

Proofpoint Shadow

Impeça a ampliação de privilégios e a movimentação lateral em tempo real

Principais vantagens

- Assegura detecção antecipada do atacante e investigações abrangentes das ameaças
- Reduz falsos positivos no SOC oferecendo alertas de alta fidelidade
- Tecnologia sem agente implantada facilmente, com pouco envolvimento da TI
- Proporciona defesa contínua ajustando-se dinamicamente conforme as mudanças no ambiente de TI
- Expansibilidade comprovada em redes de mais de um milhão de endpoints
- Preenche a lacuna deixada pela detecção de ameaças com base em assinaturas e anomalias

Mais de 90% dos ataques cibernéticos envolvem identidades arriscadas. Os atacantes adaptaram suas estratégias visando identidades privilegiadas em vez de tentar invadir sistemas diretamente. Essa mudança levou a um surto em violações de dados e ataques de ransomware bem-sucedidos. Ao se concentrarem em identidades vulneráveis, os atacantes podem reduzir seu cronograma de ataque de meses para semanas ou até mesmo horas.

A Proofpoint pode ajudar. Nossa poderosa solução Proofpoint Shadow transforma os seus endpoints em uma teia de enganos que torna quase impossível para os atacantes movimentarem-se lateralmente no seu ambiente sem serem detectados. Como parte da plataforma Proofpoint Identity Threat Defense, o Shadow captura perpetradores de ameaças deterministicamente, com base em suas interações com o que parecem ser caminhos legítimos nos seus endpoints, mas que na verdade são artifícios enganosos que utilizamos.

Diferentemente de outras ferramentas, o Shadow não conta com análises baseadas em assinaturas ou comportamentos. Ele também não utiliza agentes ou “potes de mel” que possam ser explorados. Em vez disso, a arquitetura sem agentes do Shadow permite que os artifícios enganosos atuem discretamente, escondidos dos atacantes. O Shadow já conseguiu se defender de mais de 160 exercícios de “red team” com algumas das maiores organizações de segurança do mundo, como Microsoft, Mandiant, Departamento de Defesa dos EUA e Cisco.

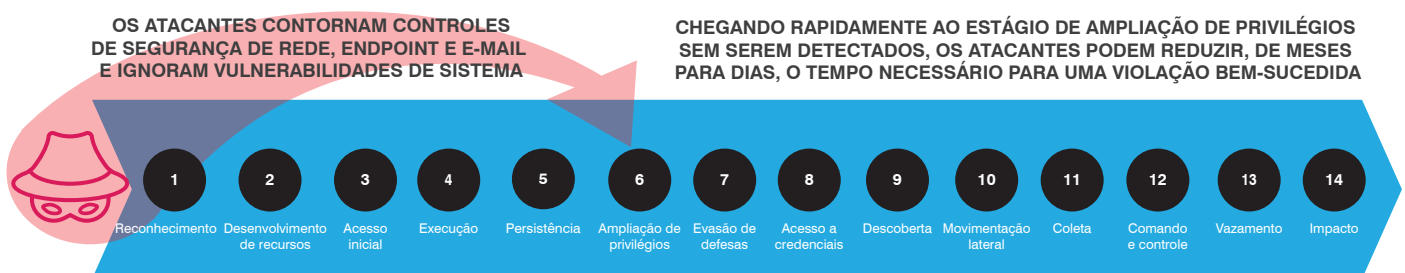


Figura 1. Atualmente, os atacantes concentram-se nas identidades vulneráveis como principal caminho na cadeia de ataque.

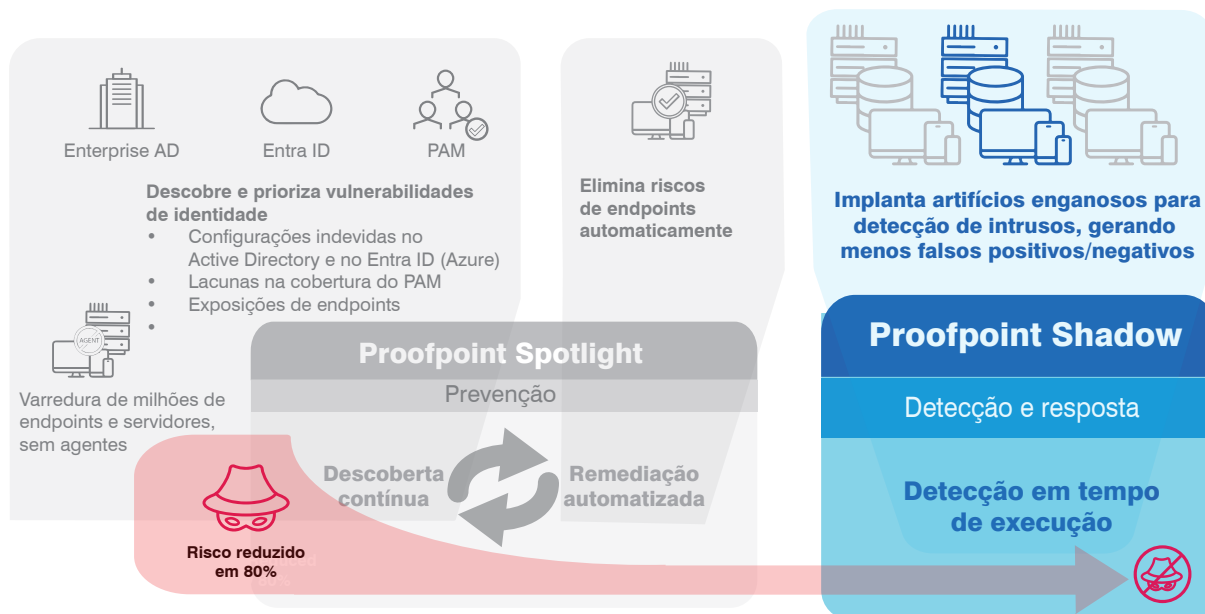


Figura 2. Como parte da plataforma Proofpoint Identity Threat Defense, o Shadow cria uma teia de enganos que detecta e alerta sobre a movimentação lateral do atacante nas suas redes.

Detecção de probabilística a determinística

Você pode detectar e responder a ameaças de várias maneiras. Você pode examinar padrões muito específicos ou assinaturas, por exemplo. Ou pode analisar como um possível perpetrador de ameaças se comporta. Ferramentas convencionais frequentemente não conseguem capturar ataques graves, como quando um perpetrador de ameaças amplia privilégios ou se movimenta lateralmente na sua rede sem ser detectado. Tais falhas de detecção podem permitir que os perpetradores de ameaças sequestrem contas, disseminem ransomware ou roubem dados. As equipes de segurança precisam de uma abordagem mais avançada e confiável para se manterem à frente desses tipos de ataque.

O Shadow oferece uma abordagem determinística. Ele utiliza artifícios enganosos amplamente distribuídos para envolver ativamente os atacantes ao longo da cadeia de ataque e rastrear suas atividades. Esses artifícios enganosos são escondidos profundamente nos endpoints da empresa. Eles se assemelham e atuam como autênticos arquivos, sessões de RDP, conexões de bancos de dados, e-mails, scripts etc. cobijados pelos atacantes. Quando um atacante se envolve com um deles, o Shadow envia à equipe de segurança um alerta em tempo real com informações forenses. A equipe pode, então, utilizar essas informações para tomar decisões inteligentes no sentido de deter o ataque e proteger a empresa contra qualquer dano.

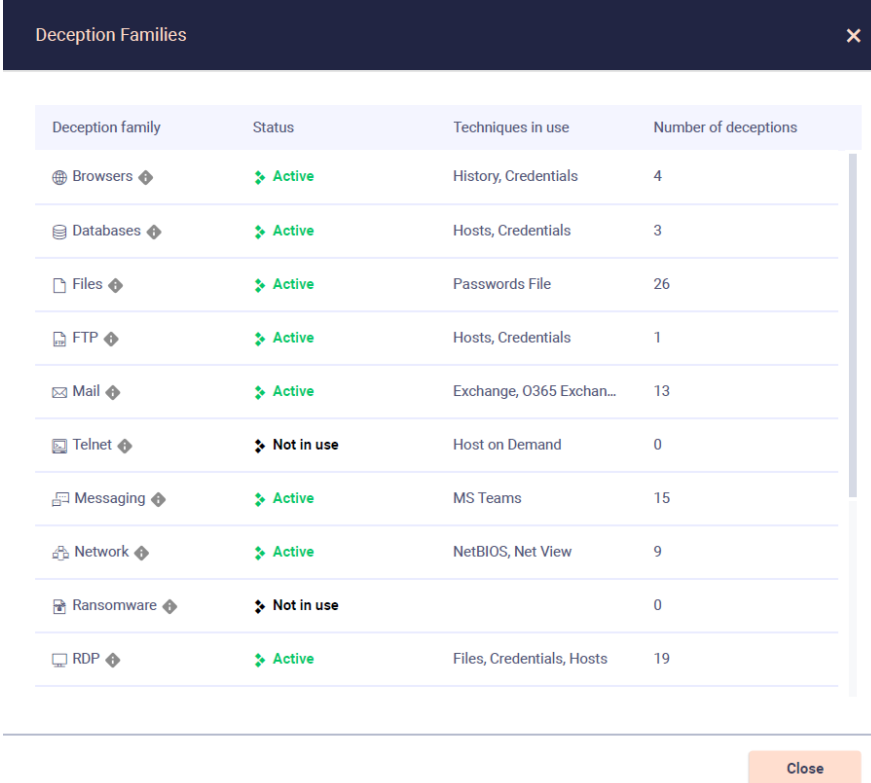
Detecção e proteção sem agentes

A abordagem exclusiva de dissolução binária sem agentes do Shadow ajuda tanto os administradores de TI quanto as equipes de segurança. Automação inteligente e uma carga operacional leve minimizam o impacto sobre a TI. Diferentemente das ferramentas de segurança que se baseiam em agentes de software, os atacantes não podem desativar ou contornar o Shadow.

Mais de 75 técnicas enganosas

O Shadow emprega mais de 75 técnicas enganosas ativas. Ele cria arquivos e compartilhamentos de arquivos falsos, conexões de banco de dados, conexões FTP e RDP/SSH, URLs e históricos de navegador, credenciais do Windows, sessões de rede, e-mails, scripts e até mesmo chats antigos do Teams que servem como armadilhas aparentemente valiosas para os atacantes. Essas técnicas funcionam conjuntamente para pegar os atacantes no ato, não importa onde comece o comprometimento — dentro ou fora do ambiente.

Com o Shadow, as equipes de segurança podem automatizar a criação de centenas de arquivos de Word e Excel personalizados que parecem autênticos; eles podem até incluir o logotipo e o timbre da sua empresa. Dados falsos dentro dos documentos disparam alarmes para os administradores de segurança, caso um atacante tente utilizá-los para obter acesso adicional.



Deception family	Status	Techniques in use	Number of deceptions
Browsers	Active	History, Credentials	4
Databases	Active	Hosts, Credentials	3
Files	Active	Passwords File	26
FTP	Active	Hosts, Credentials	1
Mail	Active	Exchange, O365 Exchan...	13
Telnet	Not in use	Host on Demand	0
Messaging	Active	MS Teams	15
Network	Active	NetBIOS, Net View	9
Ransomware	Not in use		0
RDP	Active	Files, Credentials, Hosts	19

Figura 3. Interface de usuário do Proofpoint Shadow.

Engano automatizado e personalizado para cada endpoint

O sistema de automação inteligente do Shadow cria artifícios enganosos realistas e convincentes para os atacantes. Ele pode se adaptar e se expandir facilmente, sem sobrecarregar a equipe de segurança. O Shadow analisa o cenário de endpoints, gera artifícios enganosos específicos para cada máquina e os implanta com apenas um clique. A solução também cuida do processo contínuo de ajustar e gerenciar os artifícios enganosos ao longo do tempo.

Uma visão do ponto de vista do atacante

O console de gerenciamento do Shadow oferece uma variedade de informações forenses sobre a atividade do atacante. Ele fornece às equipes de segurança dados importantes sobre o quão próximos os atacantes estão dos seus ativos críticos. Ele também pode mostrar um cronograma completo do que eles estavam fazendo quando se deixaram enganar pelos artifícios. E pode mostrar a analistas de segurança como os artifícios enganosos se apresentam, do ponto de vista dos atacantes.

SAIBA MAIS

Para obter mais informações, visite [proofpoint.com/br](https://www.proofpoint.com/br).

SOBRE A PROOFPOINT

A Proofpoint, Inc. é uma empresa líder em cibersegurança que protege as organizações em seus maiores riscos e seus ativos mais valiosos: sua equipe. Com um pacote integrado de soluções baseadas em nuvem, a Proofpoint ajuda empresas do mundo todo a deter ameaças direcionadas, proteger seus dados e tornar seus usuários mais resilientes contra ataques cibernéticos. Organizações líderes de todos os portes, incluindo 75% das empresas da Fortune 100, contam com a Proofpoint para obter soluções de segurança e conformidade centradas nas pessoas e que minimizem seus riscos mais críticos em e-mail, nuvem, redes sociais e Web. Mais informações estão disponíveis em www.proofpoint.com/br.

©Proofpoint, Inc. Proofpoint é uma marca comercial da Proofpoint, Inc. nos Estados Unidos e em outros países. Todas as demais marcas comerciais aqui mencionadas são propriedade de seus respectivos donos.