PANFLETO DA SOLUÇÃO

Sophos ITDR

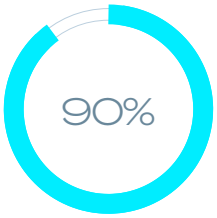
Neutralizar ameaças baseadas em identidade antes que possam impactar os seus negócios

O Sophos Identity Threat Detection and Response (ITDR) interrompe ataques baseados em identidade ao monitorar o seu ambiente continuamente em busca de riscos de identidade e configurações incorretas, e ao mesmo tempo fornece inteligência da dark web sobre credenciais comprometidas.

Ameaças de identidade: um problema de segurança em expansão

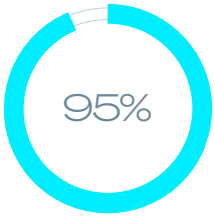
Controles e acesso baseado no usuário estão na linha de frente global da TI e da segurança cibernética da atualidade, e a mudança para a nuvem e o trabalho remoto só fez aumentar a complexidade de monitoramento e proteção da superfície de ataque de identidade. Os adversários usam identidades comprometidas, pontos fracos na infraestrutura e configurações incorretas para obter acesso não autorizado a sistemas e dados sensíveis. Portanto, detectar o abuso de identidade e bloquear ataques baseados em identidade ficam cada vez mais importantes para operações de segurança eficazes.

A prova está nos números

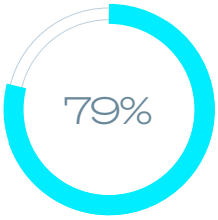


das organizações passaram por pelo menos uma violação relacionada a identidade no último ano.[1]

Custo médio de uma violação de dados.[2]



dos ambientes do Microsoft Entra ID apresentam um erro crítico de configuração.[3]



das violações de dados são relacionadas a identidade.[4]

Benefícios

- **Obtenha visibilidade** com uma exibição centralizada das identidades em todos os seus sistemas.
- **Descubra rapidamente** riscos baseados em identidade e erros de configuração com recomendações acionáveis.
- **Faça a varredura continuamente** em busca de mudanças na postura de identidade.
- **Faça a varredura da dark web** em busca de credenciais vazadas.
- **Detecte atividades potencialmente mal-intencionadas** provenientes de pessoal interno, IPs desconhecidos e locais incomuns.
- **Responda a ameaças de identidade** com velocidade e precisão.
- **Integre-o ao Sophos MDR** e acesse investigação e resposta especializadas de ameaças baseadas em identidade.

Solução Sophos ITDR

O Sophos ITDR previne os ataques baseados em identidade monitorando continuamente o seu ambiente em busca de riscos de identidade e configurações incorretas — uma questão que afeta 95% das organizações —, fornecendo também inteligência da dark web sobre credenciais comprometidas. Descubra os riscos à sua identidade em minutos — comparado a dias, que às soluções legadas oferecem — e faça uma análise constante da progressão, ou regressão, da sua superfície de ataque de identidade.

Diminua sua superfície de ataque de identidade

O Sophos ITDR faz a varredura do seu ambiente Microsoft Entra ID continuamente para identificar rapidamente erros de configuração e lacunas de segurança baseadas em identidade e priorizar problemas que exigem atenção imediata. Os criminosos cibernéticos usam essas exposições para infligir danos escalonando privilégios e realizando ataques. Lide com os riscos com rapidez, incluindo lacunas da política de Acesso Condicional, contas órfãs, contas com excesso de privilégios e aplicativos arriscados.

Minimize o risco de credenciais vazadas ou roubadas

O número de credenciais roubadas postas à venda em um dos maiores marketplaces da dark web mais que dobrou só no último, baseado na inteligência de informação do Sophos X-Ops Counter Threat Unit (CTU). O Sophos ITDR detecta e responde às ameaças de identidade que burlam os controles de segurança de identidade tradicionais, protegendo contra 100% das técnicas de Acesso a credenciais MITRE ATT&CK.[5] A solução identifica os comportamentos de risco do usuário, como padrões de login incomuns, e destaca o uso de credenciais roubadas ou comprometidas para conseguir acessar seus sistemas.

O que o Sophos ITDR oferece

Catálogo de identidades
Visibilidade com uma exibição centralizada das identidades em todos os seus sistemas.

Avaliações contínuas de postura de identidade
Varredura constante do seu ambiente Microsoft Entra ID para identificar erros de configuração e lacunas de segurança.

Monitoramento de credenciais comprometidas na dark web
Pesquisa na dark web e em bancos de dados de violação em busca de credenciais vazadas.

Análise do comportamento do usuário
Monitoramento em busca de atividades anormais associadas a credenciais roubadas ou ameaças internas.

Detecção de ameaça de identidade avançada
Identifica indícios de atividades suspeitas de técnicas adversárias específicas no início da cadeia de ataque.

Ações de resposta a ameaças
Resposta com velocidade e precisão: forçar redefinição de senha forçada, bloquear contas que exibem comportamento suspeito e mais.

"O Sophos ITDR melhorou significativamente a nossa visibilidade de riscos de identidade. A exibição centralizada em nossa plataforma XDR nos permite alimentar nossos programas de segurança com os riscos de identidade e erros de configuração que o Sophos ITDR identificou, melhorando nossa postura cibernética organizacional geral e reduzindo riscos."

– Diretor de segurança da informação, serviços financeiros

"O Sophos ITDR está revelando riscos em áreas que me preocupavam no Azure e no ecossistema da Microsoft, como lacunas na política de acesso condicional e aplicativos não seguros ou com excesso de privilégios."

Diretor sênior de segurança da informação

Integrado com o Sophos MDR

O Sophos ITDR está totalmente integrado ao Sophos MDR, o serviço de detecção e resposta gerenciadas mais confiável do mundo. Essa poderosa combinação permite aos peritos de segurança da Sophos monitorar, investigar e responder às ameaças baseadas em identidade por você:

- O Sophos ITDR cria casos de MDR automaticamente para as detecções de ameaças de identidade e descobertas de alto risco.
- Os analista de segurança do Sophos MDR segurança investigam os casos e executam ações de resposta para neutralizar ameaças.

Exemplo: credenciais vazadas na dark web

- O Sophos ITDR identifica credenciais de um usuário à venda em um marketplace popular na dark web.
- Os analistas do Sophos MDR podem bloquear a conta do usuário e forçar a redefinição de senha.

Exemplo: credenciais roubadas em uso

- O Sophos ITDR identifica logons suspeitos provenientes de países, dispositivos e endereços IP que não foram observados antes.
- Os analistas do Sophos MDR podem bloquear a conta de usuário comprometida e encerrar todas as sessões ativas.

Melhores em conjunto: Sophos ITDR + Microsoft Entra ID

Basicamente, o Microsoft Entra ID é uma ferramenta IAM (Identity and Access Management) que fornece gerenciamento de identidade e grupo, controles RBAC, gerenciamento de acesso privilegiado e políticas de acesso condicional. Entregue em um painel de controle unificado para detectar e neutralizar ameaças e riscos de identidade, o Sophos ITDR se estende além das funcionalidades fundamentais de IAM, com higienização de identidade, avaliação de postura, monitoramento da dark web, detecção de ameaças avançada e mais. **A combinação do Entra ID com o Sophos ITDR proporciona aos seus negócios a cobertura de segurança de identidade mais abrangente que há.**

Licenciamento simplificado

O Sophos ITDR é fácil de implantar, fácil de usar e fácil de adquirir. A simplicidade do licenciamento por assinatura baseado no número de usuários e servidores na sua organização torna os preços previsíveis. Acrescente o Sophos ITDR à solução Sophos XDR ou ao serviço Sophos MDR, o que for mais indicado para as suas necessidades.

- **Complemento ao serviço Sophos Managed Detection and Response (MDR):** os peritos de segurança da Sophos monitoram, investigam e respondem às ameaças baseadas em identidade por você.
- **Complemento ao produto Sophos Extended Detection and Response (XDR):** Sua equipe interna pode aproveitar as ferramentas de detecção, investigação e resposta alimentadas por IA da Sophos com o Sophos ITDR.

Gartner

Selo 2025 Gartner® Peer Insights™ "Customers' Choice" em Detecção e Resposta Estendidas (XDR).

Líder nos Relatórios G2 Overall Grid® em Detecção e Resposta Estendidas (XDR) e Detecção e Resposta Gerenciadas (MDR).

MITRE | ATT&CK® Evaluations

Excelente desempenho nas avaliações MITRE ATT&CK® em Serviços Gerenciados e Produtos Enterprise.

FROST & SULLIVAN

Líder no relatório 2025 Frost Radar™ da Frost & Sullivan em Detecção e Resposta Gerenciadas.

Para saber mais, visite
sophos.com/ITDR

1 - Estudo de 2024, Identity Defined Security Alliance (IDSA).
2 - IBM, Cost of a Data Breach 2024.
3 - Pesquisa da equipe do Sophos Incident Response.
4 - Identity Defined Security Alliance.
5 - Baseado em detectores disponíveis mapeados à estrutura MITRE ATT&CK.

Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: brasil@sophos.com

2025-09-15 BR-PTBR (MP)

SOPHOS