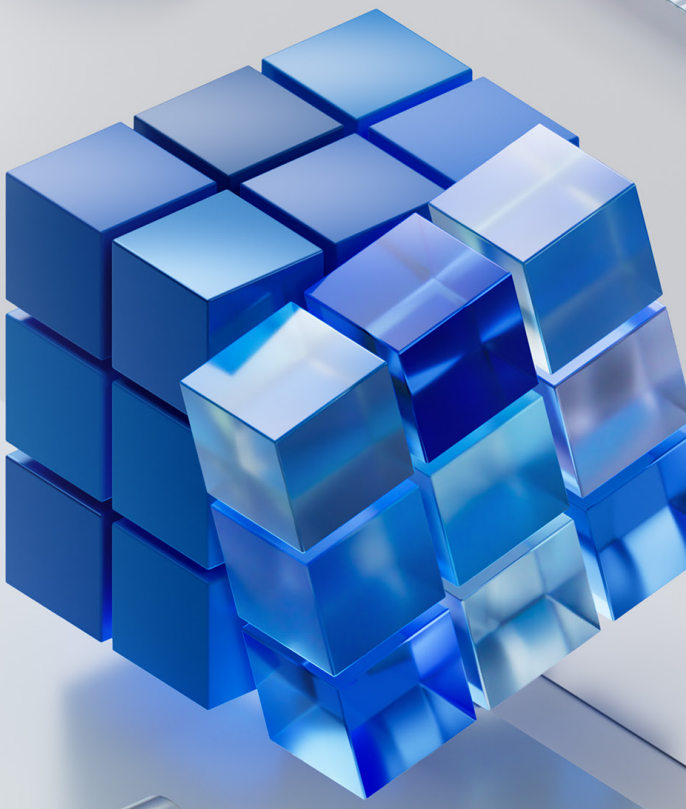
Acronis

Ataques à identidade e ao plano de controle do Microsoft 365



Nove ameaças reais, seus alvos e como os MSPs podem reduzir o risco com o Acronis SPM

Os ataques modernos ao Microsoft 365 têm se direcionado cada vez mais ao plano de controle — identidades, aplicativos OAuth, permissões, sessões e configurações — em vez de endpoints.

Recentemente, em incidentes reais, os invasores usaram fluxos de autenticação legítimos, permissões excessivas, controles de acesso fracos e configurações incorretas para conseguir acesso permanente a locatários do Microsoft 365.

Esta lista de verificação resume:

- as técnicas de ataque usadas em incidentes reais;
- o que os invasores exploraram;
- os controles do Microsoft 365 recomendados para reduzir o risco;
- como o Acronis SPM ajuda os MSPs a monitorar continuamente e aplicar uma postura segura em todos os locatários.



Copyright © 2003-2026 Acronis International GmbH.

1. Ataques de password spraying

Incidente real

Midnight Blizzard (2024).

Técnica de ataque

Ataque de password spraying contra uma conta de locatário legada e de não produção.

O que foi explorado

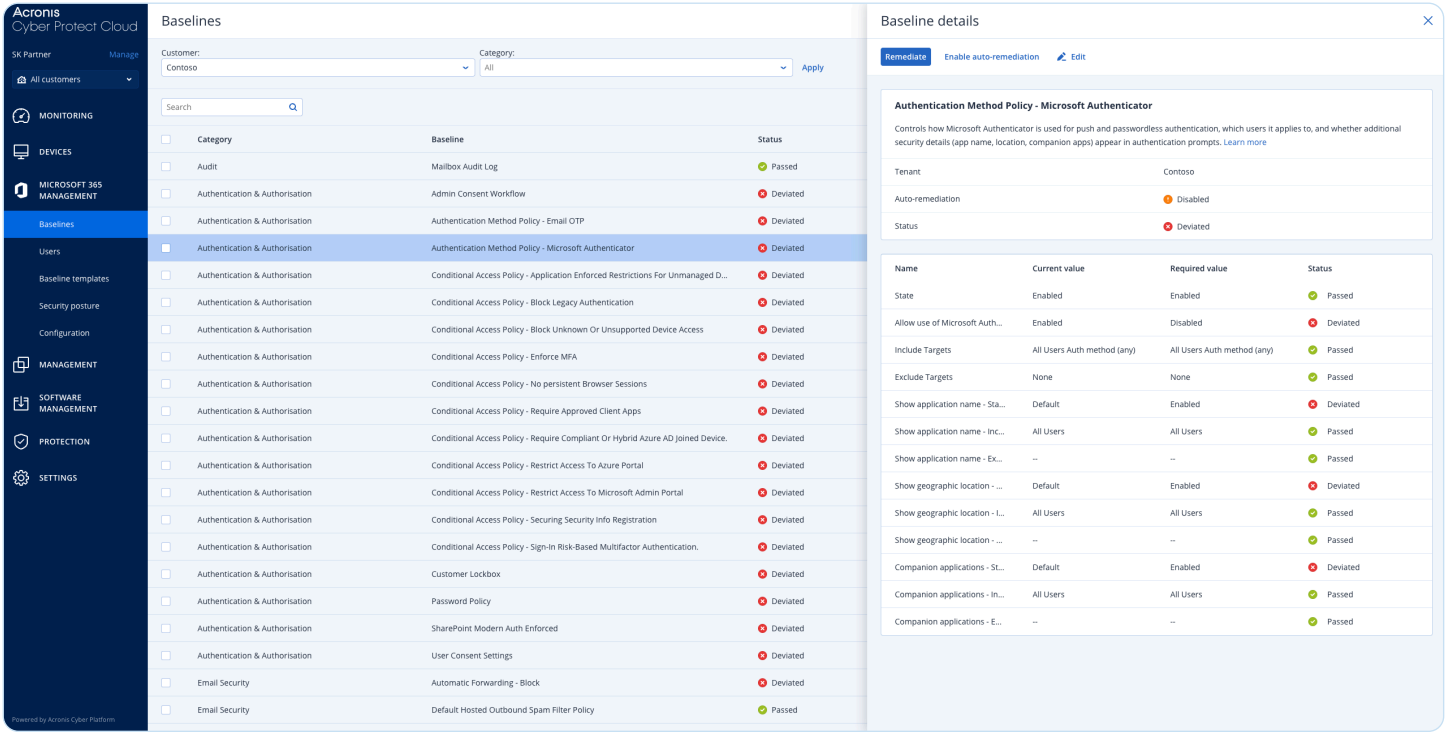
- Credenciais fracas
- Ausência de MFA em uma conta legada

Controles de segurança para reduzir o risco

- Aplicação de MFA
- Eliminação de senhas fracas
- Desativação de processos legados de autenticação
- Monitoramento de anomalias de login

Como o Acronis SPM ajuda

- Identifica lacunas de MFA
- Detecta configurações inseguras de autenticação
- Monitora desvios da referência entre locatários
- Orienta os MSPs a corrigir configurações fracas de identidade antes que elas se tornem caminhos de ataque



Copyright © 2003-2026 Acronis International GmbH.

2. Falsificação de token e abuso de sessão

Incidente real

Storm-0558 (2023).

Técnica de ataque

Tokens de autenticação falsificados usados para acessar contas de e-mail na nuvem.

O que foi explorado

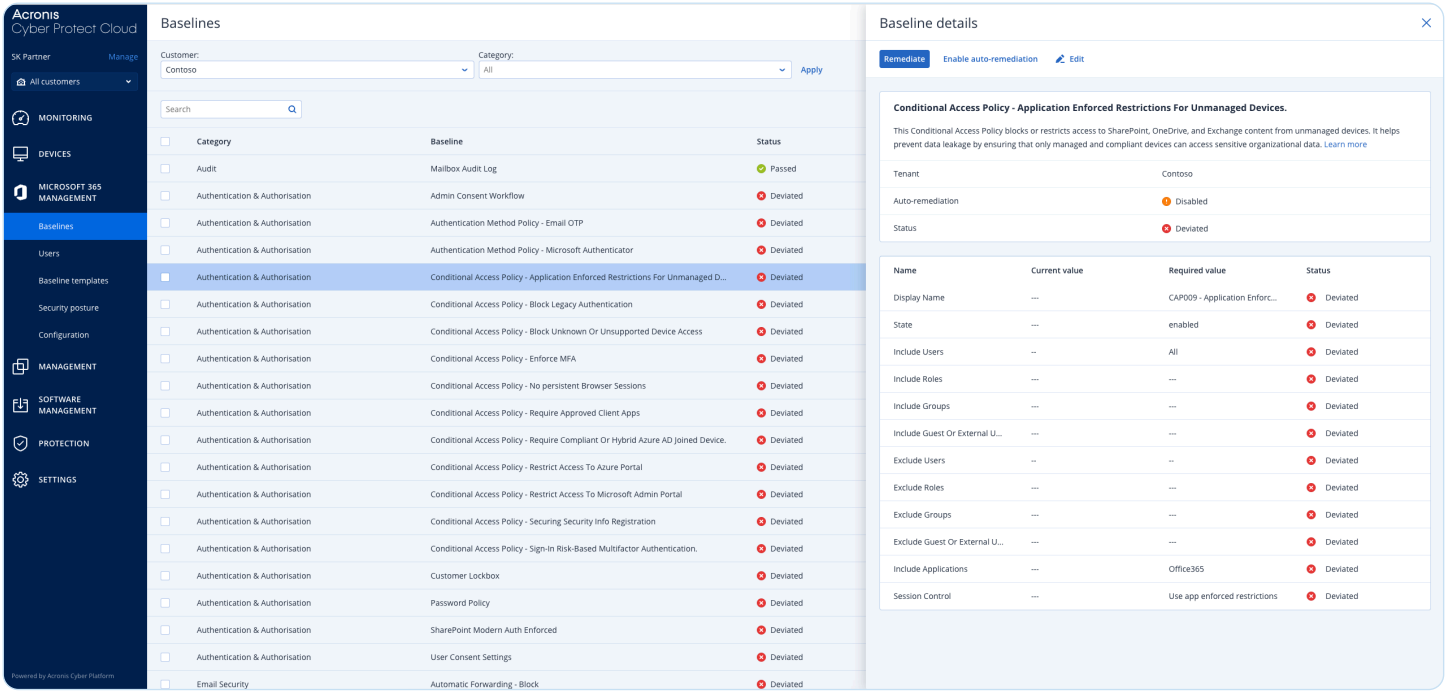
- Vulnerabilidades na validação de tokens
- Abuso de chaves de assinatura
- Visibilidade limitada do uso anômalo de tokens

Controles de segurança para reduzir o risco

- Fortificação da postura de identidade
- Aplicação de MFA e do acesso condicional
- Restrição do consentimento de aplicativos
- Proteção do acesso privilegiado
- Monitoramento de anomalias de tokens e sessões

Como o Acronis SPM ajuda

- Padroniza a postura de MFA e acesso condicional
- Identifica desvios na configuração de identidade
- Possibilita a aplicação de referências seguras de acesso de administrador
- Reduz a exposição adjacente à identidade do locatário



Copyright © 2003-2026 Acronis International GmbH.

3. Sequestro de sessão e phishing AiTM

Incidente real

Vários incidentes reais.

Técnica de ataque

Roubo de cookies de sessão por meio de phishing com proxy reverso.

O que foi explorado

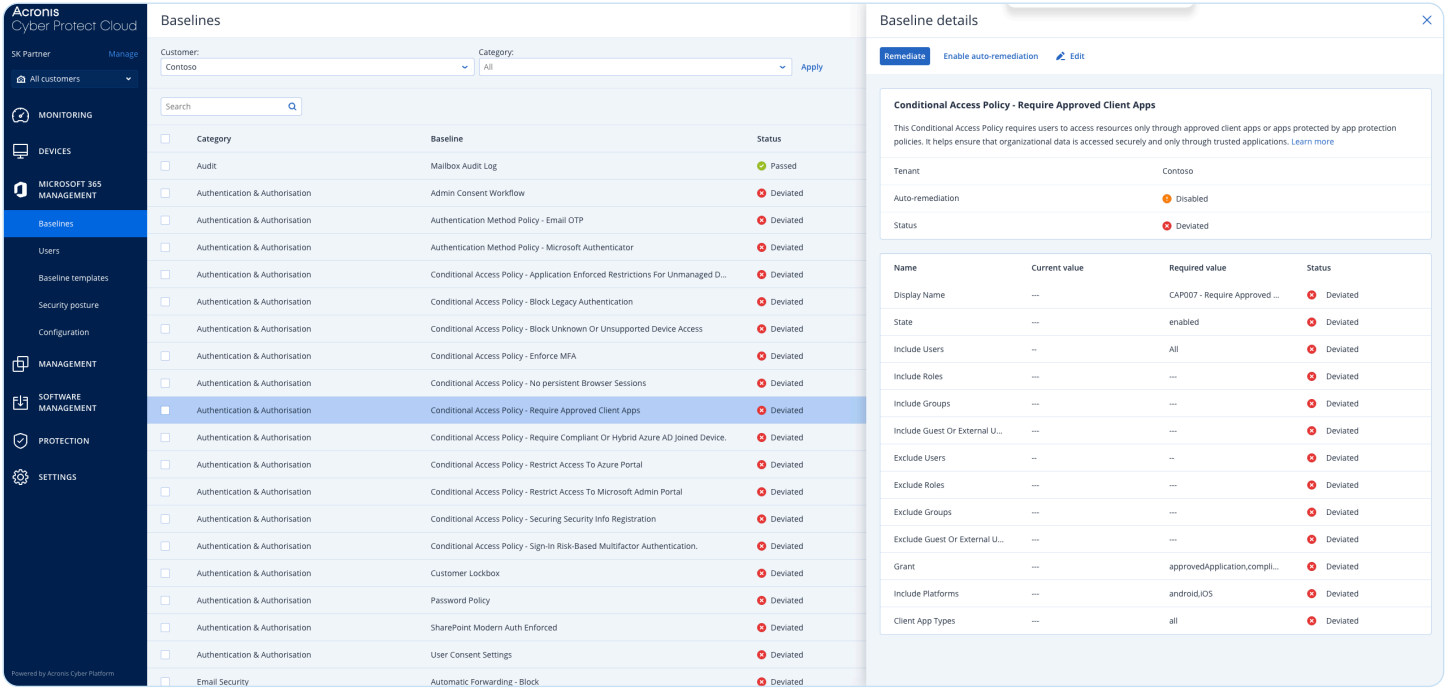
- Cookies de sessão autenticados roubados
- Aplicação fraca do acesso condicional
- Falta de restrições de acesso por dispositivo

Controles de segurança para reduzir o risco

- Exigência de dispositivos compatíveis ou gerenciados
- Aplicação do acesso condicional
- Monitoração do comportamento anômalo da sessão
- Uso da avaliação contínua de acesso quando disponível

Como o Acronis SPM ajuda

- Detecta desvios na postura de acesso condicional
- Ajuda a manter as referências da política de acesso seguro
- Possibilita a padronização dos controles de identidade e acesso ao dispositivo entre locatários



Copyright © 2003-2026 Acronis International GmbH.

4. Ataques de replay de token

Incidente real

Vários incidentes reais.

Técnica de ataque

Reutilização de tokens de atualização primária roubados.

O que foi explorado

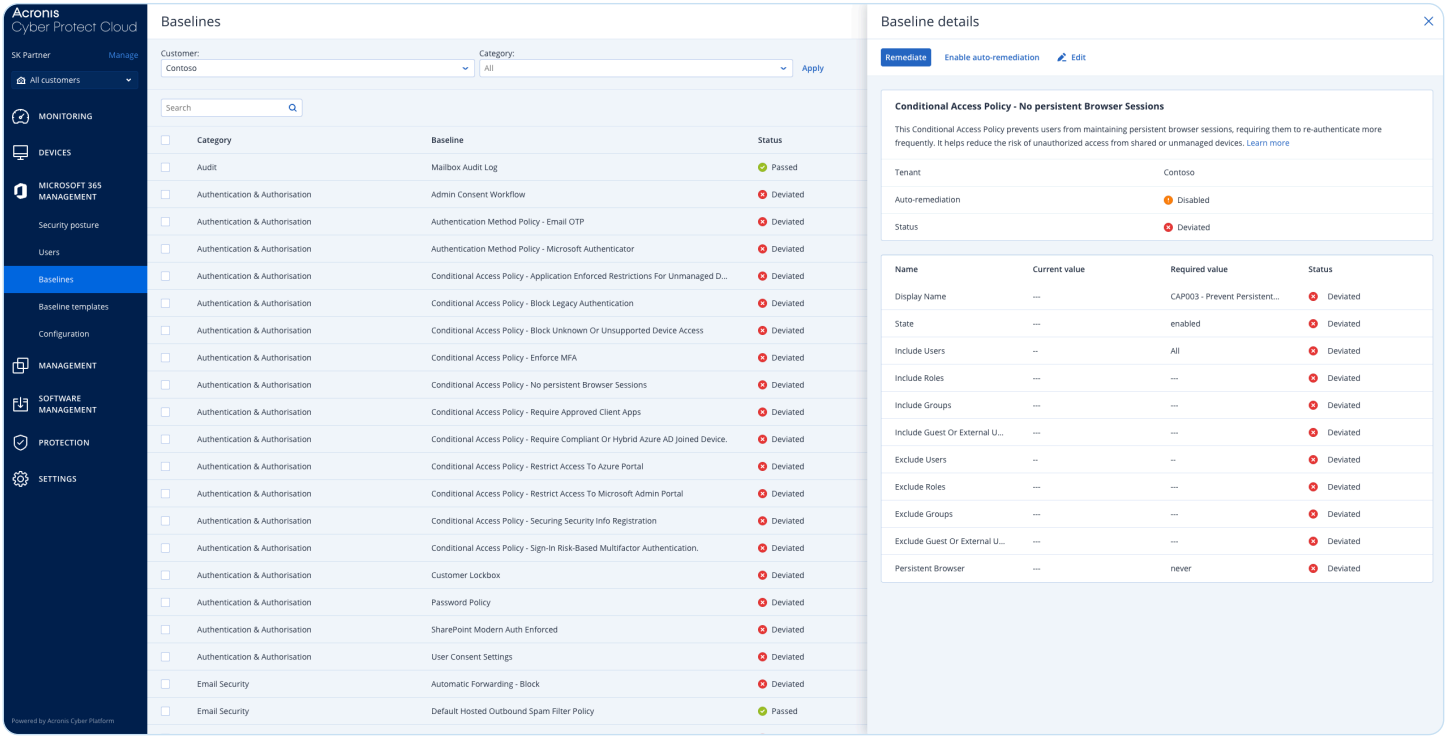
- Falta de proteção de token/sessão
- Aplicação fraca da sessão

Controles de segurança para reduzir o risco

- Aplicação da proteção de token quando permitida
- Uso de controles de sessão do acesso condicional
- Restrição do acesso de dispositivos não gerenciados

Como o Acronis SPM ajuda

- Orienta os MSPs a monitorar continuamente a postura de autenticação
- Detecta desvios da referência do acesso condicional e da configuração da sessão
- Possibilita a aplicação de referências seguras de identidade e acesso



Copyright © 2003-2026 Acronis International GmbH.

5. Phishing de consentimento OAuth

Incidente real

Vários incidentes reais.

Técnica de ataque

Concessões maliciosas de consentimento de aplicativo.

O que foi explorado

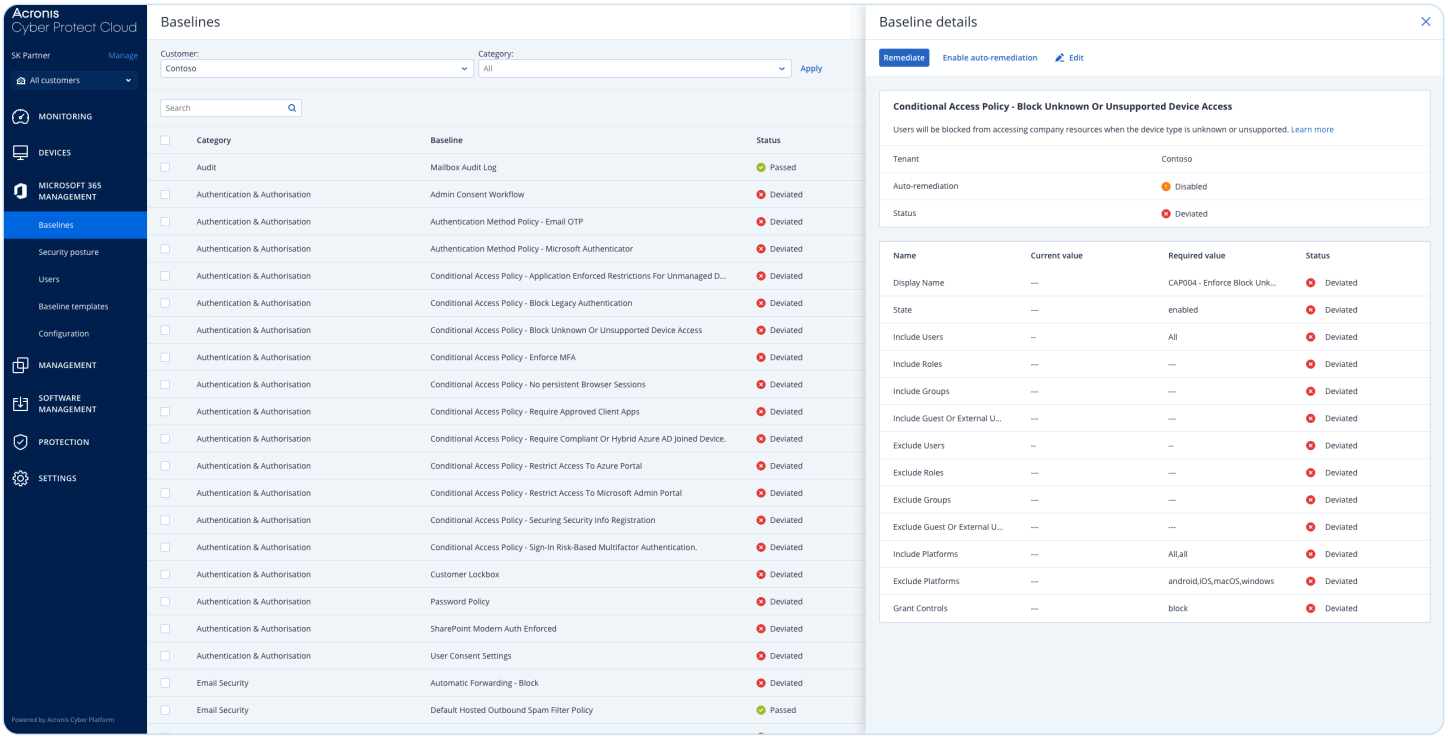
- Consentimento irrestrito do usuário
- Governança fraca de aplicativos

Controles de segurança para reduzir o risco

- Restrição do consentimento do usuário
- Exigência de aprovação para aplicativos pelo administrador
- Autorização apenas de editores verificados e permissões de baixo risco

Como o Acronis SPM ajuda

- Padroniza controles relacionados à autorização
- Detecta desvios das políticas de consentimento de aplicativo aprovadas
- Orienta os MSPs a manter uma postura segura de autorização do Microsoft 365 entre locatários



Copyright © 2003-2026 Acronis International GmbH.

6. Abuso de aplicativo OAuth e exfiltração de dados da API Graph

Incidente real

Vários incidentes reais.

Técnica de ataque

Acesso e exfiltração de dados por API com uso de aplicativos com permissões excessivas

O que foi explorado

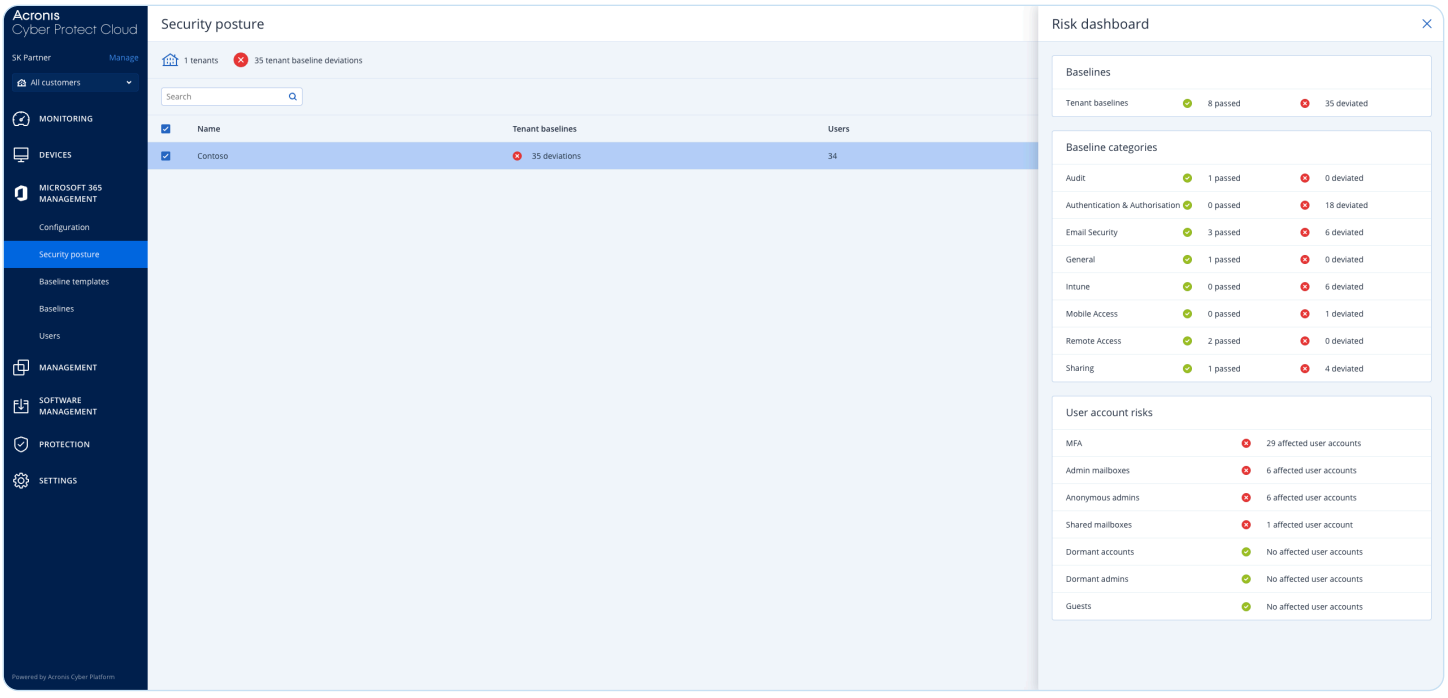
- Permissões excessivas do Graph
- Pouca visibilidade do comportamento do aplicativo
- Acesso a aplicativos não gerenciados

Controles de segurança para reduzir o risco

- Auditoria regular das permissões dos aplicativos
- Investigação de atividades incomuns do Graph
- Revisão de aplicativos autorizados por usuários externos

Como o Acronis SPM ajuda

- Mantém a governança sobre permissões de aplicativos e postura de consentimento
- Detecta desvios de autorização e exposição de aplicativos não gerenciados
- Melhora a visibilidade da postura de acesso a aplicativos do Microsoft 365



Copyright © 2003-2026 Acronis International GmbH.

7. Escalada de privilégios e abuso excessivo de funções

Incidente real

Várias escaladas de privilégios no Entra ID/ Midnight Blizzard.

Técnica de ataque

Escalada de privilégios por meio de privilégios administrativos permanentes excessivos.

O que foi explorado

- Excesso de administradores globais
- Crescimento excessivo de privilégios
- Governança fraca de funções

Controles de segurança para reduzir o risco

- Aplicação do menor privilégio
- Restrição do acesso administrativo permanente
- Revisão contínua das funções privilegiadas

Como o Acronis SPM ajuda

- Identifica funções administrativas excessivas e exposição de privilégios
- Orienta os MSPs a padronizar uma postura segura de funções em todos os locatários
- Possibilita a aplicação de referências de identidade e autorização

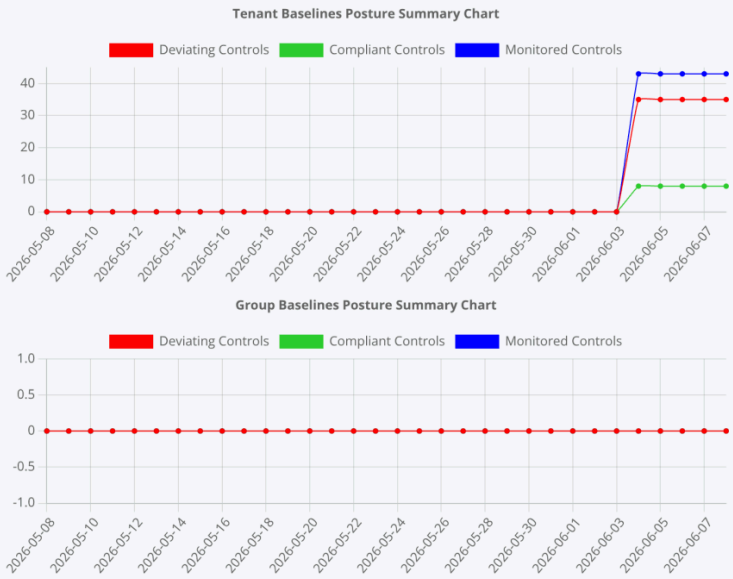
Compliance Posture Summary

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. Exposição do SharePoint e do OneDrive

Incidente real

Vários incidentes reais.

Técnica de ataque

Compartilhamento externo excessivo ou acidental.

O que foi explorado

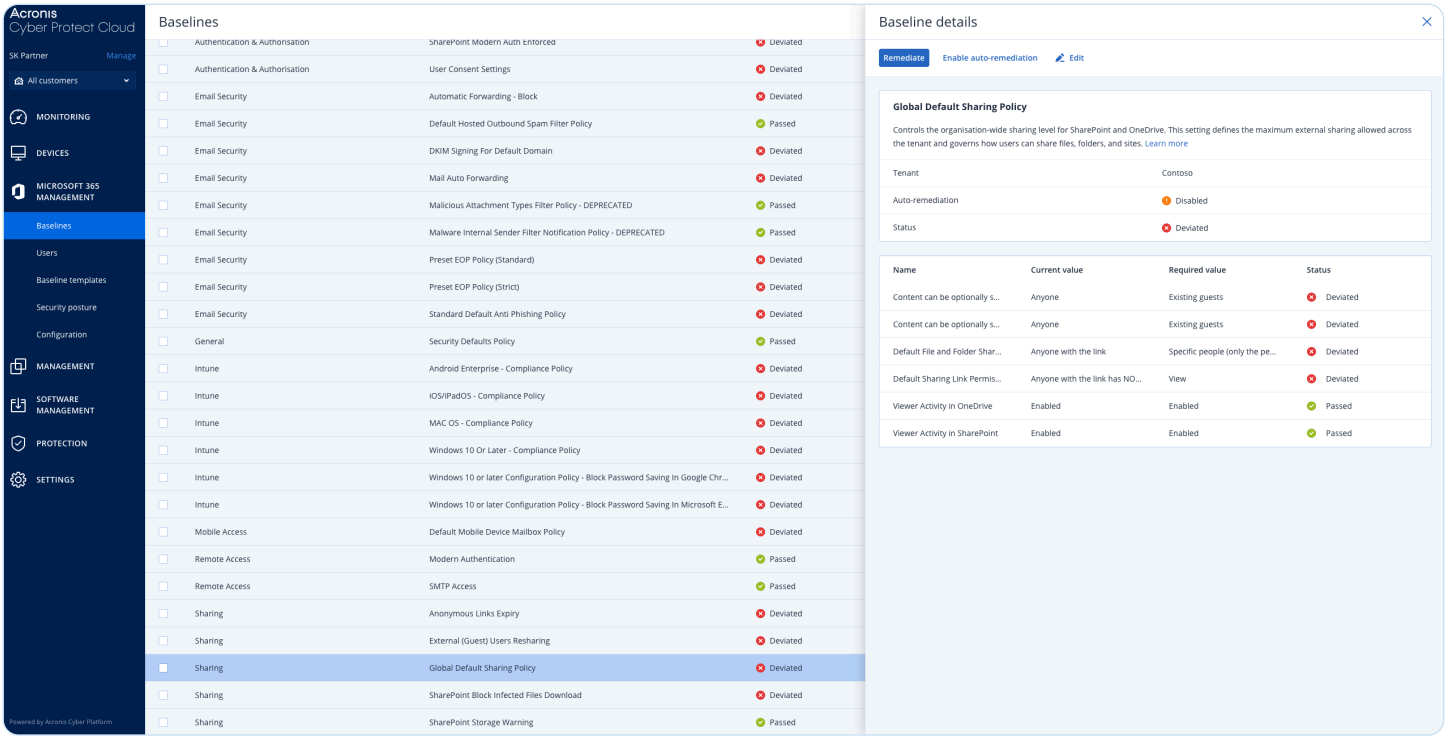
- Governança fraca de compartilhamento
- Configurações de acesso externo excessivamente permissivas

Controles de segurança para reduzir o risco

- Configuração de políticas de compartilhamento externo no nível da organização
- Restrição do compartilhamento quando necessário
- Revisão regular da postura de compartilhamento

Como o Acronis SPM ajuda

- Valida continuamente a postura de compartilhamento em relação às referências
- Detecta configurações de compartilhamento arriscadas
- Reduz o desvio de configuração de longo prazo entre locatários



Copyright © 2003-2026 Acronis International GmbH.

9. Lacunas de auditoria e investigação

Incidente real

Investigação de incidentes.

Técnica de ataque

Atividade pós-comprometimento ocultada por auditoria insuficiente.

O que foi explorado

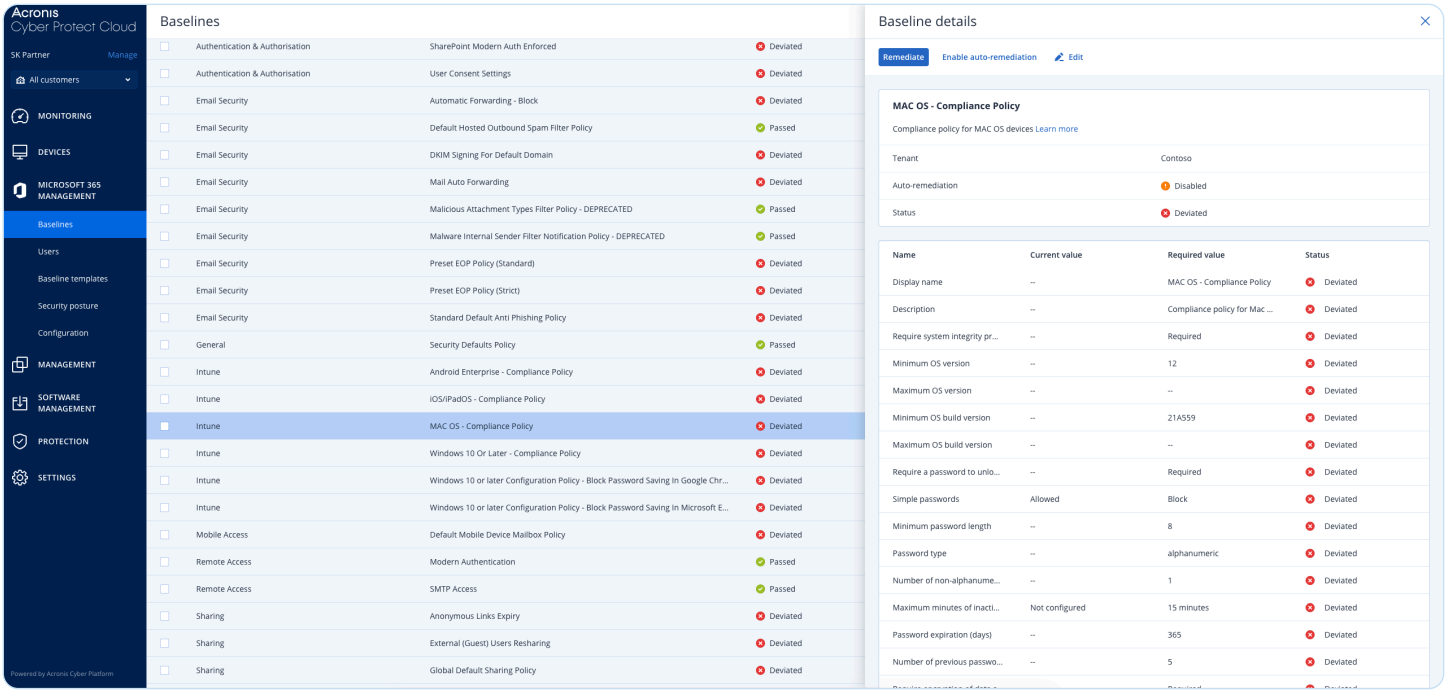
- Evidências de auditoria ausentes ou incompletas
- Prontidão fraca para investigação

Controles de segurança para reduzir o risco

- Auditoria do Microsoft Purview ativada
- Garantia de que os investigadores têm acesso apropriado
- Prontidão dos registros para consulta em auditorias

Como o Acronis SPM ajuda

- Orienta os MSPs a monitorar a postura de configuração relacionada à auditoria
- Detecta desvios nas configurações de log e auditoria
- Possibilita a investigação contínua e a prontidão para conformidade



Copyright © 2003-2026 Acronis International GmbH.

O que esses ataques têm em comum

Em todos os incidentes:

- a entrada é por identidade;
- a persistência é por configuração;
- o impacto abrange todo o locatário;
- os controles tradicionais de endpoint oferecem visibilidade limitada.

Por que o gerenciamento contínuo de postura é importante

Os ataques modernos ao Microsoft 365 são bem-sucedidos quando:

- as configurações incorretas continuam;
- a postura de segurança se desvia com o tempo;
- os locatários seguem sem perceber as lacunas de visibilidade.

Como o Acronis SPM ajuda os MSPs a reduzir riscos

- Gerencia centralmente a postura do Microsoft 365 entre os locatários
- Monitora continuamente a postura de segurança em relação às referências
- Detecta automaticamente novos riscos e desvios de configuração
- Aplica modelos de referência reutilizáveis
- Automatiza e simplifica a remediação
- Simplifica os fluxos de trabalho de integração e desligamento
- Padroniza a postura de segurança do Microsoft 365 em grande escala

Quando a prevenção não é suficiente: recupere o Entra ID

O gerenciamento da postura de segurança ajuda a reduzir os riscos de identidade. O backup oferece um caminho de recuperação quando um ataque, uma exclusão acidental ou uma configuração incorreta afeta o plano de controle de identidade.

Por que a recuperação do Entra ID é importante

O Entra ID controla quem pode acessar o Microsoft 365 e os aplicativos conectados. Os invasores podem alterar ou excluir usuários, grupos, funções, políticas e configurações para ampliar privilégios, manter a persistência ou interromper o acesso.

Restaurar apenas os dados do Microsoft 365 pode não restabelecer o acesso seguro. As organizações também precisam de uma forma confiável de recuperar as identidades, configurações e relações das quais seu ambiente depende.

Como o Acronis Entra ID Backup ajuda

- Proteja usuários, grupos, funções, políticas e configurações essenciais do Entra ID.
- Recupere objetos de identidade excluídos ou comprometidos e suas relações.
- Reverta alterações indesejadas após ataques ou erros administrativos.
- Reduza o tempo de inatividade sem depender apenas das opções nativas de retenção e recuperação.
- Gerencie a proteção dos dados e das identidades do Microsoft 365 pela plataforma Acronis.

Copyright © 2003-2026 Acronis International GmbH.

Fortaleça a resiliência de identidade

Combine o gerenciamento proativo da postura de segurança com backups recuperáveis do Entra ID. Assim, você ajuda seus clientes a prevenir ataques baseados em identidade, limitar seu impacto e acelerar a recuperação.

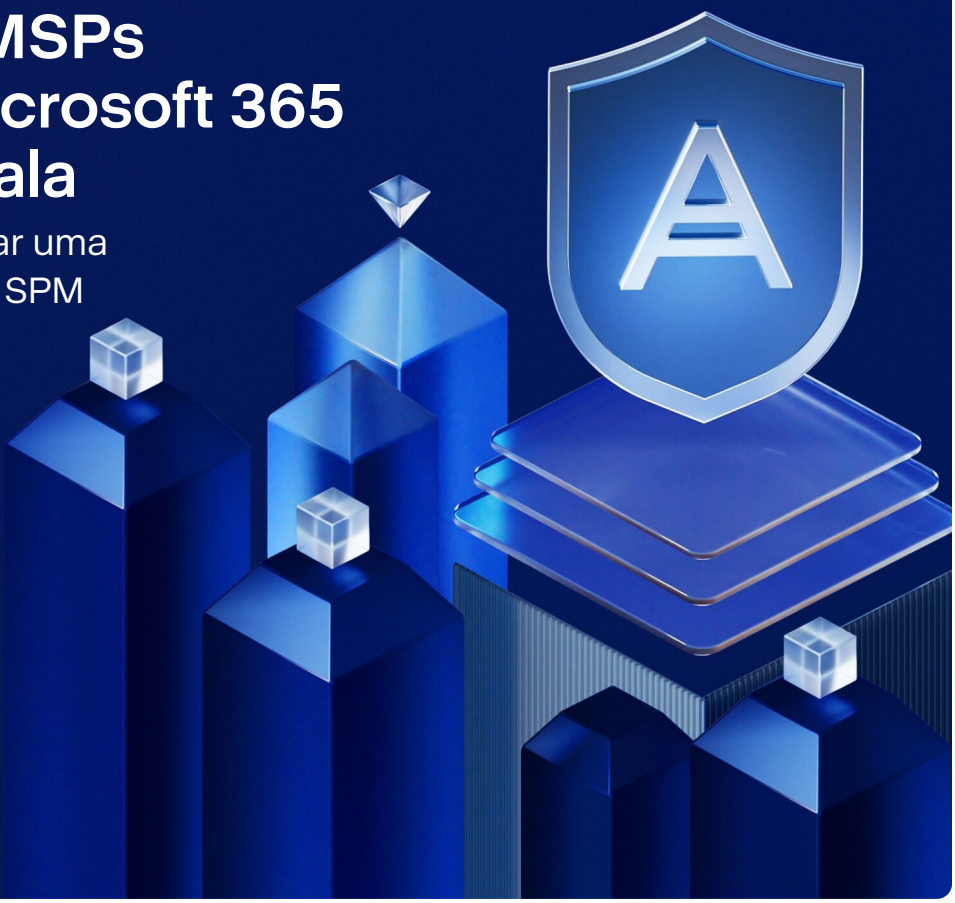


Conheça o Acronis Entra ID Backup

SAIBA MAIS

Saiba como o Acronis SPM ajuda os MSPs a proteger o Microsoft 365 em grande escala

Leia o código para agendar uma demonstração do Acronis SPM



Acronis

Saiba mais em
www.acronis.com

Copyright © 2003-2026 Acronis International GmbH. Todos os direitos reservados. A Acronis e o logotipo da Acronis são marcas comerciais da Acronis International GmbH nos Estados Unidos e/ou em outros países. Quaisquer outras marcas comerciais ou registradas são propriedade de seus respectivos donos. Pode haver alterações técnicas e diferenças em relação às ilustrações, bem como erros. 2026-10