Sophos Network Detection and Response

Uma poderosa adição ao Sophos XDR e Sophos MDR

O NDR trabalha em conjunto com seus endpoints e firewalls gerenciados para monitorar a atividade da rede em busca de padrões de comportamento suspeito e malicioso que as soluções não conseguem ver. O Sophos NDR detecta fluxos anormais de tráfego de dispositivos IoT e sistemas não gerenciados, dispositivos ilegítimos, ameaças internas, ataques de dia zero nunca antes vistos e padrões incomuns nas profundezas da rede.

O Sophos NDR oferece visibilidade crítica das atividades na rede que outros produtos deixam passar despercebido

Os invasores são diplomados em se evadir da detecção, mas todo ataque precisa se mover pela rede. O Sophos NDR detecta padrões de tráfego suspeito na rede que passam despercebidos por seus endpoints e firewalls gerenciados, incluindo:

- **Dispositivos de rede desconhecidos ou desprotegidos** – engloba dispositivos IoT ou OT legítimos que não podem ser totalmente gerenciados com um sensor de endpoint, e também sistemas desconhecidos ou não identificados na rede. Esses dispositivos podem estar comprometidos ou ficar comprometidos durante um ataque. O Sophos NDR identifica e monitora esses dispositivos em busca de comportamentos suspeitos ou maliciosos que podem sinalizar um ataque.
- **Equipamentos não autorizados ou ilegítimos**, que são inseridos em uma rede e que podem já estar comprometidos ou ter sido usados para lançar ataques, podem ser prontamente identificados e monitorados pelo Sophos NDR.
- **Atividades de comando e controle (C2) novas e nunca antes vistas** – muitos dos ataques e violações são orquestrados remotamente usando o que parecem ser comunicações legítimas entre um agente nocivo e seus processos remotos dentro de uma rede. O Sophos NDR pode detectar atividades C2 de dia zero para identificar um ataque direcionado e estrategicamente criado que esteja prestes a ser iniciado.
- **Padrões e fluxos suspeitos ou mal-intencionados de tráfego na rede** – podem ser sinais importantes para identificar os estágios iniciais de um ataque cibernético. Alguns indícios incluem: acesso remoto e trabalho em horários incomuns, exfiltração ou upload suspeito de dados, padrões anormais de tráfego e tráfego malicioso gerado por um malware conhecido.

O NDR trabalha com o seu firewall

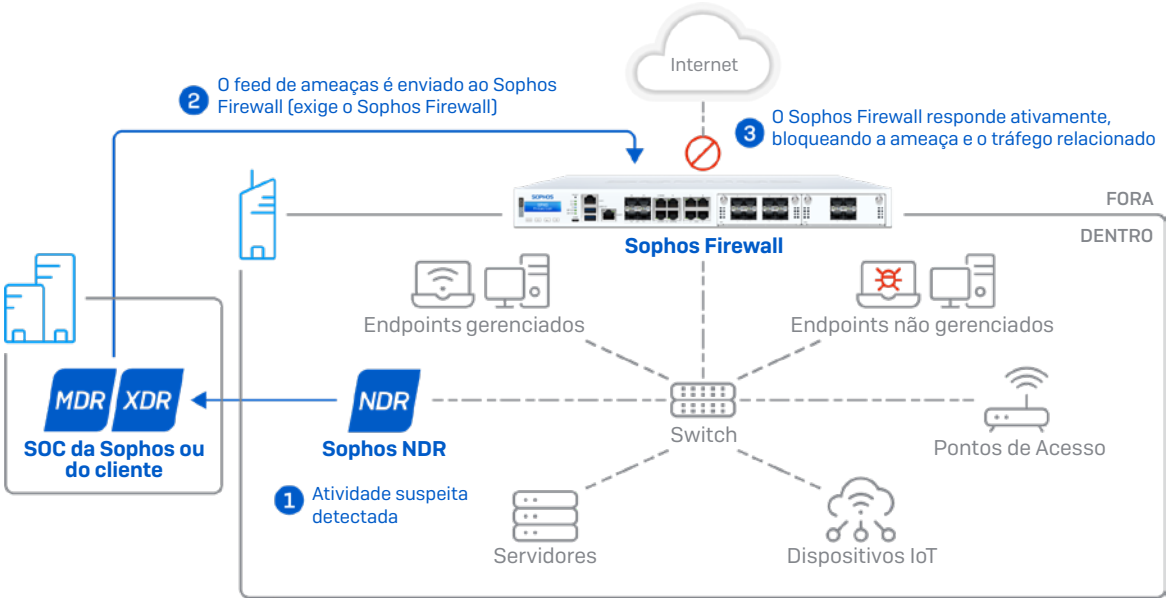
Os firewalls têm um papel crítico na segurança do perímetro da sua rede e no controle do que entra e sai dela. O Sophos NDR é o complemento perfeito para a sua solução de firewall, trabalhando em conjunto para oferecer insights e uma cobertura aprofundada do interior da sua rede e onde seu firewall não consegue enxergar. Também inclui tecnologias que identificam de maneira exclusiva atividades suspeitas e maliciosas que atravessam a sua rede internamente e que não poderiam ser detectadas de nenhum outro modo por outros produtos de proteção de endpoint ou firewall.

Destaques

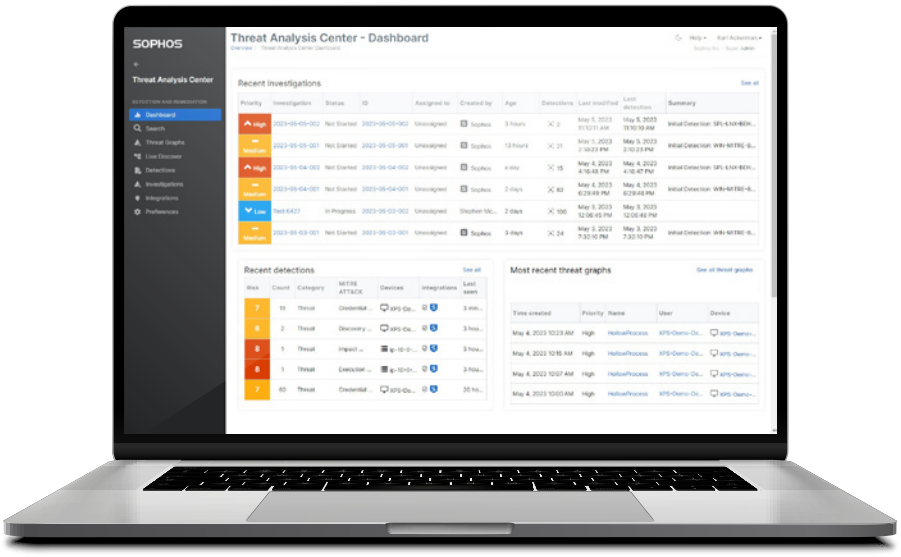
- A adição perfeita ao Sophos XDR e MDR, oferecendo detecções profundas na rede.
- Trabalha com o seu firewall para detectar atividades na rede e ameaças.
- Detecta atividades suspeitas na rede que se originam em dispositivos desconhecidos e não gerenciados, ativos ilegítimos e servidores de C2 de dia zero.
- Inspeciona os fluxos do tráfego criptografado sem comprometer informações PII.
- Implante, configure e gerencie no Sophos Central.
- Use o Console de investigação para obter insights de atividades suspeitas na rede e analisar ou investigar padrões anômalos.

SOPHOS

O Sophos NDR opera nas profundezas da sua rede para detectar um ataque

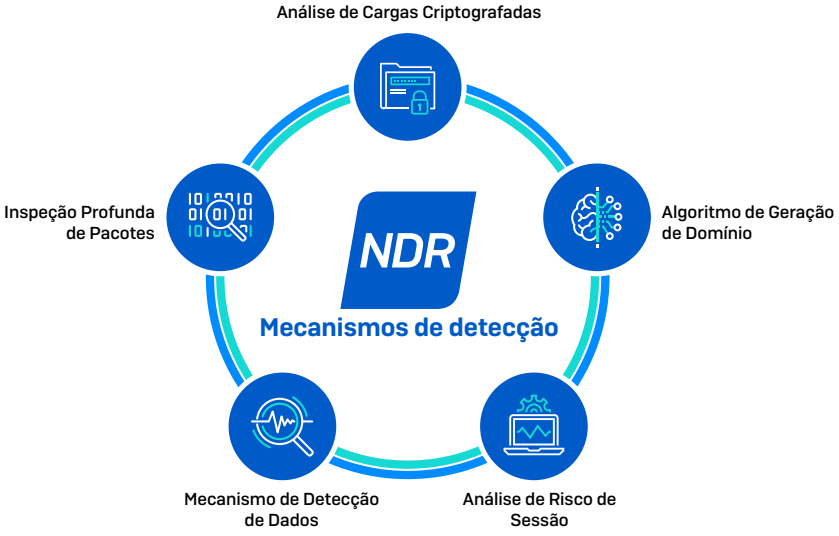


- Monitora profundamente o tráfego em uma rede usando cinco mecanismos em tempo real.
- Detecta a atividade de todos os recursos de rede, incluindo sistemas não gerenciados, dispositivos IoT e ativos ilegítimos, identificando o fabricante e o SO e padrões de tráfego suspeitos originados desses dispositivos.
- Envia feeds de dados e alertas ao Data Lake do Sophos Central e à equipe MDR do SOC da Sophos ou à sua equipe XDR.
- Obtenha visibilidade e insights das atividades na rede e aplicativos, fluxos de risco e tráfego suspeito com a facilidade de uso do Console de investigação.
- Se você tem o Sophos Firewall, a resposta automatizada a ameaças está disponível para bloquear a ameaça imediatamente e prevenir o movimento lateral.
- Funciona como um dispositivo virtual em plataformas populares de hipervisores, como VMware e Hyper- V.
- Conecta-se diretamente ao seu switch através do espelhamento da porta SPAN para monitorar todo o tráfego.
- Inspeciona dados de pacotes criptografados sem comprometer as informações PII.



Mecanismos de detecção do Sophos NDR

O Sophos NDR inclui cinco mecanismos de detecção que analisam continuamente os fluxos de tráfego na rede e aplicam análises de Machine Learning e IA para identificar atividades suspeitas e mal-intencionadas na sua rede.



Mecanismos de detecção	Descrição
Encrypted Payload Analytics (EPA, Análise de cargas criptografadas)	Detecta servidores C2 de dia zero e as novas variantes de famílias de malwares com base em padrões encontrados no tamanho de sessão, direção e tempo entre chegadas.
Domain Generation Algorithms (DGA, Algoritmo de geração de domínio)	Identifica a presença da tecnologia de geração de domínio dinâmica usada por um malware para evitar ser detectado.
Deep Packet Inspection (DPI, Inspeção profunda de pacotes)	Monitora o tráfego criptografado e não criptografado usando IOCs conhecidos, e identifica rapidamente os agentes de ameaças e TTPs.
Session Risk Analytics (SRA, Análise de risco de sessão)	Poderoso mecanismo de lógica que utiliza regras que alertam sobre uma infinidade de fatores de risco com base na sessão.
Device Detection Engine (DDE, Mecanismo de detecção de dispositivo)	Mecanismo de consulta expansível que usa um modelo de predição Deep Learning para analisar o tráfego criptografado em busca de padrões correlatos entre fluxos de rede que não se relacionam e detectar atividades de força bruta SSH e varredura de porta.

Licenciamento do Sophos NDR

O Sophos NDR é o complemento perfeito ao Sophos XDR e ao Sophos MDR como um pacote de integração. O preço do Sophos NDR se baseia no número total de usuários e servidores da organização. O software do dispositivo virtual está incluído na licença, e você pode implantar tantos sensores NDR quantos forem necessários. Isso é muito mais econômico e flexível do que as ofertas dos concorrentes, que cobram por instância.

Especificações técnicas do Sophos NDR

Plataformas compatíveis

- VMware ESXi6.7 e posterior
- Microsoft Hyper-V 6.0.600118016 (Windows Server 2016) ou posterior
- Amazon AWS c5n.2xlarge
- Certificação de hardware

Hardware	Taxa de transferência máx	Conexões máximas/s	CPUs	Memória
Dell R660 (2 soquetes)	40 Gb/s	120K	64	128 GB
Dell R660 (1 soquete)	40 Gb/s	80K	32	64 GB
Dell R650	20 Gb/s	40K	24	64 GB
Dell R450	10 Gb/s	20K	16	32 GB
Dell R350	4 Gb/s	8K	8	32 GB
Intel Nuc 13ª Gen	2,5 Gb/s	4K	12	32 GB

Requisitos do sistema de VM

As VMs do Sophos NDR suportam até 1 Gb/s por sensor:

- Use configurações padrão da VM para volumes médios de tráfego:
  - Até 500 Mb/s
  - Até 70.000 pacotes/s
  - Até 1.200 fluxos/s
- Redimensionar a VM para 8 vCPUs para volumes altos de tráfego:
  - Até 1 Gb/s
  - Até 300.000 pacotes/s
  - Até 4.500 fluxos/s

Recursos adicionais:

- Recursos da Comunidade do Sophos NDR
- Operações de segurança aprimoradas com o Sophos Network Detection and Response (NDR)
- Especificações de certificação de hardware

Para saber mais, visite

sophos.com/ndr

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

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

24-12-19 DS-PTBR (MP)