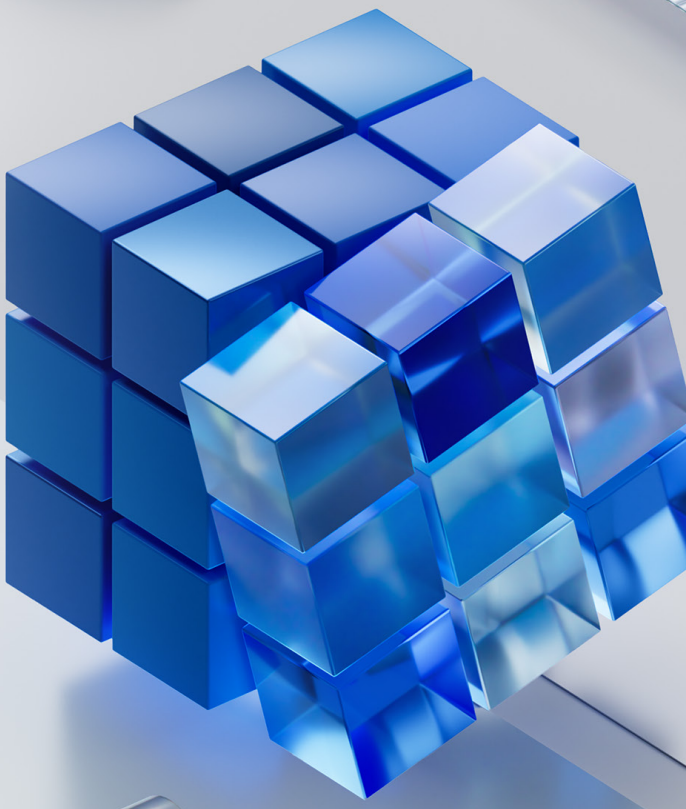
Acronis

Ataques a identidades y al plano de control de Microsoft 365

9 amenazas del mundo real: qué explotan y cómo los MSP pueden reducir el riesgo con Acronis SPM



Los ataques modernos a Microsoft 365 se dirigen cada vez más al plano de control (identidades, aplicaciones OAuth, permisos, sesiones y configuraciones) en lugar de a los endpoints.

En incidentes recientes del mundo real, los atacantes utilizaron flujos de autenticación legítimos, permisos excesivos, controles de acceso débiles y configuraciones incorrectas para obtener acceso persistente a los inquilinos de Microsoft 365.

Esta lista de verificación resume lo siguiente:

- Las técnicas de ataque utilizadas en incidentes reales.
- Qué explotaron los atacantes.
- Los controles de Microsoft 365 recomendados para reducir el riesgo.
- Cómo Acronis SPM ayuda a los MSP a supervisar continuamente y a aplicar una postura de seguridad en todos los inquilinos.



Copyright © 2003-2026 Acronis International GmbH.

1. Ataques de pulverización de contraseñas

Incidente del mundo real

Midnight Blizzard (2024).

Técnica de ataque

Ataque de pulverización de contraseñas contra una cuenta de inquilino heredada que no es de producción.

Qué se explotó

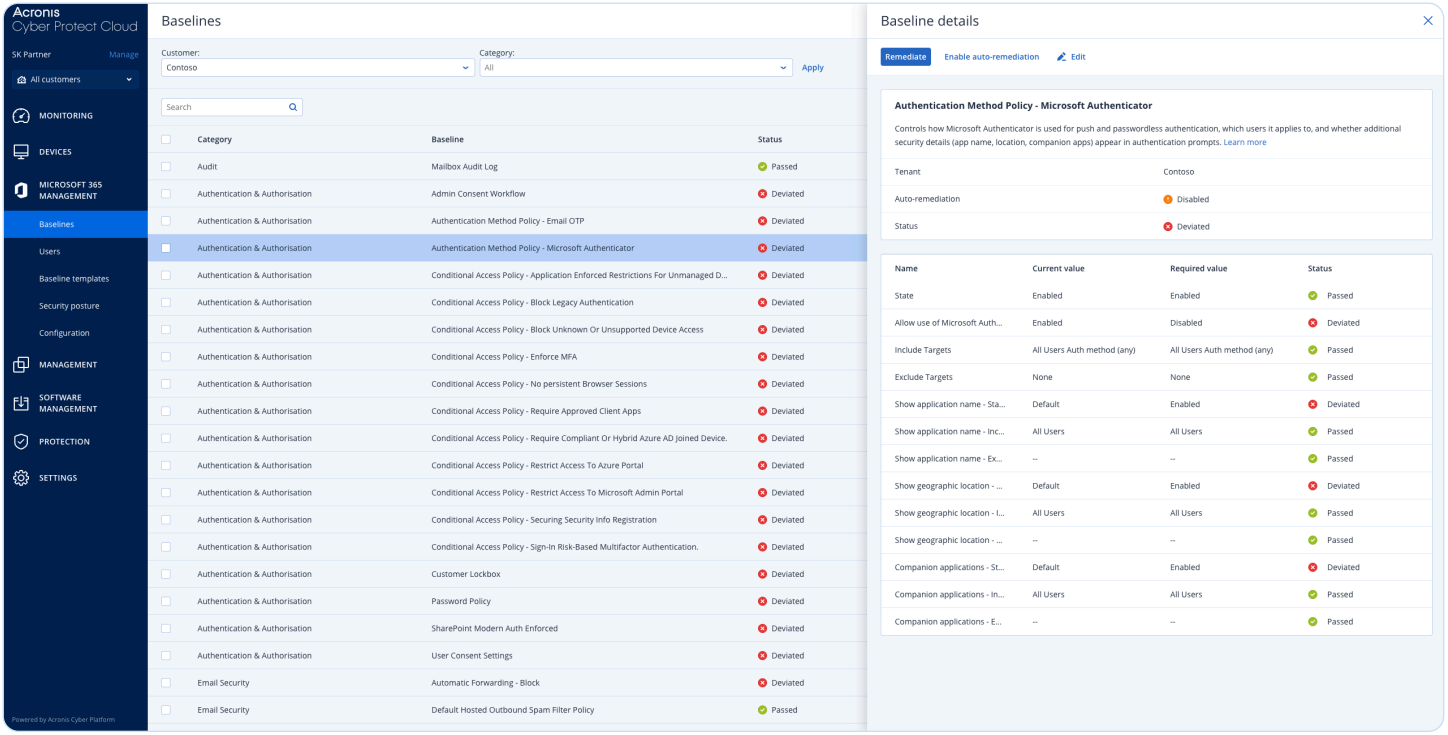
- Credenciales débiles.
- Falta de autenticación multifactor en una cuenta heredada.

Controles de seguridad para reducir el riesgo

- Aplicar la autenticación multifactor.
- Eliminar las contraseñas débiles.
- Desactivar las rutas de autenticación heredadas.
- Supervisar anomalías en el inicio de sesión.

Cómo ayuda Acronis SPM

- Identifica brechas de autenticación multifactor.
- Detecta configuraciones de autenticación inseguras.
- Supervisa las desviaciones de los criterios de referencia en todos los inquilinos.
- Ayuda a los MSP a corregir las configuraciones de identidad débiles antes de que se conviertan en rutas de ataque.



Copyright © 2003-2026 Acronis International GmbH.

2. Falsificación de tokens y abuso de sesiones

Incidente del mundo real

Storm-0558 (2023).

Técnica de ataque

Tokens de autenticación falsificados utilizados para acceder a cuentas de correo electrónico en la nube.

Qué se explotó

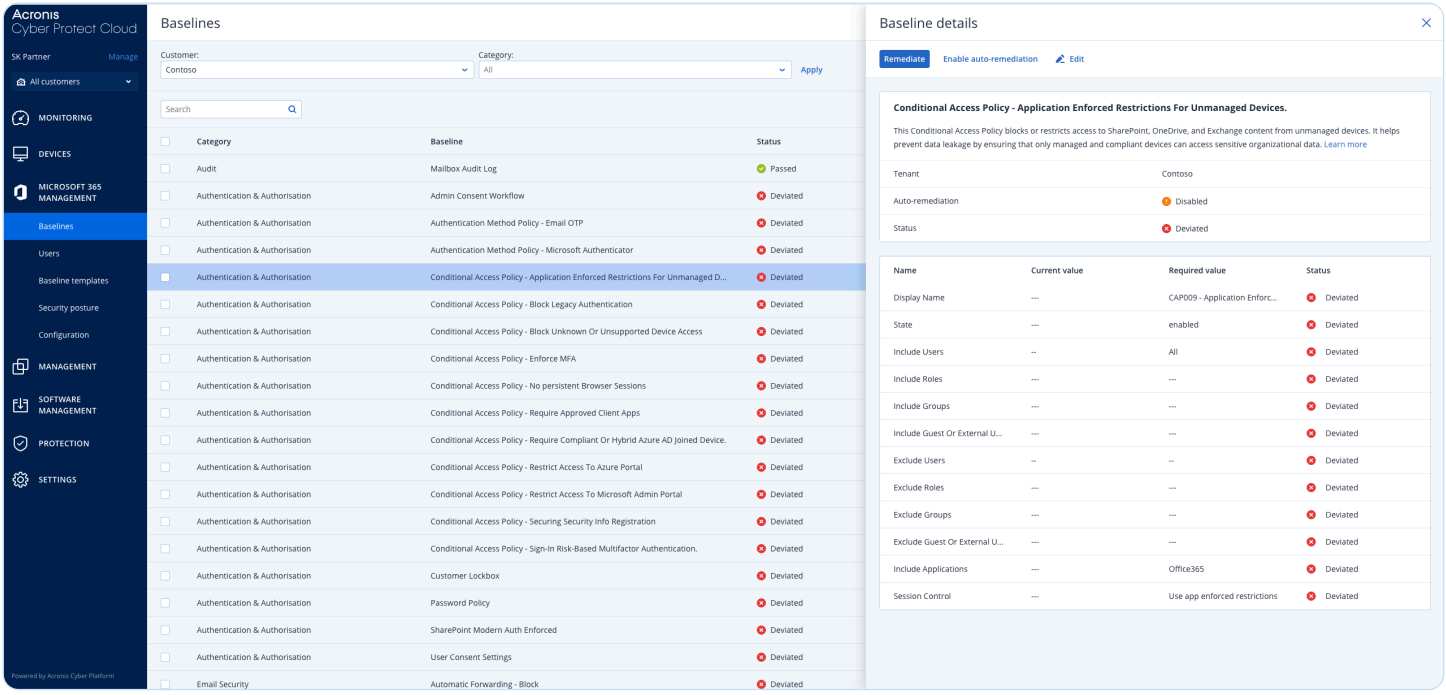
- Debilidades en la validación de tokens.
- Abuso de claves de firma.
- Visibilidad limitada del uso anómalo de tokens.

Controles de seguridad para reducir el riesgo

- Reforzar la postura de identidad.
- Aplicar la autenticación multifactor y el Acceso condicional.
- Restringir el consentimiento de aplicaciones.
- Proteger el acceso privilegiado.
- Supervisar anomalías de tokens y sesiones.

Cómo ayuda Acronis SPM

- Ayuda a estandarizar la postura de la autenticación multifactor y del Acceso condicional.
- Identifica la desviación en la configuración de la identidad.
- Apoya la aplicación de criterios de referencia seguros para el acceso de administradores.
- Reduce la exposición de identidad adyacente del lado del inquilino.



Copyright © 2003-2026 Acronis International GmbH.

3. Secuestro de sesiones y suplantación de identidad de tipo AiTM

Incidente del mundo real

Múltiples incidentes del mundo real.

Técnica de ataque

Robo de cookies de sesión a través de suplantación de identidad de proxy inverso.

Qué se explotó

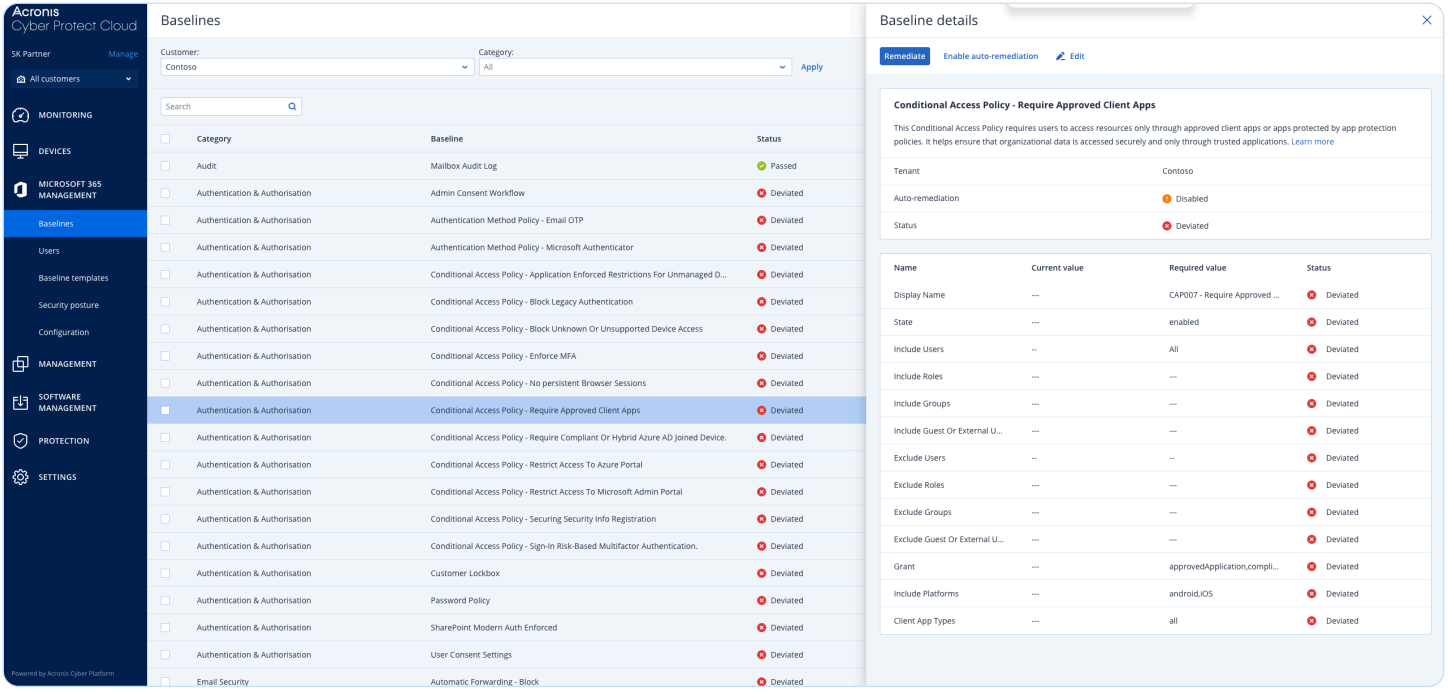
- Cookies de sesión autenticadas robadas.
- Aplicación débil del Acceso condicional.
- Falta de restricciones de acceso basadas en dispositivos.

Controles de seguridad para reducir el riesgo

- Requerir dispositivos administrados o que cumplan con las normativas.
- Exigir el Acceso condicional.
- Supervisar el comportamiento anómalo de la sesión.
- Utilizar la evaluación de acceso continuo donde esté disponible.

Cómo ayuda Acronis SPM

- Detecta la desviación en la postura del Acceso condicional.
- Ayuda a mantener criterios de referencia seguros para las directivas de acceso.
- Apoya la estandarización de los controles de identidad y de acceso a dispositivos en todos los inquilinos.



Copyright © 2003-2026 Acronis International GmbH.

4. Ataques de reproducción de tokens

Incidente del mundo real

Múltiples incidentes del mundo real.

Técnica de ataque

Reutilización de Primary Refresh Tokens robados.

Qué se explotó

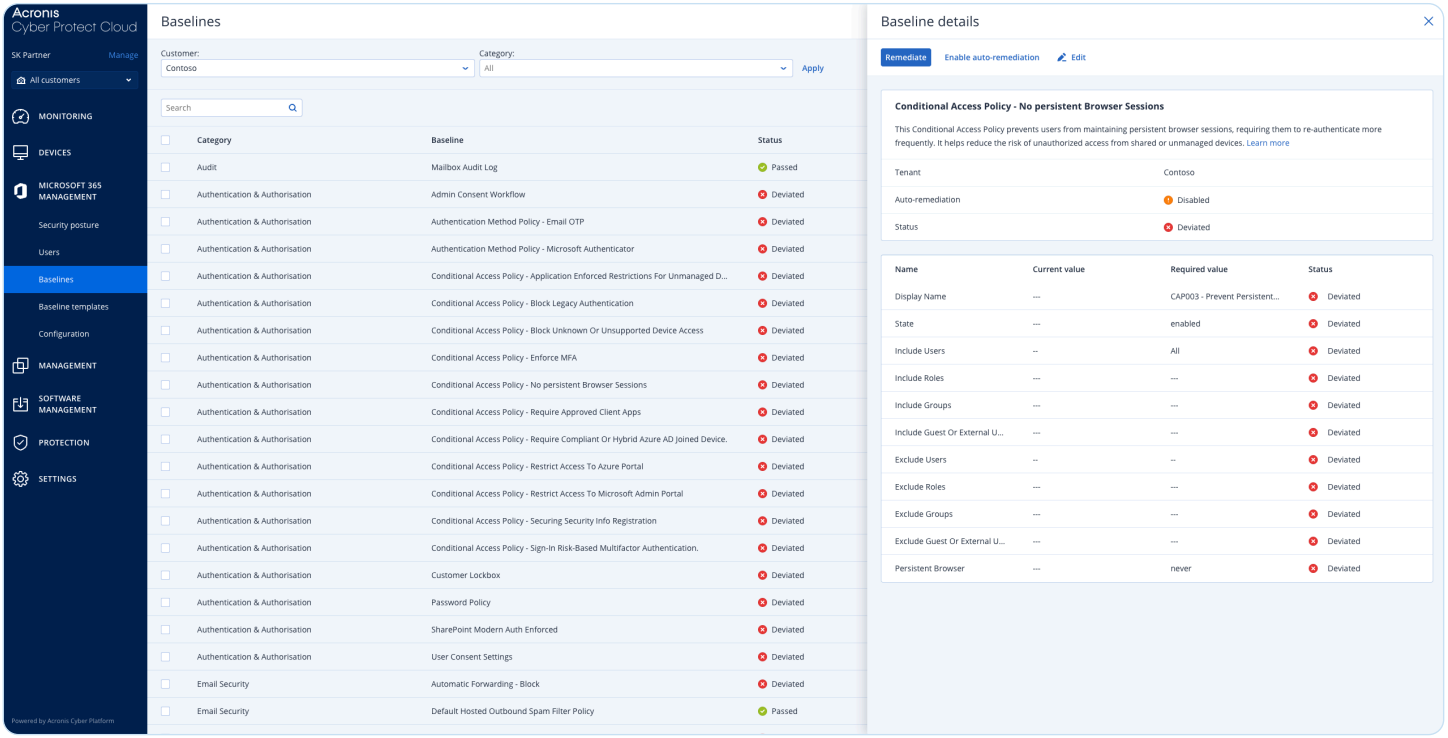
- Falta de protección de tokens/sesiones.
- Aplicación de sesión débil.

Controles de seguridad para reducir el riesgo

- Exigir la protección de tokens donde sea compatible.
- Utilizar los controles de sesión de Acceso condicional.
- Restringir el acceso desde dispositivos no administrados.

Cómo ayuda Acronis SPM

- Ayuda a los MSP a a supervisar continuamente la postura de autenticación.
- Detecta la desviación de los criterios de referencia en torno al Acceso condicional y la configuración de la sesión.
- Apoya la aplicación de criterios de referencia seguros para la identidad y el acceso.



Copyright © 2003-2026 Acronis International GmbH.

5. Suplantación de identidad de consentimiento de OAuth

Incidente del mundo real

Múltiples incidentes del mundo real.

Técnica de ataque

Concesiones de consentimiento de aplicaciones maliciosas.

Qué se explotó

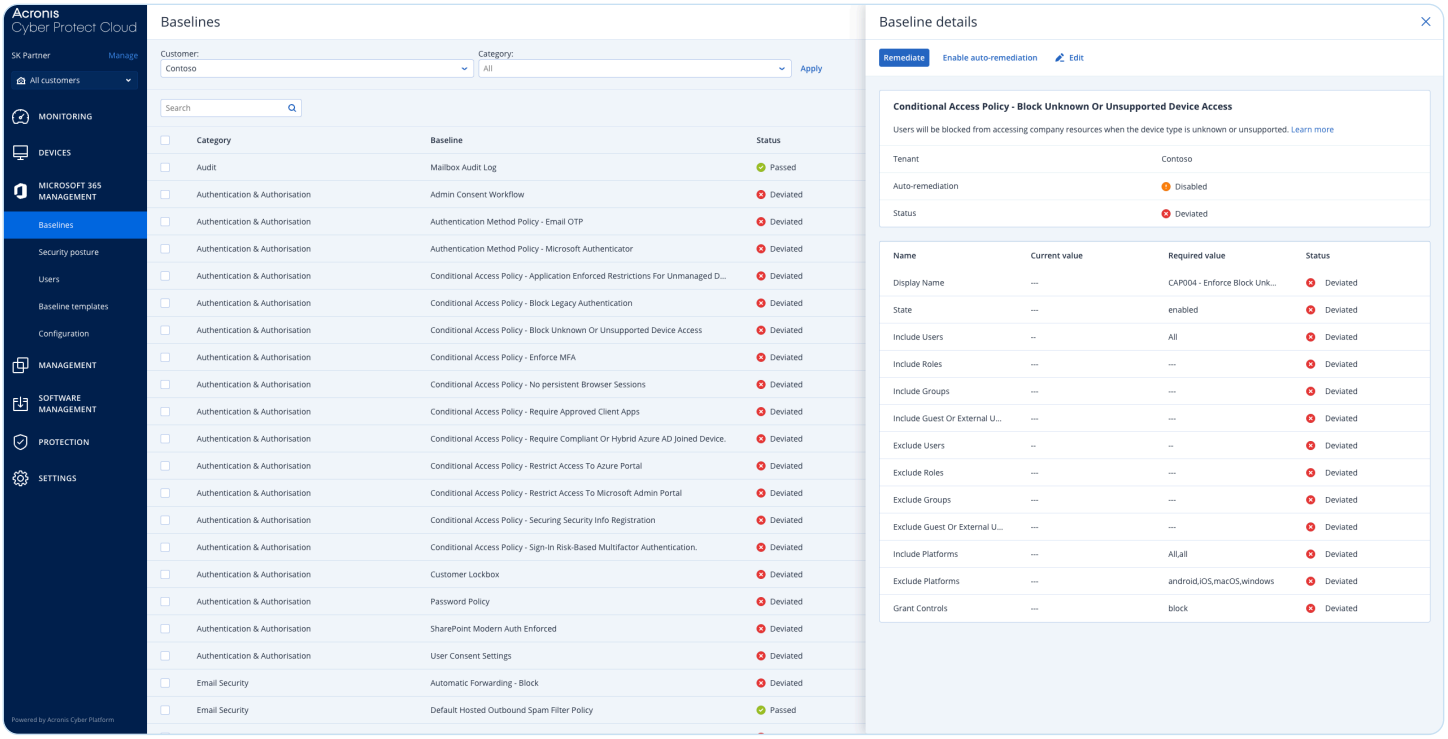
- Consentimiento de usuario sin restricciones.
- Administración de aplicaciones débil.

Controles de seguridad para reducir el riesgo

- Restringir el consentimiento del usuario.
- Requerir la aprobación del administrador para las aplicaciones.
- Permitir únicamente editores verificados y permisos de bajo riesgo.

Cómo ayuda Acronis SPM

- Estandariza los controles relacionados con la autorización.
- Detecta la desviación de las directivas de consentimiento de aplicaciones aprobadas.
- Ayuda a los MSP a mantener una postura de autorización segura de Microsoft 365 en todos los inquilinos.



Copyright © 2003-2026 Acronis International GmbH.

6. Abuso de aplicaciones OAuth y exfiltración de datos de Graph API

Incidente del mundo real

Múltiples incidentes del mundo real.

Técnica de ataque

Acceso y exfiltración de datos basados en API a través de aplicaciones con permisos excesivos.

Qué se explotó

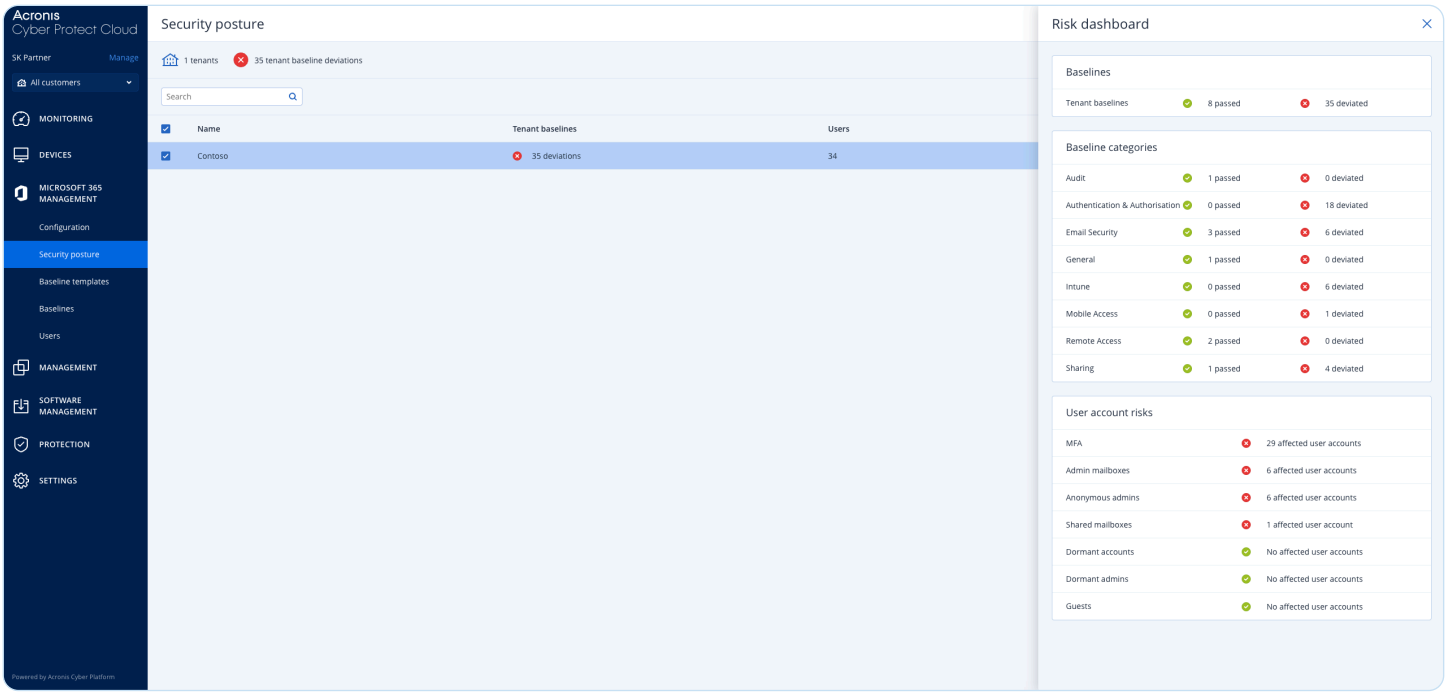
- Permisos excesivos de Graph.
- Visibilidad deficiente del comportamiento de la aplicación.
- Acceso a aplicaciones no administradas.

Controles de seguridad para reducir el riesgo

- Auditar los permisos de las aplicaciones con regularidad.
- Investigar la actividad inusual de Graph.
- Revisar las aplicaciones autorizadas por usuarios externos.

Cómo ayuda Acronis SPM

- Ayuda a mantener la administración sobre los permisos de las aplicaciones y la postura de consentimiento.
- Detecta la desviación de la autorización y la exposición de aplicaciones no administradas.
- Mejora la visibilidad de la postura de acceso a las aplicaciones de Microsoft 365.



Copyright © 2003-2026 Acronis International GmbH.

7. Remisión de privilegios y abuso excesivo de roles

Incidente del mundo real

Múltiples remisiones de privilegios de Entra ID/ Midnight Blizzard.

Técnica de ataque

Remisión de privilegios a través de privilegios de administrador permanentes excesivos.

Qué se explotó

- Demasiados administradores globales.
- Acumulación de privilegios.
- Administración de roles débil.

Controles de seguridad para reducir el riesgo

- Aplicar el principio de menor privilegio.
- Restringir el acceso de administrador permanente.
- Revisar los roles privilegiados continuamente.

Cómo ayuda Acronis SPM

- Identifica roles de administrador excesivos y exposición de privilegios.
- Ayuda a los MSP a estandarizar una postura de roles segura en todos los inquilinos.
- Apoya la aplicación de criterios de referencia de identidad y autorización.

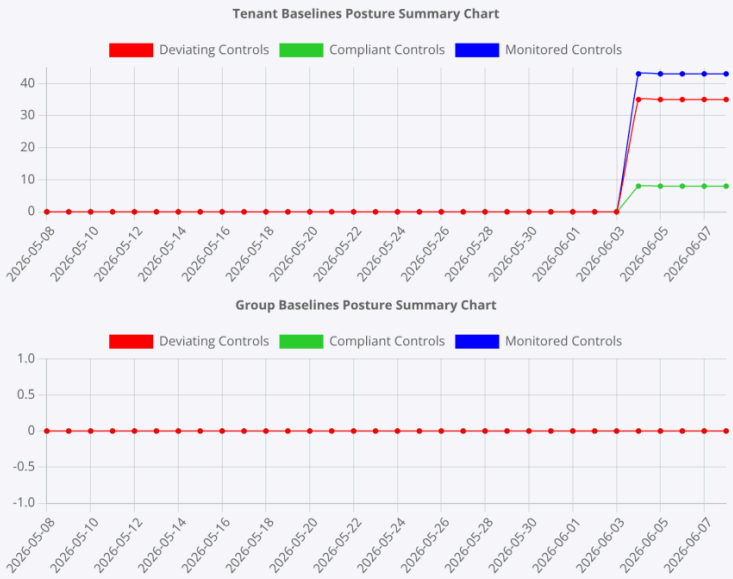
Compliance Posture Summary

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. Exposición de SharePoint y OneDrive

Incidente del mundo real

Múltiples incidentes del mundo real.

Técnica de ataque

Uso compartido externo excesivo o accidental.

Qué se explotó

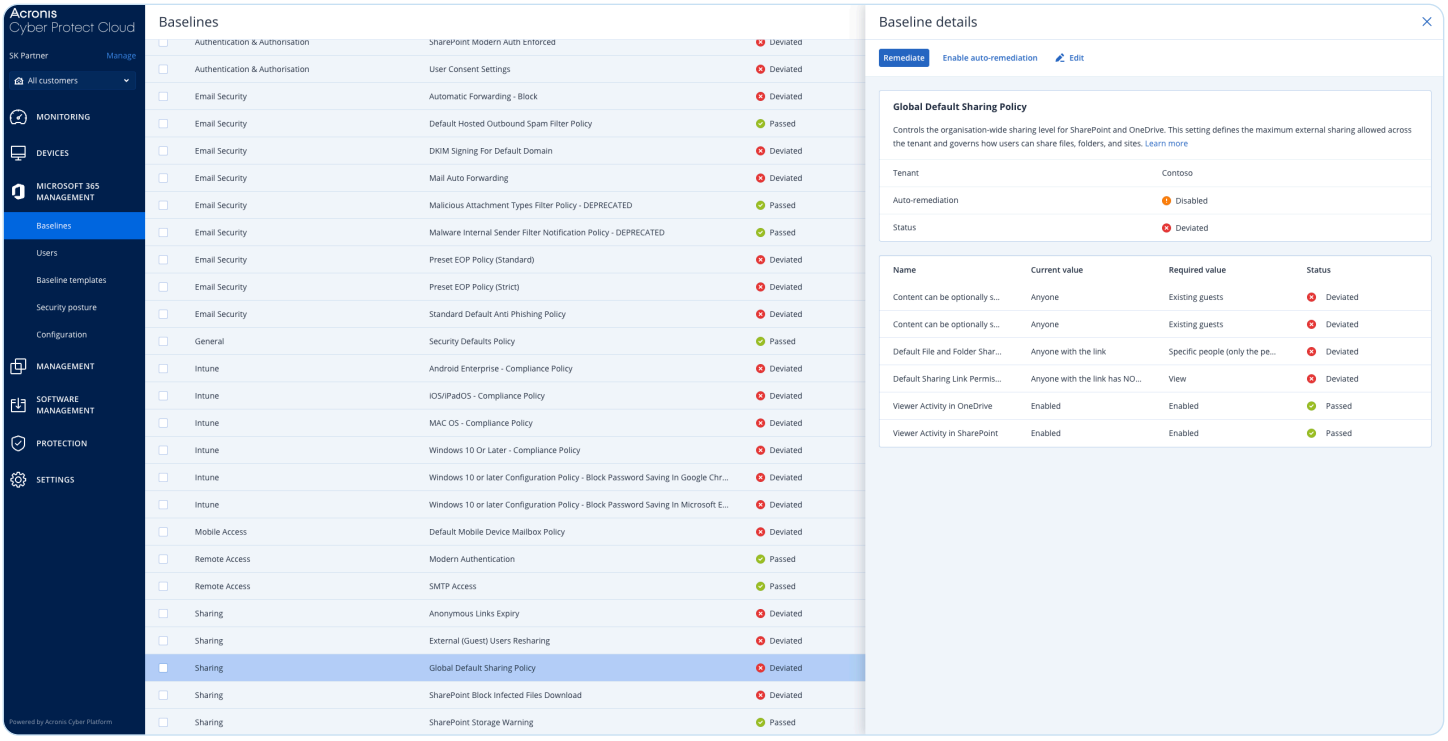
- Administración de uso compartido débil.
- Configuraciones de acceso externo excesivamente permisivas.

Controles de seguridad para reducir el riesgo

- Configurar directivas de uso compartido externo a nivel de la organización.
- Restringir el uso compartido cuando sea necesario.
- Revisar la postura de uso compartido con regularidad.

Cómo ayuda Acronis SPM

- Valida continuamente la postura de uso compartido con respecto a los criterios de referencia.
- Detectar configuraciones de uso compartido de riesgo.
- Reducir la desviación de configuración a largo plazo en todos los inquilinos.



Copyright © 2003-2026 Acronis International GmbH.

9. Brechas de auditoría e investigación

Incidente del mundo real

Investigaciones de incidentes.

Técnica de ataque

Actividad posterior a la vulneración oculta por una auditoría insuficiente.

Qué se explotó

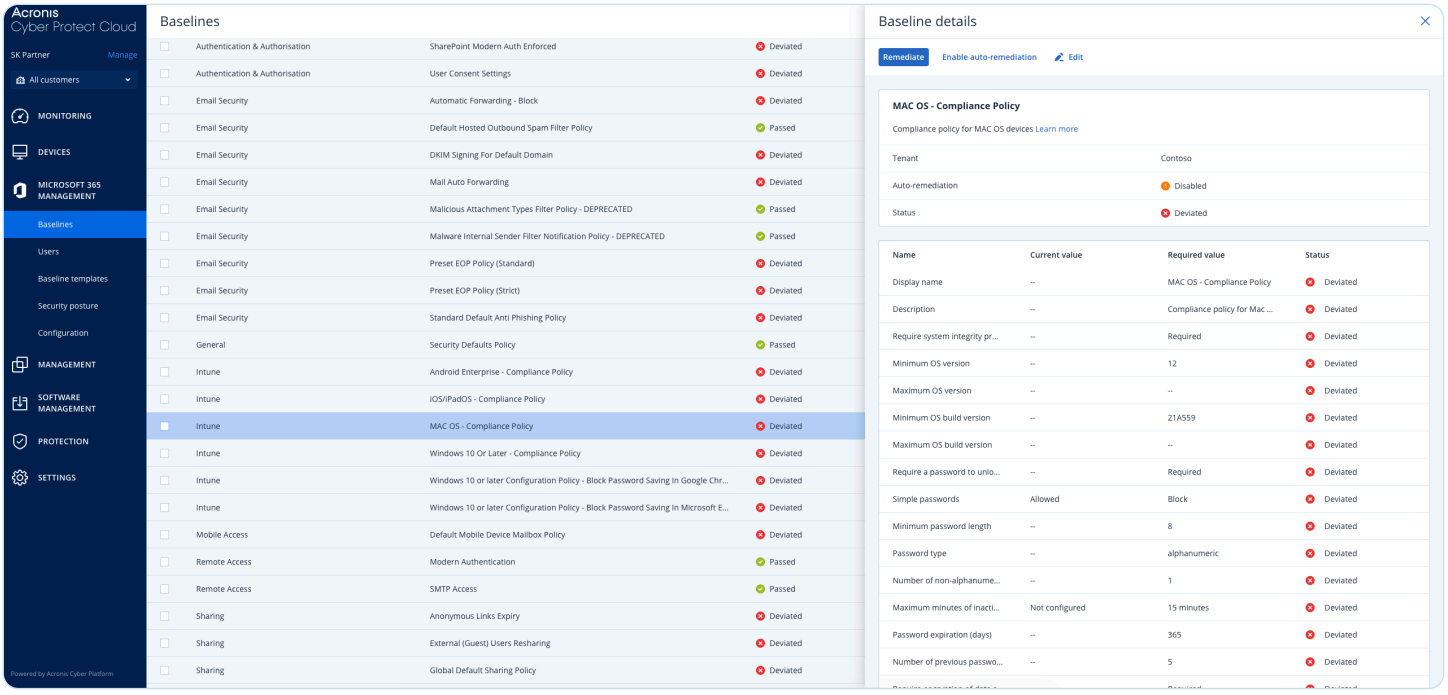
- Evidencia de auditoría faltante o incompleta.
- Preparación deficiente para la investigación.

Controles de seguridad para reducir el riesgo

- Mantener habilitada la auditoría de Microsoft Purview.
- Asegurarse de que los investigadores tengan el acceso adecuado.
- Mantener la preparación para la búsqueda de auditorías.

Cómo ayuda Acronis SPM

- Ayuda a los MSP a supervisar la postura de configuración relacionada con la auditoría.
- Detecta desviaciones en la configuración de registro y auditoría.
- Admite la investigación continua y la preparación para el cumplimiento normativo.



Copyright © 2003-2026 Acronis International GmbH.

Qué tienen en común estos ataques

En todos los incidentes:

- El ingreso se basa en la identidad.
- La persistencia se basa en la configuración.
- El impacto afecta a todo el inquilino.
- Los controles de endpoints tradicionales ofrecen una visibilidad limitada.

Por qué es importante la administración continua de la postura

Los ataques modernos a Microsoft 365 tienen éxito cuando sucede lo siguiente:

- Las configuraciones incorrectas persisten.
- La postura de seguridad se desvía con el tiempo.
- Las brechas de visibilidad pasan desapercibidas en todos los inquilinos.

Cómo ayuda Acronis SPM a los MSP a reducir el riesgo

- Administra centralizadamente la postura de Microsoft 365 en todos los inquilinos.
- Supervisa continuamente la postura de seguridad con respecto a los criterios de referencia.
- Detecta automáticamente nuevos riesgos y desviaciones de configuración.
- Aplica plantillas de referencia reutilizables.
- Automatiza y optimiza la corrección.
- Simplifica los flujos de trabajo de incorporación y salida.
- Estandariza la postura de seguridad de Microsoft 365 a escala.

Cuando la prevención no basta: recupere Entra ID

La administración de la postura de seguridad ayuda a reducir el riesgo de identidad. El backup ofrece una ruta de recuperación cuando un ataque, una eliminación accidental o una configuración incorrecta interrumpe el plano de control de identidad.

Por qué importa la recuperación de Entra ID

Entra ID controla quién puede acceder a Microsoft 365 y a las aplicaciones conectadas. Los atacantes pueden modificar o eliminar usuarios, grupos, roles, políticas y configuraciones para ampliar privilegios, mantener la persistencia o interrumpir el acceso.

Restaurar solo los datos de Microsoft 365 puede no bastar para recuperar el acceso seguro a ellos. Las organizaciones también necesitan una forma confiable de recuperar las identidades, la configuración y las relaciones de las que depende su entorno.

Cómo ayuda Acronis Entra ID Backup

- Proteja los usuarios, grupos, roles, políticas y configuraciones críticos de Entra ID.
- Recupere objetos de identidad eliminados o comprometidos y sus relaciones.
- Revierta los cambios no deseados tras ataques o errores administrativos.
- Reduzca el downtime sin depender solo de la retención y la recuperación nativas.
- Administre la protección de datos e identidades de Microsoft 365 desde la plataforma de Acronis.

Copyright © 2003-2026 Acronis International GmbH.

Fortalezca la resiliencia de identidad

Combine la gestión proactiva de la postura con backups recuperables de Entra ID y ayude a sus clientes a prevenir ataques de identidad, limitar su impacto y recuperarse más rápido.



Explore Acronis Entra ID Backup

CONOCER MÁS

Explore cómo Acronis SPM ayuda a los MSP a proteger Microsoft 365 a escala

Escanee para reservar una demostración de Acronis SPM



Copyright © 2003-2026 Acronis International GmbH. Reservados todos los derechos. Acronis y el logotipo de Acronis son marcas comerciales de Acronis International GmbH en los Estados Unidos u otros países. Todas las demás marcas comerciales o registradas son propiedad de sus respectivos propietarios. Reservado el derecho a realizar modificaciones técnicas y diferencias respecto de las ilustraciones; excepto error u omisión. 2026-10