Sophos MDR para Microsoft Defender

Resposta a ameaças conduzida por especialistas em ambientes Microsoft

O Sophos Managed Detection and Response (MDR) para Microsoft Defender é uma extensão da sua equipe, com peritos altamente especializados que monitoram, investigam e respondem aos alertas do Microsoft Security 24 horas.

Maximize seus investimentos no Microsoft Security

Muitas organizações investem na suíte Microsoft Security, mas nem sempre têm a expertise interna necessária para usar o arsenal de tecnologias e produtos da Microsoft com eficiência para detectar, investigar e responder às centenas de alertas diários de segurança:

- A escassez global de profissionais em segurança cibernética atingiu 3,4 milhões[1].
- 71% das equipes de segurança acham difícil determinar quais alertas de segurança investigar em meio ao ruído gerado por suas ferramentas[2].
- O tempo médio de resposta a ameaças das organizações com equipes de operações de segurança dedicadas é de 16 horas, dando tempo suficiente para os invasores explorarem a sua rede[3].

O Sophos MDR para Microsoft Defender oferece as mais robustas habilidades de detecção, busca e resposta disponíveis para ambientes Microsoft. Nossos analistas monitoram, investigam e respondem aos alertas do Microsoft Security 24 horas por dia, sete dias por semana, realizando ações imediatas conduzidas por humanos para interromper ameaças confirmadas com o tempo médio de resposta líder do setor de 38 minutos — 96% mais rápido do que o benchmark do setor.

Detecte e bloqueie ameaças que vão além do Microsoft Defender

Com o Sophos MDR para Microsoft Defender, nossos especialistas em Microsoft Security detectam, investigam e respondem a ameaças usando dados de segurança dos seguintes produtos Microsoft:

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Identity Protection (Azure AD)
- 0365 Security & Compliance Center
- Microsoft Sentinel
- Office 365 Management Activity

Além desses, os nossos meios proprietários de detecção, inteligência de ameaças de nível mundial e caça a ameaças conduzida por humanos incorporam camadas adicionais de defesa, identificando e bloqueando mais ameaças do que as ferramentas do Microsoft Security por si só.

As organizações também podem integrar fontes de telemetria e ferramentas de segurança de diferentes provedores que estão incorporadas às soluções da Sophos ou de vários outros fornecedores como Palo Alto Networks, Fortinet, Check Point, AWS, Google, Okta, Darktrace etc. para obter completa visibilidade e proteção.

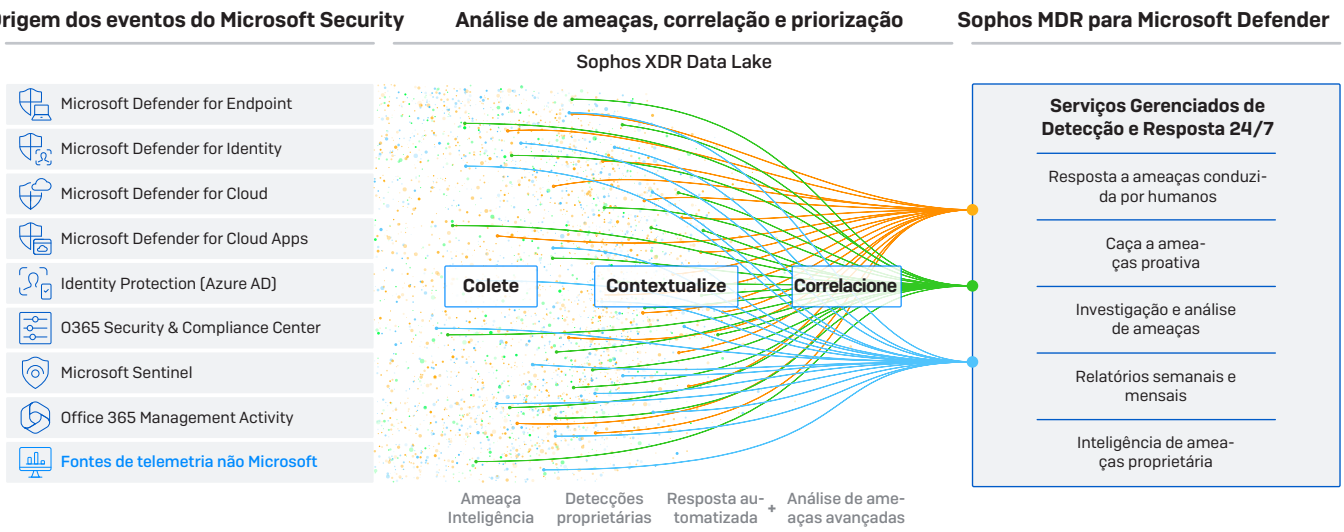
Destaques

- Os analistas do Sophos MDR monitoram, investigam e respondem a alertas do Microsoft Security continuamente, agindo imediatamente para interromper ameaças confirmadas
- Os recursos se estendem além do Microsoft Defender for Endpoint e Microsoft Sentinel, cobrindo toda a plataforma do Microsoft Security
- Quando uma ameaça ativa é identificada, a equipe de operações do Sophos MDR executa um extenso conjunto de ações para responder à ameaça por você
- Meios proprietários da Sophos, como detecções, inteligência de ameaças e caça a ameaças conduzidas por humanos, incorporam camadas adicionais de defesa
- Integre ferramentas não Microsoft e fontes de telemetria para interromper ataques que visam sua rede, seus usuários e seus clientes

1 2022 Cybersecurity Workforce Study, (ISC)2
2 O Estado da Segurança Cibernética 2023: O impacto comercial dos adversários, Sophos
3 Gartner Cybersecurity Business Value Benchmark database, 2022

SOPHOS

Sophos MDR para Microsoft Defender: principais ofertas de serviços



Monitoramento de ameaças 24 horas

Nossos especialistas no Microsoft Security detectam e bloqueiam ameaças antes que elas possam comprometer os seus dados ou causar interrupções operacionais. Com o suporte mundial de seis centros de operações de segurança (SOC), a Sophos oferece cobertura dia e noite.

Resposta a ameaças conduzida por humanos

A equipe do Sophos MDR pode executar um extenso conjunto de ações de resposta a ameaças por você para interromper, conter e eliminar os invasores. Entre essas ações de resposta a ameaças estão:

- Isolar hosts utilizando o Sophos Central
- Aplicar blocos de IP de firewall baseados em host
- Encerrar processos
- Forçar o log off de sessões de usuários
- Desativar contas de usuários
- Remover artefatos mal-intencionados
- Adicionar hashes mal-intencionados a itens bloqueados no Sophos Central

Caça a ameaças proativa conduzida por humanos

Caças proativas a ameaças são desempenhadas por analistas altamente treinados para descobrir e eliminar rapidamente ameaças e identificar comportamentos de invasores que conseguem escapar da detecção pelas ferramentas implantadas.

Compatível com ferramentas de segurança de outros fornecedores

O Sophos MDR pode integrar ferramentas de segurança e fontes de telemetria de outros provedores além da Microsoft para detectar e bloquear ameaças em todo o seu ambiente.

Relatórios semanais e mensais

Além de alertas em tempo real, relatórios e opções de gerenciamento prontos para usar no Sophos Central, você usufrui de relatórios semanais e mensais que oferecem insights sobre investigações de segurança, ameaças cibernéticas e a postura de segurança da sua organização.

Resumos mensais de inteligência de ameaças

Preparado pela equipe do Sophos MDR, o "Sophos MDR ThreatCast" é um documento mensal que oferece insights sobre as mais recentes novidades em inteligência de ameaças e boas práticas.

Detecções proprietárias

Meios proprietários de detecção, análise de ameaças avançadas e inteligência de ameaças de nível mundial integrados à plataforma Sophos incorporam camadas adicionais de defesa, identificando mais ameaças do que as ferramentas do Microsoft Security por si só.

Para saber mais, visite:

sophos.com/microsoft-defender

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

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

23-07-10 DS-PTBR (DD)

SOPHOS