Folheto de soluções

Sophos Managed Detection and Response

Detecção e resposta a ameaças 24/7

O Sophos MDR é um serviço totalmente gerenciado – 24 horas por dia, sete dias por semana – realizado por peritos em detecção e resposta a ataques cibernéticos direcionados a seus computadores, servidores, redes, cargas de trabalho na nuvem, contas de e-mail e mais.

Serviços de prevenção de violações e ransomwares

A necessidade de operações de segurança *always-on* se tornou um fator imprescindível em qualquer configuração. Entretanto, a complexidade dos ambientes operacionais modernos e a velocidade das ameaças cibernéticas deixam cada vez mais difícil para a maioria das organizações obter sucesso no gerenciamento da detecção e resposta sem um respaldo extra.

Com o Sophos MDR, nossa equipe de peritos interrompe os ataques avançados realizados por humanos. Nós agimos na neutralização das ameaças antes que elas possam causar interrupções em suas operações comerciais ou comprometer seus dados confidenciais. O Sophos MDR é personalizado com diferentes níveis de atendimento e responde às suas necessidades por meio da nossa tecnologia proprietária ou utilizando os seus investimentos tecnológicos atuais em segurança cibernética.

Cybersecurity Delivered as a Service

Com a capacidade de detecção e resposta estendidas (XDR) que oferece cobertura completa de segurança onde quer que seus dados residam, o Sophos MDR pode:

- Detectar mais ameaças cibernéticas do que as ferramentas de segurança podem identificar sozinhas
  Nossas ferramentas bloqueiam automaticamente 99,98% das ameaças, o que permite a nossos analistas se concentrarem na caça aos invasores mais sofisticados que só podem ser detectados e bloqueados por humanos altamente treinados.
- Agir por você para impedir que as ameaças perturbem os seus negócios
  Nossos analistas detectam, investigam e respondem a ameaças em minutos – seja na resposta a incidentes de grande escala ou na tomada de decisões precisas.
- Identificar a causa principal das ameaças para evitar incidentes futuros
  Atuamos de forma proativa e oferecemos recomendações que diminuem os riscos à sua organização. Menos incidentes significa menos interrupções para suas equipes de TI e de segurança, seus funcionários e seus clientes.

Compatível com as ferramentas de segurança cibernética que você já tem

Podemos oferecer a tecnologia de que você precisa diretamente do nosso portfólio premiado; ou nossos analistas podem adaptar as suas tecnologias de segurança cibernética já existentes para detectar e responder a ameaças.

O Sophos MDR é compatível com a telemetria de segurança de fornecedores como Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google, Okta, Darktrace e muitos outros. A telemetria é consolidada, correlacionada e priorizada automaticamente com insights do Ecossistema de Segurança Cibernética Adaptativa da Sophos (ACE) e a unidade de inteligência de ameaças Sophos X-Ops.

Destaques

- Bloqueie ransomwares e outros ataques avançados conduzidos por humanos com uma equipe 24 horas de peritos de resposta a ameaças
- Maximize o ROI das suas tecnologias de segurança cibernética existentes
- Deixe que o Sophos MDR controle a resposta a incidentes de grande escala, trabalhe com você para gerenciar os incidentes de segurança ou forneça notificações e orientações detalhadas sobre ameaças
- Melhore a sua elegibilidade a uma cobertura de seguro de proteção digital com a capacidade de monitoramento e detecção e resposta a endpoint (EDR) 24 horas
- Libere o pessoal interno de TI e segurança para se concentrarem nas iniciativas de negócios

O MDR que acompanha você a qualquer lugar

O Sophos MDR é personalizado com diferentes níveis de atendimento e opções de resposta a ameaças. Deixe que a equipe de operações do Sophos MDR controle a resposta a incidentes de grande escala, trabalhe com você para gerenciar as ameaças cibernéticas ou notifique as suas equipes internas de segurança sempre que uma ameaça for detectada. Nossa equipe descobrirá rapidamente quem gerou o ataque, quando e como. Nós podemos responder a ameaças em minutos.

Principais recursos

Monitoramento e resposta a ameaças 24/7

Detectamos e respondemos a ameaças antes que elas possam comprometer os seus dados ou causar períodos de inatividade. Com o suporte mundial de sete centros de operações de segurança (SOC), o Sophos MDR oferece cobertura dia e noite.

Compatível com ferramentas de segurança de outros fornecedores

O Sophos MDR pode integrar telemetria de endpoint, firewall, rede, identidade, e-mail, backup e recuperação, e outras tecnologias de terceiros.

Resposta a incidentes de grande escala

Quando identificamos uma ameaça ativa, a equipe de operações do Sophos MDR pode executar remotamente um extenso conjunto de ações de resposta por você para interromper, conter e eliminar o adversário por completo. Com a licença Sophos MDR Complete, você se beneficia de resposta a incidentes completa e ilimitada, sem taxas extras.

Relatórios semanais e mensais

O Sophos Central é o nosso painel unificado de alertas em tempo real, relatórios e gerenciamento. Relatórios semanais e mensais oferecem insights sobre investigações de segurança, ameaças cibernéticas e a sua postura de segurança.

Ecossistema de Segurança Cibernética Adaptativa da Sophos

O Sophos ACE previne automaticamente as atividades mal-intencionadas e nos permite buscar indícios de ameaças que exigem a intervenção humana para sua detecção, investigação e eliminação.

Caça a ameaças conduzida por peritos

Caças proativas a ameaças são desempenhadas por analistas altamente treinados para descobrir e eliminar rapidamente mais ameaças do que os produtos de segurança podem detectar por si só. As equipes de operações do Sophos MDR podem usar a telemetria de terceiros para conduzir a caça a ameaças e identificar comportamentos dos invasores que escapam à detecção realizada pelos conjuntos de ferramentas implantados.

Chamada direta para assistência

Seu pessoal tem acesso direto ao nosso Centro de Operações de Segurança (SOC) para analisar ameaças potenciais e incidentes ativos. A equipe de operações de MDR está disponível 24 horas por dia, todos os dias do ano, e recebe o apoio de equipes distribuídas em 26 localidades mundo afora.

Liderança dedicada à resposta a incidentes

Disponibilizamos um líder de resposta a incidentes dedicado para colaborar diretamente com a sua equipe interna e parceiros externos assim que identificamos um incidente, e trabalhamos junto com você até que o incidente esteja resolvido.

Análise de causas primárias

Além de oferecermos recomendações proativas para melhorar a sua postura de segurança, realizamos a análise das causas primárias para identificar os problemas que levaram ao incidente. Oferecemos orientação prescritiva para tratar das vulnerabilidades na segurança de modo que não possam ser exploradas no futuro.

Status de integridade da conta da Sophos

Revisamos continuamente os parâmetros e as configurações dos endpoints gerenciados pelo Sophos MDR para assegurar que estejam operando nos níveis ideais.

Contenção de ameaças

As organizações que preferem outros níveis de atendimento, que não a resposta a incidentes de grande escala, podem trabalhar com as equipes de operações do Sophos MDR que atuam na contenção e bloqueio de ameaças, evitando que se alastrem. Isso reduz a carga de trabalho para as equipes internas de operações de segurança e permite que executem rapidamente ações de remediação.

Dados da Inteligência: “Sophos MDR ThreatCast”

Oferecido pela equipe de operações do Sophos MDR, o “Sophos MDR ThreatCast” é um documento mensal disponível exclusivamente para os clientes do Sophos MDR. Ele fornece insights sobre a inteligência de ameaças mais atual e as melhores práticas de segurança.

Breach Protection Warranty

Incluída em todas as licenças anuais (de um a cinco anos) e mensais do Sophos MDR Complete, a garantia cobre até US$ 1 milhão em despesas de resposta. Não há níveis de garantia, prazo mínimo de contrato ou requisitos adicionais de compra.

Integrações incluídas no Sophos MDR

Dados de segurança das seguintes fontes podem ser integrados para serem usados pela equipe de operações do Sophos MDR sem custos adicionais. As fontes de telemetria são usadas para expandir a visibilidade em todo o seu ambiente, gerar detecções de novas ameaças e melhorar a fidelidade das detecções de ameaças existentes, conduzir a caça a ameaças e oferecer recursos adicionais de resposta.

Sophos Endpoint

Bloqueie ameaças avançadas e detecte comportamentos mal-intencionados em todos os seus endpoints

Produto incluído no preço do Sophos MDR

Workload Protection

Proteção avançada e detecção de ameaça para contêineres e servidores Linux e Windows

Produto incluído no preço do Sophos MDR

Sophos Mobile

Mantenha seus dispositivos iOS e Android e dados protegidos contra as mais recentes ameaças a dispositivos móveis

Produto vendido separadamente; integração sem custo adicional

Sophos Firewall

Monitore e filtre o tráfego de entrada e saída da rede para bloquear ameaças avançadas antes que possam causar danos

Produto vendido separadamente; integração sem custo adicional

Sophos Email

Proteja a sua caixa de entrada contra malwares com a IA avançada que impede a clonagem direcionada e os ataques de phishing

Produto vendido separadamente; integração sem custo adicional

Sophos Cloud

Interrompa as violações da nuvem e obtenha visibilidade entre todos os seus serviços de nuvem críticos, incluindo AWS, Azure e GCP

Produto vendido separadamente; integração sem custo adicional

Sophos ZTNA

Substitua a VPN de acesso remoto pelo acesso de privilégio mínimo para a conexão segura dos usuários aos seus aplicativos na rede

Produto vendido separadamente; integração sem custo adicional

Endpoint Protection para terceiros

Compatível com:

- Microsoft
- CrowdStrike
- SentinelOne
- Trend Micro
- BlackBerry (Cylance)
- Broadcom (Symantec)

+ compatível com outras soluções com o agente Sophos "XDR Sensor"

Ferramentas de segurança Microsoft

- Defender for Endpoint
- Defender for Cloud
- Defender for Cloud Apps
- Defender for Identity
- Microsoft Entra ID
- Azure Sentinel
- Office 365 Security and Compliance Center

90 dias de retenção de dados

Retém dados dos produtos Sophos e de terceiros (diferentes fornecedores) no Sophos Data Lake

Prorrogável até 1 ano como complemento opcional

Logs de auditoria da Microsoft

Oferece informações sobre usuário, administração, sistema e ações e eventos da política inserida pelo Office 365 Management Activity API

Google Workspace

Insere telemetria de segurança do Google Workspace Alert Center API

Integrações complementares

Dados de segurança das seguintes fontes de terceiros podem ser integrados para serem usados pela equipe de operações do Sophos MDR por meio da compra de pacotes de integração. As fontes de telemetria são usadas para expandir a visibilidade em todo o seu ambiente, gerar detecções de novas ameaças e melhorar a fidelidade das detecções de ameaças existentes, conduzir a caça a ameaças e oferecer recursos adicionais de resposta.

Sophos NDR

Monitore continuamente a atividade dentro da sua rede para detectar ações suspeitas ocorrendo entre dispositivos que poderiam passar sem ser percebidas

Compatível com qualquer rede via espelhamento de porta SPAN

Firewall

Compatível com:

- Check Point
- Cisco Firepower
- Cisco Meraki
- Fortinet
- Palo Alto Networks
- SonicWall
- WatchGuard

Rede

Compatível com:

- Cisco Umbrella
- Darktrace
- Secutec
- Skyhigh Security
- Thinkst Canary

Identity

Compatível com:

- Auth0
- Duo
- ManageEngine
- Okta

Integração da Microsoft incluída sem custos adicionais

Email

Compatível com:

- Proofpoint
- Mimecast

Integrações do Microsoft 365 e Google Workspace incluídas sem custos adicionais

Nuvem pública

Compatível com:

- AWS Security Hub
- AWS CloudTrail
- Orca Security

Integre dados adicionais da AWS, Azure e GCP via produtos Sophos Cloud, vendido separadamente

Backup e recuperação

Compatível com:

- Veeam

1 ano de retenção de dados

Retém dados dos produtos Sophos e de terceiros (diferentes fornecedores) no Sophos Data Lake

Níveis de atendimento Sophos

	Sophos MDR Essentials	Sophos MDR Complete
Monitoramento e resposta a ameaças conduzidos por peritos 24/7	✓	✓
Compatível com produtos de segurança de outros fornecedores	✓	✓
Relatórios semanais e mensais	✓	✓
Dados mensais da Inteligência: "Sophos MDR ThreatCast"	✓	✓
Status de integridade da conta da Sophos	✓	✓
Caça a ameaças conduzida por peritos	✓	✓
Contenção de ameaças: ataques são interrompidos, evitando que se alastrem Usa o agente Sophos MDR completo (proteção, detecção e resposta) ou o Sophos MDR Sensor (detecção e resposta)	✓	✓
Chamada direta para assistência durante incidentes ativos	✓	✓
Resposta a incidentes de grande escala: ameaças totalmente eliminadas Requer o agente Sophos MDR completo (proteção, detecção e resposta)	Complemento IR por honorário	✓
Análise de causas primárias		✓
Liderança dedicada à resposta a incidentes		✓
Breach Protection Warranty Cobre até US$ 1 milhão em despesas de resposta		✓

Sophos MDR Guided Onboarding

O Sophos MDR Guided Onboarding está disponível para dar assistência remota na integração como material adicional para compra opcional. O serviço oferece suporte prático para uma implantação fluida e eficiente, assegura o uso das boas práticas de configuração e fornece treinamento para maximizar o valor do seu investimento no serviço MDR. Você terá uma pessoa de contato dedicada da organização Sophos Professional Services que acompanhará os primeiros 90 dias do processo para garantir que a sua implementação seja um sucesso. O Sophos MDR Guided Onboarding inclui:

Dia 1 – Implementação

- Reunião inicial do projeto
- Configure o Sophos Central e verifique os recursos
- Crie e teste processos de implantação
- Configure as integrações MDR
- Configure o(s) sensor(es) Sophos NDR
- Implantação no âmbito empresarial

Dia 30 – Treinamento em MDR

- Aprenda a pensar e agir como um SOC
- Saiba como sair em busca de indicadores de comprometimento
- Entenda como usar a nossa plataforma MDR nas tarefas administrativas
- Aprenda a montar consultas para investigações futuras

Dia 90 – Avaliação de postura de segurança

- Analise as políticas atuais e as recomendações de melhores práticas
- Considere quais recursos não estão em uso que poderiam oferecer proteção adicional
- Avaliação da segurança seguindo a estrutura NIST
- Receba relatórios resumidos com nossas observações e recomendações

Veja por que os clientes escolhem o Sophos MDR

A Sophos é líder consagrada em Detecção e Resposta Gerenciada com premiações reconhecidas pelo setor.

Gartner

Fornecedor "Representative Vendor" na Gartner Market Guide em Serviços Gerenciados de Detecção e Resposta

Gartner peerinsights

Selo "Customers' Choice" da Gartner Peer Insights em Detecção e Resposta Gerenciada

G2 Leader

Classificada a solução MDR Nº 1 pelos consumidores nos relatórios Grid Winter 2024 da G2

FROST & SULLIVAN

Líder no relatório 2024 Frost Radar em Global Managed Detection and Response

MITRE ATT&CK

Resultados excepcionais na primeira versão do MITRE Engenuity ATT&CK Evaluation of Security Service Providers

Para saber mais, visite

sophos.com/mdr

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

2024-04-02 PTBR (NP)

SOPHOS