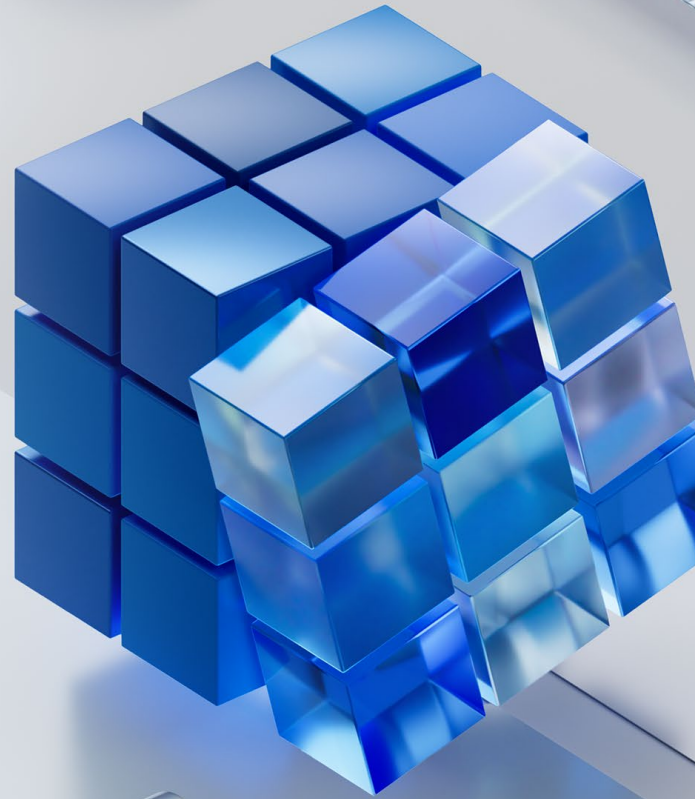


Acronis

Microsoft 365 identity and control-plane attacks

9 real-world threats, what they exploit
and how MSPs can reduce risk with
Acronis SPM



Modern Microsoft 365 attacks increasingly target the control plane — identities, OAuth applications, permissions, sessions, and configurations — rather than endpoints.

Across recent real-world incidents, attackers used legitimate authentication flows, excessive permissions, weak access controls, and misconfigurations to gain persistent access to Microsoft 365 tenants.

This checklist summarizes:

- The attack techniques used in real incidents.
- What attackers exploited.
- The Microsoft 365 controls recommended to reduce risk.
- How Acronis SPM helps MSPs continuously monitor and enforce secure posture across tenants.



1. Password spraying attacks



Real-world incident

Midnight Blizzard (2024).



Attack technique

Password spray attack against a legacy non-production tenant account.



What was exploited

- Weak credentials.
- No MFA on a legacy account.



Security controls to reduce risk

- Enforce MFA.
- Eliminate weak passwords.
- Disable legacy authentication paths.
- Monitor sign-in anomalies.



How Acronis SPM helps

- Identifies MFA gaps.
- Detects insecure authentication settings.
- Monitors baseline deviations across tenants.
- Helps MSPs remediate weak identity configurations before they become attack paths.

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
<input type="checkbox"/>	Audit Mailbox Audit Log	Passed
<input type="checkbox"/>	Authentication & Authorisation Admin Consent Workflow	Deviated
<input type="checkbox"/>	Authentication & Authorisation Authentication Method Policy - Email OTP	Deviated
<input checked="" type="checkbox"/>	Authentication & Authorisation Authentication Method Policy - Microsoft Authenticator	Deviated
<input type="checkbox"/>	Authentication & Authorisation Conditional Access Policy - Application Enforced Restrictions For Unmanaged D...	Deviated
<input type="checkbox"/>	Authentication & Authorisation Conditional Access Policy - Block Legacy Authentication	Deviated
<input type="checkbox"/>	Authentication & Authorisation Conditional Access Policy - Block Unknown Or Unsupported Device Access	Deviated
<input type="checkbox"/>	Authentication & Authorisation Conditional Access Policy - Enforce MFA	Deviated
<input type="checkbox"/>	Authentication & Authorisation Conditional Access Policy - No persistent browser sessions	Deviated
<input type="checkbox"/>	Authentication & Authorisation Conditional Access Policy - Require Approved Client Apps	Deviated
<input type="checkbox"/>	Authentication & Authorisation Conditional Access Policy - Require Compliant Or Hybrid Azure AD joined Device.	Deviated
<input type="checkbox"/>	Authentication & Authorisation Conditional Access Policy - Restrict Access To Azure Portal	Deviated
<input type="checkbox"/>	Authentication & Authorisation Conditional Access Policy - Restrict Access To Microsoft Admin Portal	Deviated
<input type="checkbox"/>	Authentication & Authorisation Conditional Access Policy - Securing Security Info Registration	Deviated
<input type="checkbox"/>	Authentication & Authorisation Conditional Access Policy - Sign-In Risk Based Multifactor Authentication.	Deviated
<input type="checkbox"/>	Authentication & Authorisation Customer Lockbox	Deviated
<input type="checkbox"/>	Authentication & Authorisation Password Policy	Deviated
<input type="checkbox"/>	Authentication & Authorisation SharePoint Modern Auth Enforced	Deviated
<input type="checkbox"/>	Authentication & Authorisation User Consent Settings	Deviated
<input type="checkbox"/>	Email Security Automatic Forwarding - Block	Deviated
<input type="checkbox"/>	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 app) appear in authentication prompts. [Learn more](#)

Tenant: Contoso

Auto-remediation: Disabled

Status: Deviased

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 - Ek...	--	--	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. Token forgery and session abuse



Real-world incident

Storm-0558 (2023).



Attack technique

Forged authentication tokens used to access cloud email accounts.



What was exploited

- Token-validation weaknesses.
- Signing-key abuse.
- Limited visibility into anomalous token usage.



Security controls to reduce risk

- Harden identity posture.
- Enforce MFA and Conditional Access.
- Restrict app consent.
- Protect privileged access.
- Monitor token and session anomalies.



How Acronis SPM helps

- Helps standardize MFA and Conditional Access posture.
- Identifies identity configuration drift.
- Supports enforcement of secure admin-access baselines.
- Reduces adjacent tenant-side identity exposure.

The screenshot displays the Acronis Cyber Protect Cloud interface. On the left is a navigation sidebar with categories like MONITORING, DEVICES, MICROSOFT 365 MANAGEMENT, Users, Baseline templates, Security posture, Configuration, MANAGEMENT, SOFTWARE MANAGEMENT, PROTECTION, and SETTINGS. The main area is titled 'Baselines' and shows a list of baselines for a customer named 'Contoso'. The list includes various categories like Audit, Authentication & Authorisation, and Email Security, with their respective status (Passed or Deviated). A 'Baseline details' window is open on the right, showing details for a 'Conditional Access Policy - Application Enforced Restrictions For Unmanaged Devices'. This window includes a description, tenant information, auto-remediation status, and a table of policy settings.

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. Session hijacking and AiTM phishing



Real-world incident

Multiple real-world incidents.



Attack technique

Session cookie theft through reverse-proxy phishing.



What was exploited

- Stolen authenticated session cookies.
- Weak Conditional Access enforcement.
- Lack of device-based access restrictions.



Security controls to reduce risk

- Require compliant or managed devices
- Enforce Conditional Access.
- Monitor anomalous session behavior.
- Use Continuous Access Evaluation where available.



How Acronis SPM helps

- Detects drift in Conditional Access posture.
- Helps maintain secure access-policy baselines.
- Supports standardization of identity and device-access controls across tenants.

The screenshot displays the Acronis Cyber Protect Cloud interface. On the left is a navigation sidebar with categories like MONITORING, DEVICES, MICROSOFT 365 MANAGEMENT, Users, Baseline templates, Security posture, Configuration, MANAGEMENT, SOFTWARE MANAGEMENT, PROTECTION, and SETTINGS. The main area is titled 'Baselines' and shows a table of various security baselines for a customer named 'Contoso'. The table has columns for Category, Baseline, and Status. One baseline, 'Conditional Access Policy - Require Approved Client Apps', is highlighted. To the right, a 'Baseline details' window is open, showing the configuration for this specific policy. It includes a description, tenant information, and a table of policy settings.

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. Token replay attacks



Real-world incident

Multiple real-world incidents.



Attack technique

Reuse of stolen Primary Refresh Tokens.



What was exploited

- Lack of token / session protection.
- Weak session enforcement.



Security controls to reduce risk

- Enforce Token Protection where supported.
- Use Conditional Access session controls.
- Restrict access from unmanaged devices.



How Acronis SPM helps

- Helps MSPs continuously monitor authentication posture.
- Detects baseline drift around Conditional Access and session configuration.
- Supports enforcement of secure identity and access baselines.

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. OAuth consent phishing



Real-world incident

Multiple real-world incidents.



Attack technique

Malicious application consent grants.



What was exploited

- Unrestricted user consent.
- Weak application governance.



Security controls to reduce risk

- Restrict user consent.
- Require admin approval for applications.
- Allow only verified publishers and low-risk permissions.



How Acronis SPM helps

- Standardizes authorization-related controls.
- Detects drift from approved application-consent policies.
- Helps MSPs maintain secure Microsoft 365 authorization posture across tenants.

Baselines

Customer: Contoso Category: All Apply

Search

Category	Baseline	Status
<input type="checkbox"/>	Audit	Mailbox Audit Log ● Passed
<input type="checkbox"/>	Authentication & Authorisation	Admin Consent Workflow ● Deviated
<input type="checkbox"/>	Authentication & Authorisation	Authentication Method Policy - Email OTP ● Deviated
<input type="checkbox"/>	Authentication & Authorisation	Authentication Method Policy - Microsoft Authenticator ● Deviated
<input type="checkbox"/>	Authentication & Authorisation	Conditional Access Policy - Application Enforced Restrictions For Unmanaged D... ● Deviated
<input type="checkbox"/>	Authentication & Authorisation	Conditional Access Policy - Block Legacy Authentication ● Deviated
<input type="checkbox"/>	Authentication & Authorisation	Conditional Access Policy - Block Unknown Or Unsupported Device Access ● Deviated
<input type="checkbox"/>	Authentication & Authorisation	Conditional Access Policy - enforce MFA ● Deviated
<input type="checkbox"/>	Authentication & Authorisation	Conditional Access Policy - No persistent Browser Sessions ● Deviated
<input type="checkbox"/>	Authentication & Authorisation	Conditional Access Policy - Require Approved Client Apps ● Deviated
<input type="checkbox"/>	Authentication & Authorisation	Conditional Access Policy - Require Compliant (Or Hybrid Azure AD) joined Device. ● Deviated
<input type="checkbox"/>	Authentication & Authorisation	Conditional Access Policy - Restrict Access To Azure Portal ● Deviated
<input type="checkbox"/>	Authentication & Authorisation	Conditional Access Policy - Restrict Access To Microsoft Admin Portal ● Deviated
<input type="checkbox"/>	Authentication & Authorisation	Conditional Access Policy - Securing Security Info Registration ● Deviated
<input type="checkbox"/>	Authentication & Authorisation	Conditional Access Policy - Sign-In Risk-Based Multifactor Authentication. ● Deviated
<input type="checkbox"/>	Authentication & Authorisation	Customer Lockbox ● Deviated
<input type="checkbox"/>	Authentication & Authorisation	Password Policy ● Deviated
<input type="checkbox"/>	Authentication & Authorisation	SharePoint Modern Auth Enforced ● Deviated
<input type="checkbox"/>	Authentication & Authorisation	User Consent Settings ● Deviated
<input type="checkbox"/>	Email Security	Automatic Forwarding - Block ● Deviated
<input type="checkbox"/>	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	---	CA004 - 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,windo...	● Deviated
Grant Controls	---	block	● Deviated

6. OAuth app abuse and Graph API data exfiltration



Real-world incident

Multiple real-world incidents.



Attack technique

API-based data access and exfiltration through over-permissioned applications.



What was exploited

- Excessive Graph permissions.
- Poor visibility into app behavior.
- Unmanaged application access.



Security controls to reduce risk

- Audit application permissions regularly.
- Investigate unusual Graph activity.
- Review apps authorized by external users.



How Acronis SPM helps

- Helps maintain governance over app permissions and consent posture.
- Detects authorization drift and unmanaged app exposure.

The screenshot displays the Acronis Cyber Protect Cloud interface. The main section is titled "Security posture" and shows a table of tenant baselines. The table has columns for Name, Tenant baselines, and Users. The row for "Contoso" shows 35 deviations and 34 users.

Name	Tenant baselines	Users
Contoso	35 deviations	34

The right-hand side of the interface shows a "Risk dashboard" with the following data:

Baselines

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

Baseline categories

Audit	1 passed	0 deviated
Authentication & Authorization	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. Privilege escalation and excessive role abuse



Real-world incident

Multiple Entra ID Privilege Escalations / Midnight Blizzard.



Security controls to reduce risk

- Apply least privilege.
- Restrict standing admin access.
- Review privileged roles continuously.



Attack technique

Privilege escalation through excessive standing admin privileges.



How Acronis SPM helps

- Identifies excessive admin roles and privilege exposure.
- Helps MSPs standardize secure role posture across tenants.
- Supports enforcement of identity and authorization baselines.



What was exploited

- Too many Global Admins.
- Privilege creep.
- Weak role governance.

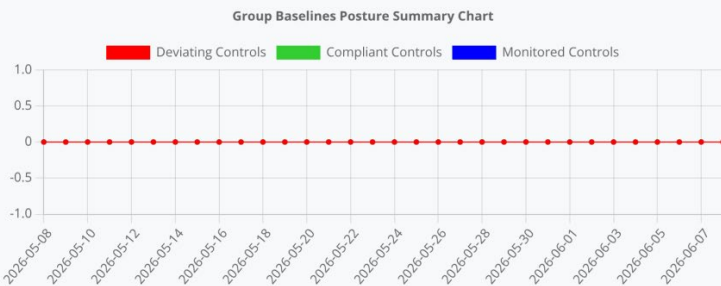
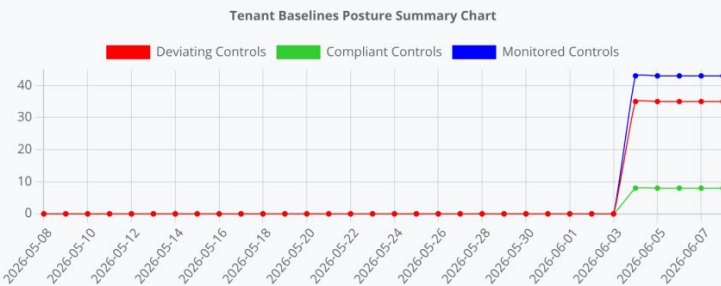
Compliance Posture Summary

Baselines

Current Posture Summary (All time)

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

Posture Summary (In this period) *



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

8. SharePoint and OneDrive exposure



Real-world incident

Multiple real-world incidents.



Attack technique

Excessive or accidental external sharing.



What was exploited

- Weak sharing governance.
- Overly permissive external access settings.



Security controls to reduce risk

- Configure organization-level external sharing policies.
- Restrict sharing where required.
- Review sharing posture regularly.



How Acronis SPM helps

- Continuously validates sharing posture against baselines.
- Detects risky sharing configurations.
- Reduces long-term configuration drift across 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

Category	Policy Name	Status
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. Audit and investigation gaps



Real-world incident

Incident Investigations.



Attack technique

Post-compromise activity hidden by insufficient auditing.



What was exploited

- Missing or incomplete audit evidence.
- Weak investigation readiness.



Security controls to reduce risk

- Keep Microsoft Purview auditing enabled.
- Ensure investigators have appropriate access.
- Maintain audit-search readiness.



How Acronis SPM helps

- Helps MSPs monitor audit-related configuration posture.
- Detects drift in logging and audit settings.
- Supports ongoing investigation and compliance readiness.

The screenshot displays the Acronis Cyber Protect Cloud interface. On the left is a navigation sidebar with categories like MONITORING, DEVICES, MICROSOFT 365 MANAGEMENT, USERS, MANAGEMENT, SOFTWARE MANAGEMENT, PROTECTION, and SETTINGS. The main area is divided into two panes. The left pane, titled 'Baselines', shows a list of various security policies with their current status (e.g., Deviated, Passed). The right pane, titled 'Baseline details', provides a detailed view of the 'MAC OS - Compliance Policy', including its tenant, auto-remediation status, and a table of specific policy requirements and their current values.

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 inactl...	Not configured	15 minutes	Deviated
Password expiration (days)	--	365	Deviated
Number of previous passwo...	--	5	Deviated

What these attacks have in common

Across all incidents:

- Entry is identity-based.
- Persistence is configuration-based.
- Impact is tenant-wide.

Why continuous posture management matters

Modern Microsoft 365 attacks succeed when:

- Misconfigurations persist.
- Security posture drifts over time.
- Visibility gaps remain unnoticed across tenants.

How Acronis SPM helps MSPs reduce risk

- Centrally manage Microsoft 365 posture across tenants.
- Continuously monitor security posture against baselines.
- Detect new risks and configuration drift automatically.
- Apply reusable baseline templates.
- Automate and streamline remediation.
- Simplify onboarding and offboarding workflows.
- Standardize Microsoft 365 security posture at scale.

Explore how Acronis SPM helps MSPs secure Microsoft 365 at scale

Scan to book an Acronis SPM demo

