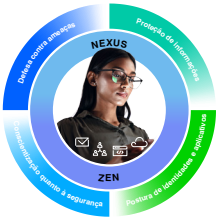
Proofpoint Account Takeover Protection

Detecte e responda a sequestros de contas de nuvem

Principais vantagens

- Detecte contas de Microsoft 365, Google Workspace e Okta comprometidas
- Defenda-se de ataques de sequestro de contas que contornam MFA
- Acelere suas investigações com uma visão centralizada das atividades subsequentes ao sequestro de contas
- Reduza o tempo de permanência dos atacantes suspendendo contas e forçando redefinição de senhas
- Reverta alterações maliciosas em regras de caixa de entrada e configurações de MFA
- Remova aplicativos suspeitos de terceiros

Esse conjunto de soluções é parte da plataforma integrada Human-Centric Security da Proofpoint que atende as quatro áreas de risco baseado em pessoas.



O Proofpoint Account Takeover Protection (ATO Protection) estende o Proofpoint Targeted Attack Protection (TAP) para detectar contas de nuvem comprometidas e proteger os seus ambientes de nuvem.

O Proofpoint ATO Protection estende o Proofpoint Targeted Attack Protection (TAP) para detectar e proteger contas de nuvem comprometidas. O Proofpoint ATO Protection utiliza inteligência artificial (IA), inteligência correlacionada sobre ameaças e análise comportamental para detectar atividades suspeitas em toda a cadeia de ataque. Ele detecta mudanças subsequentes ao comprometimento feitas pelos atacantes e elimina o acesso destes. Ele reverte atualizações maliciosas em regras de caixa de entrada e configurações de autenticação por múltiplos fatores (MFA). Ele também remove aplicativos suspeitos de terceiros, bem como coloca em quarentena e remove arquivos suspeitos.

O Proofpoint ATO Protection oferece relatórios detalhados que mostram logins suspeitos, usuários atacados e configurações e sistemas afetados. A integração com o Proofpoint Identity Threat Defense mostra, com um único clique, o impacto potencial do sequestro de uma conta sobre outras contas e hosts. Esses insights ajudam você a deter os ataques antes que estes se tornem violações graves que prejudiquem a sua empresa.

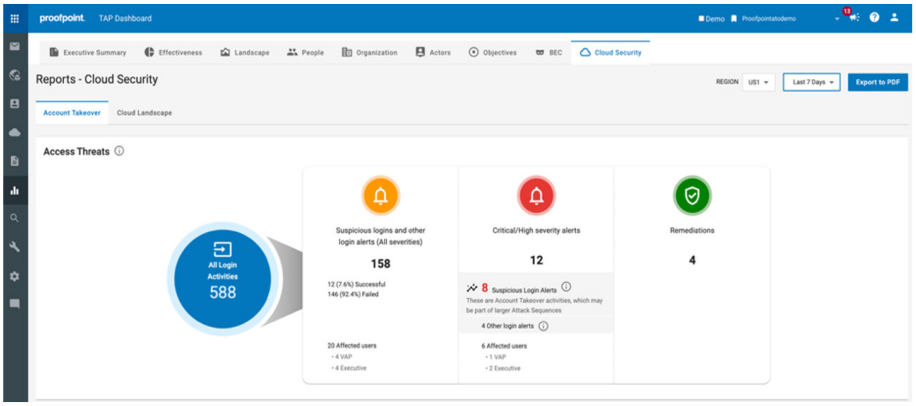


Figura 1. O Proofpoint ATO Protection detecta logins suspeitos, oferece insights detalhados que ajudam a investigar ameaças e reverte alterações maliciosas.

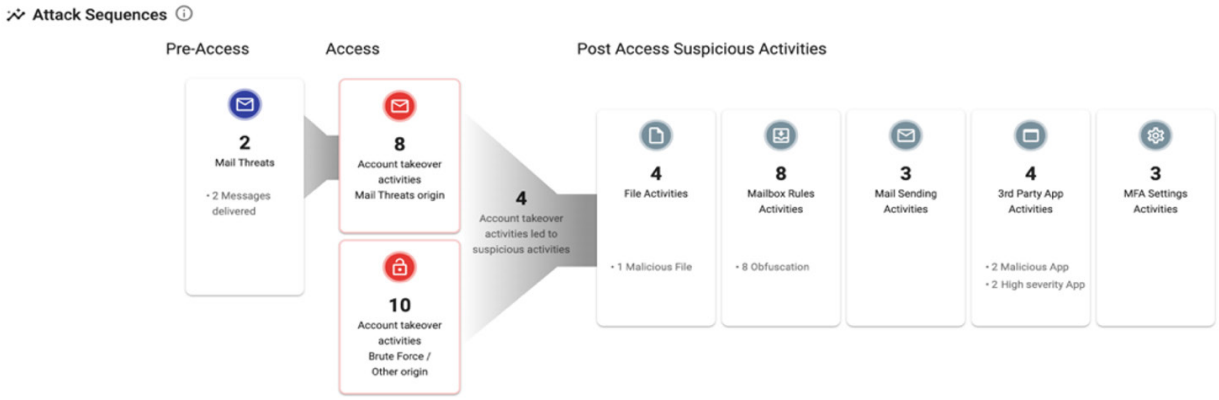


Figura 2. O relatório Attack Sequence (Sequência de ataque) mostra atividades de ameaça anteriores e posteriores ao acesso nas contas afetadas.

Detecção e visibilidade melhoradas

O Proofpoint ATO Protection detecta contas comprometidas, e-mails suspeitos e outras atividades nos seus ambientes de nuvem. Ele utiliza inteligência sobre ameaças obtida de mais de 40 milhões de usuários monitorados em milhares de organizações. Ele combina essas informações com inteligência artificial e análise comportamental para detectar atividades incomuns no seu ambiente. Essa combinação de técnicas reduz os alertas de falsos positivos. Você tem a confiança proporcionada por detecções precisas e uma visão clara de todas as atividades nas suas contas atacadas.

Quando uma conta é sequestrada, o Proofpoint ATO Protection adiciona alertas ao dashboard do TAP. Um cronograma do ataque mostra atividades de sequestro de conta, atividades de arquivo e de e-mail, mudanças em regras de caixa de entrada e em configurações de MFA e o acréscimo de aplicativos de terceiros.

Investigações aceleradas

O Proofpoint ATO Protection mostra aos seus analistas de segurança a causa de um sequestro de contas e como limitar riscos adicionais. Essas informações são integradas com o processo e o sistema de investigação do Proofpoint TAP. Assim, você obtém insights que complementam aqueles proporcionados pelo Proofpoint TAP. Um cronograma do ataque mostra as contas que foram sequestradas. Você pode clicar e investigar cada evento do cronograma.

Você pode ver como a conta foi atacada e a localização do atacante. Você também pode saber se outros usuários foram atingidos por ameaças semelhantes. A análise avançada oferece cronogramas de atividades detalhados sobre usuários, endereços IP, domínios e outros atributos. Esses insights minuciosos ajudam você a avaliar os riscos adicionais para a sua organização.

Resposta automatizada

O Proofpoint ATO Protection detecta e reverte alterações maliciosas em regras de caixa de entrada e em configurações de MFA. Os atacantes frequentemente alteram regras de caixa de entrada para se ocultar no seu sistema e monitorá-lo antes de iniciar phishing interno ou realizar outras etapas de ataque. O Proofpoint ATO Protection também remove aplicativos maliciosos de terceiros. Todas essas ações limitam os danos à sua organização e reduzem o tempo necessário para investigar e responder às ameaças. Caso a sua investigação mostre outras atividades maliciosas, você pode corrigir as contas que foram sequestradas. Você também pode remover os arquivos acrescentados pelos atacantes à conta de um usuário.

O “Proofpoint Account Takeover Protection” anteriormente se chamava “Proofpoint TAP Account Takeover”.

SAIBA MAIS

Para obter mais informações, visite **proofpoint.com/br**.