

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.

Acronis Cyber Protect Cloud

SK Partner

Manage

All customers

MONITORING

DEVICES

MICROSOFT 365 MANAGEMENT

Baselines

Users

Baseline templates

Security posture

Configuration

MANAGEMENT

SOFTWARE MANAGEMENT

PROTECTION

SETTINGS

Powered by Acronis Cyber Platform

Baselines

Customer: Contoso

Category: All

Apply

Search

Category	Baseline	Status	
☐	Audit	Mailbox Audit Log	Passed
☐	Authentication & Authorisation	Admin Consent Workflow	Deviated
☐	Authentication & Authorisation	Authentication Method Policy - Email OTP	Deviated
☒	Authentication & Authorisation	Authentication Method Policy - Microsoft Authenticator	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Application Enforced Restrictions For Unmanaged D...	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Block Legacy Authentication	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Block Unknown Or Unsupported Device Access	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Enforce MFA	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - No persistent Browser Sessions	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Require Approved Client Apps	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Require Compliant Or Hybrid Azure AD joined Device.	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Restrict Access To Azure Portal	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Restrict Access To Microsoft Admin Portal	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Securing Security Info Registration	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Sign-In Risk-Based Multifactor Authentication.	Deviated
☐	Authentication & Authorisation	Customer Lockbox	Deviated
☐	Authentication & Authorisation	Password Policy	Deviated
☐	Authentication & Authorisation	SharePoint Modern Auth Enforced	Deviated
☐	Authentication & Authorisation	User Consent Settings	Deviated
☐	Email Security	Automatic Forwarding - Block	Deviated
☐	Email Security	Default Hosted Outbound Spam Filter Policy	Passed

Baseline details

Remediate

Enable auto-remediation

Edit

Authentication Method Policy - Microsoft Authenticator

Controls how Microsoft Authenticator is used for push and passwordless authentication, which users it applies to, and whether additional security details (app name, location, companion apps) appear in authentication prompts. [Learn more](#)

Tenant

Contoso

Auto-remediation

Disabled

Status

Deviated

Name	Current value	Required value	Status
State	Enabled	Enabled	Passed
Allow use of Microsoft Auth...	Enabled	Disabled	Deviated
Include Targets	All Users Auth method (any)	All Users Auth method (any)	Passed
Exclude Targets	None	None	Passed
Show application name - Sta...	Default	Enabled	Deviated
Show application name - Inc...	All Users	All Users	Passed
Show application name - Ex...	--	--	Passed
Show geographic location - ...	Default	Enabled	Deviated
Show geographic location - L...	All Users	All Users	Passed
Show geographic location - ...	--	--	Passed
Companion applications - St...	Default	Enabled	Deviated
Companion applications - In...	All Users	All Users	Passed
Companion applications - E...	--	--	Passed

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.

Acronis Cyber Protect Cloud

SK Partner

Manage

All customers

MONITORING

DEVICES

MICROSOFT 365 MANAGEMENT

Baselines

Users

Baseline templates

Security posture

Configuration

MANAGEMENT

SOFTWARE MANAGEMENT

PROTECTION

SETTINGS

Baselines

Customer: Contoso

Category: All

Apply

Search

Category	Baseline	Status
Audit	Mailbox Audit Log	Passed
Authentication & Authorisation	Admin Consent Workflow	Deviated
Authentication & Authorisation	Authentication Method Policy - Email OTP	Deviated
Authentication & Authorisation	Authentication Method Policy - Microsoft Authenticator	Deviated
Authentication & Authorisation	Conditional Access Policy - Application Enforced Restrictions For Unmanaged D...	Deviated
Authentication & Authorisation	Conditional Access Policy - Block Legacy Authentication	Deviated
Authentication & Authorisation	Conditional Access Policy - Block Unknown Or Unsupported Device Access	Deviated
Authentication & Authorisation	Conditional Access Policy - Enforce MFA	Deviated
Authentication & Authorisation	Conditional Access Policy - No persistent Browser Sessions	Deviated
Authentication & Authorisation	Conditional Access Policy - Require Approved Client Apps	Deviated
Authentication & Authorisation	Conditional Access Policy - Require Compliant Or Hybrid Azure AD joined Device	Deviated
Authentication & Authorisation	Conditional Access Policy - Restrict Access To Azure Portal	Deviated
Authentication & Authorisation	Conditional Access Policy - Restrict Access To Microsoft Admin Portal	Deviated
Authentication & Authorisation	Conditional Access Policy - Securing Security Info Registration	Deviated
Authentication & Authorisation	Conditional Access Policy - Sign-In Risk-Based Multifactor Authentication	Deviated
Authentication & Authorisation	Customer Lockbox	Deviated
Authentication & Authorisation	Password Policy	Deviated
Authentication & Authorisation	SharePoint Modern Auth Enforced	Deviated
Authentication & Authorisation	User Consent Settings	Deviated
Email Security	Automatic Forwarding - Block	Deviated

Baseline details

Remediate Enable auto-remediation Edit

Conditional Access Policy - Application Enforced Restrictions For Unmanaged Devices.

This Conditional Access Policy blocks or restricts access to SharePoint, OneDrive, and Exchange content from unmanaged devices. It helps prevent data leakage by ensuring that only managed and compliant devices can access sensitive organizational data. [Learn more](#)

Tenant

Contoso

Auto-remediation

Disabled

Status

Deviated

Name	Current value	Required value	Status
Display Name	---	CAP009 - Application Enforc...	Deviated
State	---	enabled	Deviated
Include Users	---	All	Deviated
Include Roles	---	---	Deviated
Include Groups	---	---	Deviated
Include Guest Or External U...	---	---	Deviated
Exclude Users	---	---	Deviated
Exclude Roles	---	---	Deviated
Exclude Groups	---	---	Deviated
Exclude Guest Or External U...	---	---	Deviated
Include Applications	---	Office365	Deviated
Session Control	---	Use app enforced restrictions	Deviated

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.

Acronis Cyber Protect Cloud

5K Partner

Manage

All customers

MONITORING

DEVICES

MICROSOFT 365 MANAGEMENT

Baselines

Users

Baseline templates

Security posture

Configuration

MANAGEMENT

SOFTWARE MANAGEMENT

PROTECTION

SETTINGS

Baselines

Customer: Contoso

Category: All

Apply

Search

Category	Baseline	Status
☐ Audit	Mailbox Audit Log	Passed
☐ Authentication & Authorisation	Admin Consent Workflow	Deviated
☐ Authentication & Authorisation	Authentication Method Policy - Email OTP	Deviated
☐ Authentication & Authorisation	Authentication Method Policy - Microsoft Authenticator	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Application Enforced Restrictions For Unmanaged D...	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Block Legacy Authentication	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Block Unknown Or Unsupported Device Access	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Enforce MFA	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - No persistent Browser Sessions	Deviated
☒ Authentication & Authorisation	Conditional Access Policy - Require Approved Client Apps	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Require Compliant Or Hybrid Azure AD joined Device	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Restrict Access To Azure Portal	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Restrict Access To Microsoft Admin Portal	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Securing Security Info Registration	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Sign-In Risk-Based Multifactor Authentication	Deviated
☐ Authentication & Authorisation	Customer Lockbox	Deviated
☐ Authentication & Authorisation	Password Policy	Deviated
☐ Authentication & Authorisation	SharePoint Modern Auth Enforced	Deviated
☐ Authentication & Authorisation	User Consent Settings	Deviated
☐ Email Security	Automatic Forwarding - Block	Deviated

Baseline details

Remediate

Enable auto-remediation

Edit

Conditional Access Policy - Require Approved Client Apps

This Conditional Access Policy requires users to access resources only through approved client apps or apps protected by app protection policies. It helps ensure that organizational data is accessed securely and only through trusted applications. [Learn more](#)

Tenant

Contoso

Auto-remediation

Disabled

Status

Deviated

Name	Current value	Required value	Status
Display Name	---	CA007 - Require Approved ...	Deviated
State	---	enabled	Deviated
Include Users	---	All	Deviated
Include Roles	---	---	Deviated
Include Groups	---	---	Deviated
Include Guest Or External U...	---	---	Deviated
Exclude Users	---	---	Deviated
Exclude Roles	---	---	Deviated
Exclude Groups	---	---	Deviated
Exclude Guest Or External U...	---	---	Deviated
Grant	---	approvedApplication,compl...	Deviated
Include Platforms	---	android,iOS	Deviated
Client App Types	---	all	Deviated

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.

Acronis Cyber Protect Cloud

SK Partner

Manage

All customers

MONITORING

DEVICES

MICROSOFT 365 MANAGEMENT

Security posture

Users

Baselines

Baseline templates

Configuration

MANAGEMENT

SOFTWARE MANAGEMENT

PROTECTION

SETTINGS

Powered by Acronis Cyber Platform

Baselines

Customer: Contoso

Category: All

Apply

Search

	Category	Baseline	Status
☐	Audit	Mailbox Audit Log	Passed
☐	Authentication & Authorisation	Admin Consent Workflow	Deviated
☐	Authentication & Authorisation	Authentication Method Policy - Email OTP	Deviated
☐	Authentication & Authorisation	Authentication Method Policy - Microsoft Authenticator	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Application Enforced Restrictions For Unmanaged D...	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Block Legacy Authentication	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Block Unknown Or Unsupported Device Access	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Enforce MFA	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - No persistent Browser Sessions	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Require Approved Client Apps	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Require Compliant Or Hybrid Azure AD joined Device	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Restrict Access To Azure Portal	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Restrict Access To Microsoft Admin Portal	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Securing Security Info Registration	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Sign-In Risk-Based Multifactor Authentication	Deviated
☐	Authentication & Authorisation	Customer Lockbox	Deviated
☐	Authentication & Authorisation	Password Policy	Deviated
☐	Authentication & Authorisation	SharePoint Modern Auth Enforced	Deviated
☐	Authentication & Authorisation	User Consent Settings	Deviated
☐	Email Security	Automatic Forwarding - Block	Deviated
☐	Email Security	Default Hosted Outbound Spam Filter Policy	Passed

Baseline details

Remediate Enable auto-remediation Edit

Conditional Access Policy - No persistent Browser Sessions

This Conditional Access Policy prevents users from maintaining persistent browser sessions, requiring them to re-authenticate more frequently. It helps reduce the risk of unauthorized access from shared or unmanaged devices. [Learn more](#)

Tenant

Contoso

Auto-remediation

Disabled

Status

Deviated

Name	Current value	Required value	Status
Display Name	---	CAPO03 - Prevent Persistent...	Deviated
State	---	enabled	Deviated
Include Users	---	All	Deviated
Include Roles	---	---	Deviated
Include Groups	---	---	Deviated
Include Guest Or External U...	---	---	Deviated
Exclude Users	---	---	Deviated
Exclude Roles	---	---	Deviated
Exclude Groups	---	---	Deviated
Exclude Guest Or External U...	---	---	Deviated
Persistent Browser	---	never	Deviated

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.

Acronis
Cyber Protect Cloud

SK Partner

Manage

All customers

MONITORING

DEVICES

MICROSOFT 365
MANAGEMENT

Baselines

Security posture

Users

Baseline templates

Configuration

MANAGEMENT

SOFTWARE
MANAGEMENT

PROTECTION

SETTINGS

Powered by Acronis Cyber Platform

Baselines

Customer: Contoso

Category: All

Apply

Search

Category	Baseline	Status	
☐	Audit	Mailbox Audit Log	Passed
☐	Authentication & Authorisation	Admin Consent Workflow	Deviated
☐	Authentication & Authorisation	Authentication Method Policy - Email OTP	Deviated
☐	Authentication & Authorisation	Authentication Method Policy - Microsoft Authenticator	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Application Enforced Restrictions For Unmanaged D...	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Block Legacy Authentication	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Block Unknown Or Unsupported Device Access	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Enforce MFA	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - No persistent Browser Sessions	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Require Approved Client Apps	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Require Compliant Or Hybrid Azure AD joined Device...	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Restrict Access To Azure Portal	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Restrict Access To Microsoft Admin Portal	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Securing Security Info Registration	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Sign-In Risk-Based Multifactor Authentication...	Deviated
☐	Authentication & Authorisation	Customer Lockbox	Deviated
☐	Authentication & Authorisation	Password Policy	Deviated
☐	Authentication & Authorisation	SharePoint Modern Auth Enforced	Deviated
☐	Authentication & Authorisation	User Consent Settings	Deviated
☐	Email Security	Automatic Forwarding - Block	Deviated
☐	Email Security	Default Hosted Outbound Spam Filter Policy	Passed

Baseline details

Remediate

Enable auto-remediation

Edit

Conditional Access Policy - Block Unknown Or Unsupported Device Access

Users will be blocked from accessing company resources when the device type is unknown or unsupported. Learn more

Tenant: Contoso

Auto-remediation: Disabled

Status: Deviated

Name	Current value	Required value	Status
Display Name	---	CAPO04 - Enforce Block Unk...	Deviated
State	---	enabled	Deviated
Include Users	---	All	Deviated
Include Roles	---	---	Deviated
Include Groups	---	---	Deviated
Include Guest Or External U...	---	---	Deviated
Exclude Users	---	---	Deviated
Exclude Roles	---	---	Deviated
Exclude Groups	---	---	Deviated
Exclude Guest Or External U...	---	---	Deviated
Include Platforms	---	All,all	Deviated
Exclude Platforms	---	android,iOS,macOS,windows	Deviated
Grant Controls	---	block	Deviated

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.

The screenshot displays the Acronis Cyber Protect Cloud interface. The left sidebar shows the navigation menu with categories like MONITORING, DEVICES, MICROSOFT 365 MANAGEMENT, and SETTINGS. The main content area is divided into two panels:

Security posture

At the top, it shows "1 tenants" and "35 tenant baseline deviations". Below this is a table with columns for Name, Tenant baselines, and Users.

Name	Tenant baselines	Users
Contoso	35 deviations	34

Risk dashboard

The Risk dashboard provides a detailed overview of security baselines and user account risks.

Baselines

Tenant baselines	8 passed	35 deviated
------------------	----------	-------------

Baseline categories

Category	Passed	Deviated
Audit	1 passed	0 deviated
Authentication & Authorisation	0 passed	18 deviated
Email Security	3 passed	6 deviated
General	1 passed	0 deviated
Intune	0 passed	6 deviated
Mobile Access	0 passed	1 deviated
Remote Access	2 passed	0 deviated
Sharing	1 passed	4 deviated

User account risks

Risk Category	Affected user accounts
MFA	29 affected user accounts
Admin mailboxes	6 affected user accounts
Anonymous admins	6 affected user accounts
Shared mailboxes	1 affected user account
Dormant accounts	No affected user accounts
Dormant admins	No affected user accounts
Guests	No affected user accounts

7. Escalation dei privilegi e abuso eccessivo dei ruoli



Incidente reale

Molteplici escalation dei privilegi in Entra ID / Midnight Blizzard.



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.



Tecnica di attacco

Escalation dei privilegi tramite privilegi amministrativi permanenti eccessivi.



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.



Quali vulnerabilità sono state sfruttate

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

Compliance Posture Summary

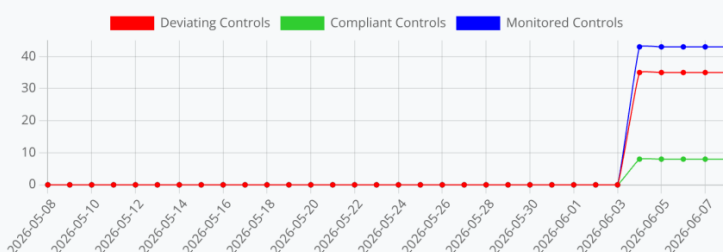
Baselines

Current Posture Summary (All time)

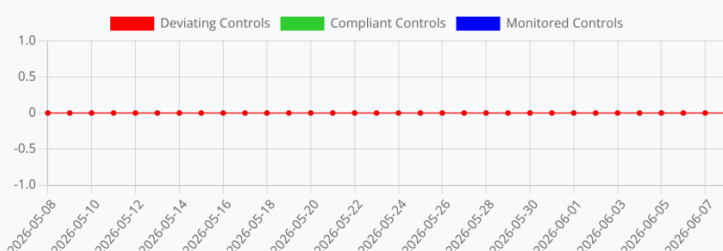
Tenant	Group
Passing: 8	Passing: -
Deviating: 35	Deviating: -

Posture Summary (In this period) *

Tenant Baselines Posture Summary Chart



Group Baselines Posture Summary Chart



Please noted that baseline created/passing were not recorded before 27/09/2022.
Only Deviations after this date will be accurate.

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.

Acronis Cyber Protect Cloud

SK Partner Manage

All customers

MONITORING

DEVICES

MICROSOFT 365 MANAGEMENT

Baselines

Users

Baseline templates

Security posture

Configuration

MANAGEMENT

SOFTWARE MANAGEMENT

PROTECTION

SETTINGS

Baselines

☐	Authentication & Authorisation	SharePoint Modern Auth Enforced	Deviated
☐	Authentication & Authorisation	User Consent Settings	Deviated
☐	Email Security	Automatic Forwarding - Block	Deviated
☐	Email Security	Default Hosted Outbound Spam Filter Policy	Passed
☐	Email Security	DKIM Signing For Default Domain	Deviated
☐	Email Security	Mail Auto Forwarding	Deviated
☐	Email Security	Malicious Attachment Types Filter Policy - DEPRECATED	Passed
☐	Email Security	Malware Internal Sender Filter Notification Policy - DEPRECATED	Passed
☐	Email Security	Preset EOP Policy (Standard)	Deviated
☐	Email Security	Preset EOP Policy (Strict)	Deviated
☐	Email Security	Standard Default Anti Phishing Policy	Deviated
☐	General	Security Defaults Policy	Passed
☐	Intune	Android Enterprise - Compliance Policy	Deviated
☐	Intune	iOS/iPadOS - Compliance Policy	Deviated
☐	Intune	MAC OS - Compliance Policy	Deviated
☐	Intune	Windows 10 Or Later - Compliance Policy	Deviated
☐	Intune	Windows 10 or later Configuration Policy - Block Password Saving in Google Chr...	Deviated
☐	Intune	Windows 10 or later Configuration Policy - Block Password Saving in Microsoft E...	Deviated
☐	Mobile Access	Default Mobile Device Mailbox Policy	Deviated
☐	Remote Access	Modern Authentication	Passed
☐	Remote Access	SMTP Access	Passed
☐	Sharing	Anonymous Links Expiry	Deviated
☐	Sharing	External (Guest) Users Resharing	Deviated
☒	Sharing	Global Default Sharing Policy	Deviated
☐	Sharing	SharePoint Block Infected Files Download	Deviated
☐	Sharing	SharePoint Storage Warning	Passed

Baseline details

Remediate Enable auto-remediation Edit

Global Default Sharing Policy

Controls the organisation-wide sharing level for SharePoint and OneDrive. This setting defines the maximum external sharing allowed across the tenant and governs how users can share files, folders, and sites. [Learn more](#)

Tenant	Contoso
Auto-remediation	Disabled
Status	Deviated

Name	Current value	Required value	Status
Content can be optionally s...	Anyone	Existing guests	Deviated
Content can be optionally s...	Anyone	Existing guests	Deviated
Default File and Folder Shar...	Anyone with the link	Specific people (only the pe...	Deviated
Default Sharing Link Permis...	Anyone with the link has NO...	View	Deviated
Viewer Activity in OneDrive	Enabled	Enabled	Passed
Viewer Activity in SharePoint	Enabled	Enabled	Passed

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.

Acronis Cyber Protect Cloud

SK Partner

Manage

All customers

MONITORING

DEVICES

MICROSOFT 365 MANAGEMENT

Baselines

Users

Baseline templates

Security posture

Configuration

MANAGEMENT

SOFTWARE MANAGEMENT

PROTECTION

SETTINGS

Baselines			
☐	Authentication & Authorisation	SharePoint Modern Auth Enforced	Deviated
☐	Authentication & Authorisation	User Consent Settings	Deviated
☐	Email Security	Automatic Forwarding - Block	Deviated
☐	Email Security	Default Hosted Outbound Spam Filter Policy	Passed
☐	Email Security	DKIM Signing For Default Domain	Deviated
☐	Email Security	Mail Auto Forwarding	Deviated
☐	Email Security	Malicious Attachment Types Filter Policy - DEPRECATED	Passed
☐	Email Security	Malware Internal Sender Filter Notification Policy - DEPRECATED	Passed
☐	Email Security	Preset EOP Policy (Standard)	Deviated
☐	Email Security	Preset EOP Policy (Strict)	Deviated
☐	Email Security	Standard Default Anti Phishing Policy	Deviated
☐	General	Security Defaults Policy	Passed
☐	Intune	Android Enterprise - Compliance Policy	Deviated
☐	Intune	iOS/iPadOS - Compliance Policy	Deviated
☒	Intune	MAC OS - Compliance Policy	Deviated
☐	Intune	Windows 10 Or Later - Compliance Policy	Deviated
☐	Intune	Windows 10 or later Configuration Policy - Block Password Saving in Google Chr...	Deviated
☐	Intune	Windows 10 or later Configuration Policy - Block Password Saving in Microsoft E...	Deviated
☐	Mobile Access	Default Mobile Device Mailbox Policy	Deviated
☐	Remote Access	Modern Authentication	Passed
☐	Remote Access	SMTS Access	Passed
☐	Sharing	Anonymous Links Expiry	Deviated
☐	Sharing	External (Guest) Users Resharing	Deviated
☐	Sharing	Global Default Sharing Policy	Deviated

Baseline details

Remediate

Enable auto-remediation

Edit

MAC OS - Compliance Policy

Compliance policy for MAC OS devices [Learn more](#)

Tenant

Contoso

Auto-remediation

Disabled

Status

Deviated

Name	Current value	Required value	Status
Display name	—	MAC OS - Compliance Policy	Deviated
Description	—	Compliance policy for Mac ...	Deviated
Require system integrity pr...	—	Required	Deviated
Minimum OS version	—	12	Deviated
Maximum OS version	—	—	Deviated
Minimum OS build version	—	21A559	Deviated
Maximum OS build version	—	—	Deviated
Require a password to unlo...	—	Required	Deviated
Simple passwords	Allowed	Block	Deviated
Minimum password length	—	8	Deviated
Password type	—	alphanumeric	Deviated
Number of non-alphanume...	—	1	Deviated
Maximum minutes of inacti...	Not configured	15 minutes	Deviated
Password expiration (days)	—	365	Deviated
Number of previous passwo...	—	5	Deviated

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

