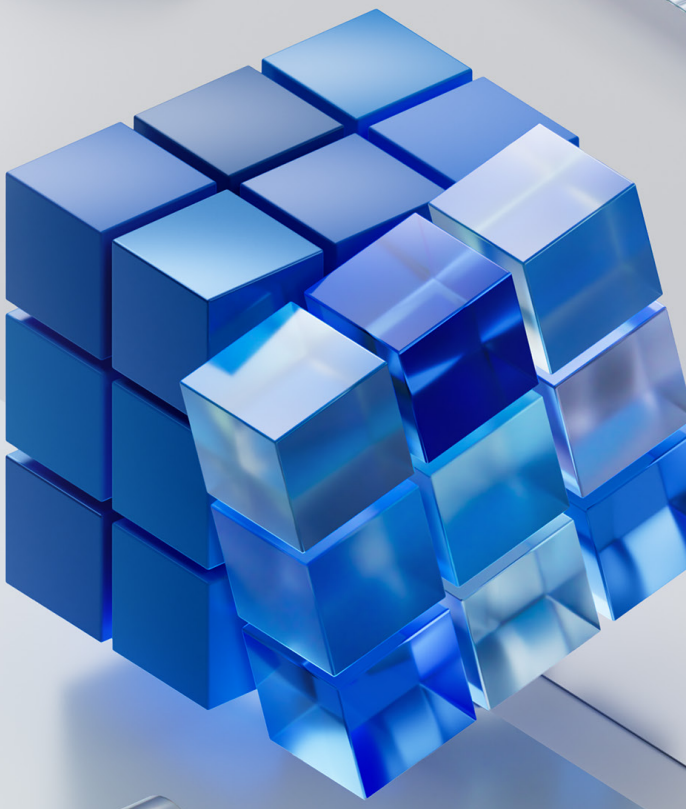
Acronis

Ataques contra la identidad y el plano de control de Microsoft 365



9 amenazas reales, qué vulnerabilidades aprovechan y cómo los MSP pueden reducir el riesgo gracias a Acronis SPM

Los ataques modernos contra 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, los atacantes utilizaron flujos de autenticación legítimos, permisos excesivos, controles de acceso débiles y configuraciones incorrectas para obtener acceso persistente a inquilinos de Microsoft 365.

Esta lista de comprobación resume:

- Las técnicas de ataque empleadas en incidentes reales.
- Las vulnerabilidades que aprovecharon los atacantes.
- Los controles de Microsoft 365 recomendados para reducir el riesgo.
- Cómo Acronis SPM ayuda a los MSP a supervisar y aplicar de forma continua una postura de seguridad adecuada en todos los inquilinos.

1. Ataques de difusión de contraseñas

Incidente real

Midnight Blizzard (2024).

Técnica de ataque

Ataque de difusión de contraseñas ("password spraying") contra una cuenta heredada de un inquilino y sin uso en producción.

Cuál fue el factor de riesgo

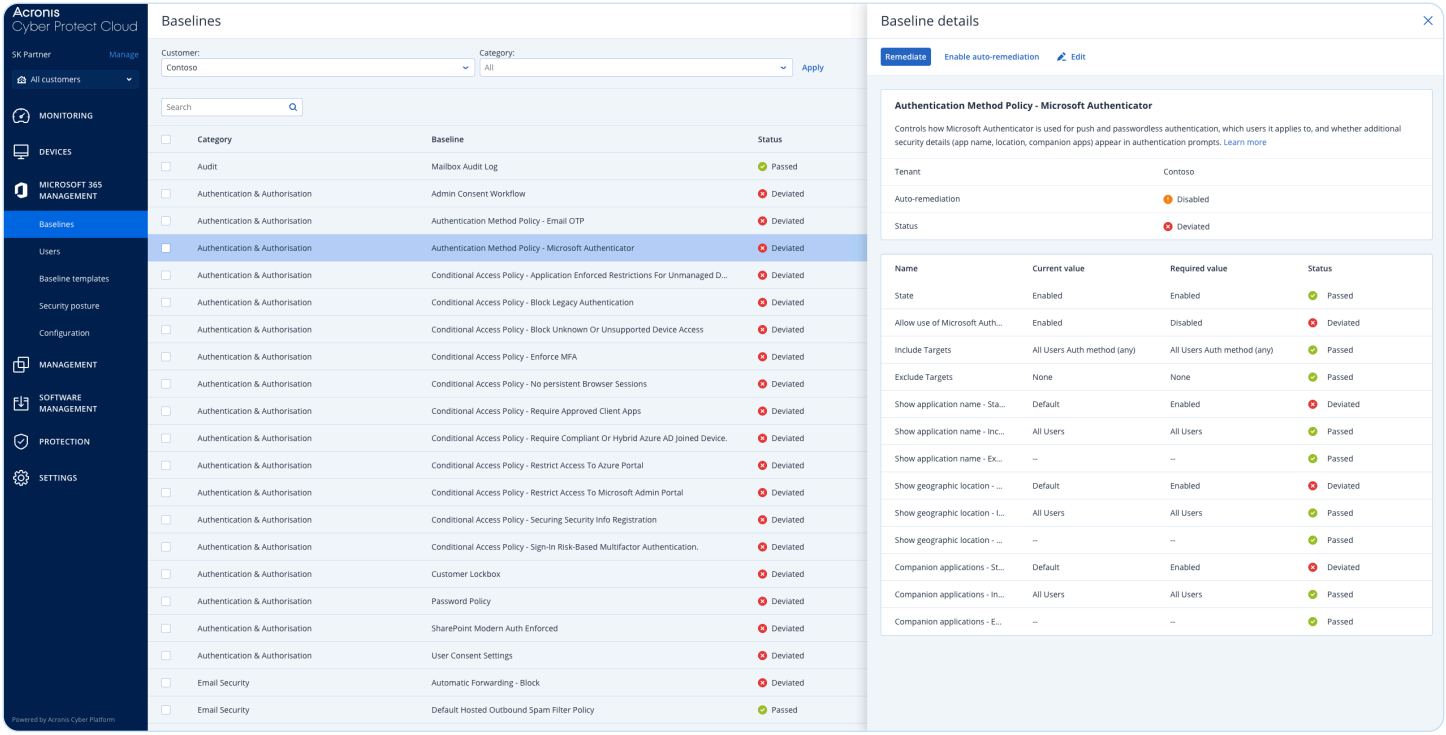
- Credenciales débiles.
- Ausencia de autenticación multifactor (MFA) en una cuenta heredada.

Controles de seguridad para reducir el riesgo

- Aplicar la MFA.
- Eliminar las contraseñas débiles.
- Deshabilitar las rutas de autenticación heredadas.
- Supervisar anomalías de inicio de sesión.

Cómo ayuda Acronis SPM

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



2. Falsificación de tokens y abuso de sesiones

Incidente real

Storm-0558 (2023).

Técnica de ataque

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

Cuál fue el factor de riesgo

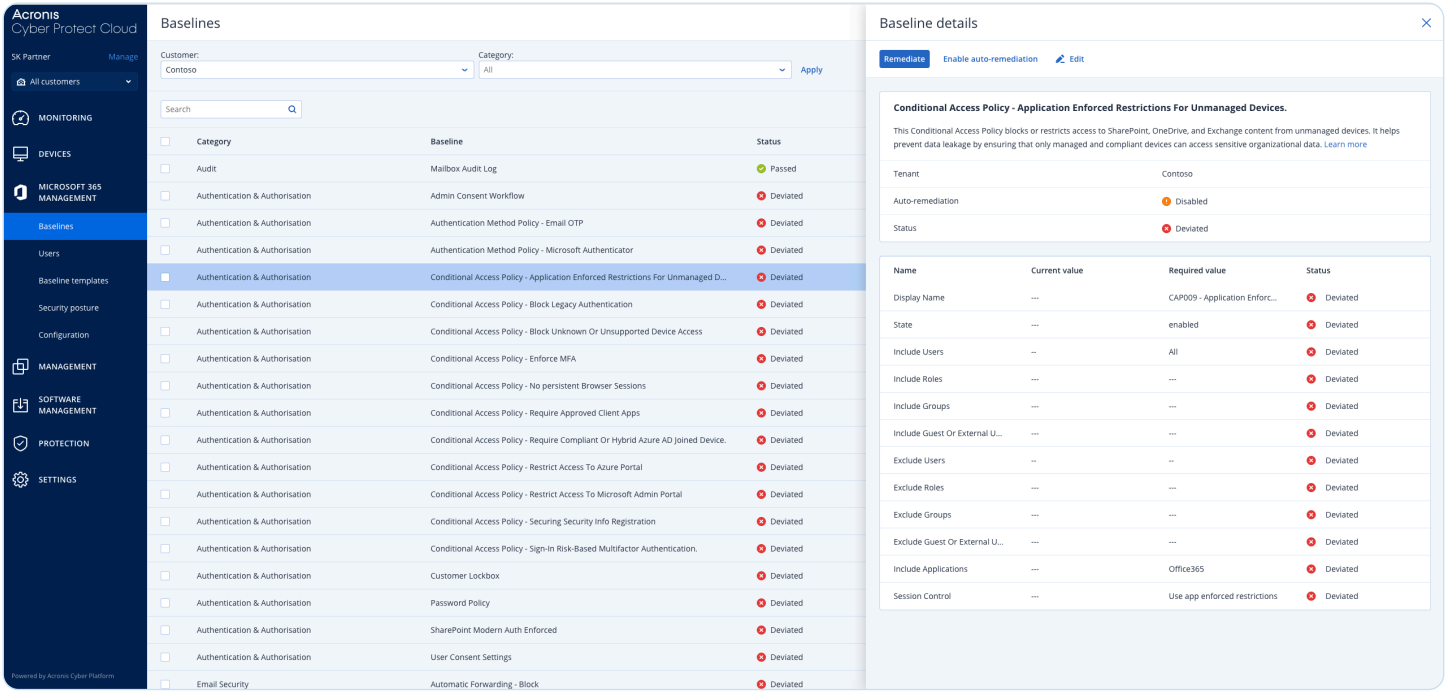
- Deficiencias en la validación de tokens.
- Uso indebido de claves de firma.
- Visibilidad limitada ante el uso anómalo de tokens.

Controles de seguridad para reducir el riesgo

- Reforzar la postura de identidad.
- Aplicar la MFA y el Acceso Condicional.
- Restringir el consentimiento de aplicaciones.
- Proteger el acceso con privilegios.
- Supervisar anomalías en tokens y sesiones.

Cómo ayuda Acronis SPM

- Contribuye a estandarizar la postura de la MFA y el Acceso Condicional.
- Identifica desviaciones en la configuración de identidad.
- Ayuda a aplicar estándares de referencia seguros para el acceso administrativo.
- Reduce la exposición de identidad en inquilinos adyacentes.



3. Secuestro de sesiones y phishing AiTM

Incidente real

Varios incidentes reales.

Técnica de ataque

Robo de cookies de sesión mediante phishing con proxy inverso.

Cuál fue el factor de riesgo

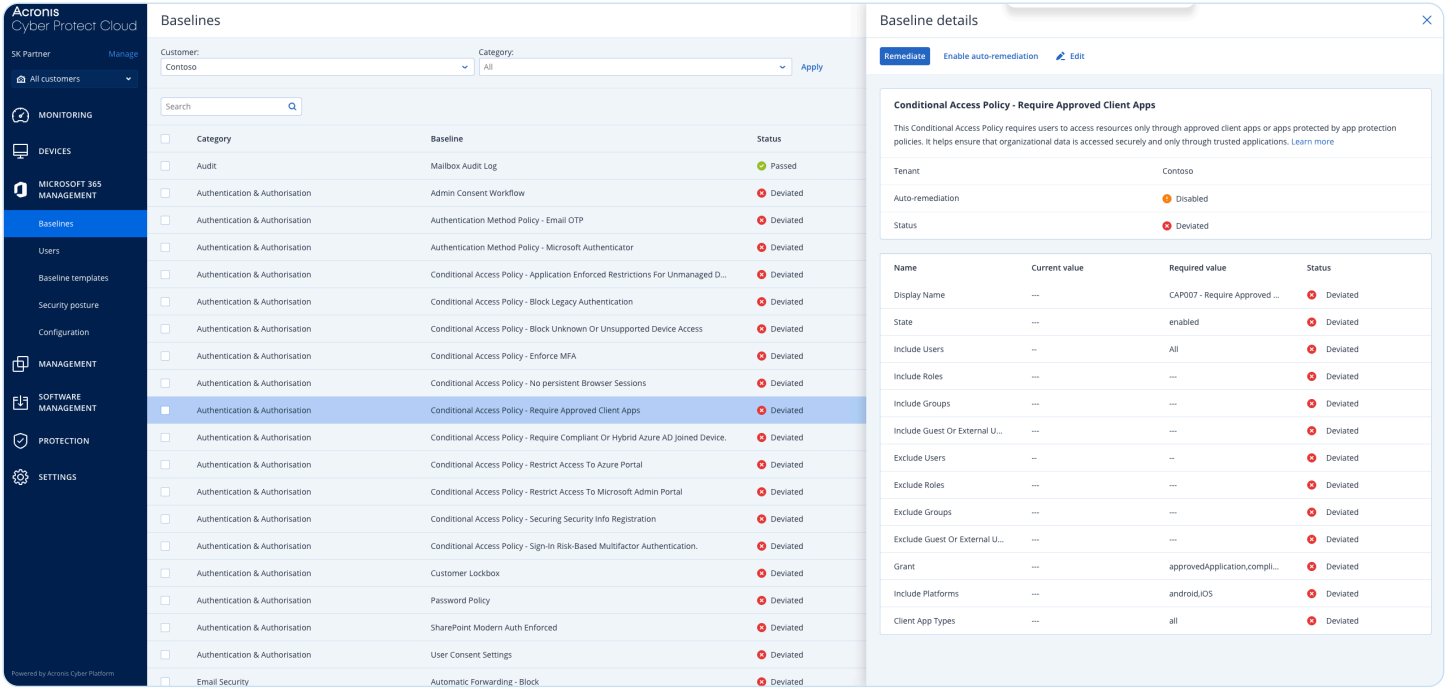
- Cookies de sesión autenticada sustraídas.
- Aplicación insuficiente de Acceso Condicional.
- Ausencia de restricciones de acceso basadas en dispositivos.

Controles de seguridad para reducir el riesgo

- Exigir dispositivos conformes o administrados.
- Aplicar el Acceso Condicional.
- Supervisar cualquier comportamiento anómalo de sesiones.
- Utilizar la "Evaluación continua de accesos" cuando esté disponible.

Cómo ayuda Acronis SPM

- Detecta desviaciones en la postura de Acceso Condicional.
- Contribuye a mantener estándares de referencia seguros para las directivas de acceso.
- Facilita la estandarización de los controles de identidad y acceso por dispositivo en todos los inquilinos.



4. Ataques de repetición de tokens

Incidente real

Varios incidentes reales.

Técnica de ataque

Reutilización de Primary Refresh Tokens sustraídos.

Cuál fue el factor de riesgo

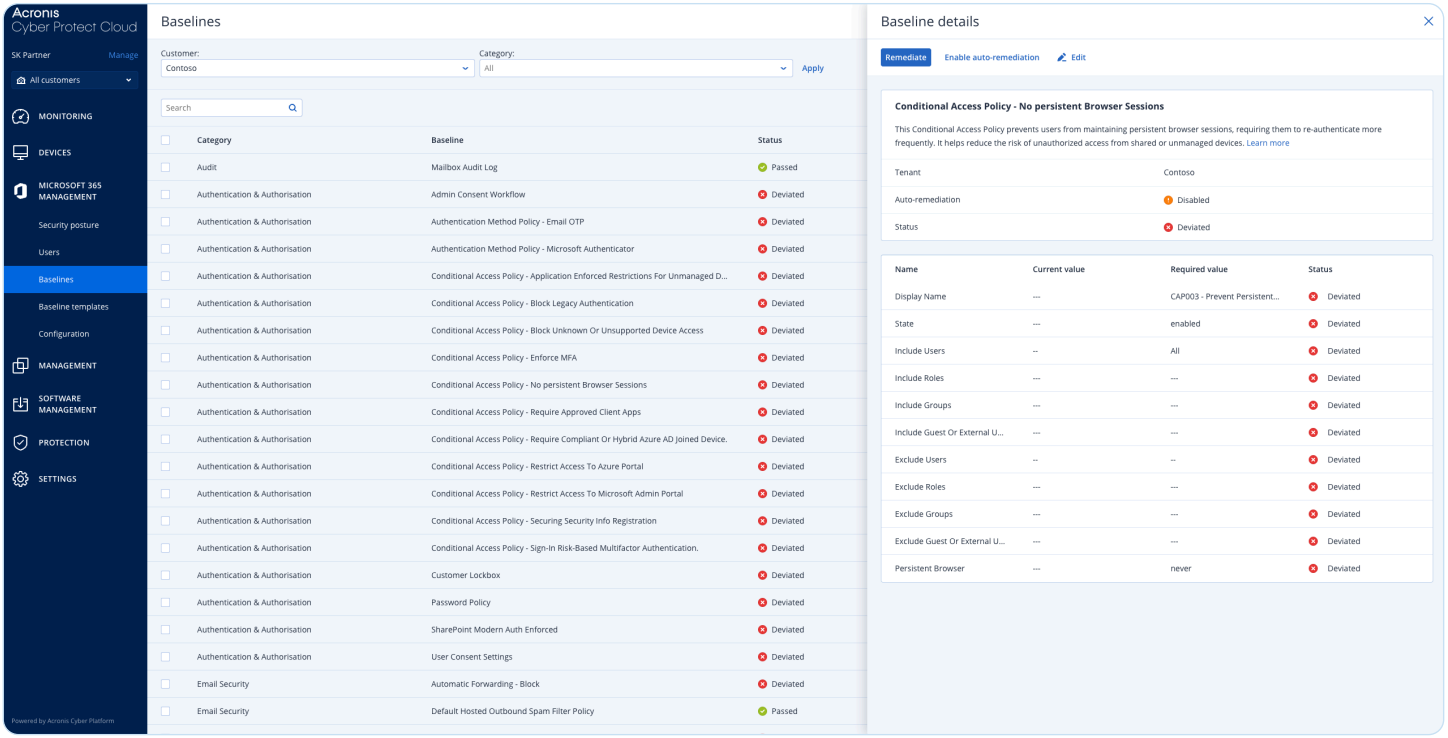
- Falta de protección de tokens y sesiones.
- Aplicación insuficiente de controles de sesión.

Controles de seguridad para reducir el riesgo

- Aplicar Token Protection cuando esté disponible.
- Utilizar controles de sesión de Acceso Condicional.
- Restringir el acceso desde dispositivos sin gestionar.

Cómo ayuda Acronis SPM

- Ayuda a los MSP a supervisar de forma continua la postura de autenticación.
- Detecta desviaciones en los estándares de referencia de Acceso Condicional y configuración de sesiones.
- Facilita la aplicación de estándares de referencia seguros para identidades y accesos.



5. Phishing de consentimiento OAuth

Incidente real

Varios incidentes reales.

Técnica de ataque

Concesión de consentimiento a aplicaciones maliciosas.

Cuál fue el factor de riesgo

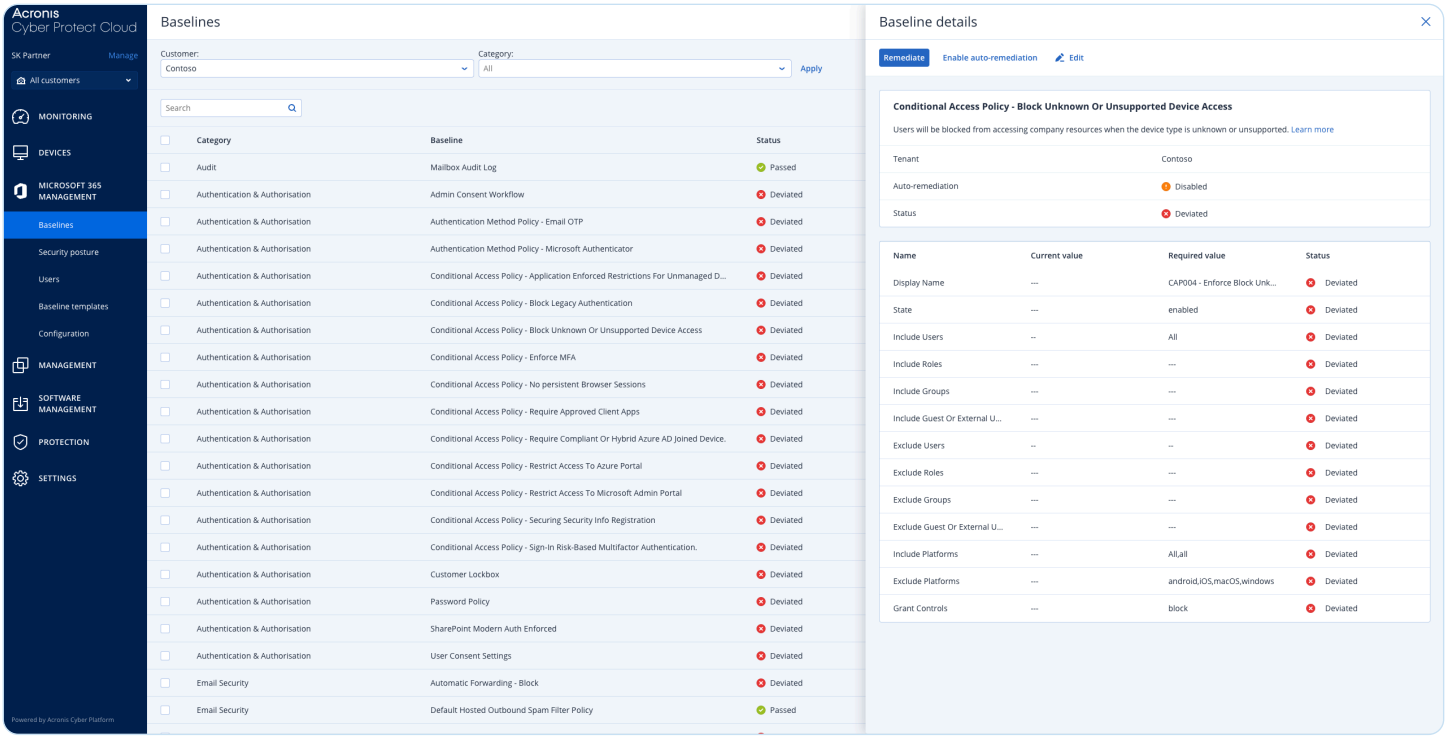
- Consentimiento de usuario sin restricciones.
- Gobernanza insuficiente de aplicaciones.

Controles de seguridad para reducir el riesgo

- Restringir el consentimiento de usuario.
- Exigir aprobación administrativa para las aplicaciones.
- Permitir solo editores verificados y permisos de bajo riesgo.

Cómo ayuda Acronis SPM

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



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

Incidente real

Varios incidentes reales.

Técnica de ataque

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

Cuál fue el factor de riesgo

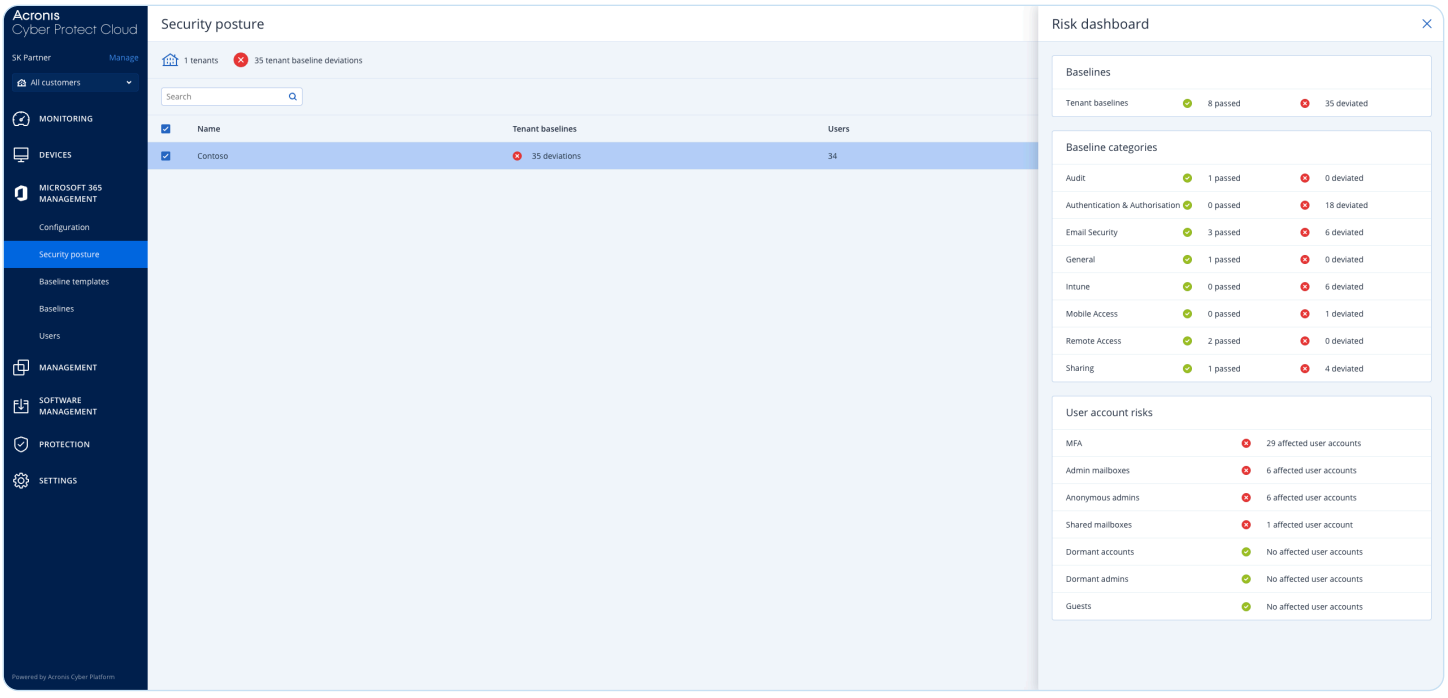
- Permisos excesivos en Graph.
- Visibilidad insuficiente del comportamiento de las aplicaciones.
- Acceso a aplicaciones sin gestionar.

Controles de seguridad para reducir el riesgo

- Auditar periódicamente los permisos de las aplicaciones.
- Investigar actividad inusual en Graph.
- Revisar las aplicaciones autorizadas por usuarios externos.

Cómo ayuda Acronis SPM

- Ayuda a mantener la gobernanza sobre los permisos de las aplicaciones y la postura de consentimiento.
- Detecta desviaciones en la autorización y la exposición de aplicaciones sin gestionar.
- Mejora la visibilidad sobre la postura de acceso a aplicaciones en Microsoft 365.



7. Elevación de privilegios y abuso excesivo de roles

Incidente real

Midnight Blizzard sufrió varias elevaciones de privilegios en Entra ID.

Técnica de ataque

Elevación de privilegios mediante roles administrativos permanentes y excesivos.

Cuál fue el factor de riesgo

- Número excesivo de administradores globales.
- Acumulación progresiva de privilegios.
- Gobernanza insuficiente de roles.

Controles de seguridad para reducir el riesgo

- Aplicar el principio de privilegio mínimo.
- Restringir el acceso administrativo permanente.
- Revisar de forma continua los roles con privilegios.

Cómo ayuda Acronis SPM

- Identifica roles administrativos excesivos y exposición de privilegios.
- Ayuda a los MSP a estandarizar una postura segura de roles en todos los inquilinos.
- Facilita la aplicación de estándares de referencia para identidades y autorizaciones.

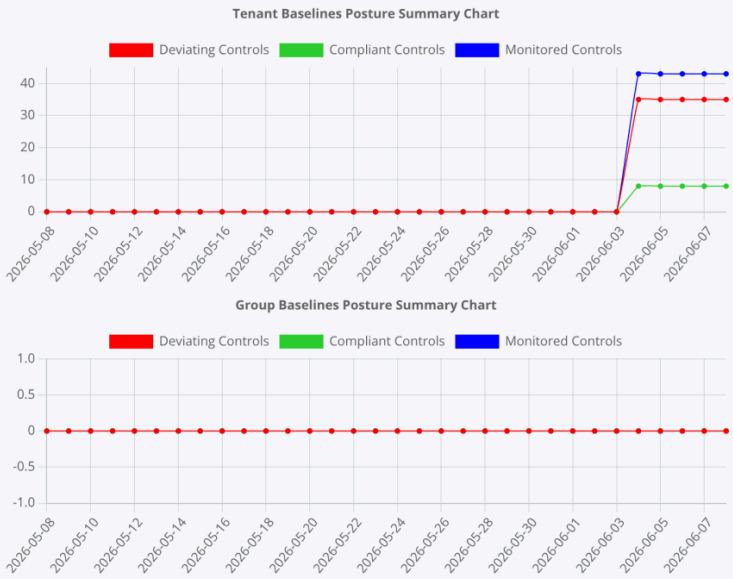
Compliance Posture Summary

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. Exposición en SharePoint y OneDrive

Incidente real

Varios incidentes reales.

Técnica de ataque

Uso excesivo o accidental del uso compartido externo.

Cuál fue el factor de riesgo

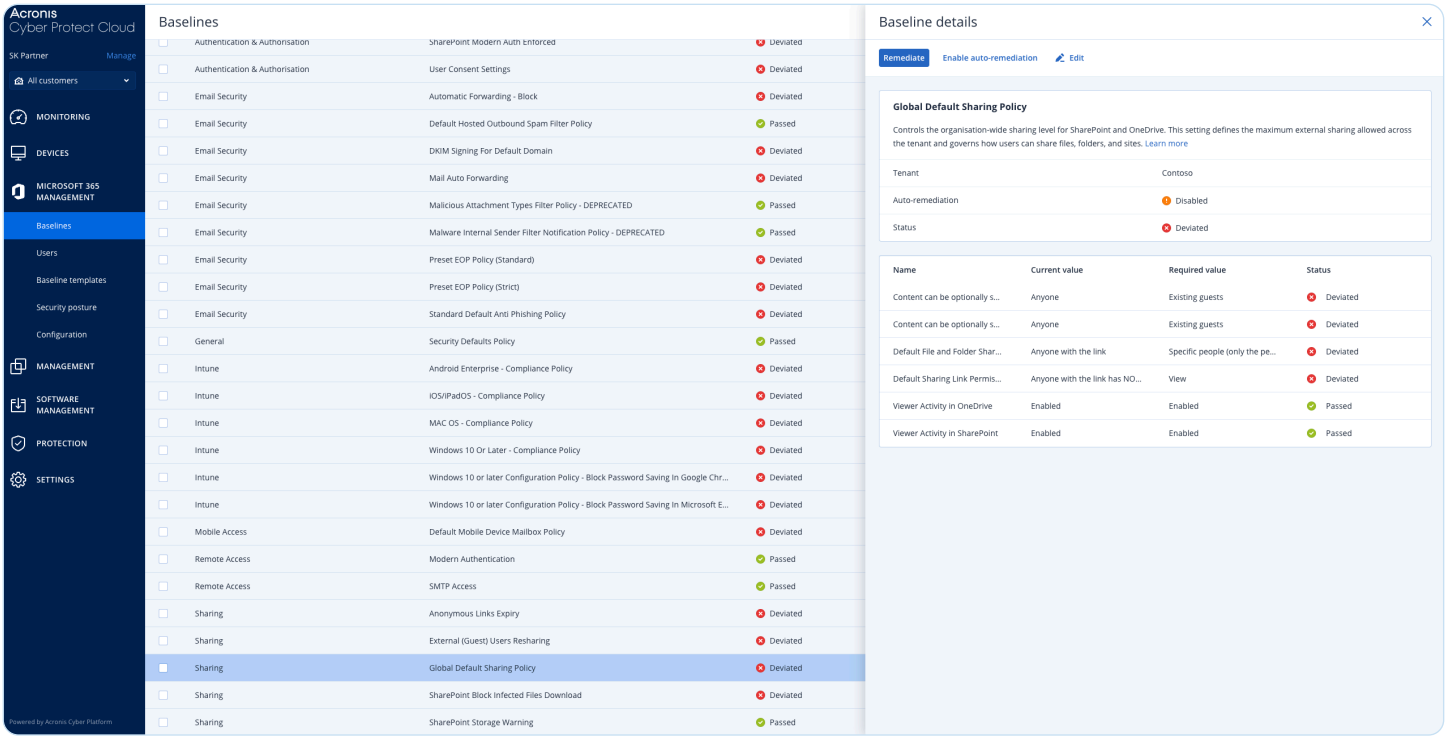
- Gobernanza insuficiente del uso compartido.
- Configuraciones de acceso externo demasiado permisivas.

Controles de seguridad para reducir el riesgo

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

Cómo ayuda Acronis SPM

- Valida de forma continua la postura de uso compartido frente a los estándares de referencia.
- Detecta configuraciones de riesgo en el uso compartido.
- Reduce las desviaciones en la configuración a largo plazo en todos los inquilinos.



9. Brechas en auditorías e investigaciones

Incidente real

Investigaciones de incidentes.

Técnica de ataque

Actividad posterior al compromiso ocultada por una auditoría insuficiente.

Cuál fue el factor de riesgo

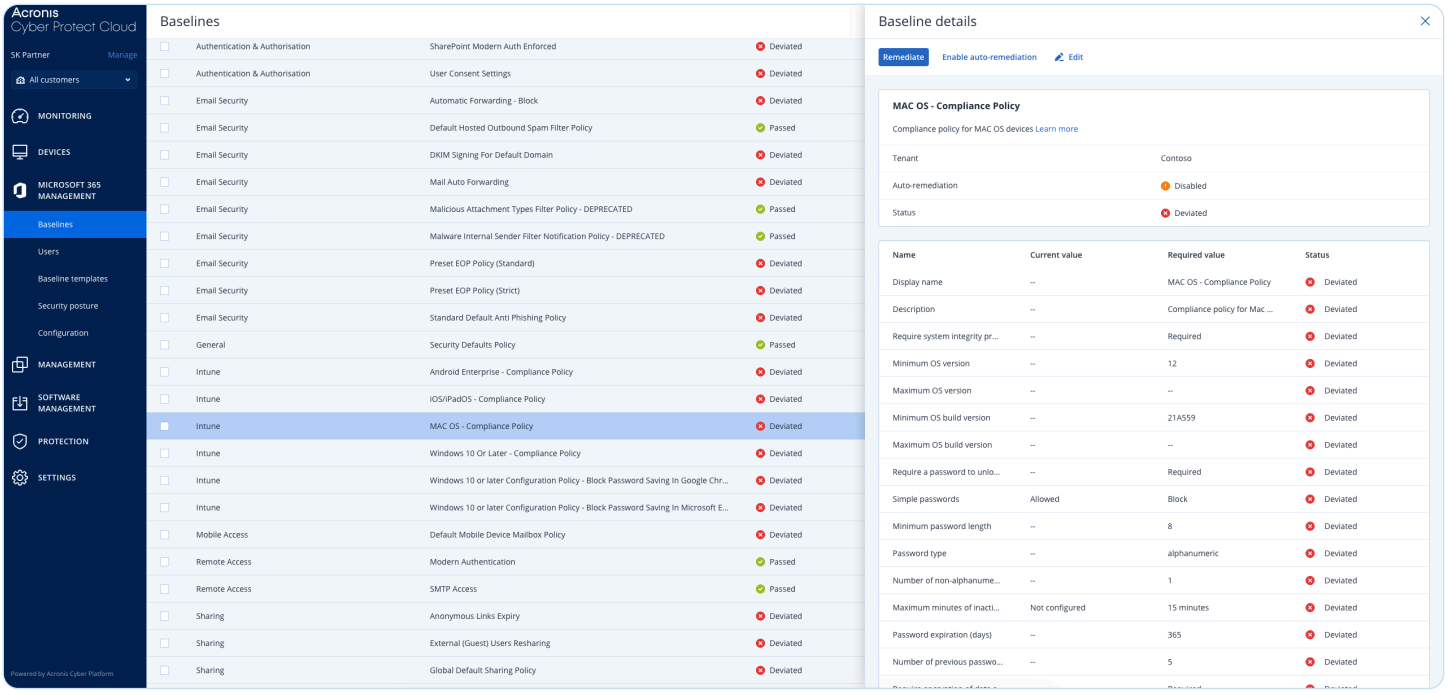
- Evidencias de auditoría ausentes o incompletas.
- Escasa preparación para la investigación.

Controles de seguridad para reducir el riesgo

- Mantener activada la auditoría de Microsoft Purview.
- Garantizar que los investigadores dispongan del acceso adecuado.
- Mantener la preparación para búsquedas de auditoría.

Cómo ayuda Acronis SPM

- Ayuda a los MSP a supervisar la postura de configuración relacionada con las auditorías.
- Detecta desviaciones en la configuración de registros y auditorías.
- Facilita la investigación continua y la preparación para el cumplimiento normativo.



Qué tienen en común estos ataques

En todos los incidentes:

- El acceso se basó en identidades.
- La persistencia dependió de la configuración.
- El impacto afectó a todo el inquilino.
- Los controles tradicionales en los endpoints ofrecían una visibilidad limitada.

Por qué es importante la gestión continua de la postura

Los ataques modernos contra Microsoft 365 tienen éxito cuando:

- Las configuraciones incorrectas persisten.
- La postura de seguridad presenta desviaciones con el tiempo.
- Las brechas de visibilidad pasan desapercibidas entre inquilinos.

Cómo ayuda Acronis SPM a los MSP a reducir el riesgo

- Gestiona de forma centralizada la postura de seguridad de Microsoft 365 en todos los inquilinos.
- Supervise continuamente la postura de seguridad frente a los estándares de referencia.
- Detecta automáticamente nuevos riesgos y desviaciones de configuración.
- Permite aplicar plantillas reutilizables de estándares de referencia.
- Automatiza y agiliza la corrección.
- Simplifica los flujos de incorporación y baja de usuarios.
- Estandariza la postura de seguridad de Microsoft 365 a gran escala.

Descubra cómo Acronis SPM ayuda a los MSP a proteger Microsoft 365 a gran escala

Escanee el código QR para reservar una demostración de Acronis SPM.

Acronis

Más información en acronis.com