

# 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.

Acronis Cyber Protect Cloud

SK Partner

Manage

All customers

MONITORING

DEVICES

MICROSOFT 365 MANAGEMENT

Baselines

Users

Baseline templates

Security posture

Configuration

MANAGEMENT

SOFTWARE MANAGEMENT

PROTECTION

SETTINGS

Baselines

Customer: Contoso

Category: All

Apply

Search

| Category                            | Baseline                       | Status                                                                           |          |
|-------------------------------------|--------------------------------|----------------------------------------------------------------------------------|----------|
| <input type="checkbox"/>            | Audit                          | Mailbox Audit Log                                                                | Passed   |
| <input type="checkbox"/>            | Authentication & Authorisation | Admin Consent Workflow                                                           | Deviated |
| <input type="checkbox"/>            | Authentication & Authorisation | Authentication Method Policy - Email OTP                                         | Deviated |
| <input checked="" type="checkbox"/> | Authentication & Authorisation | Authentication Method Policy - Microsoft Authenticator                           | Deviated |
| <input type="checkbox"/>            | Authentication & Authorisation | Conditional Access Policy - Application Enforced Restrictions For Unmanaged D... | Deviated |
| <input type="checkbox"/>            | Authentication & Authorisation | Conditional Access Policy - Block Legacy Authentication                          | Deviated |
| <input type="checkbox"/>            | Authentication & Authorisation | Conditional Access Policy - Block Unknown Or Unsupported Device Access           | Deviated |
| <input type="checkbox"/>            | Authentication & Authorisation | Conditional Access Policy - Enforce MFA                                          | Deviated |
| <input type="checkbox"/>            | Authentication & Authorisation | Conditional Access Policy - No persistent Browser Sessions                       | Deviated |
| <input type="checkbox"/>            | Authentication & Authorisation | Conditional Access Policy - Require Approved Client Apps                         | Deviated |
| <input type="checkbox"/>            | Authentication & Authorisation | Conditional Access Policy - Require Compliant Or Hybrid Azure AD joined Device.  | Deviated |
| <input type="checkbox"/>            | Authentication & Authorisation | Conditional Access Policy - Restrict Access To Azure Portal                      | Deviated |
| <input type="checkbox"/>            | Authentication & Authorisation | Conditional Access Policy - Restrict Access To Microsoft Admin Portal            | Deviated |
| <input type="checkbox"/>            | Authentication & Authorisation | Conditional Access Policy - Securing Security Info Registration                  | Deviated |
| <input type="checkbox"/>            | Authentication & Authorisation | Conditional Access Policy - Sign-In Risk-Based Multifactor Authentication.       | Deviated |
| <input type="checkbox"/>            | Authentication & Authorisation | Customer Lockbox                                                                 | Deviated |
| <input type="checkbox"/>            | Authentication & Authorisation | Password Policy                                                                  | Deviated |
| <input type="checkbox"/>            | Authentication & Authorisation | SharePoint Modern Auth Enforced                                                  | Deviated |
| <input type="checkbox"/>            | Authentication & Authorisation | User Consent Settings                                                            | Deviated |
| <input type="checkbox"/>            | Email Security                 | Automatic Forwarding - Block                                                     | Deviated |
| <input type="checkbox"/>            | Email Security                 | Default Hosted Outbound Spam Filter Policy                                       | Passed   |

Baseline details

Remediate

Enable auto-remediation

Edit

Authentication Method Policy - Microsoft Authenticator

Controls how Microsoft Authenticator is used for push and passwordless authentication, which users it applies to, and whether additional security details (app name, location, companion apps) appear in authentication prompts. [Learn more](#)

Tenant

Contoso

Auto-remediation

Disabled

Status

Deviated

| Name                            | Current value               | Required value              | Status   |
|---------------------------------|-----------------------------|-----------------------------|----------|
| State                           | Enabled                     | Enabled                     | Passed   |
| Allow use of Microsoft Auth...  | Enabled                     | Disabled                    | Deviated |
| Include Targets                 | All Users Auth method (any) | All Users Auth method (any) | Passed   |
| Exclude Targets                 | None                        | None                        | Passed   |
| Show application name - Sta...  | Default                     | Enabled                     | Deviated |
| Show application name - Inc...  | All Users                   | All Users                   | Passed   |
| Show application name - Ex...   | --                          | --                          | Passed   |
| Show geographic location - ...  | Default                     | Enabled                     | Deviated |
| Show geographic location - L... | All Users                   | All Users                   | Passed   |
| Show geographic location - ...  | --                          | --                          | Passed   |
| Companion applications - St...  | Default                     | Enabled                     | Deviated |
| Companion applications - In...  | All Users                   | All Users                   | Passed   |
| Companion applications - E...   | --                          | --                          | Passed   |

## 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.

Acronis  
Cyber Protect Cloud

SK Partner

All customers

MONITORING

DEVICES

MICROSOFT 365 MANAGEMENT

Baselines

Users

Baseline templates

Security posture

Configuration

MANAGEMENT

SOFTWARE MANAGEMENT

PROTECTION

SETTINGS

Powered by Acronis Cyber Platform

Baselines

Customer: Contoso

Category: All

Apply

Search

| Category                       | Baseline                                                                         | Status   |
|--------------------------------|----------------------------------------------------------------------------------|----------|
| Audit                          | Mailbox Audit Log                                                                | Passed   |
| Authentication & Authorisation | Admin Consent Workflow                                                           | Deviated |
| Authentication & Authorisation | Authentication Method Policy - Email OTP                                         | Deviated |
| Authentication & Authorisation | Authentication Method Policy - Microsoft Authenticator                           | Deviated |
| Authentication & Authorisation | Conditional Access Policy - Application Enforced Restrictions For Unmanaged D... | Deviated |
| Authentication & Authorisation | Conditional Access Policy - Block Legacy Authentication                          | Deviated |
| Authentication & Authorisation | Conditional Access Policy - Block Unknown Or Unsupported Device Access           | Deviated |
| Authentication & Authorisation | Conditional Access Policy - Enforce MFA                                          | Deviated |
| Authentication & Authorisation | Conditional Access Policy - No persistent Browser Sessions                       | Deviated |
| Authentication & Authorisation | Conditional Access Policy - Require Approved Client Apps                         | Deviated |
| Authentication & Authorisation | Conditional Access Policy - Require Compliant Or Hybrid Azure AD joined Device   | Deviated |
| Authentication & Authorisation | Conditional Access Policy - Restrict Access To Azure Portal                      | Deviated |
| Authentication & Authorisation | Conditional Access Policy - Restrict Access To Microsoft Admin Portal            | Deviated |
| Authentication & Authorisation | Conditional Access Policy - Securing Security Info Registration                  | Deviated |
| Authentication & Authorisation | Conditional Access Policy - Sign-In Risk-Based Multifactor Authentication        | Deviated |
| Authentication & Authorisation | Customer Lockbox                                                                 | Deviated |
| Authentication & Authorisation | Password Policy                                                                  | Deviated |
| Authentication & Authorisation | SharePoint Modern Auth Enforced                                                  | Deviated |
| Authentication & Authorisation | User Consent Settings                                                            | Deviated |
| Email Security                 | Automatic Forwarding - Block                                                     | Deviated |

Baseline details

Remediate Enable auto-remediation Edit

Conditional Access Policy - Application Enforced Restrictions For Unmanaged Devices

This Conditional Access Policy blocks or restricts access to SharePoint, OneDrive, and Exchange content from unmanaged devices. It helps prevent data leakage by ensuring that only managed and compliant devices can access sensitive organizational data. [Learn more](#)

Tenant: Contoso

Auto-remediation: Disabled

Status: Deviased

| Name                           | Current value | Required value                 | Status   |
|--------------------------------|---------------|--------------------------------|----------|
| Display Name                   | ---           | CAP009 - Application Enforc... | Deviated |
| State                          | ---           | enabled                        | Deviated |
| Include Users                  | ---           | All                            | Deviated |
| Include Roles                  | ---           | ---                            | Deviated |
| Include Groups                 | ---           | ---                            | Deviated |
| Include Guest Or External U... | ---           | ---                            | Deviated |
| Exclude Users                  | ---           | ---                            | Deviated |
| Exclude Roles                  | ---           | ---                            | Deviated |
| Exclude Groups                 | ---           | ---                            | Deviated |
| Exclude Guest Or External U... | ---           | ---                            | Deviated |
| Include Applications           | ---           | Office365                      | Deviated |
| Session Control                | ---           | Use app enforced restrictions  | Deviated |

### 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.

Acronis Cyber Protect Cloud

5K Partner

Manage

All customers

▼

MONITORING

DEVICES

MICROSOFT 365 MANAGEMENT

Baselines

Users

Baseline templates

Security posture

Configuration

MANAGEMENT

SOFTWARE MANAGEMENT

PROTECTION

SETTINGS

Powered by Acronis Cyber Platform

Baselines

Customer: Contoso

Category: All

Apply

Search

Q

| Category                                                           | Baseline                                                                         | Status   |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------|----------|
| <input type="checkbox"/> Audit                                     | Mailbox Audit Log                                                                | Passed   |
| <input type="checkbox"/> Authentication & Authorisation            | Admin Consent Workflow                                                           | Deviated |
| <input type="checkbox"/> Authentication & Authorisation            | Authentication Method Policy - Email OTP                                         | Deviated |
| <input type="checkbox"/> Authentication & Authorisation            | Authentication Method Policy - Microsoft Authenticator                           | Deviated |
| <input type="checkbox"/> Authentication & Authorisation            | Conditional Access Policy - Application Enforced Restrictions For Unmanaged D... | Deviated |
| <input type="checkbox"/> Authentication & Authorisation            | Conditional Access Policy - Block Legacy Authentication                          | Deviated |
| <input type="checkbox"/> Authentication & Authorisation            | Conditional Access Policy - Block Unknown Or Unsupported Device Access           | Deviated |
| <input type="checkbox"/> Authentication & Authorisation            | Conditional Access Policy - Enforce MFA                                          | Deviated |
| <input type="checkbox"/> Authentication & Authorisation            | Conditional Access Policy - No persistent Browser Sessions                       | Deviated |
| <input checked="" type="checkbox"/> Authentication & Authorisation | Conditional Access Policy - Require Approved Client Apps                         | Deviated |
| <input type="checkbox"/> Authentication & Authorisation            | Conditional Access Policy - Require Compliant Or Hybrid Azure AD joined Device.  | Deviated |
| <input type="checkbox"/> Authentication & Authorisation            | Conditional Access Policy - Restrict Access To Azure Portal                      | Deviated |
| <input type="checkbox"/> Authentication & Authorisation            | Conditional Access Policy - Restrict Access To Microsoft Admin Portal            | Deviated |
| <input type="checkbox"/> Authentication & Authorisation            | Conditional Access Policy - Securing Security Info Registration                  | Deviated |
| <input type="checkbox"/> Authentication & Authorisation            | Conditional Access Policy - Sign-In Risk-Based Multifactor Authentication.       | Deviated |
| <input type="checkbox"/> Authentication & Authorisation            | Customer Lockbox                                                                 | Deviated |
| <input type="checkbox"/> Authentication & Authorisation            | Password Policy                                                                  | Deviated |
| <input type="checkbox"/> Authentication & Authorisation            | SharePoint Modern Auth Enforced                                                  | Deviated |
| <input type="checkbox"/> Authentication & Authorisation            | User Consent Settings                                                            | Deviated |
| <input type="checkbox"/> Email Security                            | Automatic Forwarding - Block                                                     | Deviated |

Baseline details

Remediate

Enable auto-remediation

Edit

Conditional Access Policy - Require Approved Client Apps

This Conditional Access Policy requires users to access resources only through approved client apps or apps protected by app protection policies. It helps ensure that organizational data is accessed securely and only through trusted applications. [Learn more](#)

|                  |          |
|------------------|----------|
| Tenant           | Contoso  |
| Auto-remediation | Disabled |
| Status           | Deviated |

| Name                           | Current value | Required value                | Status   |
|--------------------------------|---------------|-------------------------------|----------|
| Display Name                   | ---           | CA007 - Require Approved ...  | Deviated |
| State                          | ---           | enabled                       | Deviated |
| Include Users                  | ---           | All                           | Deviated |
| Include Roles                  | ---           | ---                           | Deviated |
| Include Groups                 | ---           | ---                           | Deviated |
| Include Guest Or External U... | ---           | ---                           | Deviated |
| Exclude Users                  | ---           | ---                           | Deviated |
| Exclude Roles                  | ---           | ---                           | Deviated |
| Exclude Groups                 | ---           | ---                           | Deviated |
| Exclude Guest Or External U... | ---           | ---                           | Deviated |
| Grant                          | ---           | approvedApplication,compil... | Deviated |
| Include Platforms              | ---           | android,iOS                   | Deviated |
| Client App Types               | ---           | all                           | Deviated |

# 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.

Acronis  
Cyber Protect Cloud

SK Partner

Manage

All customers

MONITORING

DEVICES

MICROSOFT 365  
MANAGEMENT

Security posture

Users

Baselines

Baseline templates

Configuration

MANAGEMENT

SOFTWARE  
MANAGEMENT

PROTECTION

SETTINGS

Powered by Acronis Cyber Platform

Baselines

Customer: Contoso

Category: All

Apply

Search

| Category                       | Baseline                                                                         | Status   |
|--------------------------------|----------------------------------------------------------------------------------|----------|
| Audit                          | Mailbox Audit Log                                                                | Passed   |
| Authentication & Authorisation | Admin Consent Workflow                                                           | Deviated |
| Authentication & Authorisation | Authentication Method Policy - Email OTP                                         | Deviated |
| Authentication & Authorisation | Authentication Method Policy - Microsoft Authenticator                           | Deviated |
| Authentication & Authorisation | Conditional Access Policy - Application Enforced Restrictions For Unmanaged D... | Deviated |
| Authentication & Authorisation | Conditional Access Policy - Block Legacy Authentication                          | Deviated |
| Authentication & Authorisation | Conditional Access Policy - Block Unknown Or Unsupported Device Access           | Deviated |
| Authentication & Authorisation | Conditional Access Policy - Enforce MFA                                          | Deviated |
| Authentication & Authorisation | Conditional Access Policy - No persistent Browser Sessions                       | Deviated |
| Authentication & Authorisation | Conditional Access Policy - Require Approved Client Apps                         | Deviated |
| Authentication & Authorisation | Conditional Access Policy - Require Compliant Or Hybrid Azure AD joined Device   | Deviated |
| Authentication & Authorisation | Conditional Access Policy - Restrict Access To Azure Portal                      | Deviated |
| Authentication & Authorisation | Conditional Access Policy - Restrict Access To Microsoft Admin Portal            | Deviated |
| Authentication & Authorisation | Conditional Access Policy - Securing Security Info Registration                  | Deviated |
| Authentication & Authorisation | Conditional Access Policy - Sign-In Risk-Based Multifactor Authentication        | Deviated |
| Authentication & Authorisation | Customer Lockbox                                                                 | Deviated |
| Authentication & Authorisation | Password Policy                                                                  | Deviated |
| Authentication & Authorisation | SharePoint Modern Auth Enforced                                                  | Deviated |
| Authentication & Authorisation | User Consent Settings                                                            | Deviated |
| Email Security                 | Automatic Forwarding - Block                                                     | Deviated |
| Email Security                 | Default Hosted Outbound Spam Filter Policy                                       | Passed   |

Baseline details

Remediate Enable auto-remediation Edit

Conditional Access Policy - No persistent Browser Sessions

This Conditional Access Policy prevents users from maintaining persistent browser sessions, requiring them to re-authenticate more frequently. It helps reduce the risk of unauthorized access from shared or unmanaged devices. [Learn more](#)

Tenant

Contoso

Auto-remediation

Disabled

Status

Deviated

| Name                           | Current value | Required value                 | Status   |
|--------------------------------|---------------|--------------------------------|----------|
| Display Name                   | ---           | CAPO03 - Prevent Persistent... | Deviated |
| State                          | ---           | enabled                        | Deviated |
| Include Users                  | ---           | All                            | Deviated |
| Include Roles                  | ---           | ---                            | Deviated |
| Include Groups                 | ---           | ---                            | Deviated |
| Include Guest Or External U... | ---           | ---                            | Deviated |
| Exclude Users                  | ---           | ---                            | Deviated |
| Exclude Roles                  | ---           | ---                            | Deviated |
| Exclude Groups                 | ---           | ---                            | Deviated |
| Exclude Guest Or External U... | ---           | ---                            | Deviated |
| Persistent Browser             | ---           | never                          | Deviated |

## 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.

Acronis Cyber Protect Cloud

SK Partner

Manage

All customers

▼

MONITORING

DEVICES

MICROSOFT 365 MANAGEMENT

Baselines

Security posture

Users

Baseline templates

Configuration

MANAGEMENT

SOFTWARE MANAGEMENT

PROTECTION

SETTINGS

Powered by Acronis Cyber Platform

Baselines

Customer: Contoso

Category: All

Apply

Search

Q

| Category                 | Baseline                       | Status                                                                           |          |
|--------------------------|--------------------------------|----------------------------------------------------------------------------------|----------|
| <input type="checkbox"/> | Audit                          | Mailbox Audit Log                                                                | Passed   |
| <input type="checkbox"/> | Authentication & Authorisation | Admin Consent Workflow                                                           | Deviated |
| <input type="checkbox"/> | Authentication & Authorisation | Authentication Method Policy - Email OTP                                         | Deviated |
| <input type="checkbox"/> | Authentication & Authorisation | Authentication Method Policy - Microsoft Authenticator                           | Deviated |
| <input type="checkbox"/> | Authentication & Authorisation | Conditional Access Policy - Application Enforced Restrictions For Unmanaged D... | Deviated |
| <input type="checkbox"/> | Authentication & Authorisation | Conditional Access Policy - Block Legacy Authentication                          | Deviated |
| <input type="checkbox"/> | Authentication & Authorisation | Conditional Access Policy - Block Unknown Or Unsupported Device Access           | Deviated |
| <input type="checkbox"/> | Authentication & Authorisation | Conditional Access Policy - Enforce MFA                                          | Deviated |
| <input type="checkbox"/> | Authentication & Authorisation | Conditional Access Policy - No persistent Browser Sessions                       | Deviated |
| <input type="checkbox"/> | Authentication & Authorisation | Conditional Access Policy - Require Approved Client Apps                         | Deviated |
| <input type="checkbox"/> | Authentication & Authorisation | Conditional Access Policy - Require Compliant Or Hybrid Azure AD joined Device.  | Deviated |
| <input type="checkbox"/> | Authentication & Authorisation | Conditional Access Policy - Restrict Access To Azure Portal                      | Deviated |
| <input type="checkbox"/> | Authentication & Authorisation | Conditional Access Policy - Restrict Access To Microsoft Admin Portal            | Deviated |
| <input type="checkbox"/> | Authentication & Authorisation | Conditional Access Policy - Securing Security Info Registration                  | Deviated |
| <input type="checkbox"/> | Authentication & Authorisation | Conditional Access Policy - Sign-In Risk-Based Multifactor Authentication.       | Deviated |
| <input type="checkbox"/> | Authentication & Authorisation | Customer Lockbox                                                                 | Deviated |
| <input type="checkbox"/> | Authentication & Authorisation | Password Policy                                                                  | Deviated |
| <input type="checkbox"/> | Authentication & Authorisation | SharePoint Modern Auth Enforced                                                  | Deviated |
| <input type="checkbox"/> | Authentication & Authorisation | User Consent Settings                                                            | Deviated |
| <input type="checkbox"/> | Email Security                 | Automatic Forwarding - Block                                                     | Deviated |
| <input type="checkbox"/> | Email Security                 | Default Hosted Outbound Spam Filter Policy                                       | Passed   |

Baseline details

Remediate

Enable auto-remediation

Edit

Conditional Access Policy - Block Unknown Or Unsupported Device Access

Users will be blocked from accessing company resources when the device type is unknown or unsupported. [Learn more](#)

|                  |          |
|------------------|----------|
| Tenant           | Contoso  |
| Auto-remediation | Disabled |
| Status           | Deviated |

| Name                           | Current value | Required value                | Status   |
|--------------------------------|---------------|-------------------------------|----------|
| Display Name                   | ---           | CAPO04 - Enforce Block Unk... | Deviated |
| State                          | ---           | enabled                       | Deviated |
| Include Users                  | ---           | All                           | Deviated |
| Include Roles                  | ---           | ---                           | Deviated |
| Include Groups                 | ---           | ---                           | Deviated |
| Include Guest Or External U... | ---           | ---                           | Deviated |
| Exclude Users                  | ---           | ---                           | Deviated |
| Exclude Roles                  | ---           | ---                           | Deviated |
| Exclude Groups                 | ---           | ---                           | Deviated |
| Exclude Guest Or External U... | ---           | ---                           | Deviated |
| Include Platforms              | ---           | All,all                       | Deviated |
| Exclude Platforms              | ---           | android,iOS,macOS,windows     | Deviated |
| Grant Controls                 | ---           | block                         | Deviated |

## 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.

The screenshot displays the Acronis Cyber Protect Cloud interface. The left sidebar shows navigation options: SK Partner, Manage, All customers, MONITORING, DEVICES, MICROSOFT 365 MANAGEMENT, Configuration, Security posture (selected), Baseline templates, Baselines, Users, MANAGEMENT, SOFTWARE MANAGEMENT, PROTECTION, and SETTINGS.

The main content area is divided into two panels:

- Security posture:** Shows 1 tenant and 35 tenant baseline deviations. A table lists the tenant 'Contoso' with 35 deviations and 34 users.
- Risk dashboard:** Provides a summary of baseline and user account risks.
 

| Baselines        |          |             |
|------------------|----------|-------------|
| Tenant baselines | 8 passed | 35 deviated |

| Baseline categories            |          |             |
|--------------------------------|----------|-------------|
| Audit                          | 1 passed | 0 deviated  |
| Authentication & Authorisation | 0 passed | 18 deviated |
| Email Security                 | 3 passed | 6 deviated  |
| General                        | 1 passed | 0 deviated  |
| Intune                         | 0 passed | 6 deviated  |
| Mobile Access                  | 0 passed | 1 deviated  |
| Remote Access                  | 2 passed | 0 deviated  |
| Sharing                        | 1 passed | 4 deviated  |

| User account risks |                           |
|--------------------|---------------------------|
| MFA                | 29 affected user accounts |
| Admin mailboxes    | 6 affected user accounts  |
| Anonymous admins   | 6 affected user accounts  |
| Shared mailboxes   | 1 affected user account   |
| Dormant accounts   | No affected user accounts |
| Dormant admins     | No affected user accounts |
| Guests             | No affected user accounts |

# 7. Elevación de privilegios y abuso excesivo de roles



**Incidente real**  
Midnight Blizzard sufrió varias elevaciones de privilegios en Entra ID.



- 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.



**Técnica de ataque**  
Elevación de privilegios mediante roles administrativos permanentes y excesivos.

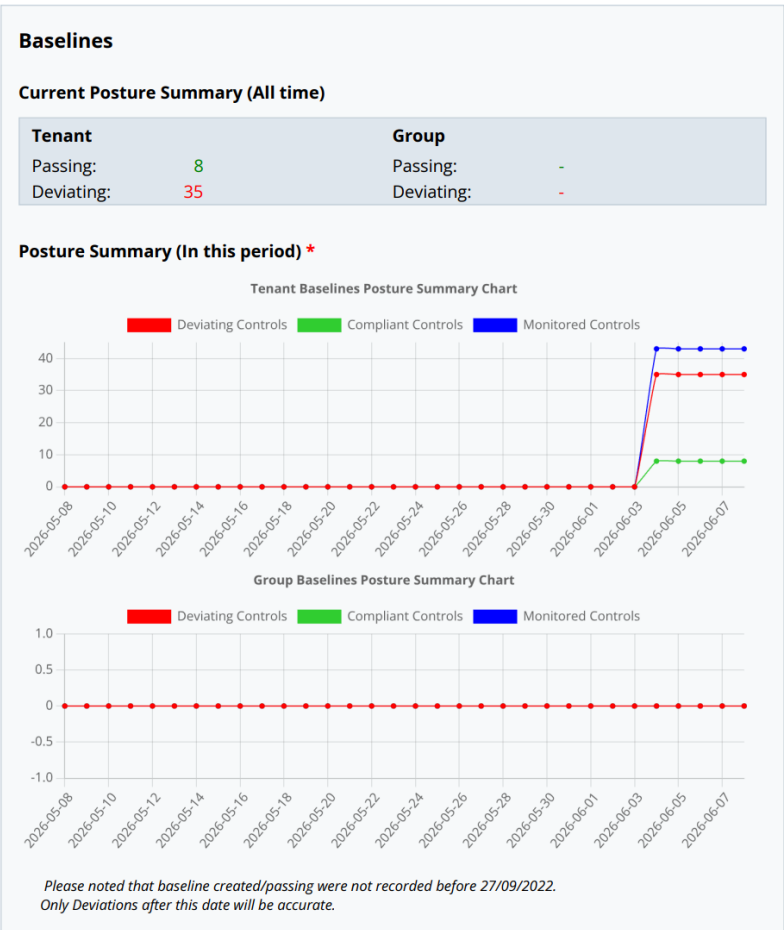


- Cómo ayuda Acronis SPM**
- Identifica roles administrativos excesivos y exposición de privilegios.
  - Ayuda a los MSP a estandarizar una postura segura de roles en todos los inquilinos.
  - Facilita la aplicación de estándares de referencia para identidades y autorizaciones.



- Cuál fue el factor de riesgo**
- Número excesivo de administradores globales.
  - Acumulación progresiva de privilegios.
  - Gobernanza insuficiente de roles.

## Compliance Posture Summary



## 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.

Acronis Cyber Protect Cloud

SK Partner Manage

All customers

MONITORING

DEVICES

MICROSOFT 365 MANAGEMENT

**Baselines**

Users

Baseline templates

Security posture

Configuration

MANAGEMENT

SOFTWARE MANAGEMENT

PROTECTION

SETTINGS

| Baselines                           |                                |                                                                                    |          |
|-------------------------------------|--------------------------------|------------------------------------------------------------------------------------|----------|
| <input type="checkbox"/>            | Authentication & Authorisation | SharePoint Modern Auth Enforced                                                    | Deviated |
| <input type="checkbox"/>            | Authentication & Authorisation | User Consent Settings                                                              | Deviated |
| <input type="checkbox"/>            | Email Security                 | Automatic Forwarding - Block                                                       | Deviated |
| <input type="checkbox"/>            | Email Security                 | Default Hosted Outbound Spam Filter Policy                                         | Passed   |
| <input type="checkbox"/>            | Email Security                 | DKIM Signing For Default Domain                                                    | Deviated |
| <input type="checkbox"/>            | Email Security                 | Mail Auto Forwarding                                                               | Deviated |
| <input type="checkbox"/>            | Email Security                 | Malicious Attachment Types Filter Policy - DEPRECATED                              | Passed   |
| <input type="checkbox"/>            | Email Security                 | Malware Internal Sender Filter Notification Policy - DEPRECATED                    | Passed   |
| <input type="checkbox"/>            | Email Security                 | Preset EOP Policy (Standard)                                                       | Deviated |
| <input type="checkbox"/>            | Email Security                 | Preset EOP Policy (Strict)                                                         | Deviated |
| <input type="checkbox"/>            | Email Security                 | Standard Default Anti Phishing Policy                                              | Deviated |
| <input type="checkbox"/>            | General                        | Security Defaults Policy                                                           | Passed   |
| <input type="checkbox"/>            | Intune                         | Android Enterprise - Compliance Policy                                             | Deviated |
| <input type="checkbox"/>            | Intune                         | iOS/iPadOS - Compliance Policy                                                     | Deviated |
| <input type="checkbox"/>            | Intune                         | MAC OS - Compliance Policy                                                         | Deviated |
| <input type="checkbox"/>            | Intune                         | Windows 10 Or Later - Compliance Policy                                            | Deviated |
| <input type="checkbox"/>            | Intune                         | Windows 10 or later Configuration Policy - Block Password Saving in Google Chr...  | Deviated |
| <input type="checkbox"/>            | Intune                         | Windows 10 or later Configuration Policy - Block Password Saving in Microsoft E... | Deviated |
| <input type="checkbox"/>            | Mobile Access                  | Default Mobile Device Mailbox Policy                                               | Deviated |
| <input type="checkbox"/>            | Remote Access                  | Modern Authentication                                                              | Passed   |
| <input type="checkbox"/>            | Remote Access                  | SMTP Access                                                                        | Passed   |
| <input type="checkbox"/>            | Sharing                        | Anonymous Links Expiry                                                             | Deviated |
| <input type="checkbox"/>            | Sharing                        | External (Guest) Users Resharing                                                   | Deviated |
| <input checked="" type="checkbox"/> | Sharing                        | Global Default Sharing Policy                                                      | Deviated |
| <input type="checkbox"/>            | Sharing                        | SharePoint Block Infected Files Download                                           | Deviated |
| <input type="checkbox"/>            | Sharing                        | SharePoint Storage Warning                                                         | Passed   |

Baseline details

Remediate Enable auto-remediation Edit

**Global Default Sharing Policy**

Controls the organisation-wide sharing level for SharePoint and OneDrive. This setting defines the maximum external sharing allowed across the tenant and governs how users can share files, folders, and sites. [Learn more](#)

|                  |          |
|------------------|----------|
| Tenant           | Contoso  |
| Auto-remediation | Disabled |
| Status           | Deviated |

| Name                            | Current value                  | Required value                  | Status   |
|---------------------------------|--------------------------------|---------------------------------|----------|
| Content can be optionally s...  | Anyone                         | Existing guests                 | Deviated |
| Content can be optionally s...  | Anyone                         | Existing guests                 | Deviated |
| Default File and Folder Shar... | Anyone with the link           | Specific people (only the pe... | Deviated |
| Default Sharing Link Permis...  | Anyone with the link has NO... | View                            | Deviated |
| Viewer Activity in OneDrive     | Enabled                        | Enabled                         | Passed   |
| Viewer Activity in SharePoint   | Enabled                        | Enabled                         | Passed   |

# 9. Brechas en auditorías e investigaciones



**Incidente real**  
Investigaciones de incidentes.



**Técnica de ataque**  
Actividad posterior al compromiso oculta 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.

Acronis Cyber Protect Cloud

SK Partner

Manage

All customers

MONITORING

DEVICES

MICROSOFT 365 MANAGEMENT

Baselines

Users

Baseline templates

Security posture

Configuration

MANAGEMENT

SOFTWARE MANAGEMENT

PROTECTION

SETTINGS

| Baselines                           |                                |                                                                                    |          |
|-------------------------------------|--------------------------------|------------------------------------------------------------------------------------|----------|
| <input type="checkbox"/>            | Authentication & Authorisation | SharePoint Modern Auth Enforced                                                    | Deviated |
| <input type="checkbox"/>            | Authentication & Authorisation | User Consent Settings                                                              | Deviated |
| <input type="checkbox"/>            | Email Security                 | Automatic Forwarding - Block                                                       | Deviated |
| <input type="checkbox"/>            | Email Security                 | Default Hosted Outbound Spam Filter Policy                                         | Passed   |
| <input type="checkbox"/>            | Email Security                 | DKIM Signing For Default Domain                                                    | Deviated |
| <input type="checkbox"/>            | Email Security                 | Mail Auto Forwarding                                                               | Deviated |
| <input type="checkbox"/>            | Email Security                 | Malicious Attachment Types Filter Policy - DEPRECATED                              | Passed   |
| <input type="checkbox"/>            | Email Security                 | Malware Internal Sender Filter Notification Policy - DEPRECATED                    | Passed   |
| <input type="checkbox"/>            | Email Security                 | Preset EOP Policy (Standard)                                                       | Deviated |
| <input type="checkbox"/>            | Email Security                 | Preset EOP Policy (Strict)                                                         | Deviated |
| <input type="checkbox"/>            | Email Security                 | Standard Default Anti Phishing Policy                                              | Deviated |
| <input type="checkbox"/>            | General                        | Security Defaults Policy                                                           | Passed   |
| <input type="checkbox"/>            | Intune                         | Android Enterprise - Compliance Policy                                             | Deviated |
| <input type="checkbox"/>            | Intune                         | iOS/iPadOS - Compliance Policy                                                     | Deviated |
| <input checked="" type="checkbox"/> | Intune                         | MAC OS - Compliance Policy                                                         | Deviated |
| <input type="checkbox"/>            | Intune                         | Windows 10 Or Later - Compliance Policy                                            | Deviated |
| <input type="checkbox"/>            | Intune                         | Windows 10 or later Configuration Policy - Block Password Saving in Google Chr...  | Deviated |
| <input type="checkbox"/>            | Intune                         | Windows 10 or later Configuration Policy - Block Password Saving in Microsoft E... | Deviated |
| <input type="checkbox"/>            | Mobile Access                  | Default Mobile Device Mailbox Policy                                               | Deviated |
| <input type="checkbox"/>            | Remote Access                  | Modern Authentication                                                              | Passed   |
| <input type="checkbox"/>            | Remote Access                  | SMTTP Access                                                                       | Passed   |
| <input type="checkbox"/>            | Sharing                        | Anonymous Links Expiry                                                             | Deviated |
| <input type="checkbox"/>            | Sharing                        | External (Guest) Users Resharing                                                   | Deviated |
| <input type="checkbox"/>            | Sharing                        | Global Default Sharing Policy                                                      | Deviated |

Baseline details

Remediate

Enable auto-remediation

Edit

MAC OS - Compliance Policy

Compliance policy for MAC OS devices [Learn more](#)

Tenant

Contoso

Auto-remediation

Disabled

Status

Deviated

| Name                           | Current value  | Required value                | Status   |
|--------------------------------|----------------|-------------------------------|----------|
| Display name                   | —              | MAC OS - Compliance Policy    | Deviated |
| Description                    | —              | Compliance policy for Mac ... | Deviated |
| Require system integrity pr... | —              | Required                      | Deviated |
| Minimum OS version             | —              | 12                            | Deviated |
| Maximum OS version             | —              | —                             | Deviated |
| Minimum OS build version       | —              | 21A559                        | Deviated |
| Maximum OS build version       | —              | —                             | Deviated |
| Require a password to unlo...  | —              | Required                      | Deviated |
| Simple passwords               | Allowed        | Block                         | Deviated |
| Minimum password length        | —              | 8                             | Deviated |
| Password type                  | —              | alphanumeric                  | Deviated |
| Number of non-alphanume...     | —              | 1                             | Deviated |
| Maximum minutes of inacti...   | Not configured | 15 minutes                    | Deviated |
| Password expiration (days)     | —              | 365                           | Deviated |
| Number of previous passwo...   | —              | 5                             | Deviated |

## 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.
- Supervisa 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.

