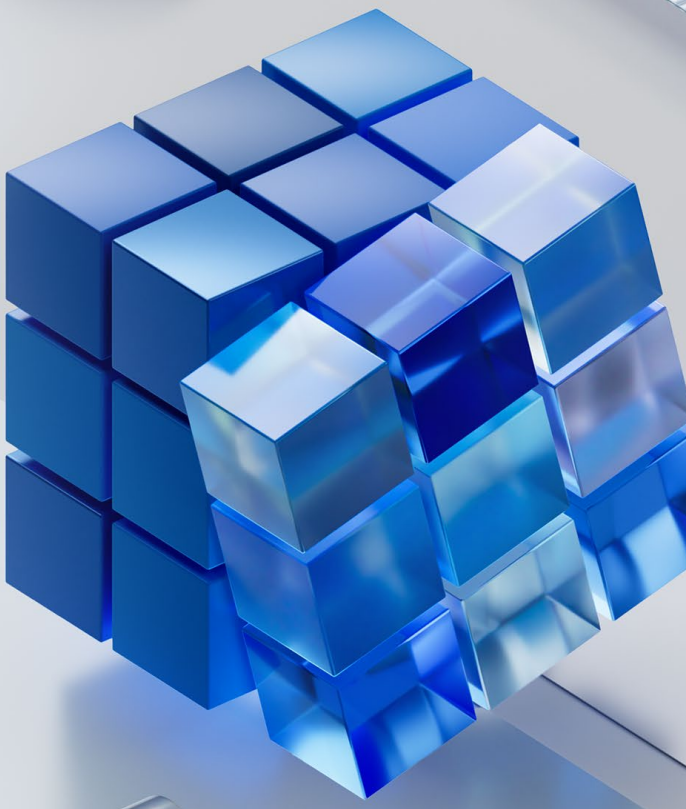
Acronis

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.



Copyright © 2003-2026 Acronis International GmbH.

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

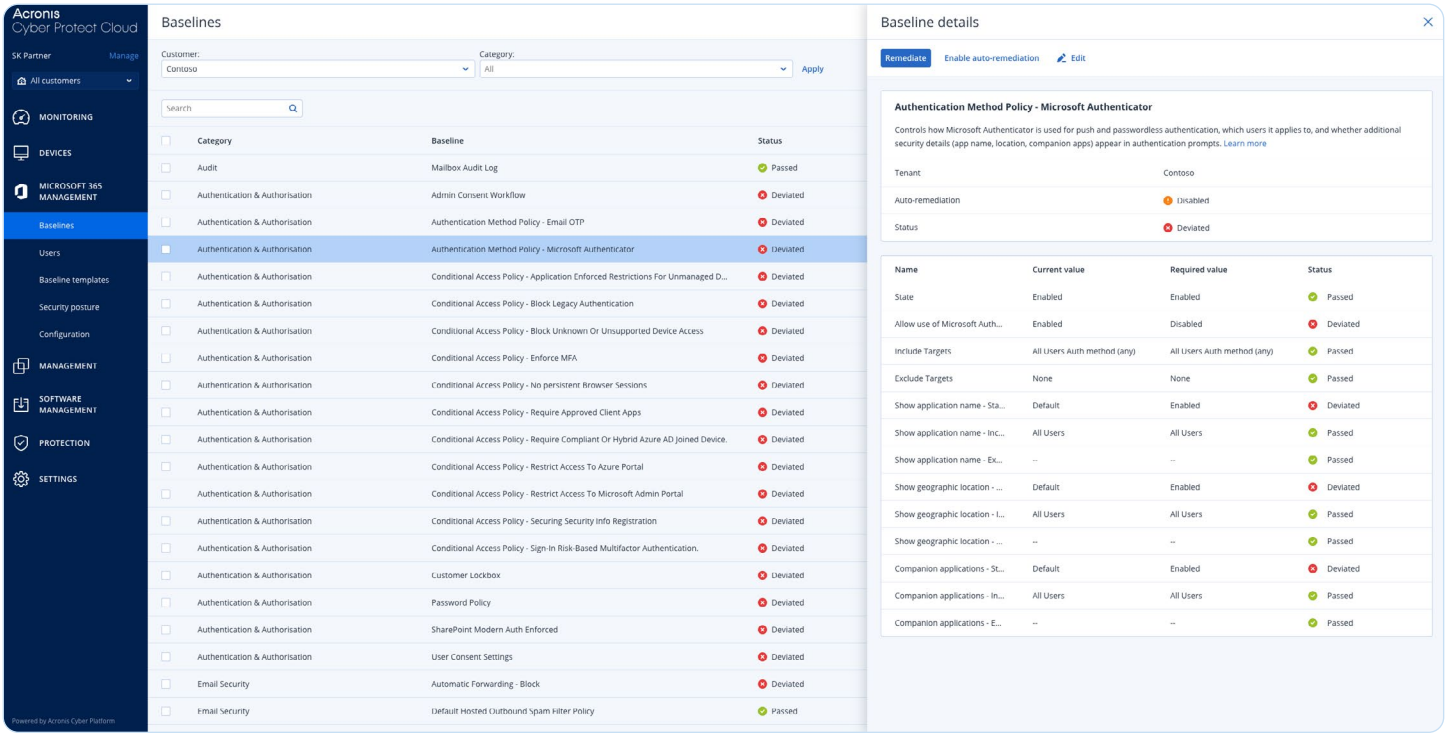
- Weak credentials.
- No MFA on a legacy account.

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.



Copyright © 2003-2026 Acronis International GmbH.

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

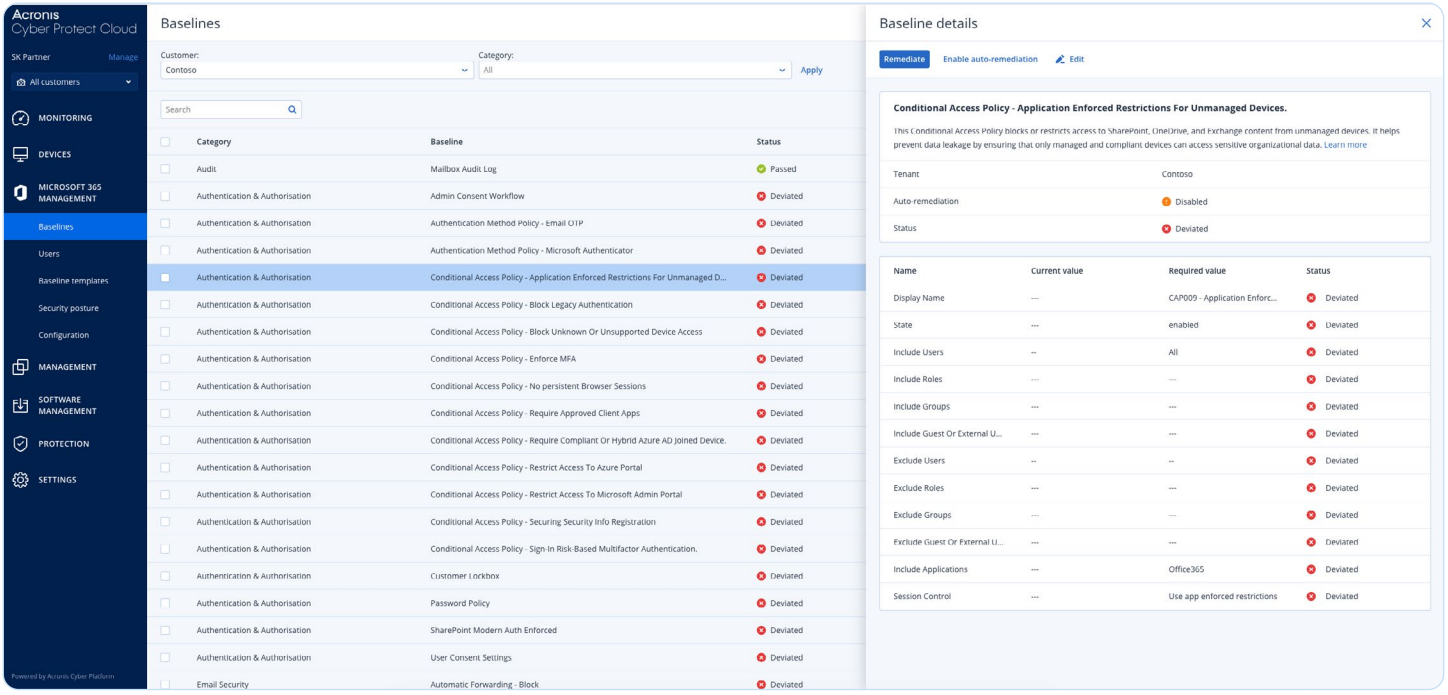
- Token-validation weaknesses.
- Signing-key abuse.
- Limited visibility into anomalous token usage.

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.



Copyright © 2003-2026 Acronis International GmbH.

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

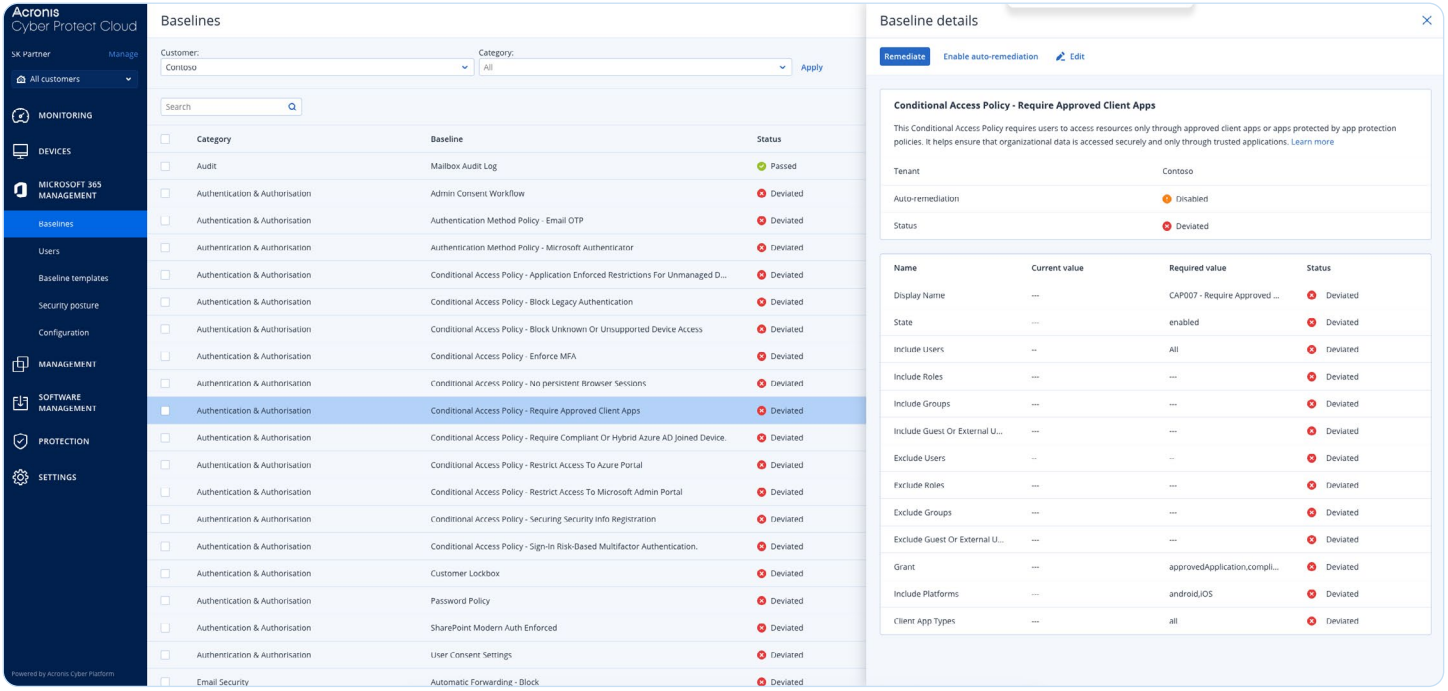
- Stolen authenticated session cookies.
- Weak Conditional Access enforcement.
- Lack of device-based access restrictions.

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.



Copyright © 2003-2026 Acronis International GmbH.

4. Token replay attacks

Real-world incident

Multiple real-world incidents.

Attack technique

Reuse of stolen Primary Refresh Tokens.

What was exploited

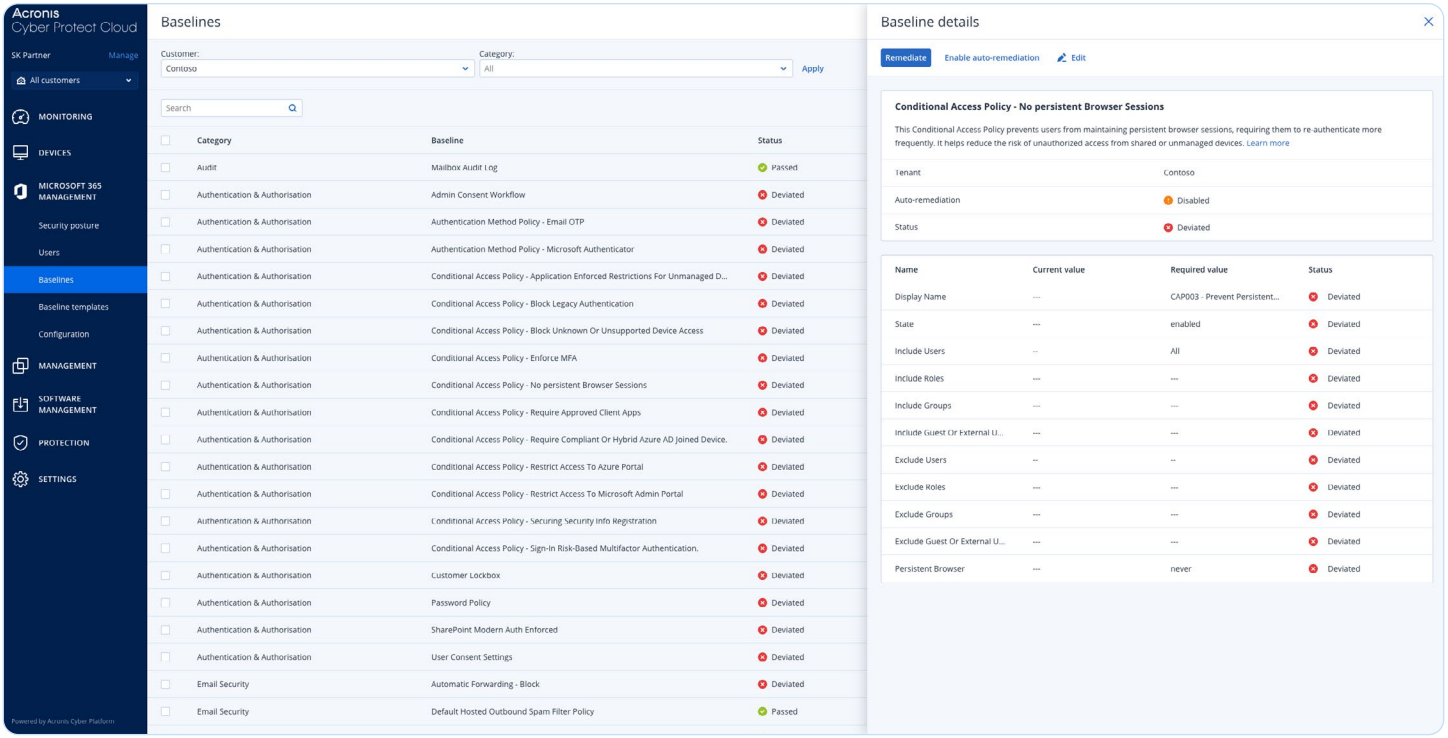
- Lack of token / session protection.
- Weak session enforcement.

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.



Copyright © 2003-2026 Acronis International GmbH.

5. OAuth consent phishing

Real-world incident

Multiple real-world incidents.

Attack technique

Malicious application consent grants.

What was exploited

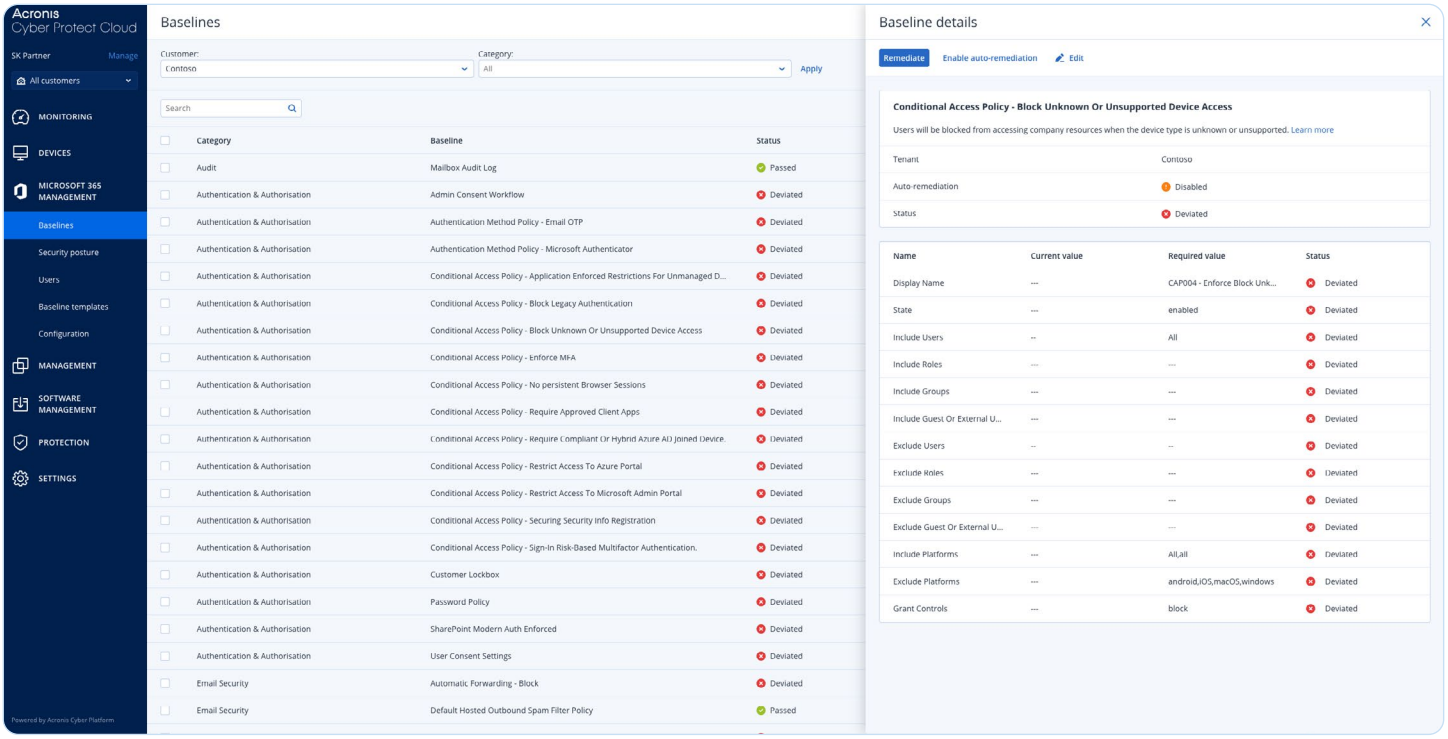
- Unrestricted user consent.
- Weak application governance.

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.



Copyright © 2003-2026 Acronis International GmbH.

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

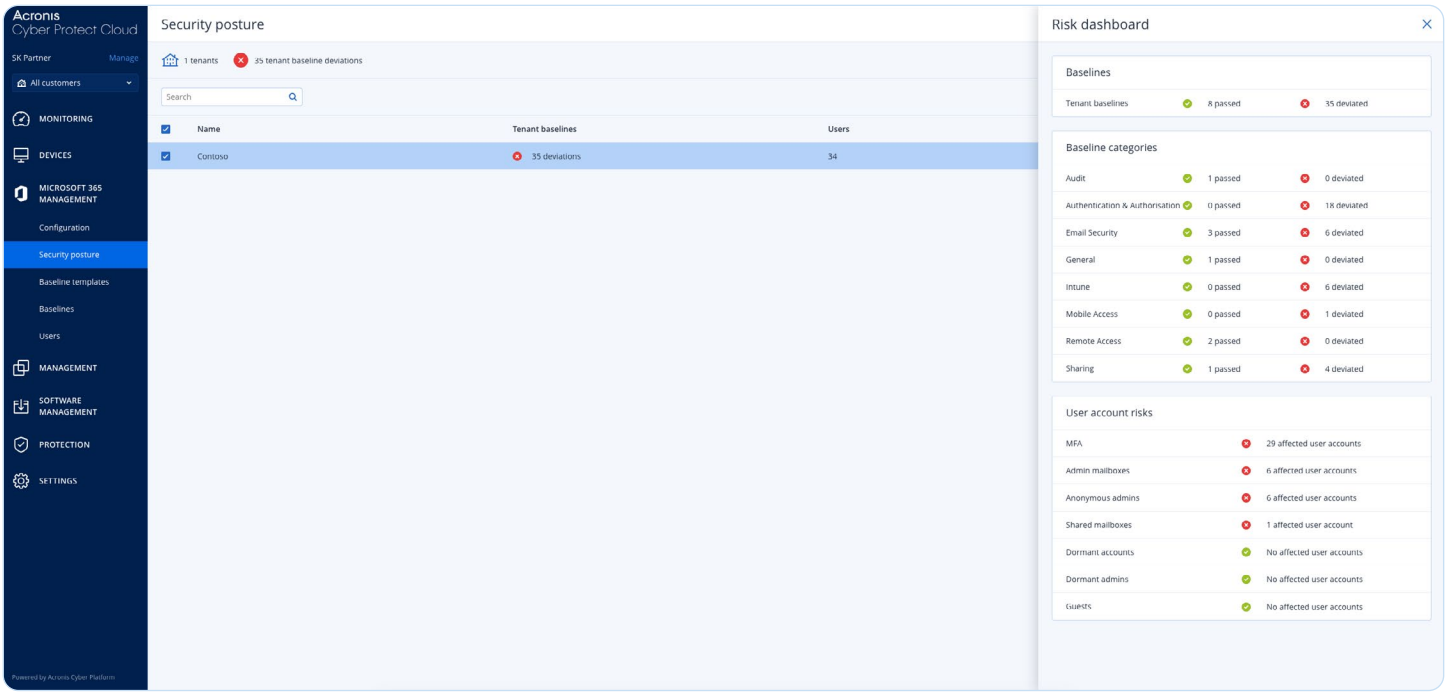
- Excessive Graph permissions.
- Poor visibility into app behavior.
- Unmanaged application access.

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.



Copyright © 2003-2026 Acronis International GmbH.

7. Privilege escalation and excessive role abuse

Real-world incident

Multiple Entra ID Privilege Escalations / Midnight Blizzard.

Attack technique

Privilege escalation through excessive standing admin privileges.

What was exploited

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

Security controls to reduce risk

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

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.

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.

Copyright © 2003-2026 Acronis International GmbH.

8. SharePoint and OneDrive exposure

Real-world incident

Multiple real-world incidents.

Attack technique

Excessive or accidental external sharing.

What was exploited

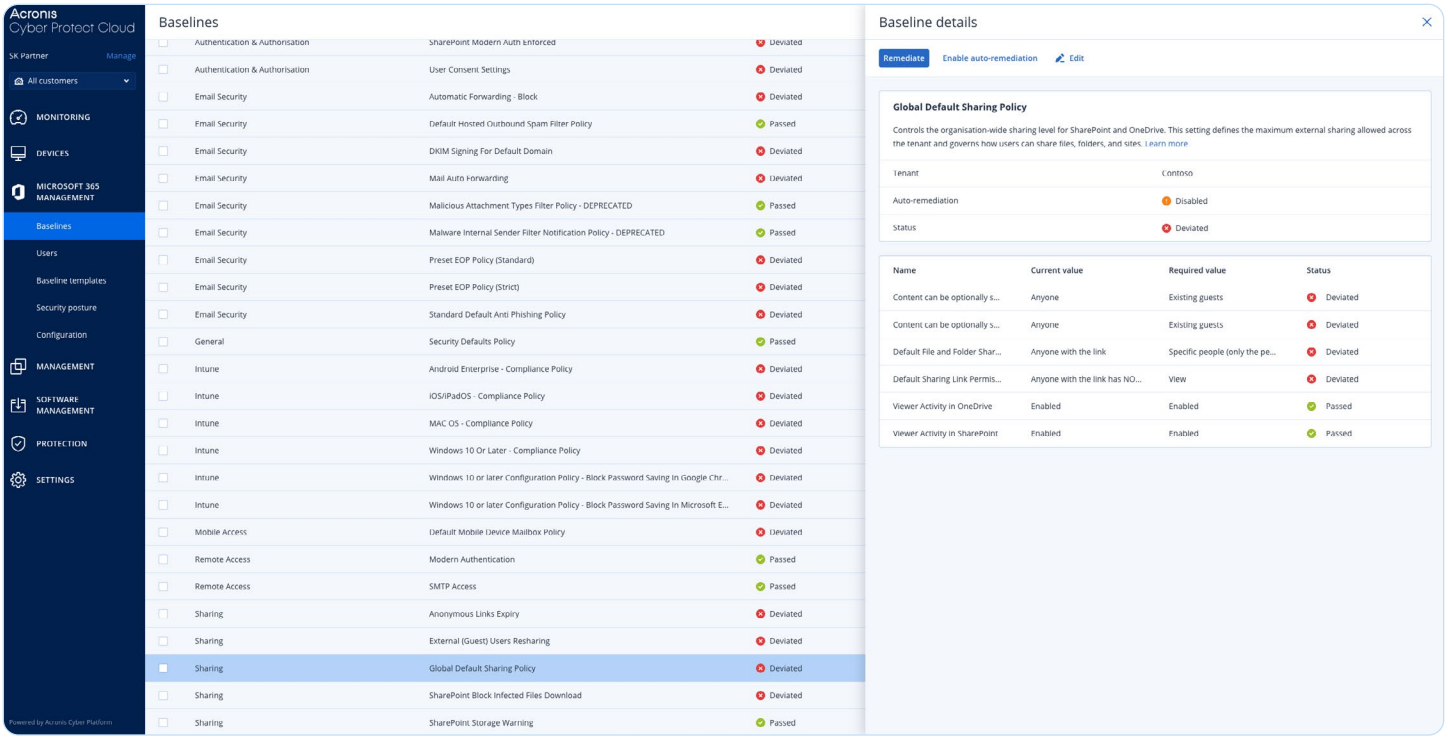
- Weak sharing governance.
- Overly permissive external access settings.

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.



Copyright © 2003-2026 Acronis International GmbH.

9. Audit and investigation gaps

Real-world incident

Incident Investigations.

Attack technique

Post-compromise activity hidden by insufficient auditing.

What was exploited

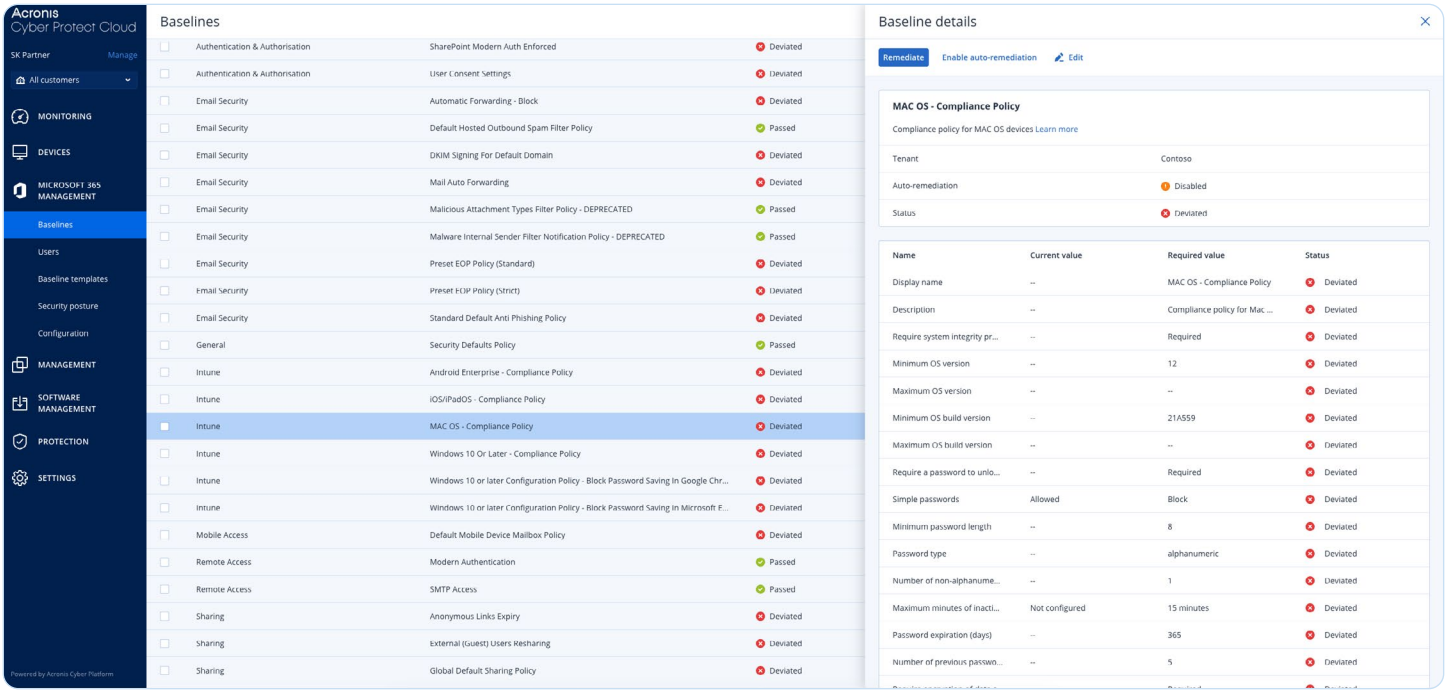
- Missing or incomplete audit evidence.
- Weak investigation readiness.

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.



Copyright © 2003-2026 Acronis International GmbH.

What these attacks have in common

Across all incidents:

- Entry is identity-based.
- Persistence is configuration-based.
- Impact is tenant-wide.
- Traditional endpoint controls provide limited visibility.

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.

When prevention is not enough: recover Entra ID

Security posture management helps reduce identity risk. Backup provides a recovery path when an attack, accidental deletion or misconfiguration disrupts the identity control plane.

Why Entra ID recovery matters

Entra ID controls who can access Microsoft 365 and connected applications. Attackers may alter or delete users, groups, roles, policies and configurations to expand privileges, maintain persistence or disrupt access.

Restoring Microsoft 365 data alone may not restore secure access to it. Organizations also need a reliable way to recover the identities, settings and relationships on which their environment depends.

How Acronis Entra ID Backup helps

- Protect critical Entra ID users, groups, roles, policies and configurations.
- Recover deleted or compromised identity objects and their relationships.
- Roll back unwanted changes following attacks or administrative errors.
- Reduce downtime without relying solely on native retention and recovery options.
- Manage Microsoft 365 data and identity protection through the Acronis platform.

Copyright © 2003-2026 Acronis International GmbH.

Strengthen identity resilience

Combine proactive posture management with recoverable Entra ID backups to help customers prevent identity-based attacks, limit their impact and recover faster.

Explore Acronis Entra ID Backup

LEARN MORE



Explore how Acronis SPM helps MSPs secure Microsoft 365 at scale

Scan to book an Acronis SPM demo



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