

Acronis

Ataques de identidade e do plano de controle no Microsoft 365

Nove ameaças reais, seus alvos e como os MSPs podem reduzir o risco com o Acronis SPM



Os ataques modernos ao Microsoft 365 têm se direcionado cada vez mais ao plano de controle — identidades, aplicativos OAuth, permissões, sessões e configurações — em vez de endpoints.

Recentemente, em incidentes reais, os invasores usaram fluxos de autenticação legítimos, permissões excessivas, controles de acesso fracos e configurações incorretas para conseguir acesso permanente a locatários do Microsoft 365.

Esta lista de verificação resume:

- as técnicas de ataque usadas em incidentes reais;
- o que os invasores exploraram;
- os controles do Microsoft 365 recomendados para reduzir o risco;
- como o Acronis SPM ajuda os MSPs a monitorar continuamente e aplicar uma postura segura em todos os locatários.



1. Ataques de password spraying



Incidente real
Midnight Blizzard (2024).



Técnica de ataque
Ataque de password spraying contra uma conta de locatário legada e de não produção.



O que foi explorado

- Credenciais fracas
- Ausência de MFA em uma conta legada



Controles de segurança para reduzir o risco

- Aplicação de MFA
- Eliminação de senhas fracas
- Desativação de processos legados de autenticação
- Monitoramento de anomalias de login



Como o Acronis SPM ajuda

- Identifica lacunas de MFA
- Detecta configurações inseguras de autenticação
- Monitora desvios da referência entre locatários
- Orienta os MSPs a corrigir configurações fracas de identidade antes que elas se tornem caminhos de ataque

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

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. Falsificação de token e abuso de sessão



Incidente real
Storm-0558 (2023).



Técnica de ataque
Tokens de autenticação falsificados usados para acessar contas de e-mail na nuvem.



O que foi explorado

- Vulnerabilidades na validação de tokens
- Abuso de chaves de assinatura
- Visibilidade limitada do uso anômalo de tokens



Controles de segurança para reduzir o risco

- Fortificação da postura de identidade
- Aplicação de MFA e do acesso condicional
- Restrição do consentimento de aplicativos
- Proteção do acesso privilegiado
- Monitoramento de anomalias de tokens e sessões



Como o Acronis SPM ajuda

- Padroniza a postura de MFA e acesso condicional
- Identifica desvios na configuração de identidade
- Possibilita a aplicação de referências seguras de acesso de administrador
- Reduz a exposição adjacente à identidade do locatário

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

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: Deviased

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. Sequestro de sessão e phishing AiTM



Incidente real

Vários incidentes reais.



Técnica de ataque

Roubo de cookies de sessão por meio de phishing com proxy reverso.



O que foi explorado

- Cookies de sessão autenticados roubados
- Aplicação fraca do acesso condicional
- Falta de restrições de acesso por dispositivo



Controles de segurança para reduzir o risco

- Exigência de dispositivos compatíveis ou gerenciados
- Aplicação do acesso condicional
- Monitoração do comportamento anômalo da sessão
- Uso da avaliação contínua de acesso quando disponível



Como o Acronis SPM ajuda

- Detecta desvios na postura de acesso condicional
- Ajuda a manter as referências da política de acesso seguro
- Possibilita a padronização dos controles de identidade e acesso ao dispositivo entre locatários

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

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

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. Ataques de replay de token



Incidente real
Vários incidentes reais.



Técnica de ataque
Reutilização de tokens de atualização primária roubados.



O que foi explorado

- Falta de proteção de token/sessão
- Aplicação fraca da sessão



Controles de segurança para reduzir o risco

- Aplicação da proteção de token quando permitida
- Uso de controles de sessão do acesso condicional
- Restrição do acesso de dispositivos não gerenciados



Como o Acronis SPM ajuda

- Orienta os MSPs a monitorar continuamente a postura de autenticação
- Detecta desvios da referência do acesso condicional e da configuração da sessão
- Possibilita a aplicação de referências seguras de identidade e acesso

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

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 de consentimento OAuth



Incidente real

Vários incidentes reais.



Técnica de ataque

Concessões maliciosas de consentimento de aplicativo.



O que foi explorado

- Consentimento irrestrito do usuário
- Governança fraca de aplicativos



Controles de segurança para reduzir o risco

- Restrição do consentimento do usuário
- Exigência de aprovação para aplicativos pelo administrador
- Autorização apenas de editores verificados e permissões de baixo risco



Como o Acronis SPM ajuda

- Padroniza controles relacionados à autorização
- Detecta desvios das políticas de consentimento de aplicativo aprovadas
- Orienta os MSPs a manter uma postura segura de autorização do Microsoft 365 entre locatários

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 de aplicativo OAuth e exfiltração de dados da API Graph



Incidente real

Vários incidentes reais.



Técnica de ataque

Acesso e exfiltração de dados por API com uso de aplicativos com permissões excessivas



O que foi explorado

- Permissões excessivas do Graph
- Pouca visibilidade do comportamento do aplicativo
- Acesso a aplicativos não gerenciados



Controles de segurança para reduzir o risco

- Auditoria regular das permissões dos aplicativos
- Investigação de atividades incomuns do Graph
- Revisão de aplicativos autorizados por usuários externos



Como o Acronis SPM ajuda

- Mantém a governança sobre permissões de aplicativos e postura de consentimento
- Detecta desvios de autorização e exposição de aplicativos não gerenciados
- Melhora a visibilidade da postura de acesso a aplicativos do Microsoft 365

The screenshot displays the Acronis Cyber Protect Cloud interface. The left sidebar contains navigation options: SK Partner, Manage, All customers, MONITORING, DEVICES, MICROSOFT 365 MANAGEMENT, Configuration, Security posture (selected), Baseline templates, Baselines, Users, MANAGEMENT, SOFTWARE MANAGEMENT, PROTECTION, and SETTINGS.

The main content area is divided into two panels:

- Security posture:** Shows 1 tenant and 35 tenant baseline deviations. A table lists tenants with columns for Name, Tenant baselines, and Users. The tenant 'Contoso' is highlighted, showing 35 deviations and 34 users.
- Risk dashboard:** Provides a summary of baseline and user account risks.

Baselines		
Tenant baselines	8 passed	35 deviated

Baseline categories		
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	
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. Escalada de privilégios e abuso excessivo de funções



Incidente real

Várias escaladas de privilégios no Entra ID/ Midnight Blizzard.



Controles de segurança para reduzir o risco

- Aplicação do menor privilégio
- Restrição do acesso administrativo permanente
- Revisão contínua das funções privilegiadas



Técnica de ataque

Escalada de privilégios por meio de privilégios administrativos permanentes excessivos.



Como o Acronis SPM ajuda

- Identifica funções administrativas excessivas e exposição de privilégios
- Orienta os MSPs a padronizar uma postura segura de funções em todos os locatários
- Possibilita a aplicação de referências de identidade e autorização



O que foi explorado

- Excesso de administradores globais
- Crescimento excessivo de privilégios
- Governança fraca de funções

Compliance Posture Summary

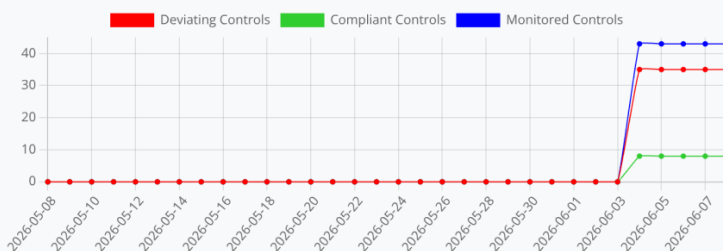
Baselines

Current Posture Summary (All time)

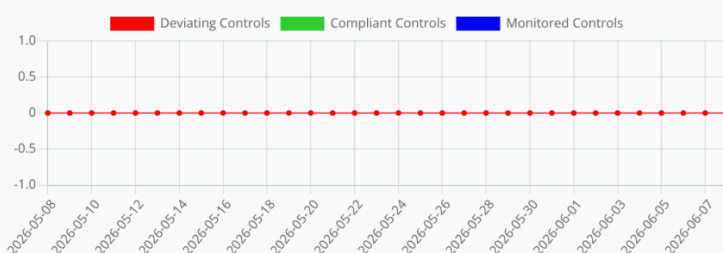
Tenant	Group
Passing: 8	Passing: -
Deviating: 35	Deviating: -

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. Exposição do SharePoint e do OneDrive



Incidente real
Vários incidentes reais.



Técnica de ataque
Compartilhamento externo excessivo ou acidental.



O que foi explorado

- Governança fraca de compartilhamento
- Configurações de acesso externo excessivamente permissivas



Controles de segurança para reduzir o risco

- Configuração de políticas de compartilhamento externo no nível da organização
- Restrição do compartilhamento quando necessário
- Revisão regular da postura de compartilhamento



Como o Acronis SPM ajuda

- Valida continuamente a postura de compartilhamento em relação às referências
- Detecta configurações de compartilhamento arriscadas
- Reduz o desvio de configuração de longo prazo entre locatários

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

O que esses ataques têm em comum

Em todos os incidentes:

- a entrada é por identidade;
- a persistência é por configuração;
- o impacto abrange todo o locatário;
- os controles tradicionais de endpoint oferecem visibilidade limitada.

Por que o gerenciamento contínuo de postura é importante

Os ataques modernos ao Microsoft 365 são bem-sucedidos quando:

- as configurações incorretas continuam;
- a postura de segurança se desvia com o tempo;
- os locatários seguem sem perceber as lacunas de visibilidade.

Como o Acronis SPM ajuda os MSPs a reduzir riscos

- Gerencia centralmente a postura do Microsoft 365 entre os locatários
- Monitora continuamente a postura de segurança em relação às referências
- Detecta automaticamente novos riscos e desvios de configuração
- Aplica modelos de referência reutilizáveis
- Automatiza e simplifica a remediação
- Simplifica os fluxos de trabalho de integração e desligamento
- Padroniza a postura de segurança do Microsoft 365 em grande escala

Saiba como o Acronis SPM ajuda os MSPs a proteger o Microsoft 365 em grande escala

Leia o código para agendar uma demonstração do Acronis SPM

