Proofpoint Spotlight

Descubra, priorize e corrija automaticamente vulnerabilidades relacionadas a identidades antes que os atacantes as explorem

Principais vantagens

- Descubra riscos de identidade em múltiplas etapas da cadeia de ataque
- Tenha visibilidade sobre as identidades, abrangendo: Active Directory, Entra ID (antigo Azure AD), PAMs, endpoints, LAPS
- Obtenha automaticamente uma lista priorizada de vulnerabilidades de identidade expostas nos endpoints
- Corrija vulnerabilidades como administradores ocultos, manual ou automaticamente
- Tenha visibilidade do risco em subsidiárias e instituições recém-adquiridas com um mapa corporativo de domínios e confianças
- Relatórios inteligentes sobre tendências de risco ao longo do tempo para melhorar a sua postura de segurança de identidade

O roubo e abuso de credenciais é uma preocupação comum e crescente. Os atacantes estão mudando o foco de ameaças baseadas em sistemas para ataques centrados em identidades. Eles podem realizar tais ataques em questão de horas ou mesmo minutos. E podem não deixar vestígio algum de comprometimento ou malware.

Mesmo com gerenciamento de contas privilegiadas (PAM) e autenticação por múltiplos fatores (MFA) em uso, 1 em cada 6 endpoints corporativos ainda tem identidades vulneráveis. Estes são os alvos principais dos atacantes cibernéticos. Ransomware e outras ameaças direcionadas concentram-se em identidades privilegiadas como um meio para atingir um objetivo.

O Proofpoint Spotlight pode ajudar a reduzir o risco de que as suas identidades sejam utilizadas contra você. A solução é parte da plataforma Proofpoint Identity Threat Defense. Ela oferece descoberta contínua e abrangente de vulnerabilidades de identidade e corrige automaticamente essas ameaças. O Spotlight resolve ameaças de identidade antes que elas venham a se tornar violações em grande escala.

Engenheiros de defesa nacional desenvolveram o Spotlight para ajudar as equipes de segurança a priorizar tarefas de autorremediação de ameaças. Os alertas servem para evitar impacto sobre os negócios. Porém, a quantidade crescente desses alertas resultou em volumes crescentes de “ruído”, cuja triagem exige tempo das equipes de segurança.

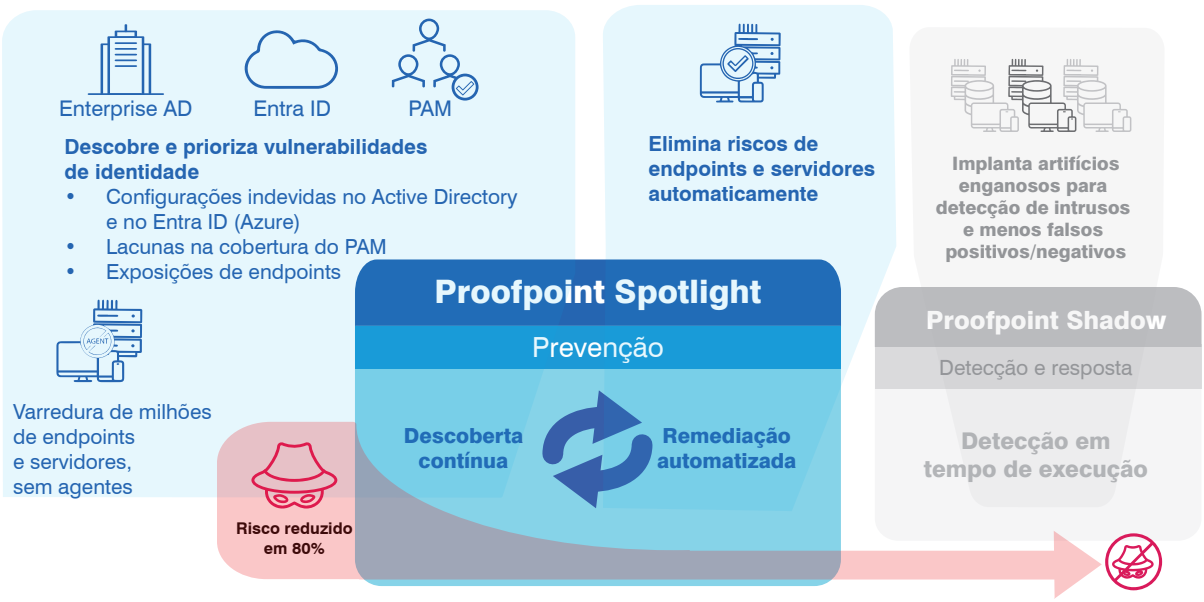

Figura 1. Como parte do Proofpoint Identity Threat Defense, o Proofpoint Spotlight oferece descoberta contínua e correção de vulnerabilidades de identidades privilegiadas e violações de política.

Como os perpetradores de ameaças se aproveitam de identidades privilegiadas

Quando os atacantes chegam pela primeira vez a um host, este não costuma ser seu objetivo final. Na maioria dos ataques, os perpetradores de ameaças tentam ampliar privilégios. Em seguida, eles movimentam-se lateralmente pelo ambiente para chegar a seu verdadeiro objetivo sem serem detectados. Eles utilizam ferramentas como Bloodhound, Cobalt Strike, Mimikatz e ADFind para explorar rapidamente credenciais privilegiadas e ocultar sua presença.

Em nossa pesquisa, mais de 90% das organizações tiveram uma violação relacionada a identidade no ano passado. E os ataques de ransomware atingiram níveis recordes. Há várias razões para esse aumento. Uma é que implantações de sistemas de gerenciamento de identidades e acessos são muito complexas. As identidades também mudam continuamente. E as organizações não têm visibilidade total sobre as brechas em seus ambientes.

Outras razões incluem:

- Configurações de PAM e gerenciamento de credenciais de contas de manutenção, de administrador local e de domínio privilegiado insuficientes ou inadequados
- Criação não intencional de contas de administrador oculto com privilégios excessivos
- Encerramento inadequado de sessões de RDP
- Aplicativos do usuário — como navegadores, SSH, FTP, PuTTY e bancos de dados — que armazenam temporariamente credenciais e tokens de acesso à nuvem nos endpoints

Exemplo do mundo real: ataque contra seguradora

Um perpetrador de ameaças recorreu ao “stuffing” de credenciais para acessar uma rede via protocolo de desktop remoto (RDP). O atacante utilizou credenciais roubadas para o acesso inicial.

A partir daí, ele ampliou os privilégios para administrador de domínio. Dados críticos foram criptografados e alguns deles foram vazados. A organização pagou um resgate de US$ 40 milhões para se recuperar do ataque.

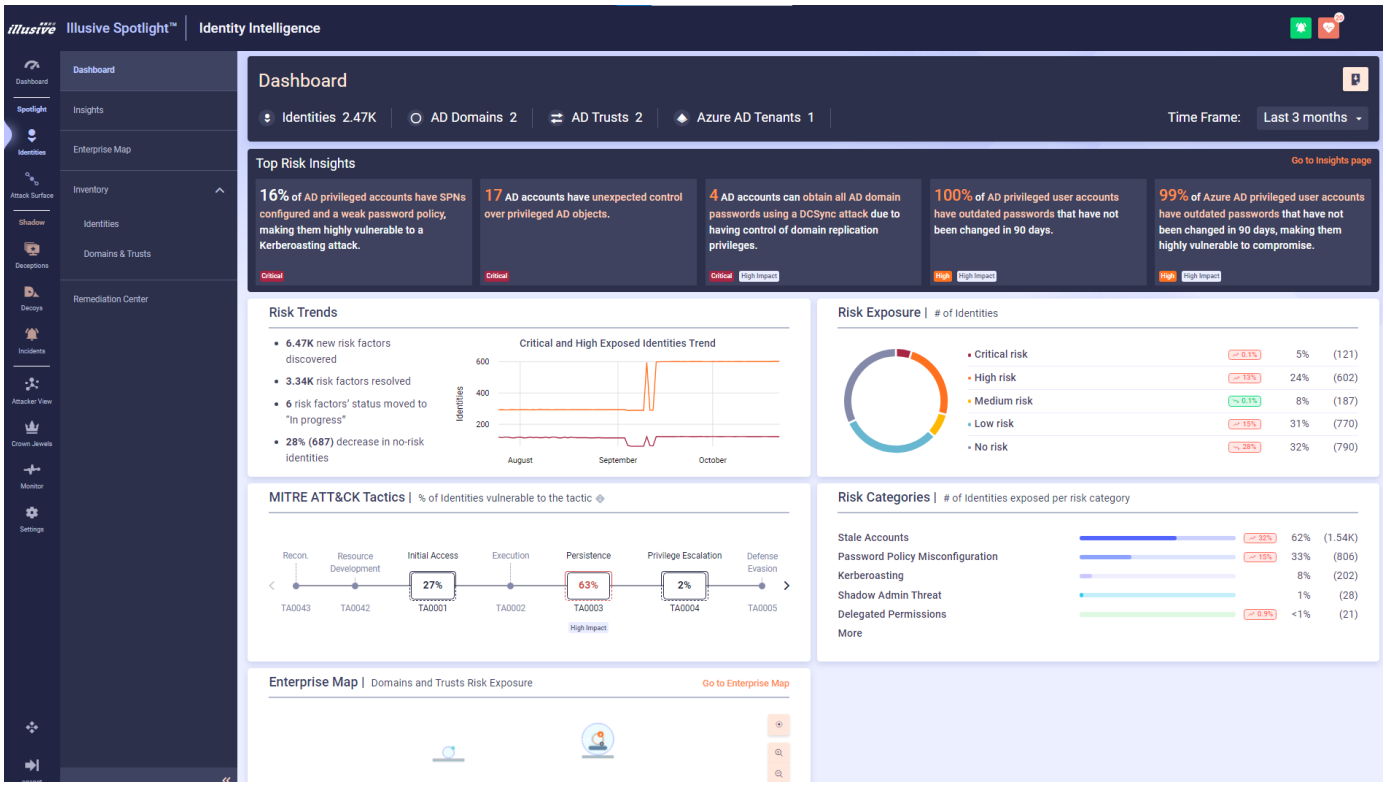

Figura 2. O dashboard de risco de identidade do Proofpoint Spotlight.

Encontre, priorize e corrija as identidades vulneráveis

O Spotlight revela as lacunas entre as suas políticas de segurança de identidade e os seus ambientes reais. Ele examina os seguintes sistemas para proporcionar visibilidade total e priorização das vulnerabilidades de identidade atuais:

- **Estruturas de diretório.** Active Directory e Entra ID (antigo Azure AD).
- **Soluções PAM.** CyberArk e Delinea Centrify.
- **Endpoints.** Clientes e servidores.
- **Tarefas.**

O Proofpoint Spotlight ajuda a evitar ataques eliminando as vulnerabilidades de identidade de que os atacantes necessitam para levar adiante crimes que podem resultar em violações significativas.

SAIBA MAIS

Para obter mais informações, visite **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**.