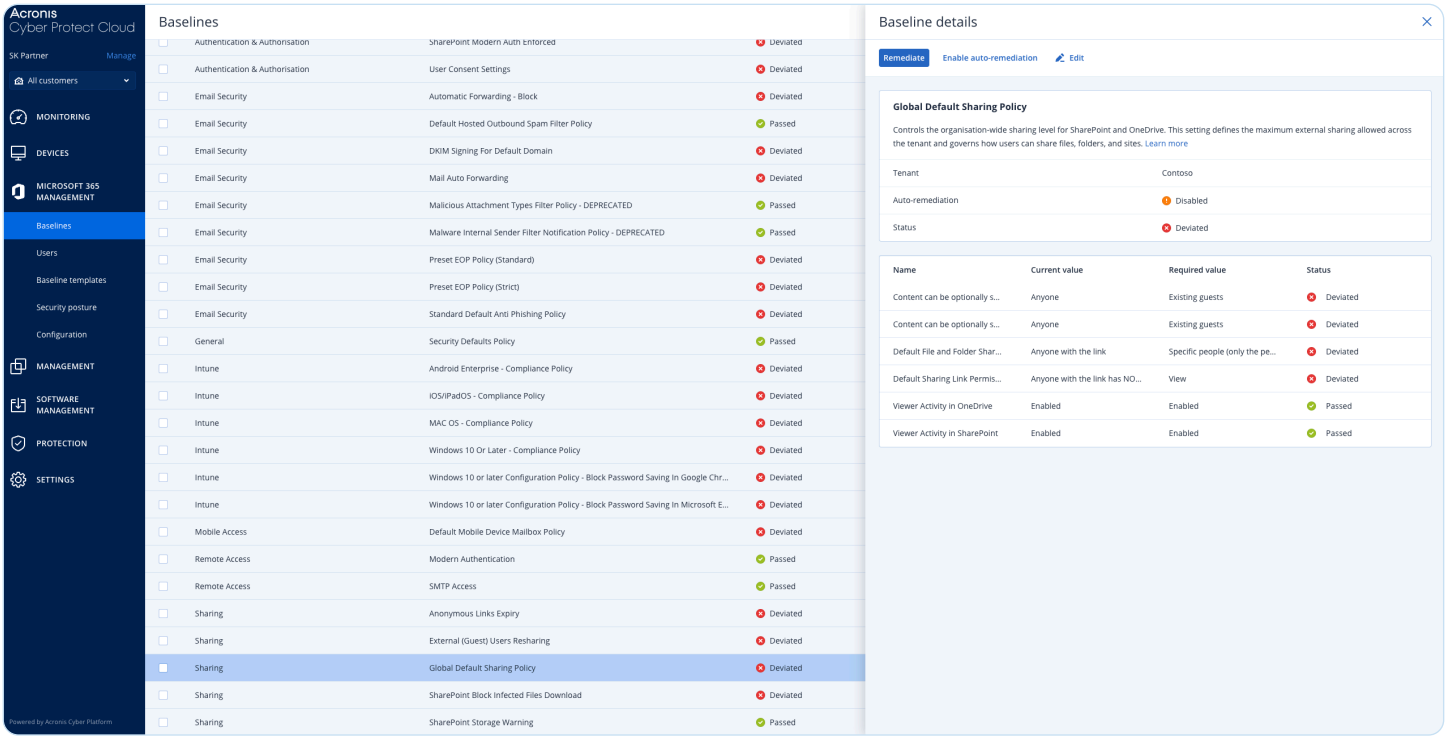
- Governance della condivisione carente.
- Impostazioni di accesso esterno eccessivamente permissive.

Controlli di sicurezza per ridurre il rischio

- Configura criteri di condivisione esterna a livello di organizzazione.
- Limita la condivisione quando necessario.
- Controlla regolarmente il livello di sicurezza della condivisione.

In che modo Acronis SPM può aiutarti

- Convalida continuamente il livello di sicurezza della condivisione rispetto alle baseline.
- Rileva le configurazioni di condivisione rischiose.
- Riduce gli scostamenti di configurazione a lungo termine tra i tenant.



9. Lacune nelle attività di audit e di indagine

Incidente reale

Indagini sugli incidenti.

Tecnica di attacco

Attività post-compromissione nascosta da controlli di audit insufficienti.

Quali vulnerabilità sono state sfruttate

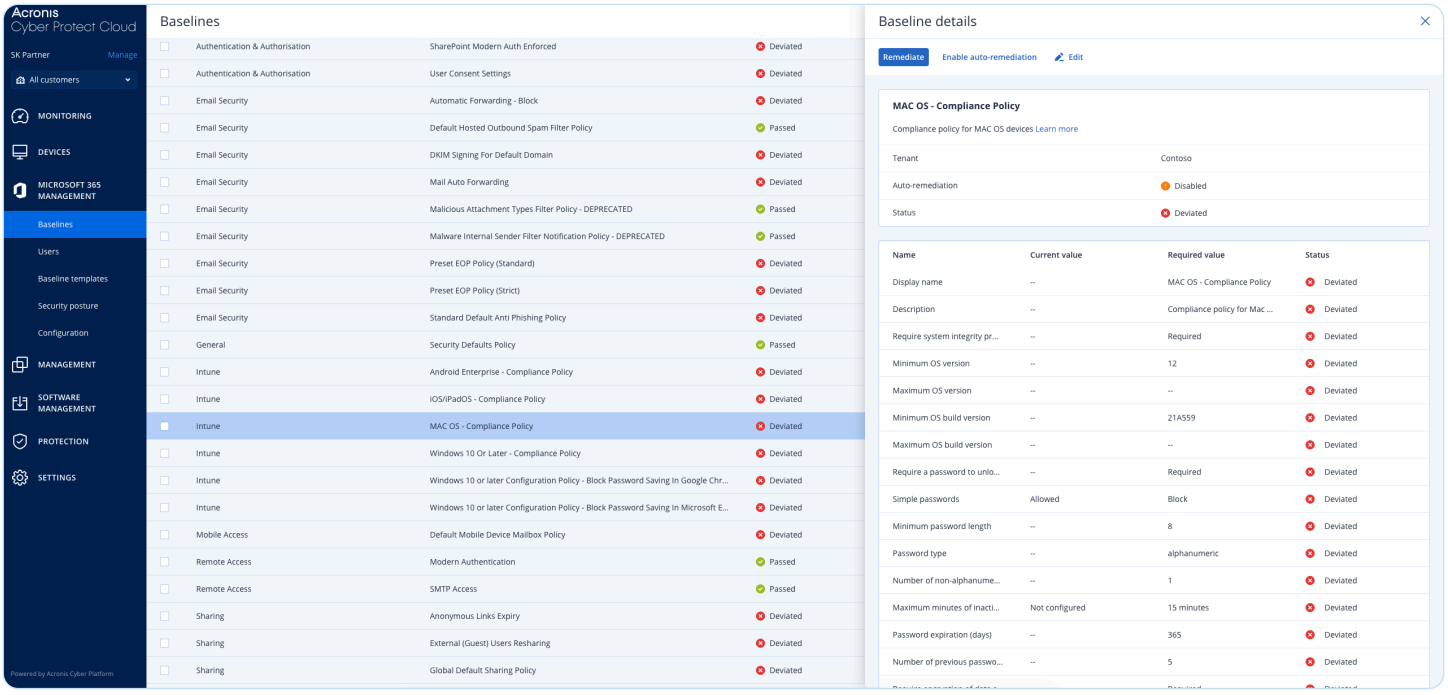
- Prove di audit mancanti o incomplete.
- Scarsa prontezza nelle indagini.

Controlli di sicurezza per ridurre il rischio

- Mantieni abilitato l'audit di Microsoft Purview.
- Assicurati che gli investigatori dispongano dell'accesso appropriato.
- Assicurati di essere sempre pronto per eventuali ricerche di audit.

In che modo Acronis SPM può aiutarti

- Aiuta gli MSP a monitorare il livello di sicurezza della configurazione relativamente all'audit.
- Rileva eventuali scostamenti nelle impostazioni di registrazione e audit.
- Supporta le indagini in corso e la preparazione alla conformità.



Cosa hanno in comune questi attacchi

In tutti gli incidenti:

- L'accesso si basa sull'identità.
- La persistenza si basa sulla configurazione.
- L'impatto riguarda l'intero tenant.
- I controlli tradizionali degli endpoint offrono una visibilità limitata.

Perché la gestione continua del livello di sicurezza è importante

Gli attacchi moderni a Microsoft 365 hanno successo quando:

- Le configurazioni errate persistono.
- Il livello di sicurezza si modifica nel tempo.
- Le lacune di visibilità rimangono inosservate in tutti i tenant.

In che modo Acronis SPM aiuta gli MSP a ridurre il rischio

- Gestisce centralmente il livello di sicurezza di Microsoft 365 tra più tenant.
- Monitora continuamente il livello di sicurezza rispetto alle baseline.
- Rileva automaticamente nuovi rischi e gli scostamenti di configurazione.
- Applica modelli di baseline riutilizzabili.
- Automatizza e semplifica la correzione dei problemi.
- Semplifica i flussi di onboarding e offboarding.
- Standardizza su larga scala il livello di sicurezza di Microsoft 365.

Scopri come Acronis SPM aiuta gli MSP a proteggere Microsoft 365 su larga scala

Effettua la scansione per prenotare una demo di Acronis SPM

Acronis

Per saperne di più, visita acronis.com