SOPHOS

Fortaleça o Microsoft Defender com o Sophos MDR

Reduza o risco cibernético, aumente a eficiência e o impacto dos investimentos em segurança e eleve sua elegibilidade às ofertas de seguro fortalecendo o Microsoft Defender com detecção e resposta a ameaças conduzida por humanos, 24 horas por dia, através do provedor de serviços MDR mais confiável do mundo.

Documento técnico Sophos. Julho, 2023

Introdução

A segurança de endpoint é uma camada essencial na proteção, mas não é capaz de bloquear todas as ameaças. Os sofisticados adversários de hoje implantam cada vez mais táticas, técnicas e procedimentos (TTPs) furtivos para evitar bloqueios impostos por tecnologias de segurança, incluindo a exploração de vulnerabilidades causadas pela falta de patches, uso de credenciais roubadas e uso indevido de ferramentas de TI legítimas.

Para interromper os ataques avançados de ransomware e as violações, é essencial que você complemente o Microsoft Defender com a detecção e resposta a ameaças conduzida por humanos, 24 horas por dia, sete dias por semana. Contudo, o grande volume de alertas gerados pelas tecnologias de segurança da Microsoft somado à complexidade do ambiente de ameaças torna as operações de segurança em uma tarefa que absorve grandes esforços e recursos da maioria das empresas.

Como resultado, as organizações estão se voltado cada vez mais para a Sophos, o provedor de Managed Detection and Response (MDR) mais cotado e mais confiável do mundo para fortalecer o Microsoft Defender. Os analistas da Sophos monitoram, priorizam e respondem aos alertas de segurança da Microsoft continuamente e agindo imediatamente para interromper as ameaças confirmadas. Eles também usam meios proprietários da Sophos, como detecções, inteligência de ameaças e caça a ameaças conduzidas por humanos, para detectar e bloquear ameaças que vão além do Microsoft Defender.

O Sophos MDR foi projetado para atender às suas exigências onde você estiver e para trabalhar em conjunto com os seus investimentos de segurança e TI já em operação e com suas equipes internas. Seja para complementar seu pessoal interno com expertise adicional, estender suas defesas cibernéticas com cobertura completa durante as 24 horas do dia ou subcontratar 100% dos trabalhos de detecção e resposta a ameaças, o Sophos MDR vai ajudar você a obter os resultados em segurança cibernética que você almeja.

Fortaleça o Microsoft Defender com o Sophos MDR

✓ Reduza riscos virtuais

- Interrompa violações e ataques de ransomware avançados, incluindo ameaças praticadas por hackers que conseguem se desviar do Microsoft Defender

✓ Aumente a eficiência e o impacto dos investimentos em segurança

- Libere seus recursos de TI para se dedicarem a programas estratégicos
- Reduza a probabilidade de incorrer em custos de recuperação de grandes incidentes
- Obtenha um maior retorno de seus investimentos existentes

✓ Melhore seu potencial de segurado

- Tenha acesso às melhores ofertas de seguro que reconhecem e recompensam a redução de exposição a riscos cibernéticos

Os adversários não se infiltram, eles acessam

A verdade é que as soluções tecnológicas por si só, inclusive o Microsoft Defender, não conseguem evitar todo e qualquer ataque cibernético. Adversários ativos são agentes de ameaças que adaptam suas táticas, técnicas e procedimentos (TTPs) atuando através de ações práticas e imediatas em resposta às tecnologias de segurança utilizadas pelas equipes de defesa e como forma de escapar da detecção.

Esses ataques, que geralmente resultam em incidentes devastadores de ransomware e violação de dados, estão entre os mais difíceis de conter. Eles se tornaram altamente presentes, com 23% das organizações de pequeno e médio porte relatando que passaram por um ataque envolvendo um adversário ativo no último ano. Refletindo sobre o potencial devastador desses ataques, 30% dos líderes de TI e segurança cibernética consideram os adversários ativos uma das ameaças cibernéticas mais preocupantes de 2023[1].

Bloquear os adversários ativos com a tecnologia de segurança não é suficiente para frustrar suas artimanhas. Esses agentes habilidosos e persistentes aplicam várias abordagens inovadoras para atingir seus objetivos:

- Explorando pontos fracos na segurança para penetrar nas organizações e mover-se lateralmente pelas redes utilizando-se de credenciais roubadas, vulnerabilidades sem patches e ferramentas de segurança configuradas incorretamente.
- Abusando de ferramentas de TI legítimas usadas pelas defesas para evitar disparar detecções, incluindo o PowerShell, PsExec e RDP.
- Modificando seus ataques em tempo real em resposta a controles de segurança e continuando a alternar entre novas técnicas até que encontrem uma maneira de atingir seus objetivos.

Exemplo de estratégia de ataque de adversário ativo

Ao emular usuários autorizados e se aproveitar dos pontos fracos nas defesas de uma organização, os agentes mal-intencionados conseguem evitar o acionamento das tecnologias de detecção automatizadas, que têm dificuldade para diferenciar entre usuários legítimos e hackers.

Para intensificar os desafios dos defensores, os adversários de hoje continuam a inovar e evoluir seus modelos de negócios. O rápido crescimento do modelo de crime cibernético "as-a-service", incluindo ransomware-as-a-service e phishing-as-a-service, diminuiu os requisitos de entrada dos aspirantes ao crime, facilitando a execução e aumentando a qualidade dos ataques.

O resultado desses desenvolvimentos no cenário das ameaças é que o índice de criptografia de dados devido a ransomwares atingiu o seu ápice, onde os criminosos cibernéticos obtêm sucesso na criptografia de dados em mais de três quartos (76%) dos ataques[2].

A realidade do ransomware

- 66% das organizações foram atingidas por ransomwares no ano passado
- 76% dos ataques de ransomware resultaram na criptografia de dados
- 30% dos ataques em que os dados foram criptografados, também resultaram em roubo de dados
- A principal causa primária do ataque: exploração de vulnerabilidade (36%)
- A segunda causa primária do ataque: comprometimento de credenciais (29%)

1 O Estado da Segurança Cibernética 2023: O impacto comercial dos adversários, Sophos

2 O Estado do Ransomware 2023, Sophos.

Detecção e resposta a ameaças 24/7: a essência da segurança cibernética moderna

A boa nova é que ao unir tecnologia com perícia humana é possível barrar os ataques avançados desempenhados pelos hackers. Toda vez que um adversário se empenha em uma ação, é criado um sinal. Ao combinar a expertise humana com os modelos avançados de Machine Learning alimentados por IA e as ferramentas XDR de detecção e resposta estendidas, os analistas de segurança podem trabalhar com os sinais disparados pelas tecnologias de segurança e de TI para detectar, investigar e neutralizar mesmo os ataques mais avançados conduzidos por humanos e evitar a violação de dados.

Ainda que a detecção e resposta a ameaças 24/7 seja hoje uma parte essencial do arsenal de segurança cibernética, a maioria das organizações enfrenta desafios na hora de oferecer a eficiência do serviço, ficando exposta aos ataques. Os dois obstáculos mais comuns ao sucesso são a falta de expertise e a escassez de pessoal.

Desafio 1: falta de expertise

Detecção, investigação e resposta a ameaças é uma atividade altamente especializada que exige profundo conhecimento de técnicas de ataque e estratégias de investigação, além da fluência nas ferramentas usadas pelos defensores. Poucas organizações têm essa composição complexa (e cara) em seu pessoal interno, com 93% delas que admitem considerar a execução de tarefas e operações essenciais de segurança algo desafiador:

- 71% acham difícil distinguir sinais de ruídos (ou seja, entender quais sinais/alertas investigar)
- 71% acham difícil reunir dados suficientes para identificar se um sinal é maligno ou benigno
- 75% acham difícil identificar a causa primária de um incidente (ou seja, como o adversário entrou na organização)

A enormidade do desafio fica clara quando analisamos os dados que os defensores coletam com suas ferramentas de segurança cibernética. A tabela a seguir contém uma lista com alguns dos eventos do Microsoft Defender acompanhados de sua categoria.

Entender os alertas é apenas uma parte do processo de detecção e resposta a ameaças: depois é preciso que os defensores apliquem percepções contextuais e inteligência de ameaças para poder entender completamente a ameaça e identificar o melhor curso de ação.

TÍTULO DE EVENTO	TIPO DE EVENTO
URL suspeita clicada	Acesso inicial
Arquivos maliciosos ou conexões de rede associadas com o processo 3CXDesktopApp.exe	Malware
Conta de novo usuário criada	Persistência
Limpar Eventlog TS_BL_Suspicious ou Configuração usando Wevtutil	Evasão de defesas
Escalonamento de privilégio de processamento	Escalonamento de privilégio
Tentativa de desativar a proteção Antivírus Microsoft Defender	Evasão de defesas
Conexão de rede ou arquivo relacionado ao agente de ameaça Storm-0867 detectado	Acesso a credenciais
Mecanismos TS_BL_Script conectando-se à internet	Comando e Controle
Possível atividade maliciosa operada por humanos	Atividade suspeita
Download de payload TS_BL_Malicious via binários do Office	Execução
Atividade de ameaça emergente do grupo DEV-0867 detectada	Acesso a credenciais
Atividade de ameaça emergente do grupo Citrine Sleet detectada	Malware

Detecções de criação de caso de exemplo do Microsoft Defender

Desafio 2: escassez de pessoal

A detecção, investigação e resposta a ameaças é uma atividade demorada. Para ilustrar esse ponto, o tempo médio para detectar, investigar e responder a um alerta é de nove horas em organizações com 100 a 3.000 funcionários, subindo para 15 horas naquelas com uma média de 3.001 a 5.000 funcionários.

Lidar com alertas de segurança consome grande quantidade de horas de TI, e a natureza urgente do trabalho pode impedir que as equipes se concentrem em situações mais estratégicas. Além disso, como os adversários executam ataques a qualquer hora do dia ou da noite, a detecção e resposta precisam ser desempenhadas ininterruptamente durante todo o ano para surtir o máximo de impacto. Muitas, senão a maioria das organizações, lutam para manter os recursos humanos necessários.

Solução: complementar suas defesas com o Managed Detection and Response (MDR)

52% dos chefes de TI dizem que os ataques cibernéticos estão agora muito avançados para as suas organizações lidarem com eles por conta própria, o que os leva a buscar provedores especializados em Managed Detection and Response como a Sophos para complementar e ampliar sua capacidade interna.

A definição de MDR

Managed Detection and Response (MDR) é um serviço totalmente gerenciado — 24 horas por dia, sete dias por semana — entregue por peritos especializados em detectar e responder a ataques cibernéticos que as soluções tecnológicas por si só não conseguem evitar.

Extended Detection and Response (XDR) é a plataforma que unifica dados de segurança de diversas fontes para automatizar e acelerar a detecção, investigação e resposta a ameaças de maneiras que as soluções isoladas não conseguem.

Os analistas do Sophos MDR se utilizam da plataforma Sophos XDR na busca, investigação e neutralização das ameaças por você. Eles aproveitam os sinais de toda a pilha de TI, incluindo firewall, e-mail, nuvem e soluções de segurança móvel, para acelerar a detecção e resposta a ameaças.

Fortaleça o Microsoft Defender com o Sophos MDR

O Sophos MDR oferece detecção e resposta 24/7 comprovada para ambientes do Microsoft Defender. Os analistas da Sophos monitoram, priorizam e respondem aos alertas de segurança da Microsoft continuamente e agindo imediatamente para interromper as ameaças confirmadas. Eles também usam meios proprietários da Sophos, como detecções, inteligência de ameaças e caça a ameaças conduzidas por humanos, para detectar e bloquear essas ameaças práticas que vão além do Microsoft Defender.

Quanto mais vemos, mais rápido agimos. O Sophos MDR combina os Event Sources adicionais do Microsoft Security incluídos nas licenças E3 e E5 com sinais de firewall, nuvem, e-mail e identidade de terceiros e com investimentos de detecção e resposta de rede (NDR) para acelerar a detecção e resposta a ameaças.

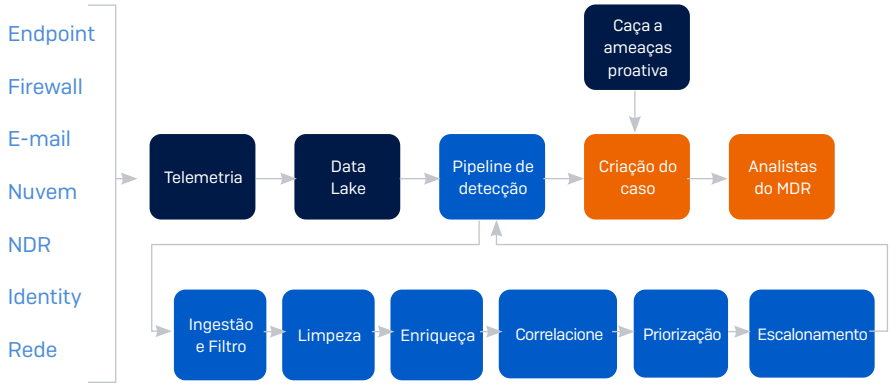
Os usuários do Microsoft Defender desfrutam de acesso imediato por telefone a peritos em operações de segurança da Sophos — 24 horas por dia, sete dias por semana —, além de um relatório detalhado da atividade da ameaça na plataforma do Sophos Central.

O Sophos MDR for Microsoft Defender é compatível com Event Sources do Microsoft Security

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Identity Protection (Azure AD)
- MS O365 Security & Compliance Center
- Microsoft Azure Sentinel
- Office 365 Management Activity (log de auditoria unificado)

Sophos MDR Security Event Flow

Nosso Security Event Flow patenteado é um elemento-chave do serviço Sophos MDR. A telemetria que cobre todo o ambiente de segurança, incluindo o Microsoft Defender, é ingerida pelo Sophos Data Lake e depois processada em nosso pipeline de detecção, que converte grandes volumes de alertas da Microsoft e de terceiros em insights priorizados utilizáveis que nos permitem investigar e responder com eficiência.



O fluxo de eventos do Sophos MDR Security

Ingestão e Filtro – Entrada de telemetria e filtragem e remoção de ruídos indesejados

Limpeza – Transformação de dados em um esquema normalizado e mapeamento para o MITRE ATT&CK®

Enriqueça – Inclua inteligência de ameaças de terceiros e informações com contexto empresarial

Correlacione – Alertas agrupados com base em entidades, categorização do MITRE ATT&CK e hora

Priorização – Pontuação e agrupamento de alertas ordenados por prioridade

Escalonamento – Aplicação de lógica para promover os grupos para casos para investigação

Cobertura 24/7 disponibilizada por sete centros de operações de segurança: nossos SOCs globais

As ameaças são investigadas e remediadas por uma equipe global de peritos em detecção e resposta a ameaças que trabalham em sete centros globais de operações de segurança na América do Norte (Indiana, Utah, Havaí), Europa (Reino Unido e Irlanda, Alemanha) e Ásia-Pacífico (Índia, Austrália). Com mais de 500 peritos que atendem a todo o cenário de ameaças, incluindo especialistas em malware, automação, IA e remediação, o Sophos MDR engloba uma imensa diversidade e grande abrangência de especialidades que é praticamente impossível replicar internamente.

Tempos de detecção e resposta que lideram o mercado

Essa combinação única de expertise humana, tecnológica e de ameaças permite que o Sophos MDR ofereça um tempo de resposta a incidentes líder de mercado de apenas 38 minutos que leva a resultados de segurança cibernética de nível superior:

- Tempo médio de detecção (MTTD): 1 minuto
- Tempo médio de investigação (MTTI): 25 minutos
- Tempo médio de resposta (MTTR): 12 minutos

Quem usa o Sophos MDR

Milhares de organizações em todos os setores usam o serviço Sophos MDR, desde pequenas empresas com recursos de TI limitados até grandes empresas com um grupo interno de SOC. Os três modelos de resposta Sophos MDR mais populares são:

- O Sophos MDR gerencia completamente a resposta a ameaças para o cliente
- O Sophos MDR trabalha com a equipe interna, cogerenciando a resposta a ameaças
- O Sophos MDR apoia e complementa a equipe interna, alertando-os sobre os incidentes que exigem atenção e oferecendo insights sobre ameaças e diretrizes de remediação

Caso de ameaça: trabalhando com o Microsoft Defender para detectar Comando e Controle

SETOR
Serviços profissionais

SEDE
Estados Unidos

FUNCIONÁRIOS
750

NÍVEL DE SERVIÇO
Sophos MDR para Microsoft Defender

FONTES DE TELEMETRIA INTEGRADAS AO SOPHOS MDR

✓ Endpoint	X Identity
✓ Firewall	X Nuvem
X E-mail	✓ Rede

O que é Comando e Controle?

Comando e Controle (também chamado de C&C, CC ou C2) consiste em técnicas que os invasores usam para se comunicar e enviar comandos a sistemas sob o controle deles na rede de uma vítima.

Os canais de comando e controle entre o ambiente alvo e a infraestrutura do invasor podem ser estabelecidos de várias formas, incluindo e-mails de phishing, engenharia social, malware, vulnerabilidades em plug-ins de navegadores e outros meios. É frequente ver os adversários utilizando-se de recursos comuns para imitar o tráfego de rede esperado para evitar serem detectados ou levantar suspeitas.

DETECÇÃO

O Microsoft Defender gera um alerta de comunicação para um endereço IP malicioso.

O alerta do Microsoft é automaticamente correlacionado aos eventos no Sophos XDR Data Lake para determinar se o ataque foi bloqueado pelo firewall do cliente e se causou impacto em outros endpoints.

INVESTIGAÇÃO

Os analistas do Sophos MDR confirmam que a conexão mal-intencionada associada ao alerta do Microsoft Defender foi bloqueada e a ameaça imediata é contida.

O SophosLabs Intelix é usado para identificar a família do ataque, os indicadores de comprometimento (IOCs) e os IPs e domínios conhecidos usados pelo invasor.

O alerta original da Microsoft é enriquecido com essa inteligência de ameaça para ser usado na Análise de Causa Primária.

RESPOSTA

O dispositivo comprometido é isolado e o ataque é contido.

O Sophos MDR confirma que o acesso inicial foi efetuado por e-mail de phishing. É realizada uma investigação para identificar a composição do e-mail de phishing e assegurar que nenhuma outra conta de usuário tenha sido comprometida.

A Sophos fornece recomendações para reduzir a possibilidade de sucesso de ataques de phishing futuros.

Benefícios aos clientes

Seja para complementar e apoiar suas operações de segurança interna ou aproveitar os benefícios de uma equipe 24 horas de especialistas em detecção e resposta sem a carga operacional de manter o seu próprio SOC, o Sophos MDR está pronto para ajudar você. As organizações que reforçam seu Microsoft Defender com o Sophos MDR desfrutam de resultados superiores, incluindo redução de risco cibernético, aumento de eficiência e impacto dos investimentos em segurança, e elevada elegibilidade às ofertas de seguro.

Bloqueie ameaças avançadas com Microsoft + Sophos MDR

Monitoramento e resposta 24/7 por uma equipe de peritos
Os analistas do Sophos MDR monitoram, priorizam e respondem aos alertas do Microsoft Defender continuamente, agindo imediatamente para interromper as ameaças confirmadas

Detecte e bloqueie as ameaças que conseguem se desviar do Microsoft Defender
Os meios proprietários da Sophos, como detecções, inteligência de ameaças e caça a ameaças conduzidas por humanos, incorporam camadas adicionais de defesa

Melhore a visibilidade e contextualize os alertas do Microsoft Defender
Integre origens de eventos adicionais do Microsoft Security incluídos nas licenças E3 ou E5

Obtenha acesso imediato a peritos em operações de segurança
Analistas do Sophos MDR estão disponíveis por telefone 24/7, e relatórios detalhados sobre a atividade da ameaça são disponibilizados no Sophos Central

Reduza riscos virtuais

Uma das maiores vantagens de intensificar a operação do Microsoft Defender com o Sophos MDR é elevar o seu nível de proteção contra ransomwares e outras ameaças cibernéticas avançadas.

Os analistas da Sophos têm especialidade diversa e abrangente somada a uma grande fluência no uso de telemetria e ferramentas de caça a ameaças que é praticamente impossível replicar internamente. Isso lhes permite responder com rapidez e precisão em todos os estágios do processo — da identificação dos indícios importantes até a investigação de possíveis incidentes e neutralização de atividades maliciosas.

O Sophos MDR protege mais organizações do que qualquer outro provedor, permitindo oferecer "imunidade comunitária" sem igual. A inteligência de defesa de um cliente é aplicada automaticamente a todos os outros com um perfil semelhante, permitindo proteger contra ataques semelhantes nessa mesma comunidade.

★★★★★

"O pessoal de pen-test ficou abismado de não conseguir achar um jeito de se infiltrar. Foi aí que constatamos que podíamos usar o serviço da Sophos com absoluta confiança."
Universidade de South Queensland, Austrália

★★★★★

"Com o Sophos MDR, reduzimos drasticamente o nosso tempo de resposta a ameaças."
Tata BlueScope Steel, Índia

★★★★★

"Recebemos notificações de ameaças em tempo real."
Bardiani Valvole, Itália

Aumente a eficiência e o impacto dos seus investimentos em segurança

O Sophos MDR permite aumentar a eficiência e o impacto do seu pessoal e de suas ferramentas de segurança.

A detecção e resposta a ameaças consome grandes quantidades da sua capacidade de TI. O Sophos MDR tira o peso dessa carga, liberando valiosos recursos de TI para se dedicarem a programas estratégicos. Paralelamente, o acesso 24 horas por telefone a peritos em operações de segurança da Sophos e relatórios detalhados sobre a atividade de ameaça através da plataforma do Sophos Central aumenta a produtividade das equipes internas ao permitir que respondam aos alertas com maior rapidez e precisão.

Ao usar a telemetria das suas ferramentas de segurança de terceiros e da Microsoft para acelerar a detecção e resposta a ameaças, o Sophos MDR eleva suas defesas ao permitir que você aumente o retorno de seus investimentos existentes.

E com a conta média para remediar um ataque de ransomware chegando à casa de US$ 1,85 milhões e 84% das vítimas de ransomware dizendo que o ataque fez com que perdessem negócios e receita[2], investir em um serviço como o Sophos MDR reduz o custo de propriedade da segurança cibernética.

★★★★★

"Desde que implementamos a solução da Sophos, conseguimos liberar horas de trabalho operacional, o que permitiu que nossas equipes se concentrassem em iniciativas que aumentaram a satisfação de nossos alunos."

Universidade London South Bank, Reino Unido

★★★★★

"A capacidade do Sophos MDR em remediar e remover ameaças de modo rápido e nos manter informados nos deixa livres para focar em tarefas mais rentáveis."

Tomago Aluminium, Austrália

2 O Estado do Ransomware 2023, Sophos.

Melhore seu potencial de segurado

O Sophos MDR permite que as organizações atendam aos vários controles cibernéticos que são chave na obtenção do seguro com ofertas de apólices superiores, incluindo 24/7 de detecção e resposta, planejamento de resposta a incidentes cibernéticos, log e monitoramento, e mais.

Os clientes relatam o acesso a melhores ofertas de seguro bem como apólices que reconhecem e recompensam a redução de exposição aos riscos cibernéticos.

★★★★★

"Nossa decisão de estabelecer uma parceria com a Sophos e usar o XDR e MDR foi um grande fator para o decréscimo nos prêmios do seguro de proteção digital em comparação com o dobro do que nos foi dito que seria sem essa parceria. Essa é uma opção vencedora que mostra o seu real valor. O CFO inclusive enviou um agradecimento pelo que alcançamos juntos e o MDR foi uma parte importante nisso."

Bob Pellerin, CISO, The Fresh Market, EUA

O serviço MDR mais confiável do mundo

A Sophos é o provedor número um de MDR em todo o mundo, protegendo mais organizações do que qualquer outro fornecedor contra ransomwares, violações e outras ameaças que a tecnologia sozinha não é capaz de deter.

O Sophos MDR protege milhares de organizações em diferentes setores em todo o mundo, oferecendo especialização profunda e abrangente incomparável para combater as ameaças enfrentadas pelos setores individualmente. Aproveitamos essa telemetria extensiva para gerar "imunidade comunitária", aplicando o aprendizado adquirido da defesa de uma organização aos outros clientes com perfil semelhante e, assim, elevando as defesas de todos.

É claro que o que mais importa são os resultados que oferecemos à segurança cibernética de nossos clientes. A Sophos tem a solução MDR com as melhores avaliações e a mais alta classificação na Gartner® Peer Insights™, com pontuação 4,8/5 em 300 avaliações em 14 de junho de 2023 e 97% de aprovação dos clientes, que dizem que recomendariam o produto.

A Sophos também é líder no G2 Grid® Reports for Managed Detection and Response, além de ser reconhecida como líder de MDR nos segmentos Overall, Midmarket e Enterprise do G2.

Para saber mais sobre o Sophos MDR e como ele capacita os usuários do Microsoft Defender a reduzir o risco cibernético, aumentar a eficiência e o impacto dos investimentos em segurança, e elevar sua elegibilidade às ofertas de seguro, visite www.sophos.com/mdr

Mais confiável

Mais de 17.000 organizações usam o Sophos MDR (T2, 2023)

A mais alta classificação

4,8/5 na classificação independente por clientes

A mais avaliada

300 avaliações na Gartner Peer Insights nos últimos 12 meses

Explore o Sophos Endpoint Protection

O Sophos Intercept X Endpoint Protection trabalha com você e para você, adaptando as suas defesas em resposta a um ataque.

Repleto de poderosas camadas de proteção que oferecem defesas contra ransomwares e ameaças avançadas em todos os estágios da cadeia de ataque, incluindo reversão de ransomware baseada em comportamento e 60 mitigações de exploit habilitadas como padrão, sem precisar aplicar nenhum ajuste.

Nossa inovadora Proteção Adaptativa contra Ataques responde dinamicamente a um ataque conduzido por humanos, implantando automaticamente defesas extras para frustrar as investidas do adversário e ganhar tempo para os defensores responderem.

Os usuários do serviço Sophos MDR que usam o Microsoft Defender podem alternar para a proteção do Sophos Endpoint a qualquer momento, dando a você total flexibilidade ao mesmo tempo que prepara as suas implantações e segurança para o futuro.

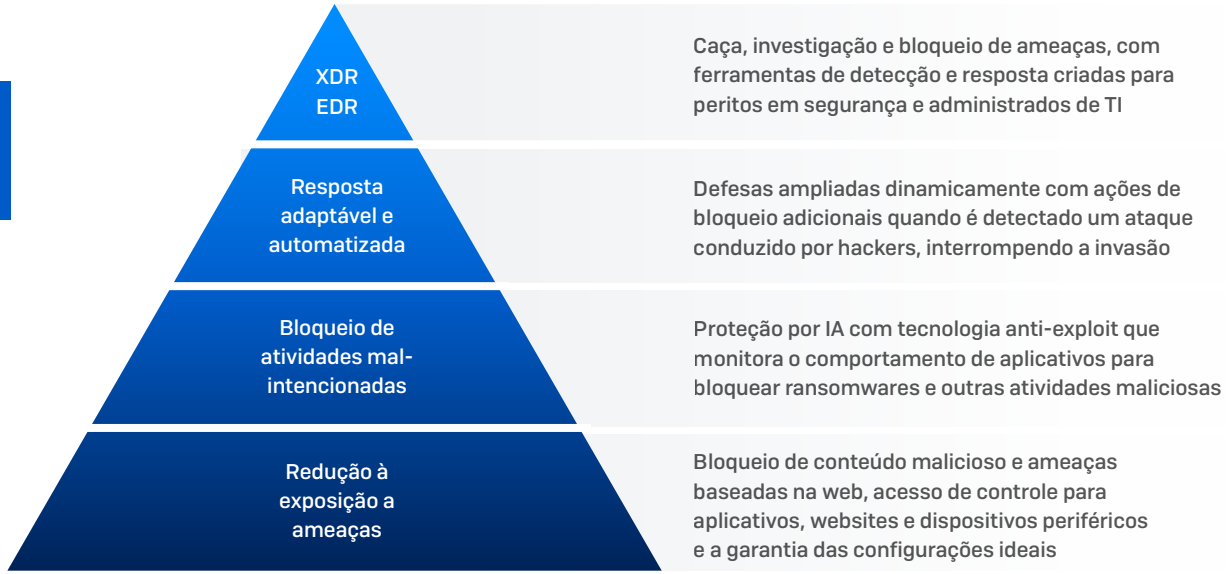
Para saber mais e começar um teste gratuito, visite www.sophos.com/endpoint

✓ Gartner Leader nos últimos 13 relatórios consecutivos
A Sophos é reconhecida como Líder no Magic Quadrant da Gartner para Plataformas de Proteção de Endpoints desde 2008

✓ A mais alta proteção pela Gartner Peer Insights
4,8/5 na classificação independente por clientes

✓ G2 Leader nos segmentos Enterprise, Midmarket e SMB
Com base exclusiva em avaliações de clientes

✓ Pontuação de proteção 100% – SE Labs
Classificação AAA em Segurança de Pequenas Empresas e Grandes Corporações



Gartner, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Chris Silva, 31 de dezembro de 2022
GARTNER é marca registrada e marca de serviço da Gartner, Inc. e/ou de suas afiliadas nos EUA e internacionalmente, e Magic Quadrant e PEER INSIGHTS são marcas registradas da Gartner, Inc. e/ou de suas afiliadas, que são utilizadas aqui com permissão. Todos os direitos reservados.
A Gartner não endossa fornecedores, produtos ou serviços representados em suas publicações de pesquisa e não faz sugestões a usuários de tecnologias para selecionarem apenas fornecedores com as mais altas pontuações ou outros reconhecimentos. As publicações de pesquisa da Gartner consistem em opiniões das organizações de pesquisa da Gartner e não devem ser interpretadas como uma declaração de fato. A Gartner se isenta de toda e qualquer garantia, expressa ou implícita, em respeito a esta pesquisa, incluindo garantias de comercialização ou de um propósito de uso específico.
O conteúdo do Gartner Peer Insights consiste em opiniões de usuários finais individuais baseadas em suas próprias experiências e não deve ser interpretado como uma declaração de fato nem como representação da visão da Gartner ou de suas afiliadas. A Gartner não endossa fornecedores, produtos ou serviços representados neste conteúdo nem estabelece qualquer garantia, expressa ou implícita, em respeito a este conteúdo, sua precisão ou completude, incluindo garantias de comercialização ou de um propósito de uso específico.

A Sophos oferece soluções de segurança cibernética líder do setor para empresas de todos os tamanhos, protegendo-as em tempo real de ameaças avançadas como malware, ransomware e phishing. Com recursos comprovados de última geração, seus dados comerciais ficam protegidos de modo eficiente por produtos que incorporam inteligência artificial e machine learning.

2023-06-27 (WP-NP)

SOPHOS