SOPHOS

Guia para o comprador de segurança de endpoint

À medida que as ameaças cibernéticas se tornam mais complexas, a pressão para encontrar a solução de endpoint correta também aumenta. No entanto, o mercado de segurança de endpoints ficou tão saturado com as muitas soluções diferentes e outras tantas declarações de marketing sem embasamento que está cada vez mais difícil tomar uma decisão informada para sua organização.

Este guia esclarece sobre as principais funcionalidades de uma solução de proteção de endpoint e o que você precisa ter para garantir a proteção certa contra as ameaças avançadas de hoje. Com esses insights, você estará mais bem preparado para tomar uma decisão com respaldo tecnológico para a sua organização.

Documento técnico Sophos. Junho de 2024

O panorama atual das ameaças à segurança

Nossa pesquisa independente com 3.000 líderes responsáveis pela segurança cibernética e TI em 14 países revela um sistema de segurança cibernética desalinhado, com adversários e defesas se movendo a diferentes velocidades. Retardadas por ventos contrários, as defesas estão ficando para trás, enquanto os adversários se antecipam.

A evolução da economia do crime cibernético

Uma das mudanças mais significativas no panorama das ameaças nos últimos anos foi a sua transformação de um grupo criminoso em uma indústria do crime, com uma rede de serviços de suporte e uma abordagem profissional e bem-estabelecida às suas operações.

A exemplo das empresas de tecnologia que mudaram para as ofertas "as-a-service", o ecossistema do crime cibernético também mudou. Isso abriu espaço para a entrada de mais criminosos cibernéticos e capacitou mais agentes de ameaças a intensificarem o volume, a velocidade e o impacto de seus ataques.

O resultado são adversários capazes de executar uma ampla gama de ataques sofisticados e em grande escala. 94% das organizações passaram por um ataque cibernético no último ano. Ainda que o ransomware tenha sido o ataque mais amplamente difundido, as organizações enfrentaram muitos outros tipos de ataques, como:[1]

27%	**27%**	**26%**
E-mail malicioso	Phishing (incluindo spear phishing)	Exfiltração de dados (por invasor)
24%	**24%**	**21%**
Extorsão cibernética	Comprometimento de e-mail corporativo	Malware móvel
18%	**24%**	**14%**
Criptomineradores	Negação de serviço (DDoS)	Wipers

Leia o nosso relatório O Estado da Segurança Cibernética 2023: o impacto comercial dos adversários para saber mais.

Ransomwares continuam a assolar as organizações

Em se tratando de ransomwares, 59% das organizações disseram ter sido vítimas de um ataque no último ano.

2020	2021	2022	2023	2024
51%	37%	66%	66%	59%

Sua organização foi atingida por ransomware neste último ano?
Sim. n=5.000 (2024), 3.000 (2023), 5.600 (2022), 5.400 (2021), 5.000 (2020).

Embora o índice de ataques registrado em 2024 tenha caído em comparação a 2023, a criptografia de dados por ransomware permanece alta, como prova o sucesso obtido pelos adversários com a criptografia de dados em 70% dos ataques.

O ransomware também ficou mais caro, com as organizações registrando custos médios de recuperação na casa de US$ 2,73 milhões, comparativamente a US$ 1,82 milhão registrado em 2023.[2]

Leia o nosso estudo anual sobre ransomware, O Estado do Ransomware 2024, para conhecer a realidade que as organizações enfrentam em 2024, incluindo a frequência, o custo e a causa primária dos ataques.

1 O Estado da Segurança Cibernética 2023: O impacto comercial dos adversários, Sophos – Resultados de um estudo independente com 3.000 líderes responsáveis pela segurança cibernética e TI distribuídos em 14 países realizado em janeiro e fevereiro de 2023.

2 O Estado do Ransomware 2024, Sophos – Resultados de um estudo independente e totalmente desvinculado com 5.000 líderes responsáveis pela segurança cibernética e TI distribuídos em 14 países realizado entre janeiro e fevereiro de 2024.

Abordagens legadas levam a resultados de segurança insatisfatórios

O ambiente comercial mudou para muitas organizações nos últimos anos. Os usuários finais podem estar no escritório, trabalhando remotamente ou continuamente em trânsito, deslocando-se entre clientes e parceiros. Os dados das empresas não são mais mantidos exclusivamente no local, eles podem estar no local, na nuvem e nos dispositivos dos usuários finais, podendo ser acessados local e remotamente para atender às necessidades dos funcionários geograficamente dispersos. Assim, seguir abordagens de segurança cibernética legadas geralmente resulta em uma segurança deficiente.

Alguns dos problemas mais comuns encontrados pelas equipes de segurança de TI são:

- **Falta de especialistas –** Funcionários de TI especializados continuam difíceis de serem encontrados e contratados. A falta de experiência implica que os funcionários talvez não ofereçam a habilidade de determinar se um alerta de segurança é maligno ou benigno.
- **Sobrecarga de ruído –** O excesso de alertas de muitos sistemas diferentes sobrecarregam os operadores que, frequentemente, acabam por não saber quais sinais priorizar e quais alertas investigar, perdendo assim os indicadores de um possível ataque.
- **Dados em silos –** Alertas e sinais de ameaças limitados a tecnologias específicas, impedindo que as equipes de TI vejam o quadro geral e solucionem alertas maliciosos e incidentes com prontidão.
- **Falta de integração –** Ferramentas de segurança que não se integram entre elas ou a uma infraestrutura comercial de TI, aumentando a complexidade.
- **Processos manuais –** Equipes de TI gastam muitas horas correlacionando eventos, logs e informações para entender o que está acontecendo. Esse tempo perdido retarda a identificação e a resposta ao ataque.
- **Resposta reativa –** Devido aos pontos acima, muitas equipes de TI ficam na defensiva, respondendo às ameaças apenas depois que elas já causaram danos, ao invés de interrompê-las com antecedência na cadeia de ataque.
- **Foco no incêndio –** Os esforços diários para bloquear as ameaças impedem melhorias de longo prazo. Quando as equipes de TI ficam apagando focos de incêndio, geralmente não têm a oportunidade de identificar a causa primária do incidente ou de manter registros precisos do ataque e das medidas tomadas. Isso impede esforços maiores para tratar de questões estruturais.
- **Dados distribuídos –** Usuários e dispositivos estão em todo lugar. Consequentemente, os dados estão em todo lugar – nos escritórios, na nuvem, nos dispositivos, prontos para o acesso local ou por meio de soluções de acesso remoto.

Uma maneira de enfrentar muitos desses desafios é implantar uma solução de proteção de endpoint de classe superior.

Pontos básicos da proteção ide endpoint

As soluções de segurança de endpoint devem trabalhar com e para você, adaptando as suas defesas em resposta a um ataque. O mínimo esperado é que uma solução moderna de segurança de endpoint opere seguindo uma abordagem que enfatize a prevenção e:

Reduza a exposição a ameaças – Bloqueando o conteúdo mal-intencionado e as ameaças baseadas na web e controlando o acesso a aplicativos, sites e dispositivos periféricos, entre outros.

Bloqueie atividades maliciosas – Prevenindo a exploração e as técnicas que codificadores mal-intencionados e ransomwares utilizam para atingir suas metas, identificando a atividade específica e interrompendo-a antes que se torne um problema concreto.

Facilite respostas adaptadas e automatizadas – Suas defesas devem responder automaticamente às ameaças e adaptarem-se para acompanhar a mudança de comportamento do invasor. Isso não apenas desestabiliza o invasor, mas também alerta a sua equipe sobre a presença do invasor, proporcionando um tempo de resposta valioso para a equipe.

Sirva como um meio para a caça de ameaças (por pessoal interno ou gerenciada) – Sinais de alta qualidade enriquecidos com sinais de segurança podem acelerar drasticamente o tempo de detecção e resposta a uma ameaça. Quanto melhor o diagnóstico, mais rápida a resolução.

Oferecendo ótimos resultados em segurança

Agora que descrevemos o que uma solução de proteção de endpoint deve fazer sob um aspecto funcional, é essencial traçarmos um quadro mais amplo sobre como isso pode beneficiar a sua organização. Uma proteção forte de endpoint deve trabalhar para oferecer ótimos resultados para a sua segurança.

Riscos cibernéticos reduzidos

Uma proteção forte de endpoint diminui seus riscos cibernéticos e o protege de uma amplitude de ameaças cibernéticas.

A abordagem da prevenção em primeiro lugar

Quanto mais cedo um ataque for interrompido, menos trabalho você terá mais tarde. Uma proteção superior de endpoint trabalha com várias camadas de proteção para a defesa contra ataques cibernéticos e ataques que visam computadores, notebooks, dispositivos móveis e servidores. A proteção de endpoint defende esses equipamentos, dispositivos e seus dados contra malware, vírus, ransomware e outras atividades mal-intencionadas.

Identificando desvios na postura de segurança

São vários os motivos que podem levar a desvios na sua postura de segurança. Em uma pesquisa independente recente, a configuração incorreta das ferramentas de segurança figurou no topo da lista de riscos à segurança observados pelos gerentes de TI em 2023.[2]

Busque soluções de segurança de endpoint que avaliem sua postura de segurança e otimizem a sua configuração constantemente. Essa abordagem automatizada é crítica para obter uma postura forte de segurança, reduzindo o seu risco cibernético e aliviando a carga de realizar esse processo manualmente.

Gerenciamento agilizado

Um painel de gerenciamento centralizado permite que os administradores de TI monitorem e gerenciem parâmetros de segurança, políticas, exclusões e alertas de ameaças em todos os endpoints em um só local. Isso simplifica o gerenciamento da segurança, diminui o risco de configurações incorretas e garante uma proteção consistente. Alguns painéis de gerenciamento centralizado vão além, verificando automaticamente a "integridade" da sua postura e sinalizando mudanças em atividades ou políticas que poderiam comprometê-la.

Detecção e resposta aceleradas

Cada segundo conta quando um adversário se aloja no seu ambiente. Uma proteção de endpoint de alta qualidade que coloca a prevenção em primeiro lugar reduz a quantidade de ruído e gera alertas de alta fidelidade. A tecnologia EDR de detecção e resposta de endpoint e a tecnologia XDR de detecção e resposta estendidas podem ser usadas para investigar esses alertas.

Algumas soluções vão além, utilizando a inteligência artificial (IA) e a inteligência de ameaças para priorizar as detecções automaticamente. Essas soluções garantem que a sua equipe saiba aonde direcionar seu foco e aceleram a resposta a ameaças que são ativamente conduzidas por humanos.

Eficiência de TI aumentada

64% das empresas gostariam que suas equipes de TI gastassem menos tempo apagando incêndios e mais tempo em questões estratégicas.[3] A proteção de endpoint automatizada e simplificada ajuda as equipes de TI a atingir essa meta.

Soluções superiores de endpoint bloqueiam e eliminam automaticamente a maioria das ameaças já no início. Elas liberam a capacidade da TI, permitindo que as equipes de TI priorizem as iniciativas de negócios. Tecnologias como o XDR trabalham para reduzir a fadiga de sinal, liberando mais tempo para projetos de maior importância.

Essa eficiência aumentada acaba por permitir que as equipes de TI mudem de uma segurança cibernética de cunho reativo para proativo. Ela dá a essas equipes tempo para saírem no encalço de ameaças antes que causem problemas concretos, o que, por sua vez, reduz os riscos cibernéticos.

2 O Estado do Ransomware 2024, Sophos – Resultados de um estudo independente e totalmente desvinculado com 5.000 líderes responsáveis pela segurança cibernética e TI distribuídos em 14 países realizado entre janeiro e fevereiro de 2024.

3 O Estado da Segurança Cibernética 2023: O impacto comercial dos adversários, Sophos – Resultados de um estudo independente com 3.000 líderes responsáveis pela segurança cibernética e TI distribuídos em 14 países realizado em janeiro e fevereiro de 2023.

Retorno do investimento na segurança cibernética melhorada

Uma segurança cibernética robusta deveria proteger as organizações contra as consequências financeiras e operacionais de um grande incidente de segurança.

Para isso, o investimento em uma proteção de endpoint superior é essencial. A boa prevenção custa muito menos do que a remediação. Uma proteção robusta de endpoint bloqueia a maioria das ameaças, reduzindo suas chances de ser alvo de um ataque e ter de encarar os custos associados.

Além disso, as soluções superiores de proteção de endpoint podem se integrar e se comunicar com seus investimentos existentes em segurança para ampliar sua proteção, reduzir a complexidade e fazer com que suas tecnologias de proteção existentes (como e-mail, firewall, rede, identidade e nuvem) trabalhem de maneira mais intensa e inteligente.

Tudo isso melhora o seu ROI em segurança cibernética enquanto reduz o seu custo total de propriedade.

Classe de bônus otimizada do seguro de proteção digital

Os prêmios de seguro cibernético subiram significativamente nos últimos anos, e as apólices se tornaram mais complexas e morosas. As seguradoras estão exigindo controles cibernéticos mais robustos – em verdade, 95% das organizações que adquiriram seguro de proteção digital no último ano disseram que a qualidade de suas defesas afetou diretamente sua classe de bônus no mercado de seguros[4].

A chave para otimizar sua classe de bônus no mercado de seguros é minimizar o seu risco cibernético. Investir em defesas robustas, incluindo serviços de segurança 24 horas e ferramentas de detecção e resposta de classe superior, oferece vários benefícios:

1. Facilita obter cobertura do seguro de proteção digital (ou seja, melhora a elegibilidade às ofertas de seguro)
2. Ajuda a reduzir o prêmio e melhora os termos e condições
3. Diminui a probabilidade de um sinistro, o que resulta em prêmios mais altos
4. Reduz o risco de não pagamento no caso de um sinistro

As tecnologias superiores de proteção de endpoint servem como um canal para a capacidade de detecção e resposta, portanto, certifique-se de que os fornecedores que você está analisando ofereçam isso. O sistema EDR de detecção e resposta de endpoint é agora um pré-requisito para a cobertura oferecida pela maioria das seguradoras, e as organizações sem esse recurso normalmente têm dificuldade para conseguir uma apólice.

Os serviços que otimizam a detecção e resposta, e, portanto, minimizam o risco da ocorrência de um incidente cibernético, são considerados o “padrão ouro” para as seguradoras de proteção digital. Particularmente as organizações que usam serviços gerenciados de detecção e resposta (MDR) são, geralmente, consideradas clientes de "Nível 1" pelas seguradoras, pois representam o nível de risco mais baixo.

Sendo assim, procure fornecedores que ofereçam um caminho de upgrade descomplicado de uma solução de proteção de endpoint para um serviço 24/7 totalmente gerenciado de busca de ameaças, detecção e/ou resposta a incidentes que se integre a produtos existentes e controles de segurança de terceiros.

5 The Critical Role of Frontline Cyber Defenses in Cyber Insurance Adoption - Sophos.

Avaliação da Segurança de Endpoints: As 10 principais perguntas a serem feitas

Agora que você tem uma ideia mais clara de como se parece uma solução de segurança de endpoint superior, relacionamos algumas perguntas para você fazer aos seus possíveis fornecedores.

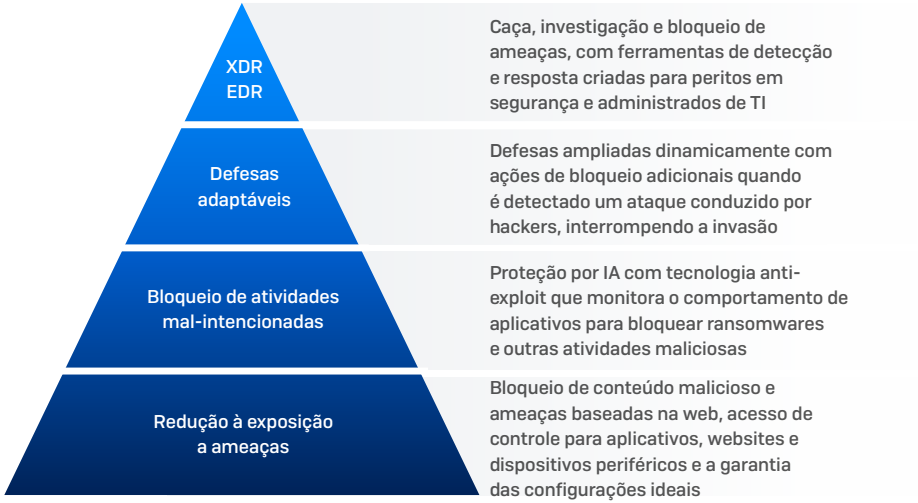
1. O produto segue uma abordagem multicamada que coloca a prevenção em primeiro lugar? Ou ele segue o princípio da detecção em primeiro lugar? Quais recursos específicos são fundamentais para a tecnologia?
2. O produto tem a funcionalidade de detectar e retificar automaticamente um desvio comportamental na postura de segurança? Ele destaca mudanças na configuração de políticas que aumentam os riscos?
3. O produto reage automaticamente a uma ameaça? Ele pode limpar uma ameaça de forma automática e reagir a um incidente?
4. O produto oferece defesas que se adaptam automaticamente quando é detectado um ataque operado diretamente pelo invasor?
5. O produto oferece funcionalidades anti-ransomware e anti-exploit robustas, incluindo proteção em tempo real contra ataques de ransomware remotos? Essas funcionalidades estão habilitadas por padrão? Essas funcionalidades precisam ser ativadas e treinadas para funcionarem no seu ambiente?
6. Quantos painéis são necessários para gerenciar o produto? Os painéis, ou painel, estão hospedados na nuvem ou exigem a instalação no local?
7. O produto oferece uma transição descomplicada para EDR/XDR usando o mesmo painel de gerenciamento e o mesmo agente no endpoint/servidor?
8. A funcionalidade XDR integra e incorpora alertas de controles de segurança nativos e de terceiros para oferecer um quadro completo do meu ambiente?
9. O produto oferece um caminho de upgrade descomplicado para um serviço 24/7 totalmente gerenciado de busca de ameaças, detecção e resposta a incidentes que se integra aos meus produtos existentes e controles de segurança de terceiros?
10. O fornecedor tem evidências de organizações de testes, análises e depoimentos de clientes que validem sua abordagem à segurança de endpoint?

A abordagem da Sophos

Vejamos agora a abordagem da Sophos à proteção de endpoint. O Sophos Endpoint oferece proteção inigualável contra ataques cibernéticos avançados. Uma abordagem de uso de defesas aprofundadas e proteção hermética contra ransomwares bloqueiam a mais ampla variedade de ameaças antes que afetem seus sistemas. Ferramentas poderosas de EDR e XDR permitem que sua equipe busque, investigue e responda às ameaças com velocidade e precisão.

Abordagem de prevenção em primeiro lugar

O Sophos Endpoint adota uma abordagem abrangente para proteger todos os endpoints sem se basear em uma única técnica de segurança. Ao interromper a aproximação de mais ameaças, as equipes de TI, já extenuadas, têm menos incidentes para investigar e resolver.



Redução à exposição a ameaças

O Sophos Endpoint diminui a sua exposição a ameaças e as oportunidades de invasores se instalarem no seu ambiente. Ele bloqueia o conteúdo de web mal-intencionado e as ameaças baseadas na web, além de permitir que você controle o acesso a aplicativos, sites e dispositivos periféricos.

Bloqueio de ameaças baseadas na web e controle de acesso à web

Há muitas ameaças baseadas na web. As organizações geralmente usam firewalls de última geração para proteger os usuários que trabalham nos escritórios contra phishing, sites mal-intencionados e outras ameaças baseadas na web. Isso protege os endpoints nas redes no escritório, mas esses endpoints podem ser usados em casa, nas viagens, nos aeroportos e em outros lugares onde um firewall não poderá protegê-los.

O Sophos Endpoint bloqueia o acesso a sites de phishing e sites mal-intencionados fazendo a análise de arquivos, páginas da web e endereços IP. Isso assegura que os endpoints estejam constantemente protegidos contra ameaças, independentemente da localização.

Além disso, o SophosLabs e a equipe do Sophos MDR oferecem inteligência de ameaça em tempo real para proteger os clientes da Sophos contra ameaças emergentes.

Controlando web, periféricos e aplicativos

A Sophos permite que você restrinja as atividades do endpoint. Esses controles são geralmente usados com a política de uso aceitável de uma organização.

O primeiro controle é o monitoramento e/ou bloqueio do acesso a categorias de sites da web (jogos de aposta, redes sociais etc.). O Sophos Endpoint permite que você monitore e bloqueie categorias de sites, e a aplicação é imposta dentro e fora das redes do escritório.

O controle do acesso a dispositivos periféricos e mídias removíveis pode diminuir mais a sua superfície de ataque. Pense nas muitas ocasiões em que um usuário conecta uma impressora ou uma unidade de armazenamento USB ou carrega o celular usando uma porta USB. Essas operações são permitidas? Essa funcionalidade não apenas impede que um vetor de ataque insira códigos maliciosos em um endpoint, mas também pode ajudar a bloquear a exfiltração de dados da empresa.

Os aplicativos são outra categoria a considerar. Com o controle de aplicativos, você pode impedir que plug-ins de aplicativos ou navegadores sejam executados em dispositivos do trabalho. Seguindo nesse tópico de exfiltração de dados, considere aplicativos como OneDrive ou Google Drive para o armazenamento na nuvem. Alternativamente, pense nos programas torrent, navegadores TOR etc., e se o uso deles deveria ou não ser permitido em seus endpoints. Existe uma ampla gama de plug-ins de navegadores da web. Muitos deles oferecem reais benefícios, enquanto outros não.

Bloqueio de atividades mal-intencionadas

O próximo patamar de defesa envolve o uso de inteligência artificial, análise comportamental, anti-ransomware, anti-exploit e outras tecnologias para interromper as ameaças rapidamente, antes que se intensifiquem.

A Sophos usa a proteção por IA primeiramente, começando pela classificação por IA dos executáveis. Ela utiliza um modelo treinado em milhões de executáveis benignos e malignos. Esse modelo pode identificar com rapidez e eficácia os executáveis mal-intencionados com base em suas propriedades e não requer assinaturas.

Proteção hermética contra ransomware

O Sophos Endpoint é a defesa zero touch de endpoint mais robusta que há contra ransomware local e remoto. Ele inclui a avançada tecnologia CryptoGuard que detecta sinais de criptografia, independentemente da fonte. Essa abordagem universal interrompe as novas variantes de ransomwares remotos e locais. Ela inspeciona alterações ao conteúdo do arquivo em tempo real, para detectar criptografia maliciosa, e bloqueia ransomwares remotos executados em um dispositivo diferente que tente criptografar arquivos pela rede. Os arquivos criptografados por ransomware são automaticamente revertidos para um estado não criptografado, independentemente do tamanho ou tipo do arquivo. Isso minimiza o impacto à produtividade dos negócios. Isso também protege o registro mestre de inicialização (MBR) contra a criptografia usada em alguns ataques de ransomware.

Anti-exploit

A tecnologia anti-exploit interrompe os comportamentos e bloqueia as técnicas empregadas pelos invasores para comprometer dispositivos, roubar credenciais e distribuir malware. A Sophos implanta novas abordagens anti-exploit no dispositivo em escala para todos os aplicativos. Pronta para o trabalho: a Sophos amplia a proteção básica oferecida pelo Microsoft Windows, adicionando pelo menos 60 processos proprietários de mitigação de exploits pré-configurados e sintonizados. Como resultado, a Sophos mantém a sua organização protegida contra ataques sem arquivo e explorações de dia zero ao bloquear as técnicas usadas em toda a cadeia de ataque.

Defesas adaptáveis

Essas defesas dinâmicas adicionais são uma iniciativa da indústria que oferece uma proteção automatizada aprimorada que se adapta ao contexto do ataque. O Sophos Endpoint bloqueia as ações que não são inerentemente mal-intencionadas em um contexto do dia a dia, mas que são perigosas no contexto de um ataque. Essa funcionalidade responde dinamicamente e interrompe os ataques ativos em que os invasores possam ter se infiltrado na sua rede sem levantar suspeitas ou usando códigos mal-intencionados.

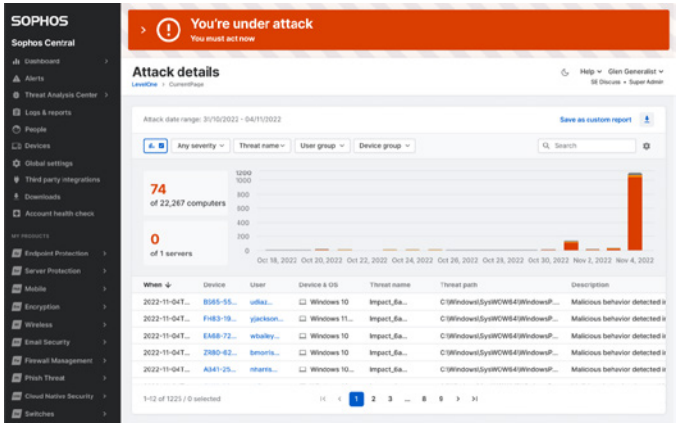
	PROTEÇÃO COMPORTAMENTAL	PROTEÇÃO ADAPTATIVA CONTRA ATAQUES	AVISO DE ATAQUE CRÍTICO
ESCOPO	DISPOSITIVO INDIVIDUAL	DISPOSITIVO INDIVIDUAL	DISPOSITIVO INDIVIDUAL
BENEFÍCIOS	Mecanismo de comportamento interrompe estágios iniciais de ataques adversários ativos	Aumenta a sensibilidade de proteção para prevenir danos	Alerta o cliente sobre um ataque que exige resposta imediata
GATILHO	Regras de comportamento	Ferramentas de exploração detectadas	Indicadores de adversários ativos de alto impacto, incluindo correlações de nível organizacional e limiares
ANALOGIA	"CUIDADO!"	"ATENÇÃO!"	"ALERTA VERMELHO!"

Proteção Adaptativa contra Ataques

A Proteção Adaptativa contra Ataques habilita dinamicamente as altas defesas em um endpoint quando é detectado um ataque prático executado diretamente pelas mãos de um hacker. Ela neutraliza a capacidade de atuação do invasor, minimiza a superfície de ataque, interrompe e contém o ataque, ganhando um tempo valioso de resposta.

Aviso de Ataque Crítico

Um Aviso de Ataque Crítico o alerta sobre um ataque severo que se estende por todo o seu arsenal digital se atividades adversas forem detectadas em vários endpoints ou servidores no seu ambiente com indicadores adicionais de alto impacto. Essa é uma situação de alerta vermelho: você está sob ataque! A tecnologia de automação o informa sobre a situação, fornecendo contexto e detalhes do ataque. Você pode responder usando o Sophos XDR, buscar assistência com o seu parceiro ou contatar a equipe do Sophos Incident Response para ajudar a responder à ameaça.



Reduza o custo total de propriedade da segurança cibernética

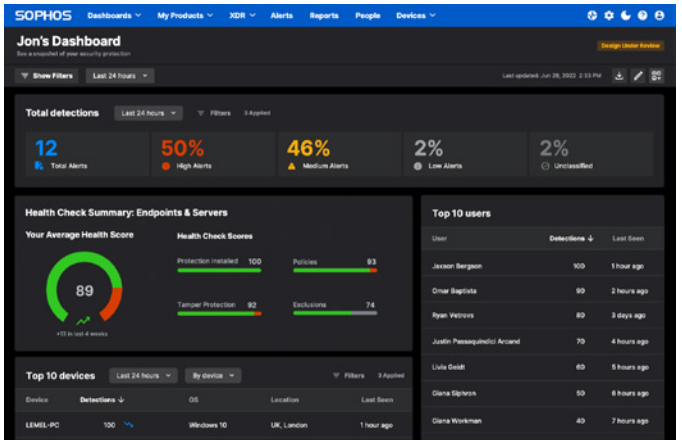
A maioria das equipes de segurança e TI está extenuada. Automatizar e poupar o tempo e os esforços dedicados são fatores-chave no Sophos Endpoint. Tudo o que puder ser automatizado, reduzido ou removido da carga de trabalho das equipes de segurança e TI permite que essas equipes se concentrem em outras iniciativas de negócios.

O Sophos Central oferece uma plataforma de gerenciamento baseada na nuvem para gerenciar produtos Sophos (endpoints, servidores, dispositivos móveis, firewalls, switches, pontos de acesso, e-mail e nuvem), incluindo o Sophos Endpoint. De um único local, você pode criar e gerenciar políticas, exibir detecções e alertas, investigar e remediar ameaças potenciais e desempenhar outras ações em todos os seus produtos Sophos.

As tecnologias de proteção da Sophos recomendadas estão todas ativadas por padrão, assegurando a facilidade de instalação e que você tenha imediatamente as configurações de proteção mais reforçadas sem necessidade de ajustes complexos. O controle granular está disponível se solicitado.

Identificar desvios na postura de segurança

Com o passar do tempo, a postura de segurança de uma organização pode se desviar de uma configuração conforme ou ideal. Políticas com parâmetros mal configurados, exclusões e outros fatores são um risco à sua postura de segurança. A Verificação de integridade de conta da Sophos identifica desvios na postura de segurança e configurações incorretas de alto risco, permitindo que você resolva problemas com um simples clique.

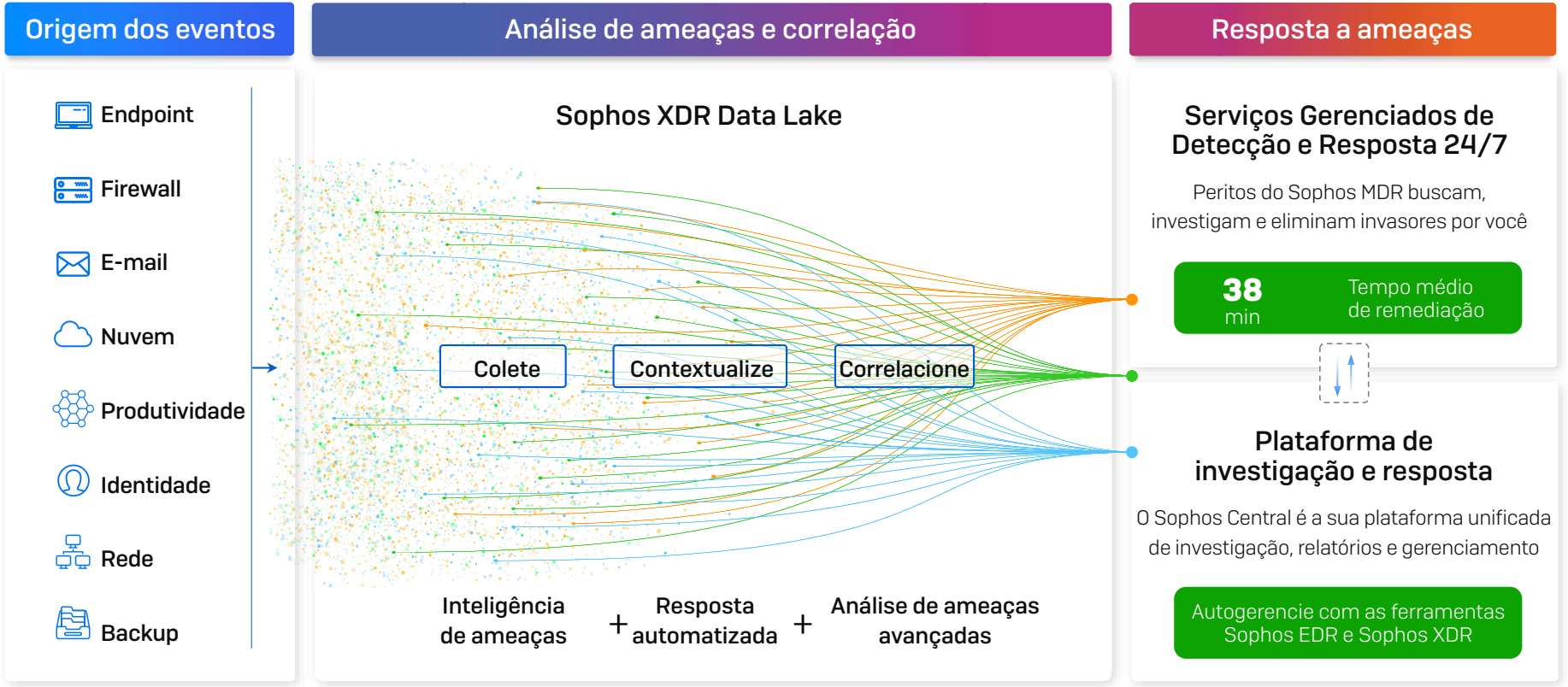


Segurança sincronizada

As soluções Sophos funcionam melhor juntas. O Sophos Endpoint compartilha informações de status e integridade com o Sophos Firewall, Sophos ZTNA e outros produtos para oferecer visibilidade adicional a ameaças e uso de aplicativos. Durante a limpeza, o Synchronized Security isola automaticamente os dispositivos comprometidos, que voltarão a ter acesso à rede assim que a ameaça for neutralizada — tudo sem a intervenção do administrador.

Acelere a detecção e a resposta: EDR, XDR e MDR

A abordagem da prevenção em primeiro lugar da Sophos bloqueia e elimina automaticamente o máximo possível de ameaças, deixando para as equipes de TI e segurança um número significativamente menor de detecções de alta qualidade para investigar.



A abordagem da Sophos de prevenção, detecção e resposta.

Sophos Endpoint Detection and Response (EDR)

A Sophos integra poderosas funcionalidades de detecção e resposta à abordagem robusta do Sophos Endpoint que focam na prevenção, permitindo que você localize, investigue e responda a atividades suspeitas em todos os seus endpoints e servidores. As detecções são priorizadas pela análise conduzida por IA, o que ajuda você a identificar para onde é melhor direcionar seu tempo e energia. Os operadores podem acessar dispositivos remotamente para investigar problemas, instalar e desinstalar software ou solucionar problemas.

Sophos Extended Detection and Response (XDR)

Para as organizações que buscam funcionalidades de detecção e resposta mais abrangentes, o Sophos XDR lhe permite localizar, investigar e responder a atividades suspeitas e ataques multiestágio em todo o seu ambiente de segurança. Projetada por analistas de segurança para analistas de segurança, essa é a única ferramenta de operações de segurança do setor que une a telemetria nativa da Sophos a controles de segurança de terceiros para acelerar a detecção e resposta. O Sophos XDR oferece integrações prontas para uso e adaptadas a um extenso ecossistema que engloba soluções de endpoint, firewall, rede, e-mail, identidade, produtividade, nuvem e backup, para que você obtenha um ROI maior de suas ferramentas de segurança existentes.

Sophos Managed Detection and Response (MDR)

Para as organizações sem recursos humanos para gerenciar internamente a detecção e a resposta a ameaças, o Sophos MDR é um serviço 24/7 fornecido por uma equipe de elite experiente formada por caçadores de ameaças e especialistas em resposta. O Sophos MDR utiliza a telemetria da Sophos e os controles de segurança de terceiros para detectar e neutralizar ameaças complexas e ultrassofisticadas.

O Sophos XDR e o Sophos MDR vão até você, integrando-se a seus investimentos existentes em tecnologia, incluindo e-mail, firewall, rede, identidade e nuvem, e capacitando-o a obter maior retorno de seus investimentos existentes.

Serviço por Honorários do Sophos Incident Response

O Sophos Incident Response Services Retainer é uma assinatura anual para clientes de Endpoint, EDR e XDR que dá acesso rápido a uma equipe de peritos em resposta a acidentes, de acordo com condições de serviço pré-estabelecidas, que bloqueia ataques ativos com rapidez para que você retome suas atividades normais.

Por que a Sophos

A Sophos é líder mundial em soluções inovadoras e avançadas em segurança cibernética, que incluem MDR, resposta a incidentes e tecnologias de segurança de endpoint, rede, e-mail e nuvem, que contribuem para a defesa das organizações contra ataques cibernéticos. Uma das maiores provedoras globais pure-play de segurança cibernética, a Sophos se incumbe da defesa de mais de 550.000 organizações e de mais de 100 milhões de usuários contra adversários ativos, ransomwares, phishing, malwares e outros ataques. Essa visibilidade inigualável da ameaça proporciona uma inteligência de ameaça sem paralelos que é usada para ajustar a capacidade defensiva dos produtos e serviços da Sophos para todos os clientes.

Testes independentes

Os testes realizados por terceiros de grande reputação são uma ferramenta importante para ajudar as organizações a tomarem decisões bem embasadas sobre seu arsenal tecnológico e investimentos em segurança. Entretanto, com os ataques aumentando em volume e complexidade, resultados de real valor só podem ser obtidos quando os testes refletem a realidade das organizações que estão no mercado.

SE Labs

A SE Labs é uma das poucas empresas de testes de segurança do setor que simula ferramentas e táticas, técnicas e procedimentos (TTPs) de ataque atuais que os criminosos cibernéticos e pen testers estão usando no momento.

Na última edição do SE Labs Endpoint Security Report (janeiro a março de 2024), a Sophos, mais uma vez, foi classificada como a melhor proteção do setor, recebendo a insígnia AAA em âmbito total, nas categorias de grandes empresas e PME.
Os relatórios da SE Labs para o 1º trimestre de 2024 você encontra em:

Endpoint Security: Enterprise | Endpoint Security: Small Business

MITRE Engenuity ATT&CK Evaluations

A Sophos foi destaque nas avaliações 2023 MITRE Engenuity ATT&CK para Enterprise (Turla). O Sophos XDR detectou 99% dos comportamentos adversários na avaliação, apontando 141 das 143 subetapas do ataque adversário. Além disso, para demonstrar sua habilidade em proporcionar às equipes de segurança um rico conteúdo contextual sobre o quê, o porquê e o como do comportamento do adversário, o Sophos XDR registrou uma excelente cobertura analítica de 98% das subetapas da avaliação.

As avaliações da MITRE Engenuity ATT&CK estão entre os testes de segurança independentes mais bem conceituados do mundo devido, em grande parte, à construção e emulação de cenários de ataque reais, transparência dos resultados e riqueza de informações de participantes.

Premiações e Relatórios de Análises

Gartner

- ✓ Líder pela Gartner Magic Quadrant em Plataformas de Proteção de Endpoints em 14 relatórios consecutivos
- ✓ Customers' Choice na Gartner® Peer Insights™ Voice of the Customer em Plataformas de Proteção de Endpoints (EPP) nos relatórios de 2022, 2023 e 2024

IDC

- ✓ Líder no IDC MarketScape de 2024 em Segurança de Endpoints Modernos para empresas de pequeno e médio porte em âmbito mundial

G2

- ✓ Líder Geral | Suítes de Proteção de Endpoints: Relatórios analíticos Spring 2023 e Fall 2023
- ✓ Líder Geral | EDR: Relatórios analíticos Spring 2023 e Fall 2023
- ✓ Líder Geral | XDR: Relatório analítico Fall 2023
- ✓ Líder Geral e Solução Nº1 | XDR: Relatório analítico Spring 2023

Omdia

- ✓ Líder Geral | Novembro de 2022. Plataformas XDR (Comprehensive Extended Detection and Response)

Prêmio CRN em Inovação Tecnológica de 2023

- ✓ Sophos Intercept X agraciado como a melhor proteção de endpoint

Readers' Choice Awards da ChannelPro

- ✓ Sophos Intercept X agraciado com o Gold Winner como Melhor Fornecedor de Segurança de Endpoint

Depoimento de clientes

★★★★★

"O recurso mais valioso do Sophos Endpoint Protection é a sua proteção contra ameaças avançadas. A Sophos utiliza uma combinação de tecnologias avançadas, como machine learning, análise comportamental e detecção baseada em assinatura, para detectar e bloquear ameaças mal-intencionadas."

Desenvolvedor de software | Finanças (não bancário)| Leia a avaliação na íntegra no Gartner Peer Insights

★★★★★

"Uma solução para ameaças de segurança cibernética centrada em um único painel."

Administrador de rede | Educação | Leia a avaliação na íntegra no Gartner Peer Insights

★★★★★

"Minha experiência foi satisfatória. Reduz a superfície de ataque e previne a disseminação de ataques na rede da nossa organização. Com anti-ransomware e IA com deep learning, os ataques são interrompidos antes que causem qualquer impacto ao sistema, o que é excelente."

Departamento de segurança de ICT | Radiodifusão | Leia a avaliação na íntegra no G2 Reviews

★★★★★

"A solução de endpoint da Sophos é potente e extremamente fácil de usar."

Gerente de operações de TI | Organização de médio porte | Leia a avaliação na íntegra no G2 Reviews

★★★★★

"O Sophos Endpoint ajuda a diminuir nossa vulnerabilidade a invasores e nos deixa tranquilos, sabendo que os sistemas de nossos clientes estão protegidos contra vetores de ataque."

Gerente de gerenciamento, backup e recuperação de sistemas | Organização de grande porte | Leia a avaliação na íntegra no G2 Reviews

Conclusão

A segurança cibernética é altamente antagonizada e se move com rapidez. Os invasores aprimoram suas técnicas incessantemente para esquivar-se das defesas – e fornecedores de segurança e organizações precisam se adaptar.

Para isso, é fundamental usar ferramentas de segurança que sigam uma abordagem de prevenção em primeiro lugar. Essas ferramentas oferecem defesas automatizadas e adaptáveis para bloquear ou desacelerar os invasores e ganhar tempo extra para responder aos ataques cibernéticos.

Entretanto, saber o que buscar em uma solução de segurança de endpoint e quais seriam os resultados da segurança ideal pode ajudar você a tomar uma decisão bem fundamentada. Ela também dá à sua organização a melhor proteção contra os ataques atuais.

Na Sophos, nós protegemos as organizações contra ameaças atuais e futuras. Nossas soluções ajudam as organizações a atingirem os melhores resultados de segurança possíveis. Para saber mais, fale conosco hoje mesmo.

Para saber mais sobre o Sophos Endpoint e como ele oferece proteção incomparável contra ataques avançados, visite **Sophos.com/endpoint**

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.

2024-06-18 PTBR-WP (PS)

SOPHOS