Acronis

Microsoft 365 bajo ataque: amenazas contra la identidad y el plano de control

Y cómo Acronis Security Posture Management las identifica y corrige

Introducción

Microsoft 365 se ha convertido en el plano de control de las operaciones empresariales modernas, ya que permite gestionar la identidad, el acceso, la comunicación y los datos en las organizaciones. A medida que ha aumentado su importancia, también lo ha hecho su valor como superficie de ataque principal.

Sin embargo, la naturaleza de los ataques ha cambiado radicalmente.

Las amenazas actuales ya no dependen del malware ni de la vulneración de endpoints. En su lugar, los ciberdelincuentes dirigen sus ataques contra identidades, permisos y configuraciones incorrectas, actuando íntegramente dentro de los servicios legítimos de Microsoft 365. Una sola cuenta de administrador comprometida, un permiso pasado por alto o una directiva de acceso condicional débil puede proporcionar a los atacantes un acceso persistente y de alto impacto sin activar las alertas de seguridad tradicionales.

Este cambio plantea un desafío crítico para los proveedores de servicios gestionados (MSP). Las herramientas de seguridad convencionales suelen ofrecer poca visibilidad sobre estos ataques, mientras que las configuraciones incorrectas y las directivas incoherentes entre inquilinos generan una exposición constante.

El resultado: el riesgo se acumula de forma silenciosa entre los distintos inquilinos.

Esta guía ofrece un recorrido práctico, basado en escenarios reales, sobre cómo se desarrollan los ataques modernos contra Microsoft 365 y cómo Acronis Security Posture Management (SPM) ayuda a los MSP a detectar, prevenir y corregir estos riesgos a gran escala.

La nueva realidad: el ataque ya está en marcha

Imagine que inicia sesión en el inquilino de un cliente. No hay alertas, ni malware, ni señales evidentes de intrusión. Todo parece normal en la superficie, pero eso no significa que el entorno sea seguro.

Es posible que un ciberdelincuente ya tenga acceso a ese inquilino, ya que podría estar utilizando credenciales válidas o tokens persistentes obtenidos mediante ataques de phishing o abuso del consentimiento. Y, lo peor de todo, podría estar operando íntegramente dentro del entorno de Microsoft 365, camuflado entre la actividad legítima y fuera del alcance de los mecanismos de detección tradicionales.

Los ataques modernos no dependen de irrumpir a la fuerza: se desarrollan dentro del plano de control.

Para los MSP, esta nueva realidad cambia el problema de raíz. Ya no se trata solo de detectar amenazas activas, sino de identificar la exposición antes de que los ciberdelincuentes la aprovechen, corregirla de forma coherente en todos los inquilinos y garantizar que esas correcciones permanezcan aplicadas con el paso del tiempo, a medida que los entornos evolucionan.

Esta guía muestra cómo se aborda ese desafío en la práctica gracias a Acronis Security Posture Management (SPM).

Escenario 1:

Difusión de contraseñas ("password spraying")

"No parece haber nada extraño, pero una cuenta acaba de entrar".

Los atacantes no necesitan irrumpir en un entorno a la fuerza: tan solo les basta con iniciar sesión. Al probar contraseñas comunes en numerosas cuentas, evitan bloqueos y acaban obteniendo acceso a alguna. Con credenciales válidas, pueden acceder a buzones de correo y archivos, y actuar como un usuario legítimo.

Por lo general, no hay alertas, ni malware, ni señales claras: solo actividad aparentemente normal.

Acronis SPM cambia el enfoque de la detección a la exposición. Destaca riesgos como la ausencia de la autenticación multifactor (MFA), la autenticación heredada habilitada y las configuraciones de identidad que no cumplen con las mejores prácticas.

A partir de ahí, usted evalúa el inquilino, aplica la MFA, deshabilita la autenticación heredada y aplica estos controles en todos los inquilinos mediante plantillas de estándares de referencia. La supervisión continua garantiza que cualquier desviación se detecte y se corrija.

En lugar de investigar una cuenta comprometida, elimina las condiciones que hicieron posible el ataque.

Lo que usted suele hacer (en la plataforma)

1. **Ejecutar una auditoría bajo demanda**
   - Evaluar al instante el inquilino frente a los estándares de referencia de seguridad.
   - Identificar debilidades de autenticación.
2. **Aplicar la corrección según el estándar de referencia**
   - Habilitar la MFA en todos los usuarios.
   - Deshabilitar la autenticación heredada.
3. **Automatizar la corrección en todos los inquilinos**
   - Utilizar plantillas de estándares de referencia.
   - Propagar las directivas a todos los clientes.
4. **Habilitar la supervisión continua**
   - Acronis SPM detecta de forma continua cualquier desviación respecto a los estándares de referencia.
   - Acronis SPM genera alertas cuando se crean nuevos usuarios sin protección.

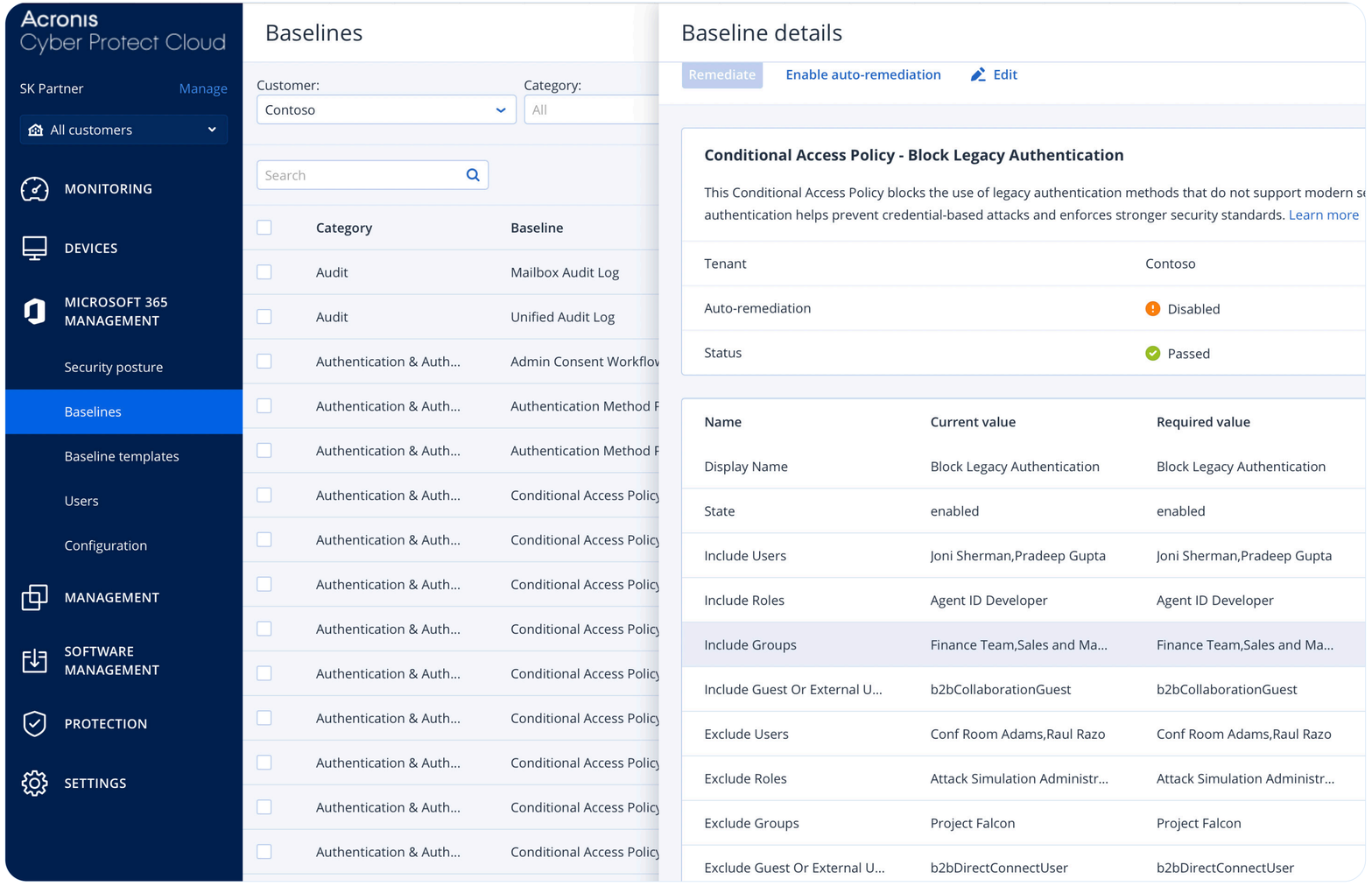
Resultado inmediato de sus acciones

Usted no investiga un inicio de sesión sospechoso.

Usted:

- Identifica brechas sistémicas de identidad.
- Las corrige una sola vez.
- Las aplica en todos los entornos.
- Se asegura de que no reaparezcan.

Acronis SPM elimina las condiciones que permiten que los ataques de difusión de contraseñas logren su objetivo a gran escala.



Escenario 2:

Abuso del consentimiento OAuth

"Los atacantes ya no necesitan al usuario".

Un usuario aprueba sin saberlo una aplicación OAuth maliciosa. A partir de ese momento, el atacante ya no necesita credenciales. Obtiene acceso persistente, a nivel de API, al correo electrónico y a los archivos a través de Microsoft Graph, normalmente sin activar ninguna alerta.

Ningún inicio de sesión se ha visto comprometido, y no hay ninguna actividad de autenticación sospechosa: todo parece legítimo.

Acronis SPM expone esta capa oculta. Proporciona visibilidad sobre todas las aplicaciones OAuth en todos los inquilinos, los permisos que se les han concedido, como Mail.Read o Files.Read.All, y destaca las aplicaciones desconocidas o de riesgo.

A partir de ahí, es posible identificar con rapidez las aplicaciones con privilegios elevados o recién añadidas, revocar sus permisos y eliminar cualquier acceso no autorizado. A continuación, las directivas pueden estandarizarse al restringir el consentimiento de los usuarios y exigir la aprobación administrativa, mientras que la automatización garantiza que estos controles se apliquen en todos los inquilinos.

En lugar de perseguir amenazas basadas en la identidad, se descubre y se elimina el acceso persistente en la capa de aplicación y se evita que vuelva a producirse.

Lo que usted suele hacer (en la plataforma)

1 **Identificar aplicaciones de riesgo**
- Filtrar aplicaciones con permisos elevados.
- Detectar aplicaciones desconocidas o recién añadidas.

2 **Aplicar medidas correctivas de inmediato**
- Revocar directamente los permisos de las aplicaciones.
- Eliminar integraciones no autorizadas.

3 **Estandarizar la directiva**
- Restringir el consentimiento de los usuarios.
- Exigir la aprobación administrativa.

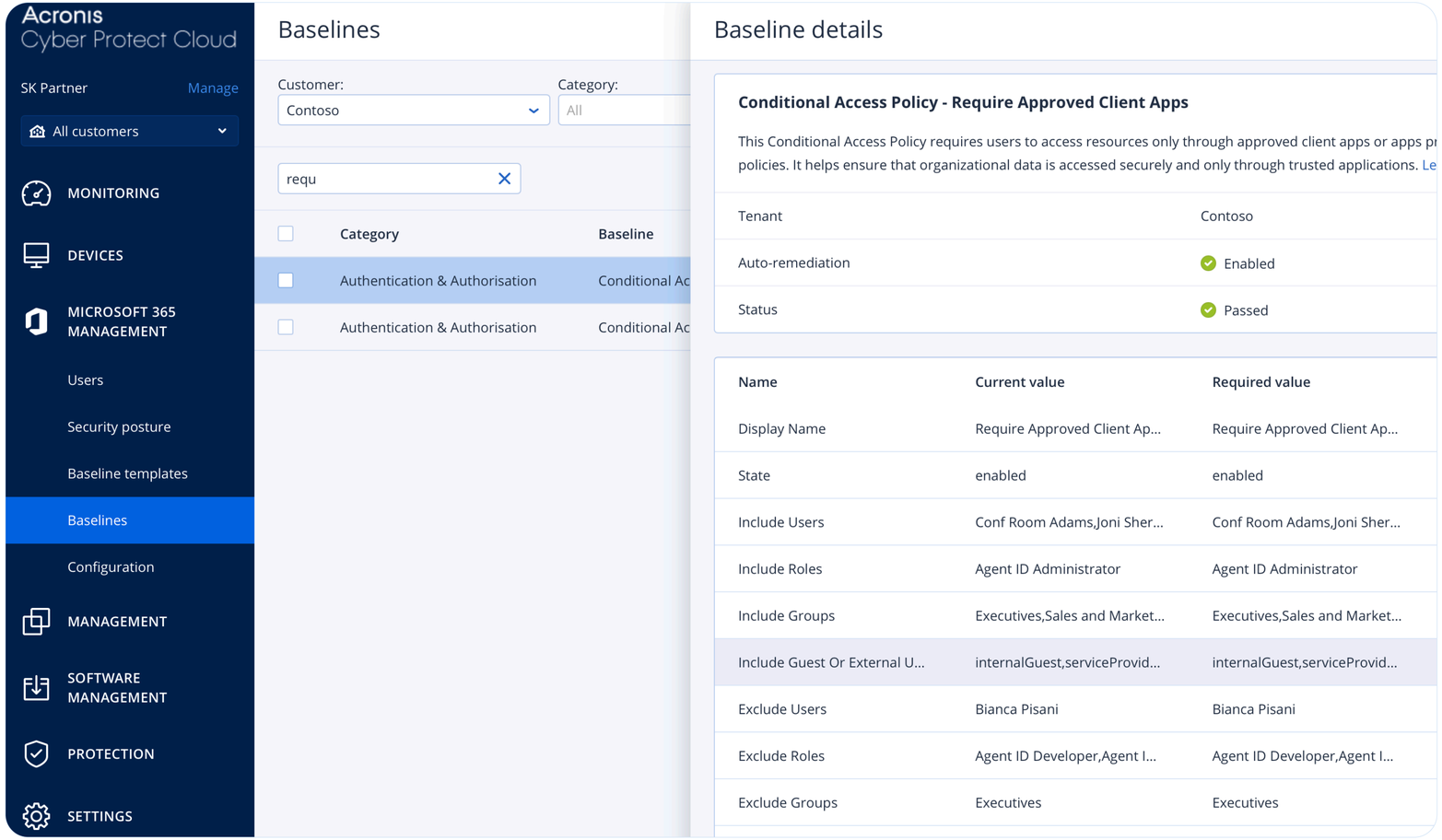
4 **Automatizar la aplicación de controles**
- Aplicar las directivas de gobernanza de aplicaciones en todos los inquilinos.
- Detectar automáticamente nuevas aplicaciones de riesgo.

Resultado inmediato de sus acciones

Usted:

- Detecta un mecanismo de persistencia que elude la identidad.
- Lo elimina de inmediato.
- Impide que vuelva a aparecer.

Acronis SPM proporciona visibilidad y control sobre la capa de aplicación de la que dependen los atacantes para mantener acceso a largo plazo.



Escenario 3:

Phishing basado en códigos de dispositivo

"La MFA funcionó y, aun así, el atacante consiguió entrar".

Un usuario completa un inicio de sesión legítimo de Microsoft y supera la MFA, pero el atacante captura el token de autenticación. Con él, obtiene acceso persistente, lee correos electrónicos y crea reglas de buzón, todo ello sin activar alertas evidentes.

No hay inicios de sesión fallidos, y la MFA parece haber funcionado correctamente.

Acronis SPM revela el problema real: brechas en las directivas. Destaca directivas de acceso condicional débiles o ausentes, falta de controles de sesión y configuraciones de identidad que no cumplen con los estándares de referencia recomendados.

A partir de ahí, usted aplica un acceso condicional más estricto, impone restricciones de sesión y estandariza estos controles en todos los inquilinos. La supervisión continua garantiza que cualquier desviación se detecte y se corrija.

En lugar de detectar el uso indebido de tokens, usted elimina las condiciones que lo permiten.

Lo que usted suele hacer (en la plataforma)

1. **Comprobar el cumplimiento de los estándares de referencia**
   - Comparar las directivas del inquilino con las mejores prácticas.
2. **Aplicar controles de identidad**
   - Reforzar el acceso condicional.
   - Aplicar restricciones de sesión.
3. **Automatizar la corrección**
   - Aplicar las directivas en todos los inquilinos.
   - Corregir automáticamente cualquier desviación.
4. **Aplicar de forma continua los controles**
   - Acronis SPM supervisa cualquier desviación de las directivas.
   - Acronis SPM señala cualquier debilitamiento de los controles.

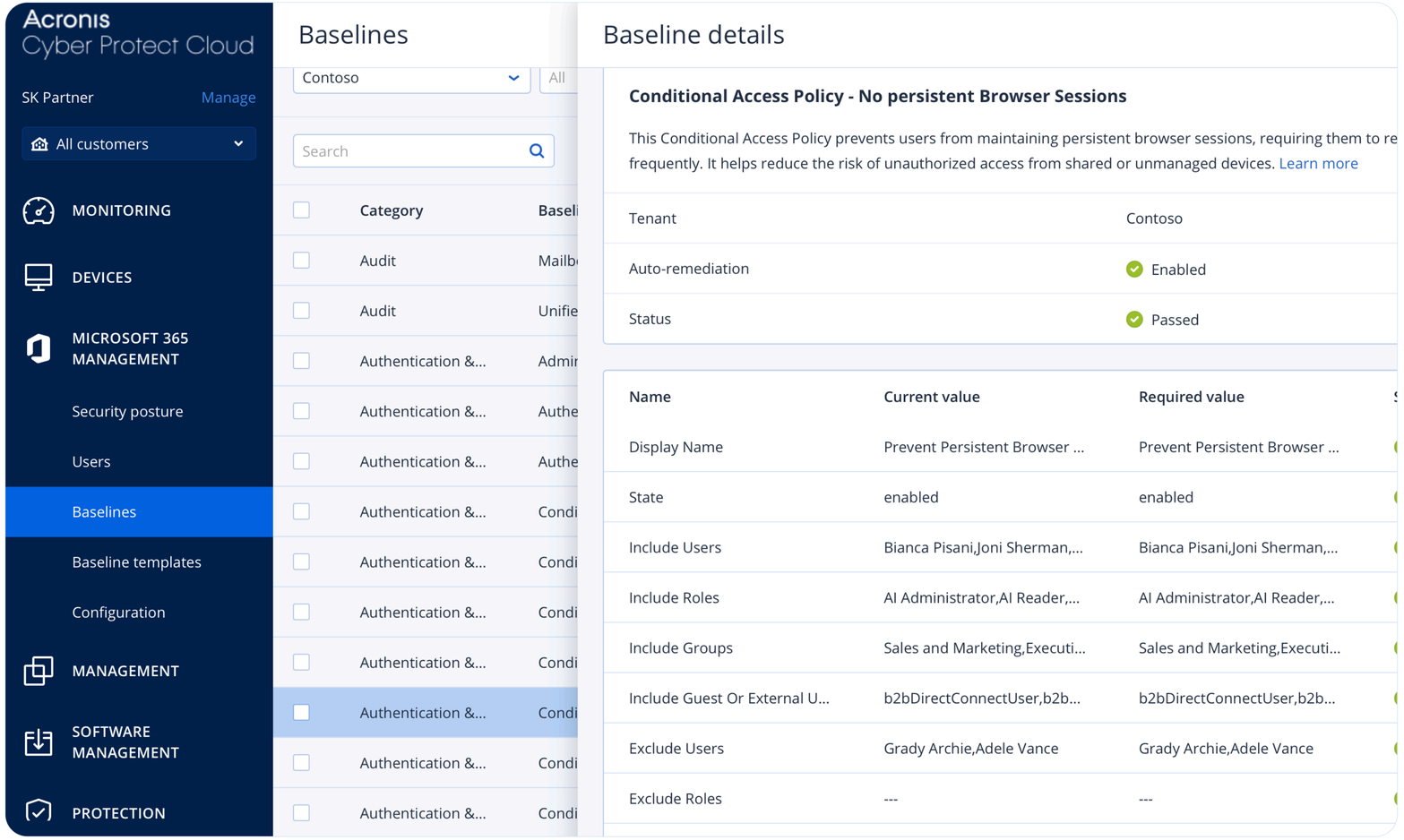
Resultado inmediato de sus acciones

Usted no detecta el robo de tokens.

Usted:

- Cierra las brechas en la directiva que lo permiten.
- Estandariza los controles en todos los inquilinos.
- Garantiza la aplicación de controles a largo plazo.

Acronis SPM protege los flujos de autenticación, no solo las identidades.



Escenario 4:

Elevación de privilegios

"Una sola cuenta comprometida se convierte en el control completo del inquilino".

Un atacante compromete una sola cuenta y empieza a explorar. Encuentra privilegios excesivos, varios administradores globales y una separación de roles deficiente. A partir de ahí, elevar privilegios es fácil y da lugar al control total del inquilino.

Por lo general, no hay alertas. La acumulación de privilegios ocurre de forma gradual y, sin visibilidad centralizada, el riesgo pasa desapercibido.

Acronis SPM expone esta situación con claridad: muestra los roles de administrador en todos los inquilinos, identifica cuentas con privilegios excesivos y asigna el nivel de riesgo según la exposición.

Lo que usted suele hacer (en la plataforma)

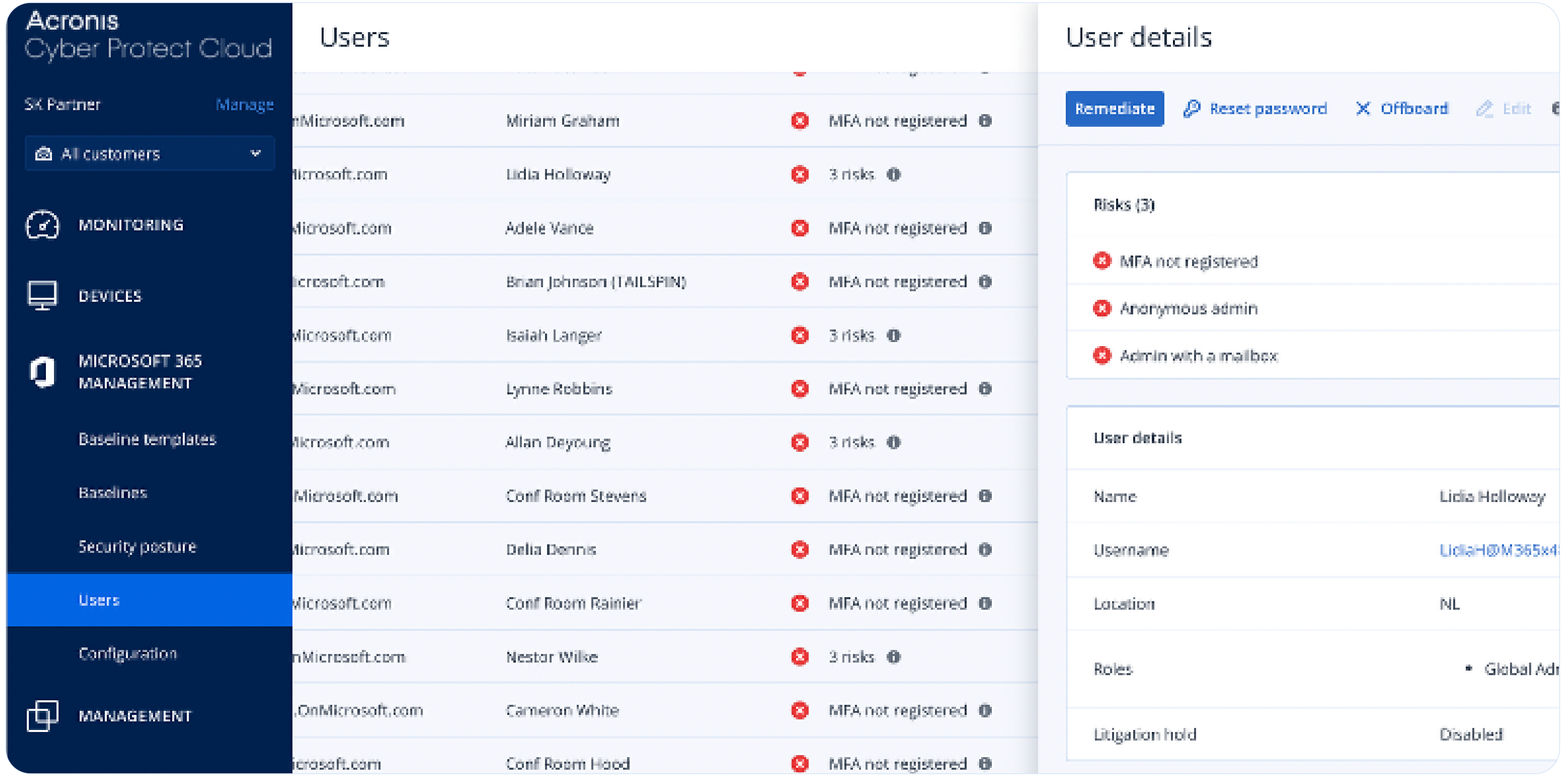
1. **Auditar los roles con privilegios**
   - Identificar cuentas con privilegios administrativos excesivos.
2. **Aplicar el principio de privilegio mínimo**
   - Reducir el número de administradores globales.
   - Estandarizar la asignación de roles.
3. **Automatizar la aplicación de las directivas en todos los inquilinos**
   - Usar plantillas de estándares de referencia para aplicar directivas de roles.
4. **Mantener el control del ciclo de vida**
   - Asignar los roles correctos durante la incorporación de usuarios.
   - Revocar accesos, sesiones y licencias durante la baja de usuarios.

Resultado inmediato de sus acciones

Usted:

- Reduce el radio de impacto de la vulneración.
- Estandariza los privilegios en todos los entornos.
- Garantiza la seguridad del ciclo de vida de las identidades.

Acronis SPM convierte la dispersión de privilegios en una directiva controlada y aplicable.



Puede auditar los roles con privilegios, reducir el número de administradores globales y aplicar directivas de privilegio mínimo en todos los inquilinos mediante plantillas de estándares de referencia. El control continuo del ciclo de vida garantiza el acceso correcto durante la incorporación de usuarios y la revocación completa durante la baja de usuarios.

En lugar de reaccionar ante una elevación de privilegios, se limita el radio de impacto desde el principio.

El factor común en todos estos ataques

En cada escenario:

Ataque	Causa raíz
Difusión de contraseñas	Controles de identidad débiles
Abuso de OAuth	Configuraciones incorrectas de permisos de aplicaciones
Phishing basado en códigos de dispositivo	Brechas en las directivas
Elevación de privilegios	Permisos excesivos

El patrón

La entrada equivale a la identidad.

La persistencia equivale a la configuración.

El impacto equivale al alcance en todos los inquilinos.

Cómo Acronis SPM marca la diferencia

Acronis SPM no solo muestra el riesgo.

Permite a los MSP gestionar la seguridad a gran escala.

Supervisión continua

- Detección continua (24/7) de desviaciones en la postura de seguridad.
- Identificación en tiempo real de nuevos riesgos.

Seguridad basada en estándares de referencia

- Estándares de referencia predefinidos con prácticas recomendadas.
- Plantillas personalizadas de estándares de referencia.
- Estandarización en todos los inquilinos.

Corrección automatizada y manual

- Corrección de problemas directamente en la consola.
- Corrección automatizada de riesgos recurrentes.
- Eliminación de trabajo manual repetitivo.

Administración multiinquilino

- Control centralizado en todos los clientes.
- Propagación de directivas a gran escala.

Control total del ciclo de vida de las identidades

- Incorporación segura de usuarios con directivas y roles correctos.
- Baja segura de usuarios con revocación de sesiones y limpieza.

Integración operativa

- Integración con herramientas de PSA.
- Flujos de trabajo optimizados para los equipos de MSP.

Reflexión final

Los ataques modernos contra Microsoft 365 tienen éxito porque:

- Nadie ve la exposición.
- Nadie la corrige de forma coherente.
- Nadie aplica controles de forma continua.

Acronis SPM cambia por completo ese panorama.

Permite a los MSP:

- Ver el riesgo en todos los inquilinos.
- Corregirlo al instante.
- Aplicar directivas automáticamente.
- Mantener las directivas aplicadas a lo largo del tiempo.

Security Posture Management: un pilar central de Protected 365

Security Posture Management (SPM) no es un complemento opcional, sino un servicio fundamental dentro de la solución Acronis Protected 365 que permite cumplir la promesa de la plataforma de ofrecer una protección integral "7 en 1" mejorada con IA para Microsoft 365. SPM incluye, por tanto, las siguientes siete funciones en una única plataforma ("7 en 1"): gestión de la postura de seguridad, copia de seguridad, seguridad del correo electrónico, seguridad de la colaboración, XDR, archivado de correos electrónicos y formación en concienciación sobre seguridad, que actúan en conjunto para cerrar por completo la brecha de responsabilidad compartida de Microsoft en Exchange, Teams, SharePoint y OneDrive.

SPM desempeña un papel crítico en la fase de "Cerrar las brechas con protección estándar" del modelo de madurez de Protected 365, ya que ayuda a las organizaciones a evolucionar desde una protección básica hacia una resiliencia proactiva. Mientras que las copias de seguridad y la seguridad del correo electrónico establecen una protección esencial, SPM introduce la evaluación continua de riesgos, la aplicación de directivas y la corrección automatizada, lo que garantiza que los entornos permanezcan alineados con las mejores prácticas y cumplan los estándares en constante evolución.

Al supervisar de forma continua las configuraciones, detectar desviaciones y permitir una corrección rápida, SPM aborda directamente uno de los riesgos más comunes y que más suelen pasarse por alto en Microsoft 365: la mala configuración por parte de los usuarios y las desviaciones de los estándares de seguridad. Transforma la seguridad de un proceso reactivo en una disciplina proactiva y basada en directivas, que reduce la exposición, refuerza el cumplimiento y mejora la ciberresiliencia global.

Lo más importante es que SPM se ofrece dentro de la misma plataforma multiinquilino y unificada de Acronis, lo que refuerza la propuesta de valor principal de Protected 365: un único proveedor, un único contrato y una solución integrada. Esto elimina la fragmentación de herramientas, reduce la carga operativa y permite a los MSP y a los equipos de TI escalar con eficacia y mejorar al mismo tiempo la calidad de sus servicios y la rentabilidad.

Actúe ya y cierre las brechas

Las malas configuraciones no dan margen, y usted no debería pasarlas por alto.
Inicie hoy mismo su prueba de Acronis Security Posture Management y descubra al instante los riesgos, aplique las mejores prácticas y refuerce la postura de seguridad de su entorno de Microsoft 365.

COMIENCE SU EVALUACIÓN GRATUITA

Acronis

Para obtener más información
acronis.com