

Acronis

Attaques contre l'identité et le plan de contrôle dans Microsoft 365

9 menaces concrètes, ce qu'elles exploitent et comment les MSP peuvent réduire les risques avec Acronis SPM



Les attaques actuelles contre Microsoft 365 ciblent davantage le plan de contrôle, les identités, applications OAuth, autorisations, sessions et configurations, que les terminaux.

Lors d'incidents récents constatés, les attaquants ont utilisé des flux d'authentification légitimes, des autorisations excessives, des contrôles d'accès insuffisants et des erreurs de configuration pour obtenir un accès persistant aux tenants Microsoft 365.

Cette liste de vérification fait le point sur :

- Les techniques d'attaque utilisées dans des incidents constatés.
- Ce que les attaquants ont exploité.
- Les contrôles Microsoft 365 recommandés pour réduire les risques.
- Comment Acronis SPM aide les MSP à surveiller et à appliquer une posture de sécurité renforcée sur l'ensemble des tenants.



1. Attaques par pulvérisation de mot de passe



Incident constaté
Midnight Blizzard (2024).



Technique d'attaque
Attaque par pulvérisation de mot de passe contre un compte tenant hérité hors production.



Ressources affectées

- Identifiants faibles.
- Absence d'authentification multifacteur sur un compte hérité.



Mesures de sécurité pour réduire le risque

- Imposer l'authentification multifacteur.
- Éliminer les mots de passe faibles.
- Désactiver les anciens chemins d'authentification.
- Surveiller les anomalies de connexion.



Comment Acronis SPM vous accompagne

- Identifie les lacunes d'authentification multifacteur.
- Détecte les paramètres d'authentification non sécurisés.
- Surveille les écarts vis-à-vis de la base de référence sur l'ensemble des tenants.
- Aide les MSP à corriger les failles de sécurité liées à l'identité des configurations avant qu'elles ne deviennent des voies d'attaque.

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
☐	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. Falsification de jetons et abus de session



Incident constaté

Storm-0558 (2023).



Technique d'attaque

Des jetons d'authentification falsifiés ont été utilisés pour accéder à des comptes e-mail cloud.



Ressources affectées

- Faiblesses de validation des jetons.
- Abus de la clé de signature.
- Visibilité limitée sur l'utilisation anormale des jetons.



Mesures de sécurité pour réduire le risque

- Renforcer la posture de sécurité de l'identité.
- Imposer l'authentification multifacteur et l'accès conditionnel.
- Restreindre le consentement d'accès aux applis.
- Protéger l'accès privilégié.
- Surveiller les anomalies de jetons et de session.



Comment Acronis SPM vous accompagne

- Aide à standardiser le niveau de sécurité de l'authentification multifacteur et de l'accès conditionnel.
- Identifie les dérives de configuration de l'identité.
- Prend en charge l'application de bases de référence pour un accès administrateur sécurisé.
- Réduit l'exposition adjacente des identités côté tenant.

Acronis
Cyber Protect Cloud

SK Partner

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	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. Détournement de session et phishing AiTM



Incident constaté
Plusieurs incidents réels.



Technique d'attaque
Vol de cookies de session via phishing par proxy inverse.



Ressources affectées

- Vol de cookies de session authentifiés.
- Application faible de l'accès conditionnel.
- Absence de restrictions d'accès basées sur le terminal.



Mesures de sécurité pour réduire le risque

- Exiger des terminaux conformes ou managés
- Appliquer l'accès conditionnel.
- Surveiller les comportements de session anormaux.
- Utiliser l'évaluation continue de l'accès si possible.



Comment Acronis SPM vous accompagne

- Détecte les écarts dans la posture d'accès conditionnel.
- Aide à maintenir des bases de référence d'accès sécurisé.
- Prend en charge la standardisation des contrôles d'identité et d'accès aux terminaux sur l'ensemble des tenants.

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 - 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,compil...	Deviated
Include Platforms	---	android,iOS	Deviated
Client App Types	---	all	Deviated

4. Attaques par rejeu de jeton



Incident constaté
Plusieurs incidents réels.



Technique d'attaque
Réutilisation de jetons récemment réactualisés.



Ressources affectées

- Absence de protection des jetons / de la session.
- Faible application en cours de session.



Mesures de sécurité pour réduire le risque

- Appliquer la protection des jetons, si possible.
- Utiliser les contrôles de session de l'accès conditionnel.
- Limiter l'accès depuis des équipements non managés



Comment Acronis SPM vous accompagne

- Aide les MSP à surveiller la posture d'authentification en continu.
- Détecte les écarts vis-à-vis de la base de référence concernant l'accès conditionnel et la configuration de la session.
- Prend en charge l'application des bases de référence sécurisées pour l'identité et l'accès.

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 de consentement OAuth



Incident constaté
Plusieurs incidents réels.



Technique d'attaque
Accords de consentement applicatif malveillants.



Ressources affectées

- Consentement utilisateur non restreint.
- Gouvernance insuffisante des applications.



Mesures de sécurité pour réduire le risque

- Restreindre le consentement utilisateur.
- Exiger une approbation administrateur pour les applications.
- N'autoriser que les éditeurs vérifiés et les autorisations à faible risque.



Comment Acronis SPM vous accompagne

- Standardise les contrôles liés à l'autorisation.
- Détecte les écarts par rapport aux stratégies de consentement applicatif approuvées.
- Aide les MSP à maintenir une posture d'autorisation Microsoft 365 sécurisée sur l'ensemble des tenants.

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: Deviased

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. Abus d'appli OAuth et exfiltration de données via l'API Graph



Incident constaté

Plusieurs incidents réels.



Technique d'attaque

Accès aux données et exfiltration via l'API au moyen d'applications surautorisées.



Ressources affectées

- Autorisations Graph excessives.
- Faible visibilité sur le comportement des applis.
- Accès non managé aux applications.



Mesures de sécurité pour réduire le risque

- Auditer régulièrement les autorisations liées aux applications.
- Enquêter sur les activités Graph inhabituelles.
- Examiner les applis autorisées par des utilisateurs externes.



Comment Acronis SPM vous accompagne

- Aide à maintenir la gouvernance des autorisations des applications et de l'état du consentement.
- Détecte les dérives d'autorisation et l'exposition des applications non gérées.
- Améliore la visibilité sur l'état d'accès des applications 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 and their associated users.

Name	Tenant baselines	Users
Contoso	35 deviations	34
- 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. Élévation de privilèges et usage excessif des rôles



Incident constaté

Multiples élévations de privilèges Entra ID / Midnight Blizzard.



Mesures de sécurité pour réduire le risque

- Appliquer le principe du moindre privilège.
- Restreindre l'accès administrateur permanent.
- Examiner continuellement les rôles à privilèges.



Technique d'attaque

Élévation de privilèges via des privilèges d'administrateur excessifs et permanents.



Comment Acronis SPM vous accompagne

- Identifie les rôles administrateurs excessifs et l'exposition aux privilèges.
- Aide les MSP à standardiser un état de sécurité des rôles sur l'ensemble des tenants.
- Soutient l'application des lignes de base d'identité et d'autorisation.



Ressources affectées

- Trop d'administrateurs globaux.
- Dérive des privilèges.
- Faible gouvernance des rôles.

Compliance Posture Summary

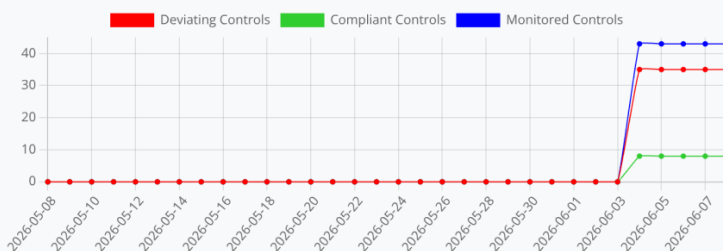
Baselines

Current Posture Summary (All time)

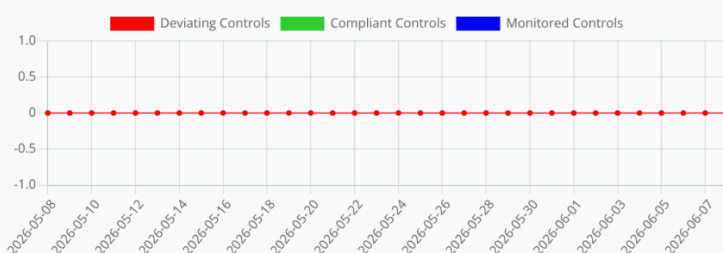
Tenant	Group
Passing: 8	Passing: -
Deviating: 35	Deviating: -

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. Exposition de SharePoint et OneDrive



Incident constaté

Plusieurs incidents réels.



Technique d'attaque

Partage externe excessif ou accidentel.



Ressources affectées

- Faible gouvernance du partage.
- Paramètres d'accès externe trop permissifs.



Mesures de sécurité pour réduire le risque

- Configurer les stratégies de partage externe dans toute l'organisation.
- Restreindre le partage si nécessaire.
- Examiner régulièrement l'état du partage.



Comment Acronis SPM vous accompagne

- Valide en continu l'état du partage par rapport aux lignes de base.
- Détecte les configurations de partage à risque.
- Réduit la dérive de configuration à long terme entre les tenants.

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. Lacunes d'audit et d'investigation



Incident constaté
Investigation sur incidents



Technique d'attaque
Activité post-compromission masquée par un audit insuffisant.



Ressources affectées

- Preuves d'audit absentes ou incomplètes.
- Insuffisance de préparation à l'investigation.



Mesures de sécurité pour réduire le risque

- Conserver l'activation de l'audit Microsoft Purview.
- S'assurer que les enquêteurs disposent d'un accès approprié.
- Maintenir la capacité de recherche dans les audits.



Comment Acronis SPM vous accompagne

- Aide les MSP à surveiller l'état de configuration lié à l'audit.
- Détecte les dérives dans les paramètres de journalisation et d'audit.
- Soutient l'investigation continue et la préparation à la conformité.

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

Ce que ces attaques ont en commun

Pour tous les incidents :

- L'entrée est basée sur l'identité.
- La persistance est basée sur la configuration.
- L'impact s'étend à l'ensemble du tenant.
- Les contrôles traditionnels des terminaux offrent une visibilité limitée.

Pourquoi la gestion continue de la posture de sécurité est décisive

Les attaques actuelles contre Microsoft 365 réussissent lorsque :

- Les erreurs de configuration persistent.
- La posture de sécurité se dégrade au fil du temps.
- Les écarts de visibilité passent inaperçus d'un tenant à l'autre.

Comment Acronis SPM aide les MSP à réduire les risques

- Gérez la posture de Microsoft 365 de manière centralisée sur l'ensemble des tenants.
- Surveillez continuellement la posture de sécurité par rapport aux bases de référence.
- Détectez automatiquement les nouveaux risques et les dérives de configuration.
- Appliquez des modèles de base réutilisables.
- Automatisez et rationalisez la remédiation.
- Simplifiez les workflows d'intégration et de désactivation.
- Standardisez la posture de sécurité Microsoft 365 à grande échelle.

Découvrez comment Acronis SPM aide les MSP à sécuriser Microsoft 365 à grande échelle

Scannez pour réserver une démonstration d'Acronis SPM

