Acronis

Microsoft 365 under attack: Identity and control plane threats



And how Acronis Security Posture Management exposes and remediates them

Introduction

Microsoft 365 has become the control plane of modern business operations, managing identity, access, communication and data across organizations. As its importance has grown, so has its value as a primary attack surface.



But the nature of attacks has fundamentally changed.

Today's threats no longer rely on malware or endpoint compromise. Instead, attackers exploit identities, permissions and misconfigurations, operating entirely within legitimate Microsoft 365 services. A single compromised admin account, an overlooked permission or a weak conditional access policy can provide attackers with persistent, high impact access without triggering traditional security alerts.

This shift creates a critical challenge for managed service providers (MSPs). Traditional security tools often provide little visibility into these attacks, while misconfigurations and inconsistent policies across tenants create persistent exposure.

The results: Risk accumulates silently across tenants.

This guide provides a practical, scenario-based walkthrough of how modern Microsoft 365 attacks unfold, and how Acronis Security Posture Management (SPM) helps MSPs detect, prevent and remediate these risks at scale.

The new reality: You're already in the attack

You log into a customer tenant. There are no alerts, no malware and no obvious signs of compromise. Everything appears normal on the surface, but that doesn't mean the environment is secure.

An attacker may already have access. They could be using valid credentials or persistent tokens obtained through phishing or consent abuse. More importantly, they may be operating entirely within Microsoft 365, blending into legitimate activity and avoiding traditional detection mechanisms.

Modern attacks don't rely on breaking in — they operate within the control plane.

For MSPs, this fundamentally changes the problem. It's no longer just about detecting active threats: It's about identifying exposure before it's exploited, remediating it consistently across all tenants, and ensuring those fixes remain enforced over time as environments evolve.

This walkthrough shows how that challenge is addressed in practice using Acronis Security Posture Management (SPM).

Scenario 1

Password spraying

“Nothing looks wrong, but one account just got in.”

Attackers don’t need to break in — they log in. By testing common passwords across many accounts, they avoid lockouts and eventually gain access to one. With valid credentials, they can access mailboxes and files, and operate as a legitimate user.

There are typically no alerts, no malware and no clear signals — just normal-looking activity.

Acronis SPM shifts the focus from detection to exposure. It highlights risks like missing MFA, enabled legacy authentication and identity configurations that deviate from best practices.

From there, you assess the tenant, enforce MFA, disable legacy authentication and apply these controls across all tenants using baseline templates. Continuous monitoring ensures any drift is detected and corrected.

Instead of chasing a compromised account, you eliminate the conditions that made the attack possible.



What you do (in platform)

1 **Run an on-demand audit**

- Instantly assess tenant against security baseline.
- Identify authentication weaknesses.

2 **Apply baseline remediation**

- Enforce MFA across users.
- Disable legacy authentication.

3 **Automate that across tenants**

- Use baseline templates.
- Propagate policies across all customers.

4 **Enable continuous monitoring**

- Acronis SPM continuously detects drift from baseline.
- Alerts when new users are created without protection.

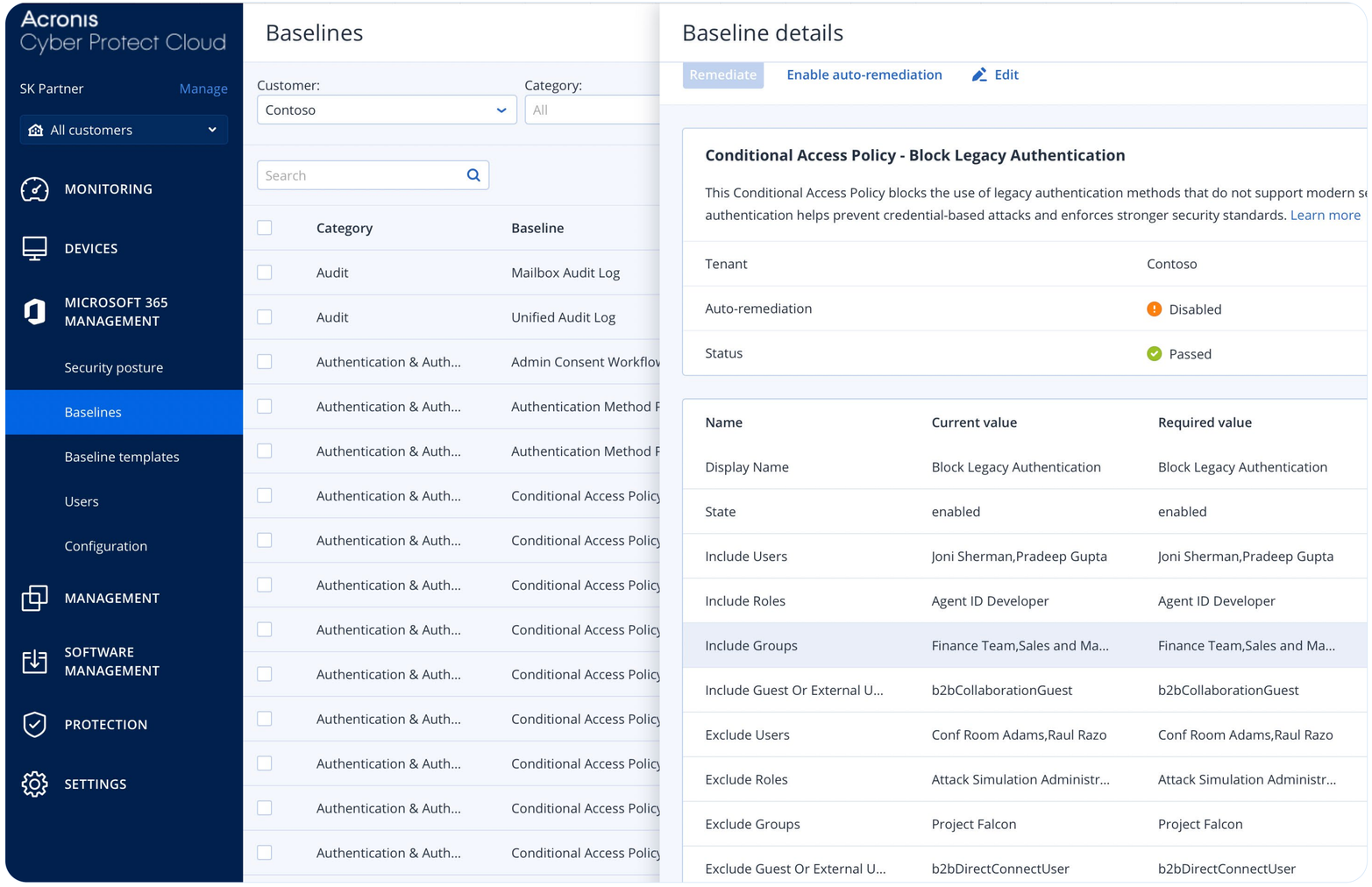
What just happened?

You didn’t chase a login.

You:

- Identified systemic identity gaps.
- Fixed them once.
- Enforced them everywhere.
- Ensured they don’t return.

Acronis SPM eliminates the conditions that make password spraying successful at scale.



Scenario 2

OAuth consent abuse

“The attacker doesn’t need the user anymore.”

A user unknowingly approves a malicious OAuth app. From that moment, the attacker no longer needs credentials. They gain persistent, API-level access to email and files via Microsoft Graph — often without triggering any alerts.

There’s no compromised login, no suspicious sign-in activity and everything appears legitimate.

Acronis SPM exposes this hidden layer. It provides visibility into all OAuth apps across tenants, the permissions they’ve been granted, such as Mail.Read or Files.Read.All, and highlights risky or unknown applications.

From there, you can quickly identify high-privilege or newly added apps, revoke their permissions and remove unauthorized access. Policies can then be standardized, restricting user consent and requiring admin approval, while automation ensures these controls are enforced across all tenants.

Instead of chasing identity-based threats, you uncover and eliminate persistent access at the application layer and prevent it from coming back.



What you do (in platform)

1 **Identify risky applications**

- Filter by high-permission apps.
- Detect newly added or unknown apps.

2 **Remediate immediately**

- Revoke app permissions directly.
- Remove unauthorized integrations.

3 **Standardize policy**

- Restrict user consent.
- Require admin approval.

4 **Automate enforcement**

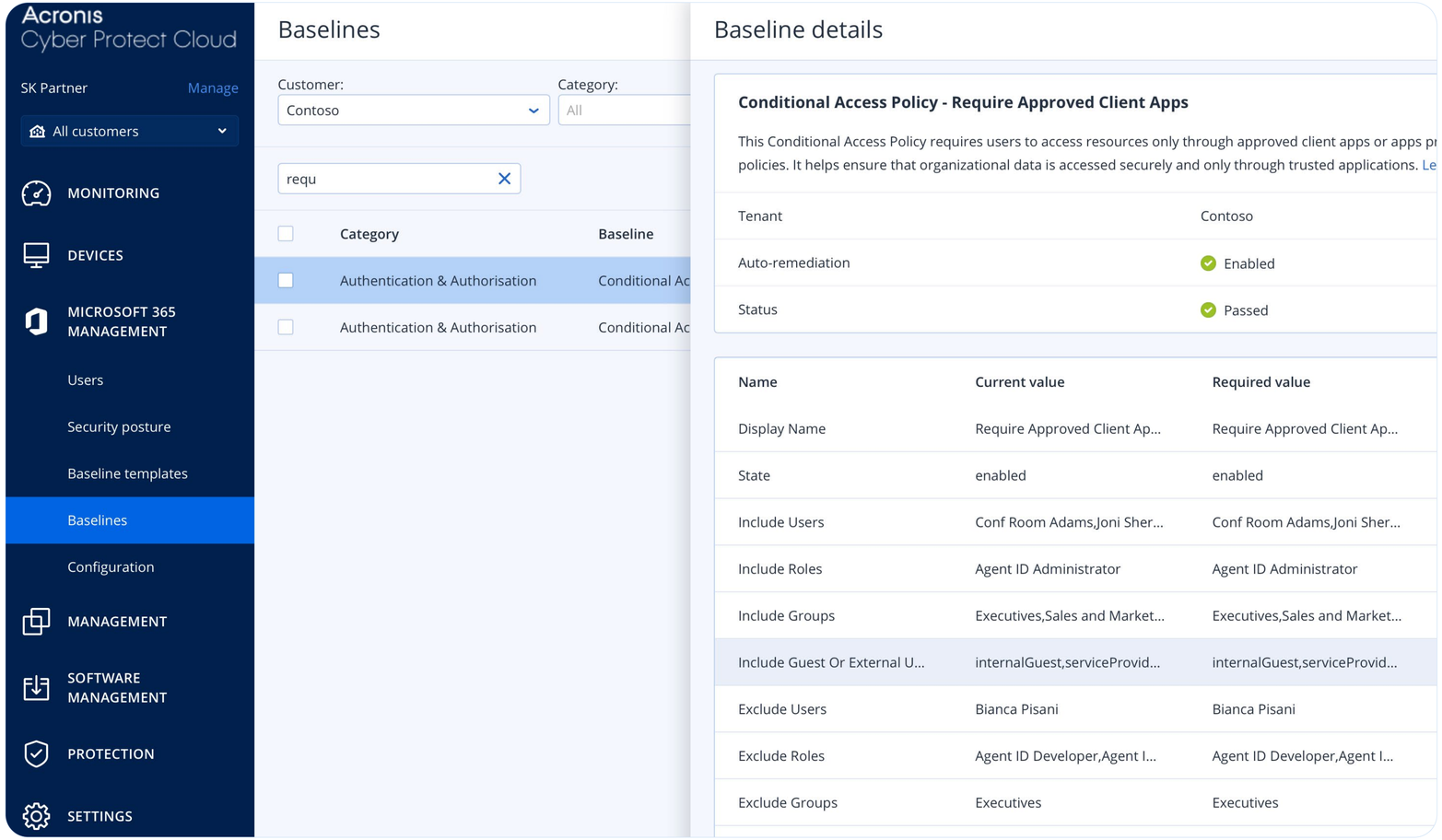
- Apply app governance policies across all tenants.
- Automatically detect new risky apps.

What just happened?

You:

- Found persistence that bypasses identity.
- Removed it instantly.
- Prevented it from reappearing.

Acronis SPM gives visibility and control over the application layer attackers rely on for long-term access.



Scenario 3

Device-code phishing

“MFA worked and the attacker still got in.”

A user completes a legitimate Microsoft login and passes MFA, but the attacker captures the authentication token. With it, they gain persistent access, read emails and create mailbox rules, all without triggering obvious alerts.

There are no failed logins, and MFA appears to have worked as expected.

Acronis SPM surfaces the real issue: policy gaps. It highlights weak or missing conditional access policies, lack of session controls and identity configurations that fall outside best-practice baselines.

From there, you enforce stronger conditional access, apply session restrictions and standardize these controls across all tenants. Continuous monitoring ensures any drift is detected and corrected.

Instead of detecting token abuse, you eliminate the conditions that allow it.



What you do (in platform)

1 **Run a baseline compliance check**

- Compare tenant policies to best practices.

2 **Enforce identity controls**

- Strengthen conditional access.
- Apply session restrictions.

3 **Automate remediation**

- Apply policies across tenants.
- Automatically correct deviations.

4 **Maintain continuous enforcement**

- Acronis SPM monitors for policy drift.
- Flags any weakening of controls.

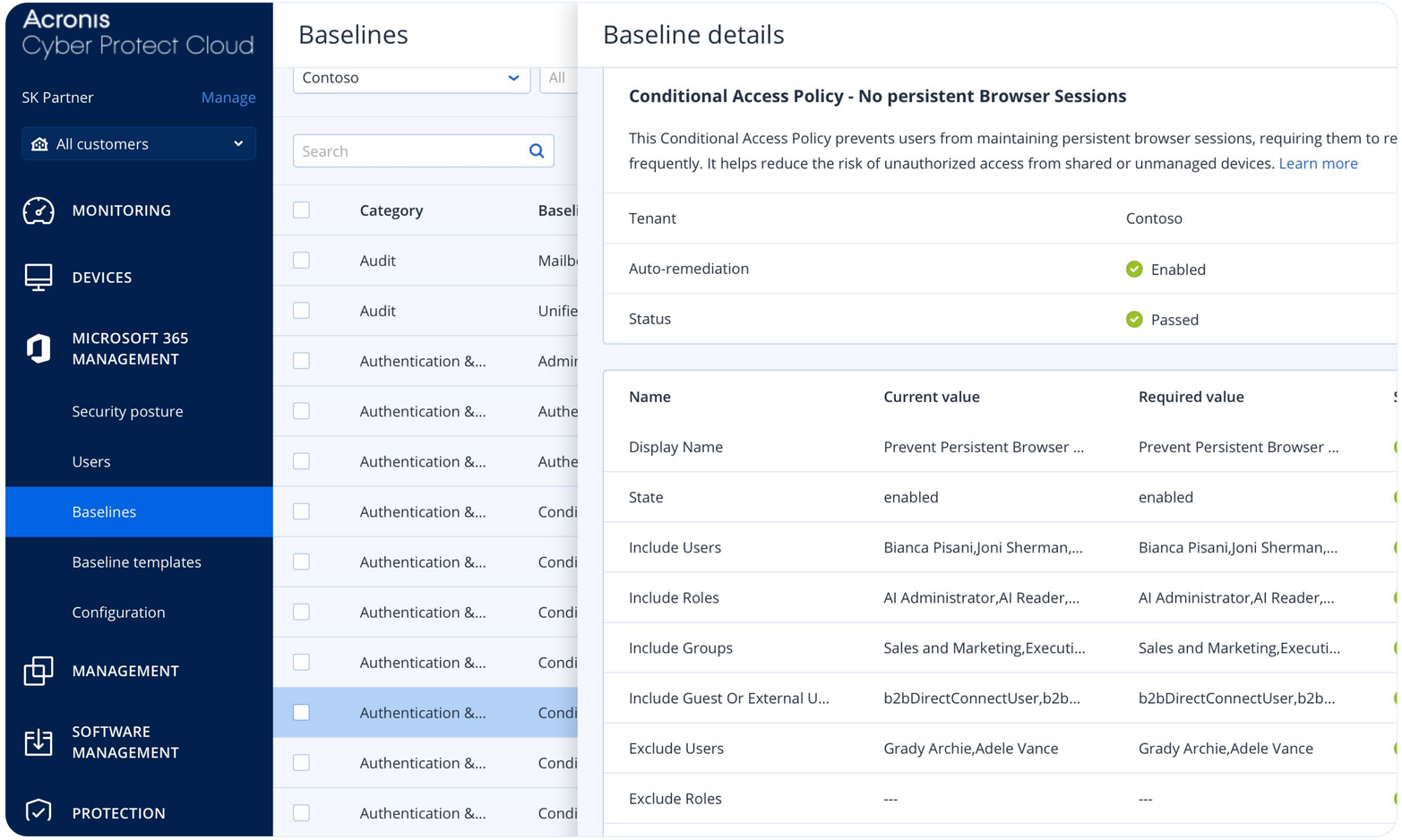
What just happened?

You didn't detect token theft.

You:

- Closed the policy gaps that allowed it.
- Standardized controls across tenants.
- Ensured long-term enforcement.

Acronis SPM secures authentication flows, not just identities.



Scenario 4

Privilege escalation

“One account becomes the entire tenant.”

An attacker compromises a single account and begins exploring. They find excessive privileges, multiple global admins and weak role separation. From there, escalation is straightforward, leading to full tenant control.

There are usually no alerts. Privilege creep happens gradually, and without centralized visibility, the risk goes unnoticed.

Acronis SPM exposes this clearly, showing admin roles across tenants, identifying over-privileged accounts and assigning risk based on exposure.



What you do (in platform)

1 **Audit privileged roles**

- Identify excessive admin accounts.

2 **Apply least privilege**

- Reduce Global Admins.
- Standardize role assignments.

3 **Automate across tenants**

- Use baseline templates to enforce role policies.

4 **Maintain lifecycle control**

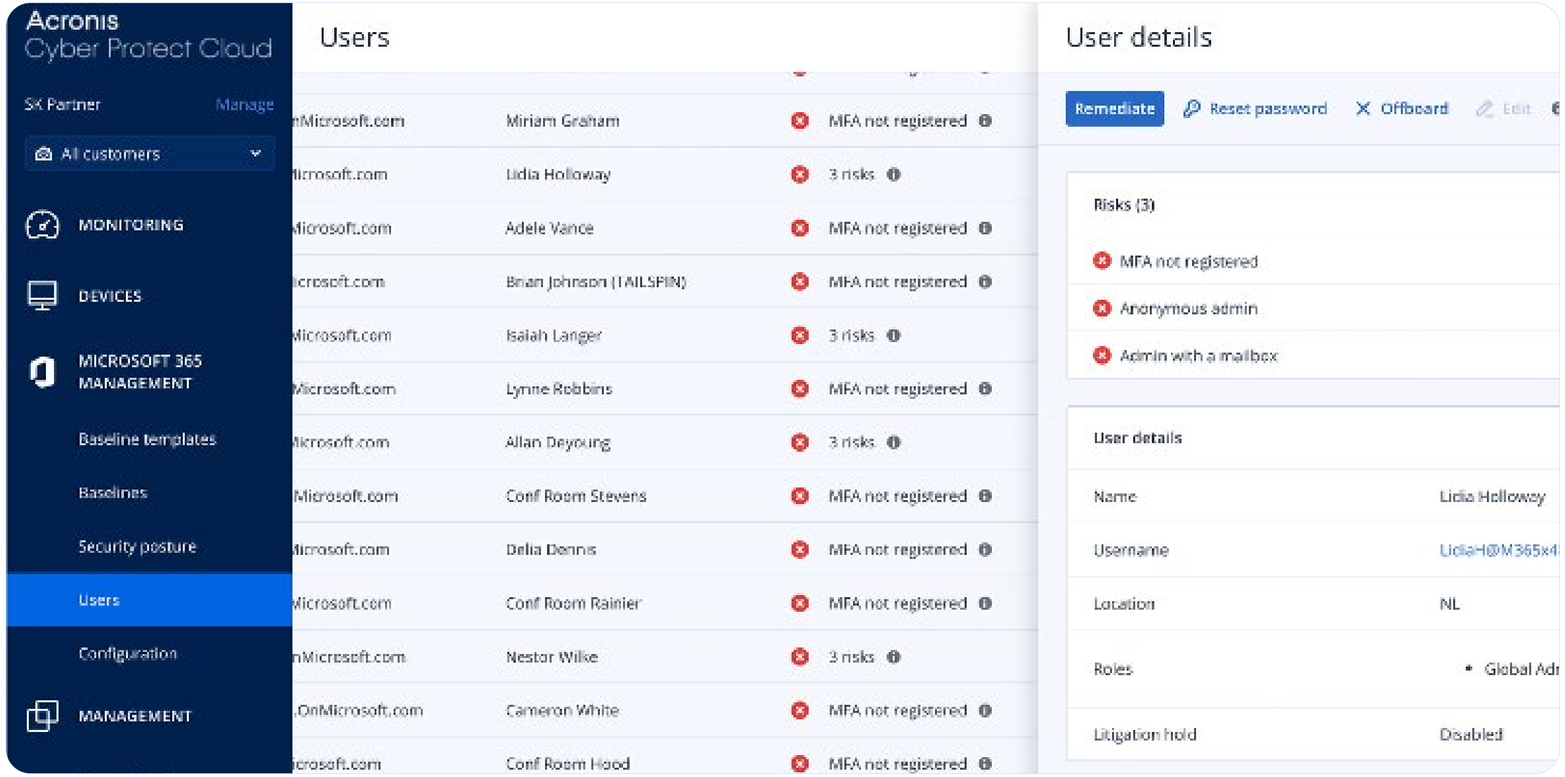
- Assign correct roles during onboarding.
- Revoke access, sessions and licenses during offboarding.

What just happened?

You:

- Reduced the blast radius of compromise.
- Standardized privilege across environments.
- Ensured identity lifecycle security.

Acronis SPM turns privilege sprawl into a controlled, enforceable policy.



You can then audit privileged roles, reduce the number of global admins and enforce least-privilege policies across all tenants using baseline templates. Ongoing lifecycle management ensures correct access during onboarding and complete revocation during offboarding.

Instead of reacting to escalation, you limit the blast radius from the start.

What ties all these attacks together

Across every scenario:

Attack	Root cause
Password spraying	Weak identity controls
OAuth abuse	App permission misconfigurations
Device-code phishing	Policy gaps
Privilege escalation	Excessive permissions

The pattern

Entry equals identity.

Persistence equals configuration.

Impact equals tenant-wide.



The Acronis SPM difference

SPM doesn’t just show risk.

It enables MSPs to operate security at scale.

Continuous monitoring

- 24/7 detection of posture drift.
- Real-time identification of new risk.

Baseline-driven security

- Predefined best-practice baselines.
- Custom baseline templates.
- Standardization across all tenants.

Automated and manual remediation

- Fix issues directly in console.
- Automate remediation of recurring risks.
- Eliminate repetitive manual work.

Multitenant management

- Centralized control across all customers.
- Policy propagation at scale.

Full identity lifecycle control

- Secure onboarding with correct roles and policies.
- Secure offboarding with session revocation and cleanup.

Operational integration

- Integration with PSA tools.
- Streamlined workflows for MSP teams.

Final thought

Modern Microsoft 365 attacks succeed because:

- No one sees the exposure.
- No one fixes it consistently.
- No one enforces it continuously.

Acronis SPM changes that.

It gives MSPs the ability to:

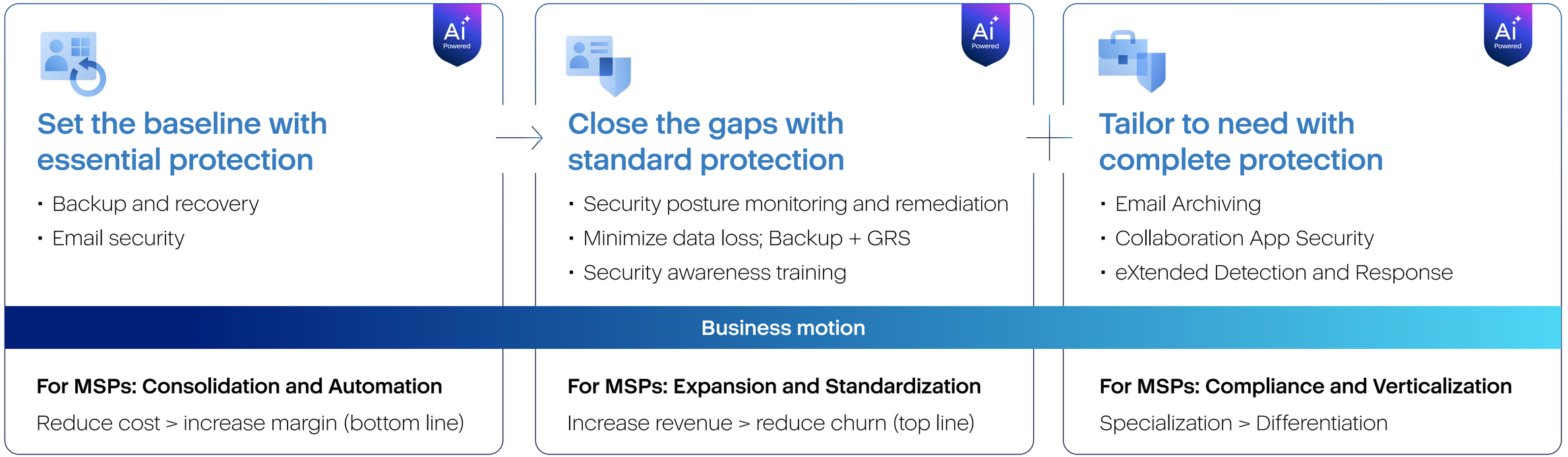
- See risk across every tenant.
- Fix it instantly.
- Enforce it automatically.
- Keep it fixed over time.



Security Posture Management: A core pillar of Protected 365

Security Posture Management (SPM) is not an optional add on but a foundational capability within the Acronis Protected 365 solution that enables the platform's promise of complete, AI-enhanced, 7-in-1 protection for Microsoft 365. SPM works in concert with backup, email security, collaboration security, XDR, email archiving and security awareness training to close the full Microsoft shared responsibility gap across Exchange, Teams, SharePoint and OneDrive.

SPM plays a critical role in the "Close the Gaps with Standard Protection" stage of the Protected 365 Maturity Model, evolving organizations from baseline protection to proactive resilience. While backup and email security establish essential protection, SPM introduces continuous risk assessment, policy enforcement and automated remediation, ensuring environments remain aligned with best practices and compliant with evolving standards.



By continuously monitoring configurations, detecting deviations and enabling rapid remediation, SPM directly addresses one of the most common and overlooked risks in Microsoft 365: user misconfiguration and security drift. It transforms security from a reactive process into a proactive, policy-driven discipline that reduces exposure, strengthens compliance and enhances overall cyber resilience.

Crucially, SPM is delivered within the same single, multitenant Acronis platform, reinforcing Protected 365's core value proposition: one vendor, one contract, one integrated solution. This eliminates tool sprawl, reduces operational overhead and empowers MSPs and IT teams to scale efficiently while improving service quality and profitability.

Take action: Close the gaps now

Misconfigurations don't wait and neither should you.
Start your Acronis Security Posture Management trial today and instantly uncover risks, enforce best practices and strengthen your Microsoft 365 security.

START YOUR FREE TRIAL



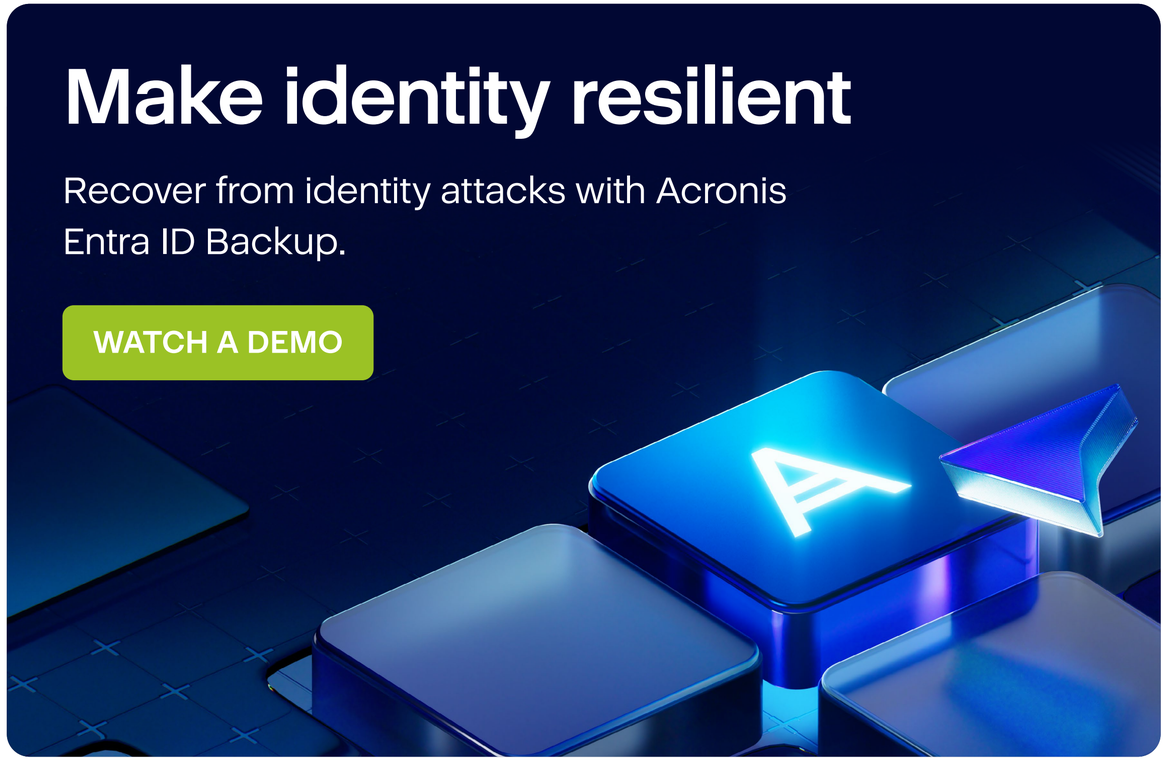
Recover the identity control plane

Acronis Security Posture Management (SPM) helps MSPs reduce the identity gaps attackers exploit. Acronis Entra ID Backup adds the recovery layer when identities, policies or configurations are deleted, corrupted or maliciously changed.

Protect and recover critical Entra ID assets, including:

- Users, groups and roles
- Conditional Access policies
- App registrations and enterprise applications
- Key relationships, permissions and configurations
- Audit and sign-in logs

Recover from a known-good point in time, reduce manual rebuilding and restore access faster through the same integrated Acronis platform used to protect Microsoft 365.



Acronis



For more information
acronis.com

Copyright © 2003-2026 Acronis International GmbH. All rights reserved. Acronis and the Acronis logo are trademarks of Acronis International GmbH in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. Technical changes and differences from the illustrations are reserved; errors are excepted. 2026-10