Acronis

Microsoft 365 sob ataque: ameaças à identidade e ao plano de controle

Saiba como o Acronis Security Posture Management expõe e corrige essas ameaças

Introdução

O Microsoft 365 se tornou o plano de controle das operações empresariais modernas, gerenciando identidade, acesso, comunicação e dados em todas as organizações. Como ele é mais importante, o valor dele como principal superfície de ataque aumentou.

Só que a natureza dos ataques mudou muito.

As ameaças atuais não dependem mais de malware nem do comprometimento de endpoints. Em vez disso, os invasores se aproveitam de identidades, permissões e configurações incorretas, operando inteiramente dentro dos serviços legítimos do Microsoft 365. Uma única conta de administrador comprometida, uma permissão negligenciada ou uma política de acesso condicional fraca pode garantir aos invasores acesso permanente e de alto impacto sem acionar alertas de segurança tradicionais.

Essa mudança cria um desafio crítico para os provedores de serviços gerenciados (MSPs). As ferramentas de segurança tradicionais geralmente oferecem pouca visibilidade sobre esses ataques, enquanto as configurações incorretas e as políticas inconsistentes entre locatários criam uma exposição permanente.

Os resultados: o risco se acumula silenciosamente entre os locatários.

Neste guia, você encontra uma visão prática e exemplificada dos ataques modernos ao Microsoft 365 e da forma como o Acronis Security Posture Management (SPM) ajuda os MSPs a detectar, prevenir e corrigir esses riscos em grande escala.

A nova realidade: você já está no ataque

Você entra em um locatário de cliente final. Não há alertas, malware nem sinais óbvios de comprometimento. Tudo parece normal à primeira vista, mas isso não significa que o ambiente esteja seguro.

Um invasor pode já ter acesso. Ele pode estar usando credenciais válidas ou tokens permanentes obtidos por meio de phishing ou abuso de consentimento. O mais importante é que ele pode estar operando inteiramente dentro do Microsoft 365, misturando-se à atividade legítima e evitando os mecanismos tradicionais de detecção.

Os ataques modernos não dependem de invasão — eles operam dentro do plano de controle.

Para os MSPs, ele muda totalmente o problema. Não basta mais detectar ameaças ativas. É preciso identificar a exposição antes que ela seja explorada, corrigi-la de forma consistente em todos os locatários e garantir que essas correções sejam aplicadas ao longo do tempo, conforme a evolução dos ambientes.

Este passo a passo mostra como enfrentar esse desafio na prática com o Acronis Security Posture Management (SPM).

Situação 1

Password spraying

“Nada parece errado, mas uma conta acabou de conseguir acesso.”

Os invasores não precisam invadir — eles fazem login. Ao testar senhas comuns em muitas contas, eles evitam bloqueios acabam tendo acesso a uma delas. Com credenciais válidas, eles podem acessar caixas de e-mail e arquivos, agindo como um usuário legítimo.

Normalmente não há alertas, malware nem sinais claros, só atividades que parecem normais.

O Acronis SPM muda o foco da detecção para a exposição. Ele destaca riscos como a ausência da autenticação multifatorial (MFA), a ativação de um tipo de autenticação legada e configurações de identidade que fogem das práticas recomendadas.

A partir daí, você avalia o locatário, aplica a MFA, desativa a autenticação legada e implementa esses controles em todos os locatários usando modelos de referência. O monitoramento contínuo garante que os desvios sejam detectados e corrigidos.

Em vez de perseguir uma conta comprometida, você elimina as condições que possibilitaram o ataque.

O que você faz (na plataforma)

1 **Realiza uma auditoria sob demanda**

- Avalia na hora o locatário em comparação à referência de segurança.
- Identifica os pontos fracos da autenticação.

2 **Aplica uma remediação de referência.**

- Aplica a MFA a todos os usuários.
- Desativa a autenticação legada.

3 **Automatiza a ação nos locatários**

- Usa modelos de referência.
- Propaga políticas em todos os clientes.

4 **Ativa o monitoramento contínuo**

- O Acronis SPM detecta continuamente desvios em relação à referência.
- Alerta quando usuários são criados sem proteção.

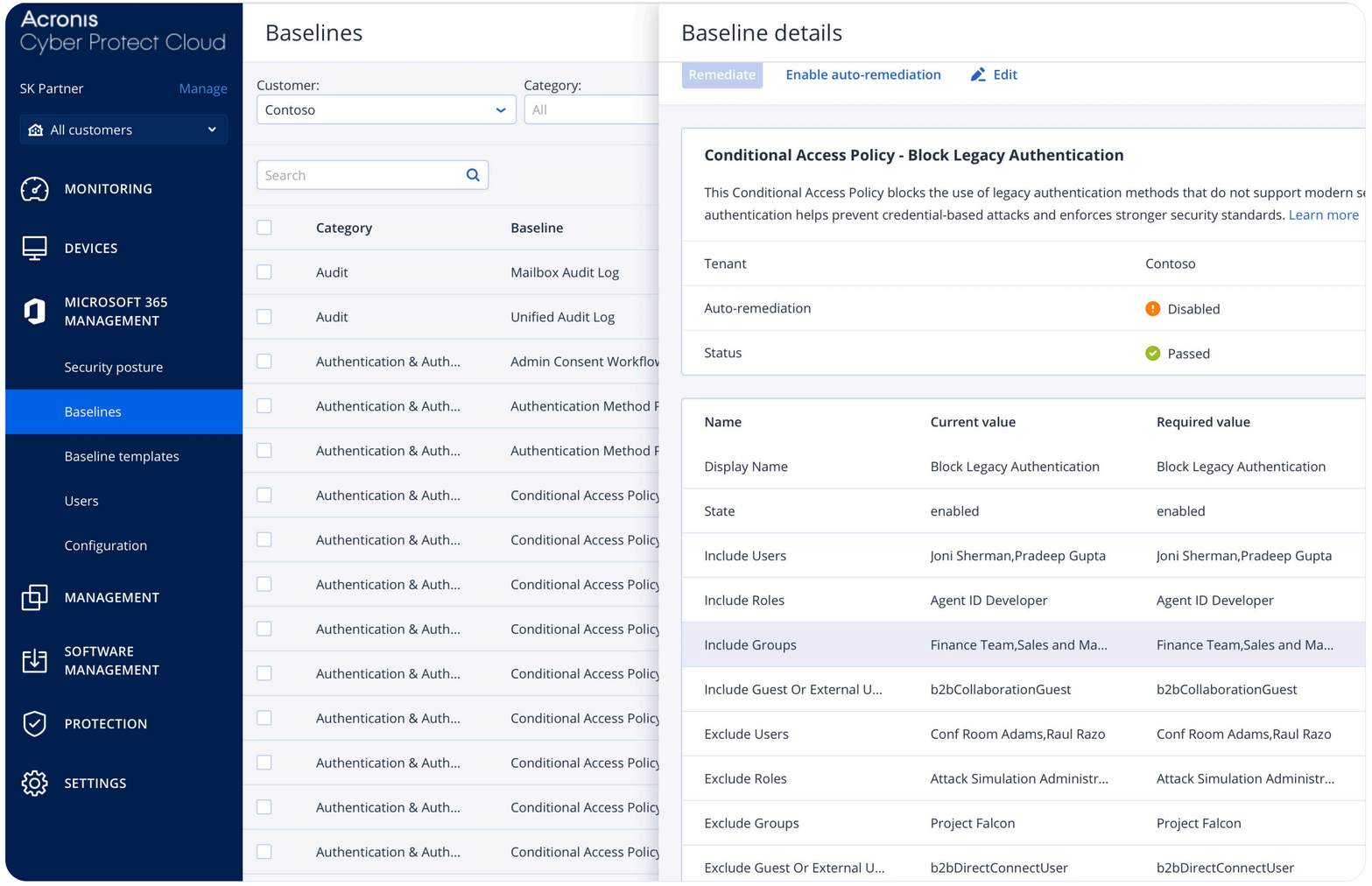
O que acabou de acontecer?

Você não perseguiu um login.

Você:

- identificou lacunas sistêmicas de identidade;
- corrigiu-as uma vez;
- aplicou-as em todos os lugares;
- garantiu que não ressurjam.

O Acronis SPM elimina as condições que contribuem para o sucesso de ataques do tipo password spraying em grande escala.



Situação 2

Abuso do consentimento OAuth

“O invasor não precisa mais do usuário.”

Um usuário aprova sem saber um aplicativo OAuth malicioso. A partir desse momento, o invasor não precisa mais de credenciais. Ele tem acesso permanente e no nível da API a e-mails e arquivos por meio do Microsoft Graph, muitas vezes sem disparar alertas.

Não há logins comprometidos nem atividades de autenticação suspeitas, e tudo parece legítimo.

O Acronis SPM expõe essa camada oculta. Ele mostra todos os aplicativos OAuth em todos os locatários e as permissões que receberam, como Mail.Read ou Files.Read.All, além de destacar aplicativos arriscados ou desconhecidos.

A partir daí, você pode identificar rapidamente aplicativos com altos privilégios ou recém-adicionados, revogar as permissões e remover o acesso não autorizado. As políticas podem ser padronizadas, restringindo o consentimento do usuário e exigindo a aprovação do administrador, enquanto a automação garante que esses controles sejam aplicados em todos os locatários.

Em vez de correr atrás de ameaças baseadas na identidade, você descobre e elimina o acesso permanente na camada de aplicativo e impede que ele volte.

O que você faz (na plataforma)

1 **Identifica aplicativos arriscados**
- Faz uma filtragem por aplicativos com altas permissões.
- Detecta aplicativos recém-adicionados ou desconhecidos.

2 **Corrige imediatamente**
- Revoga diretamente permissões de aplicativos.
- Remove integrações não autorizadas.

3 **Padroniza a política**
- Restringe o consentimento do usuário.
- Exige aprovação do administrador.

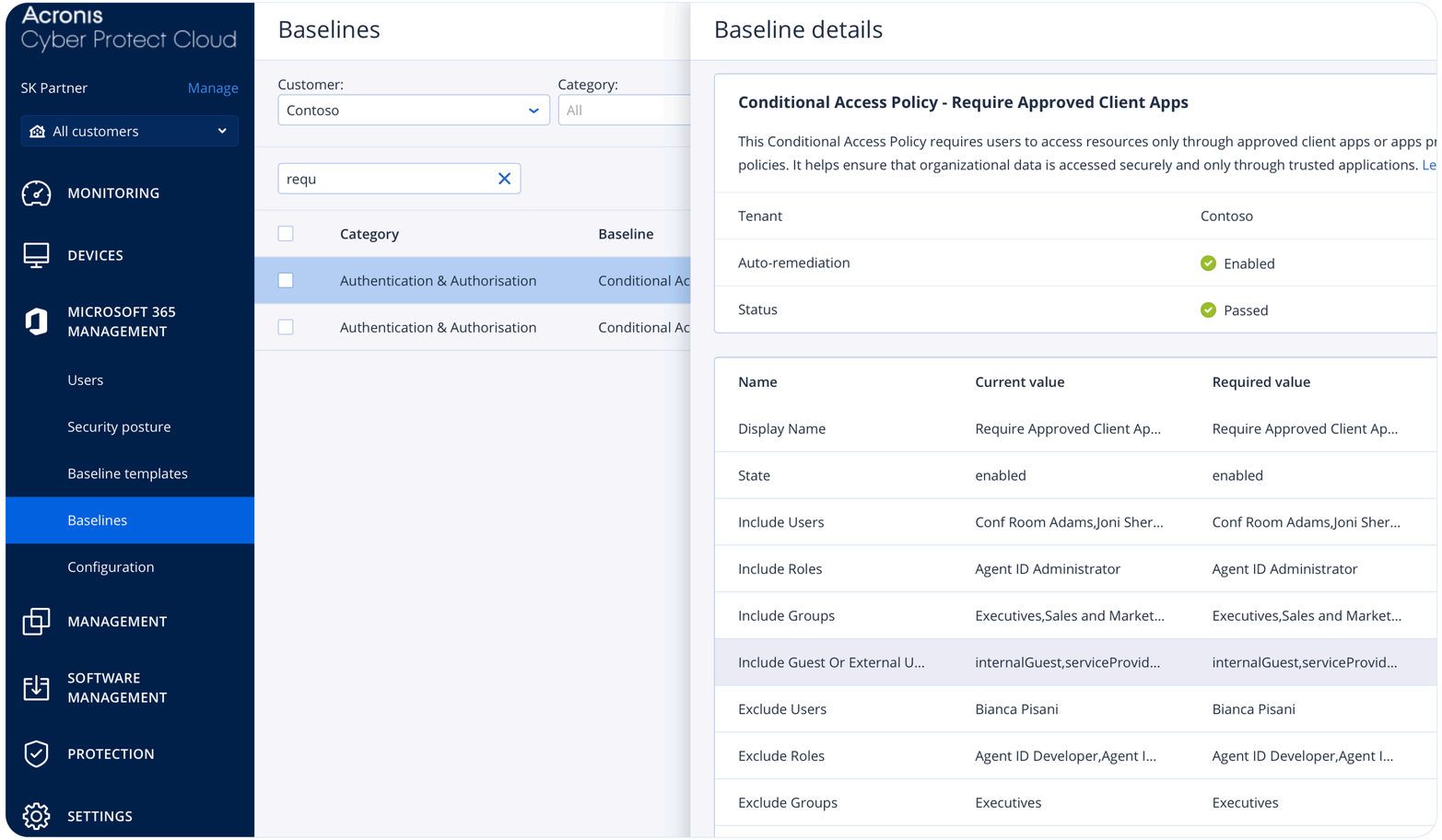
4 **Automatiza a aplicação**
- Aplica políticas de governança de aplicativos em todos os locatários.
- Detecta automaticamente novos aplicativos arriscados.

O que acabou de acontecer?

Você:

- encontrou uma persistência que contorna a identidade;
- removeu-a na hora;
- impediu que ela reaparecesse.

O Acronis SPM oferece visibilidade e controle sobre a camada de aplicativos da qual os invasores dependem para ter acesso de longo prazo.



Situação 3

Phishing por código de dispositivo

“A MFA funcionou e mesmo assim o invasor entrou.”

Um usuário conclui um login legítimo da Microsoft e passa pela MFA, mas o invasor captura o token de autenticação. Com ele, o invasor tem acesso permanente, lê e-mails e cria regras de caixa de correio, tudo sem disparar alertas óbvios.

Não há logins com falha, e a MFA parece ter funcionado como esperado.

O Acronis SPM expõe o problema real: lacunas na política. Ele destaca políticas de acesso condicional fracas ou ausentes, falta de controles de sessão e configurações de identidade que não estão de acordo com as práticas recomendadas.

A partir daí, você impõe um acesso condicional mais forte, aplica restrições de sessão e padroniza esses controles em todos os locatários. O monitoramento contínuo garante que os desvios sejam detectados e corrigidos.

Em vez de detectar o abuso de token, você elimina as condições que o permitem.

O que você faz (na plataforma)

1 **Faz uma verificação de conformidade de referência**

- Compara as políticas do locatário com as práticas recomendadas.

2 **Impõe controles de identidade**

- Fortalece o acesso condicional.
- Aplica restrições de sessão.

3 **Automatiza a remediação**

- Aplica políticas em todos os locatários.
- Corrige automaticamente os desvios.

4 **Mantém a aplicação contínua**

- O Acronis SPM monitora desvios da política.
- Sinaliza o enfraquecimento dos controles.

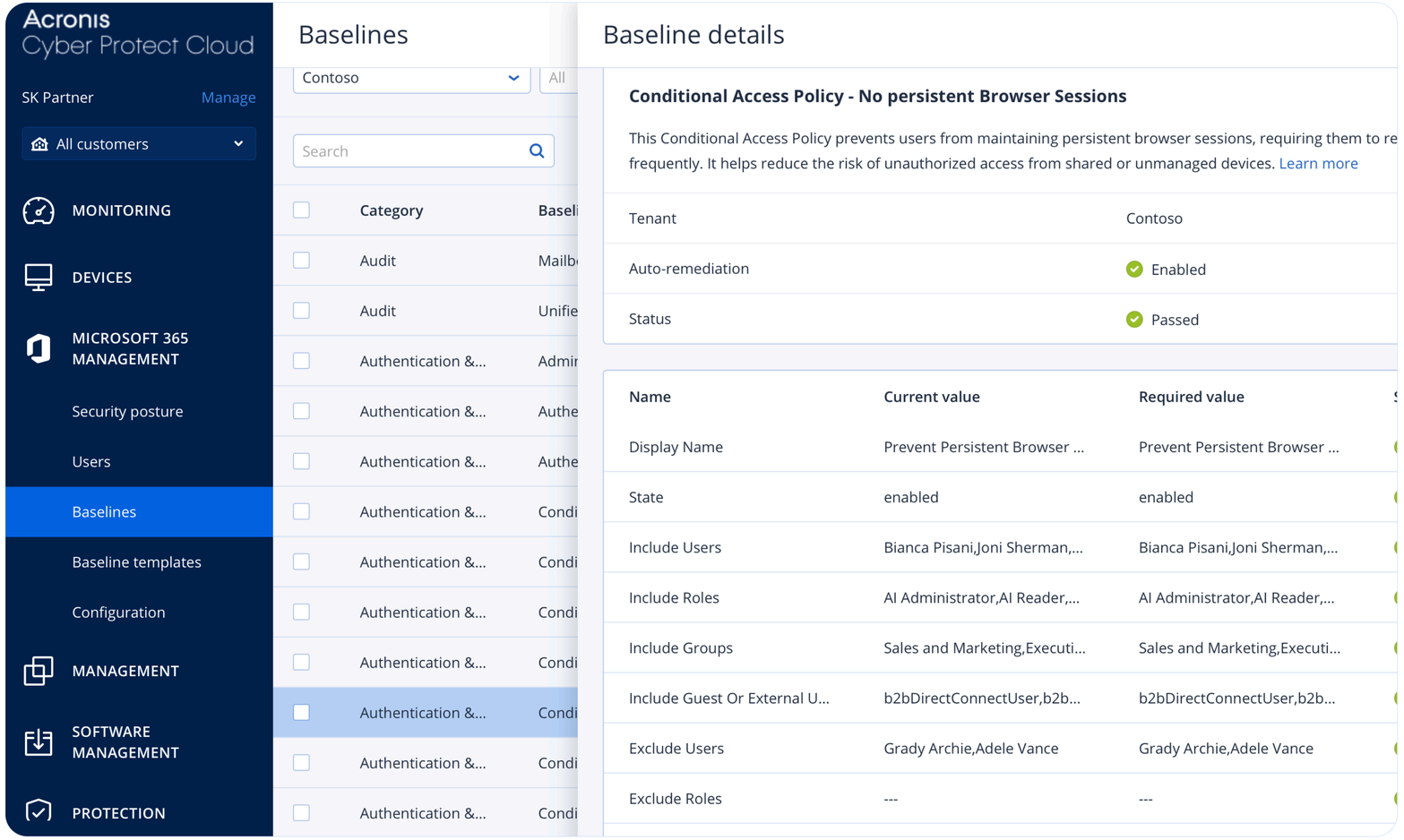
O que acabou de acontecer?

Você não detectou o roubo do token.

Você:

- fechou as lacunas de política que o permitiam;
- padronizou os controles em todos os locatários;
- garantiu a aplicação de longo prazo.

A Acronis SPM protege os fluxos de autenticação, não apenas as identidades.



Situação 4

Ampliação de privilégios

“Uma conta se torna todo o locatário.”

Um invasor compromete uma única conta e começa a explorar. Ele encontra privilégios excessivos, vários administradores globais e separação de funções fraca. A partir daí, a ampliação de privilégios é simples, levando ao controle total do locatário.

Geralmente não há alertas. O aumento de privilégios acontece gradualmente e, sem visibilidade centralizada, o risco passa despercebido.

O Acronis SPM mostra isso com clareza, apresentando funções de administrador em todos os locatários, identificando contas com privilégios excessivos e atribuindo risco com base na exposição.

O que você faz (na plataforma)

1 **Audita funções com privilégios**

- Identifica contas de administrador com privilégios excessivos.

2 **Aplica o menor privilégio**

- Reduz os administradores globais.
- Padroniza as atribuições de funções.

3 **Automatiza em todos os locatários**

- Usa modelos de referência para impor políticas de funções.

4 **Mantém o controle do ciclo de vida**

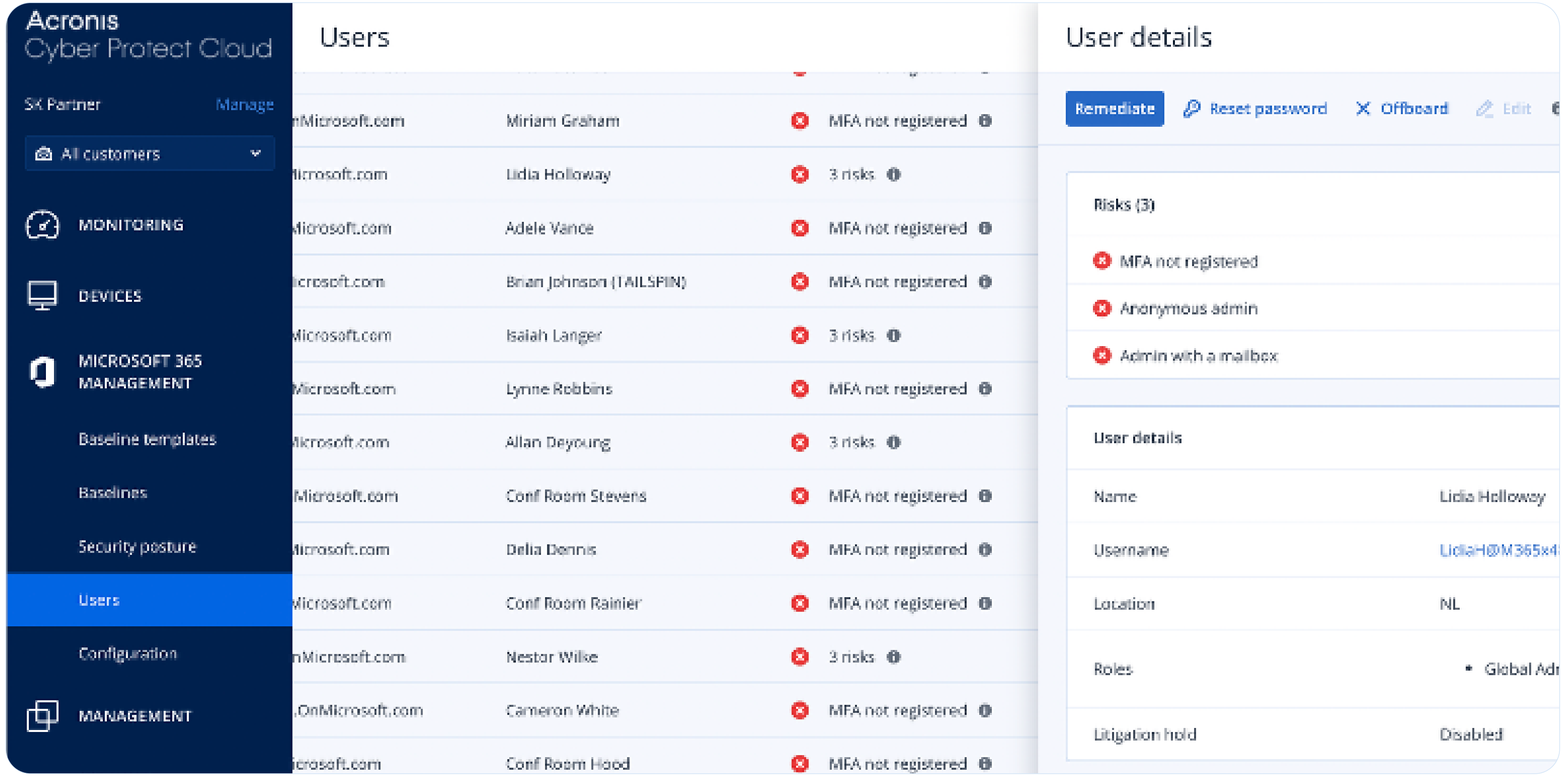
- Atribui as funções corretas durante a integração.
- Revoga o acesso, as sessões e as licenças durante a desativação.

O que acabou de acontecer?

Você:

- reduziu o raio de impacto da violação;
- padronizou os privilégios entre ambientes;
- garantiu a segurança do ciclo de vida da identidade.

O Acronis SPM transforma a dispersão de privilégios em uma política controlada e aplicável.



Depois, você pode auditar funções privilegiadas, reduzir o número de administradores globais e aplicar políticas de menor privilégio em todos os locatários usando modelos de referência. O gerenciamento contínuo do ciclo de vida garante o acesso correto durante a integração e a revogação completa durante a saída.

Em vez de reagir à ampliação, você limita o raio de impacto desde o início.

O que une todos esses ataques

Em todas as situações:

Ataque	Causa raiz
Password spraying	Controles de identidade fracos
Abuso do OAuth	Configurações incorretas de permissão de app
Phishing por código de dispositivo	Lacunas na política
Ampliação de privilégios	Permissões excessivas

O padrão

Entrada equivale a identidade.

Persistência equivale a configuração.

Impacto equivale a todo o locatário.

A diferença do Acronis SPM

O SPM não apenas mostra o risco.

Ele permite que os MSPs operem a segurança em escala.

Monitoramento contínuo

- Detecção 24/7 de desvio de postura.
- Identificação em tempo real de novos riscos.

Segurança orientada por referência

- Referências predefinidas com as práticas recomendadas.
- Modelos de referência personalizados.
- Padronização em todos os locatários.

Remediação automatizada e manual

- Correção de problemas diretamente no console.
- Automatização da remediação de riscos recorrentes.
- Eliminação de tarefas manuais repetitivas.

Gerenciamento multilocatário

- Controle centralizado em todos os clientes finais.
- Propagação da política em escala.

Controle total do ciclo de vida da identidade

- Integração segura com funções e políticas corretas.
- Desativação segura com revogação de sessão e limpeza.

Integração operacional

- Integração com ferramentas de automação de serviços professionais.
- Fluxos de trabalho simplificados para equipes de MSP.

Considerações finais

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

- ninguém vê a exposição;
- ninguém a corrige de forma consistente;
- ninguém a aplica continuamente.

O Acronis SPM muda isso.

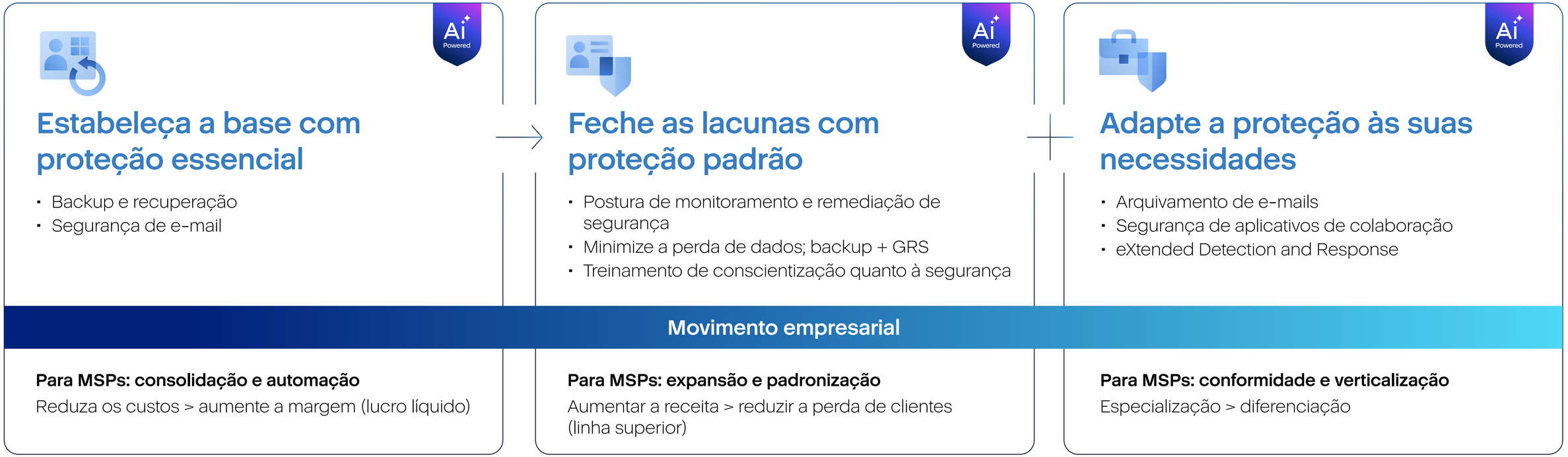
Ele dá aos MSPs a capacidade de:

- ver o risco em cada multilocatário;
- corrigi-lo instantaneamente;
- aplicá-lo automaticamente;
- mantê-lo corrigido ao longo do tempo.

Security Posture Management: um pilar central do Protected 365

O Security Posture Management (SPM) não é um complemento opcional, mas sim um recursos fundamental na solução Acronis Protected 365, que viabiliza a promessa da plataforma de proteção completa, aprimorada por IA, 7 em 1 para o Microsoft 365. O SPM funciona em conjunto com backup, segurança de e-mail, segurança de colaboração, XDR, arquivamento de e-mails e treinamento de conscientização quanto à segurança para fechar a lacuna completa de responsabilidade compartilhada da Microsoft nos aplicativos Exchange, Teams, SharePoint e OneDrive.

O SPM desempenha um papel crítico no estágio “fechamento das lacunas com proteção padrão” do modelo de maturidade do Protected 365, fazendo as organizações evoluirem da proteção básica para a resiliência proativa. Embora o backup e a segurança de e-mail estabeleçam proteção essencial, o SPM introduz avaliação contínua de riscos, aplicação de política e remediação automatizada, garantindo que os ambientes permaneçam alinhados com as melhores práticas e em conformidade com padrões em evolução.



Ao monitorar continuamente as configurações, detectar desvios e permitir a remediação rápida, o SPM aborda diretamente um dos riscos mais comuns e negligenciados no Microsoft 365: a configuração incorreta de usuários e os desvios de segurança. Ele transforma a segurança de um processo reativo em uma disciplina proativa, orientada por política, que reduz a exposição, fortalece a conformidade e aprimora a resiliência cibernética geral.

De forma crucial, o SPM é fornecido dentro da mesma plataforma multilocatária única da Acronis, reforçando a proposta de valor central do Protected 365: um fornecedor, um contrato, uma solução integrada. Isso elimina a proliferação de ferramentas, reduz a sobrecarga operacional e ajuda MSPs e equipes de TI a aumentar a escala com eficiência, além de melhorar a qualidade do serviço e a lucratividade.

Aja: feche as lacunas agora

Configurações incorretas não esperam, e você também não deveria esperar.
Comece hoje mesmo sua avaliação do Acronis Security Posture Management e descubra instantaneamente os riscos, aplique as melhores práticas e fortaleça a segurança do seu Microsoft 365.

COMEÇAR AVALIAÇÃO GRATUITA

Acronis

Para obter mais informações,
acronis.com