Sophos Network Detection e Response

Monitore o tráfego de rede para identificar atividades suspeitas mais rapidamente

Cada segundo conta quando um adversário está em seu ambiente. No entanto, com muita frequência, os defensores são retardados por visibilidade e insights limitados. E isso se torna ainda mais complicado quando as ferramentas de segurança não funcionam bem juntas.

Dados mais abrangentes conduzem à estratégia de detecção mais precisa

As organizações podem se beneficiar de uma abordagem holística para detecção e resposta a ameaças e maneiras mais rápidas de correlacionar um volume e uma variedade de dados cada vez maiores. Quanto mais profundos forem a visibilidade e o contexto, mais precisa será a investigação da atividade da ameaça. Isso significa que quando a telemetria de segurança pode se unir, ela mostra uma imagem mais precisa de todo o caminho do ataque.

Como complemento do Sophos MDR, o dispositivo virtual Sophos Network Detection and Response (NDR) monitora o tráfego de rede para identificar fluxos de rede suspeitos. Detecções são enviadas para o data lake da Sophos, avaliadas e atribuídas a uma pontuação de risco correspondente, gerando casos para a equipe de resposta a ameaças da Sophos investigar e validar. As detecções de NDR podem acionar uma investigação sobre conexões internas de host para servidores de rede e também podem ser usadas para enriquecer as buscas de ameaças para atividades de endpoint para determinar quais dispositivos estão se comunicando.

Sua segurança precisa de ferramentas que funcionem bem juntas

O Sophos NDR é uma integração nativa do Sophos MDR. Ele se conecta prontamente, não produz ruído excessivo ou pontuações de risco incompatíveis e não requer tempo para estabelecer uma linha de base como outras soluções. A tabela abaixo descreve a funcionalidade dos mecanismos de detecção do Sophos NDR.

O Sophos NDR é fornecido como um dispositivo virtual. Depois de implantado, ele se autentica com o console de gerenciamento do Sophos Central e começa a enviar dados. O status e as detecções de NDR podem ser visualizados no Sophos Central.

Destaques

- Adicione detecções de rede ao Sophos MDR para monitorar fluxos de rede suspeitos que o software de endpoint não pode acessar
- Permita investigações de ameaças e buscas em conexões internas de host para serviços de rede e outras conexões de rede
- Detecte malware no tráfego criptografado, onde geralmente permanece oculto
- Visualize facilmente o status e as detecções do sensor NDR no Sophos Central

Mecanismos de detecção de NDR da Sophos e casos de uso

Detection Engines	Description
Análise de payload criptografada (EPA)	Detecta servidores de comando e controle (C2) de dia zero e novas variantes de famílias de malware com base em padrões encontrados no tamanho da sessão, direção e tempos entre chegadas.
Algoritmos de Geração de Domínio (DGA)	Identifica a presença de tecnologia de geração de domínio dinâmico usada por malware para evitar a detecção.
Deep Packet Inspection (DPI)	Monitora tráfego criptografado e não criptografado usando IoCs conhecidos para identificar rapidamente agentes de ameaças e TTPs.
Análise de risco de sessão (SRA)	Mecanismo lógico poderoso que utiliza regras que alertam sobre vários fatores de risco baseados em sessão.
Mecanismo de Detecção de Dispositivo (DDE)	Mecanismo de consulta extensível que usa um modelo de previsão de aprendizado profundo para analisar o tráfego criptografado em busca de padrões em fluxos de rede não relacionados.

SOPHOS

Reconheça comportamentos suspeitos além de seus endpoints

O Sophos NDR usa mecanismos de detecção de ameaças independentes para detectar comportamentos de tráfego de rede suspeitos e anormais, como:

- Conexões de um dispositivo desconhecido
- Dados carregados durante uma sessão remota
- Maior uso de arquivos de dados proprietários
- Sessões de rede geradas por famílias de malware

Com a capacidade de detectar comportamentos potencialmente maliciosos, o Sophos NDR identifica:

- Dispositivos desprotegidos – o Sophos NDR identifica dispositivos legítimos que não foram protegidos e podem ser usados como pontos de entrada para ataques cibernéticos. Rogue Assets – In addition to monitoring traffic to unprotected devices, Sophos NDR identifies unauthorized devices that communicate across the network.
- Sensores de IoT e OT – Dispositivos de Internet das Coisas (IoT) e tecnologia operacional (OT) representam desafios para o monitoramento de ameaças porque muitos desses dispositivos não podem suportar um agente de proteção de endpoint. O Sophos NDR monitora dados de dispositivos IoT e OT para detectar a atividade do invasor. Zero-Day Attacks – Sophos NDR has a patented process for detecting zero-day C2 servers used by attackers based on patterns found in session packet size, direction, and interarrival times.
- Ameaças internas – O Sophos NDR oferece visibilidade dos fluxos de tráfego de rede e da exfiltração de dados que podem inicialmente parecer “normais” por quem está de dentro.

O preço do Sophos NDR é baseado no número total de usuários e servidores de uma organização. O software do dispositivo virtual está incluído na licença. A tabela abaixo descreve os requisitos do sistema Sophos NDR.

Requisitos do sistema Sophos NDR

Network Throughput	1 Gbps	5 Gbps	10 Gbps
CPU	4	8	16
RAM	16 GB	32 GB	64 GB
Storage	160 GB	320 GB	640 GB
Estimated User Range*	Up to 2,000	Up to 10,000	Up to 30,000

* Varia de acordo com a organização.

Saiba mais sobre Sophos NDR

sophos.com/ndr

Revenda Autorizada
Tel: +55 21 2215 7892
sninformatica@sninformatica.com.br

SN Informatica Ltda
Tel: +55 21 2215 9681
https://www.sninformatica.rio/

Rio de Janeiro
Tel: +55 11 4950 8764
-

Brazil
-
-

22-11-29 DS-EN (DD)