Sophos Network Detection and Response

Monitora o tráfego na rede para identificar atividades suspeitas com mais rapidez

Cada segundo conta quando um adversário se aloja no seu ambiente. Ainda assim, é frequente observar lentidão na hora de defender devido a visibilidade e insights limitados. Isso fica ainda mais complicado quando as ferramentas de segurança não funcionam em sincronia.

Dados mais abrangentes levam a uma estratégia de detecção mais precisa

Os organizações podem se beneficiar de uma abordagem holística à detecção e resposta a ameaças e formas mais rápidas de correlacionar o volume e a variedade crescentes de dados. Quanto mais visibilidade e contexto, maior precisão na investigação da atividade da ameaça. Isso significa que quando a telemetria de segurança se alia ao contexto,
o caminho do ataque pode ser traçado com mais precisão.

Um complemento ao Sophos MDR, o dispositivo virtual Sophos Network Detection and Response (NDR) monitora o tráfego da rede para identificar fluxos suspeitos na rede. As detecções são enviadas ao Sophos Data Lake, avaliadas e recebem uma pontuação de risco correspondente, gerando casos para a equipe de resposta a ameaças da Sophos investigar e validar. As detecções NDR podem disparar uma investigação de conexões internas de host aos servidores da rede e também podem ser usadas para aprofundar a caça a ameaças nas atividades do endpoint a fim de determinar quais dispositivos estão se comunicando.

Sua segurança precisa de ferramentas que trabalhem em conjunto

O Sophos NDR é uma integração Sophos MDR nativa. Ele vem pronto para conexão, não gera ruído excedente ou incongruência nas pontuações de risco, e não exige tempo para estabelecer uma linha de base, como acontece com outras soluções. A tabela abaixodescreve a funcionalidade dos mecanismos de detecção do Sophos NDR.

O Sophos NDR é entregue como um dispositivo virtual. Uma vez implantado, ele faz a autenticação no painel de gerenciamento do Sophos Central e começa a enviar dados. As detecções e o status do NDR podem ser vistos no Sophos Central.

Destaques

- Adicione detecções de rede ao Sophos MDR para monitorar fluxos suspeitos na rede que softwares de endpoint não alcançam
- Investigue e saia no encalço de ameaças em conexões internas de host a serviços de rede e outras conexões de rede
- Detecte malwares no tráfegocriptografado, onde muito frequentemente eles se escondem
- Veja facilmente detecçõese status do sensor NDR no Sophos Central

Mecanismos de detecção Sophos NDR e casos de uso

Mecanismos de detecção	Descrição
Encrypted Payload Analytics (EPA, Análise de cargas criptografadas)	Detecta servidores de comando e controle (C2) de dia zero e as novas variantes de famílias de malwarescom 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.

SOPHOS

Reconhece um comportamento suspeito além dos endpoints

O Sophos NDR usa mecanismos independentes de detecção de ameaças para detectar comportamentos suspeitos ou anormais no tráfego de rede; por exemplo:

- Conexões provenientes de dispositivos desconhecidos
- Dados carregados durante uma sessão remota
- Aumento no uso de arquivos de dados proprietários
- Sessões de rede geradas por famílias de malwares

Com a capacidade de detectar comportamentos potencialmente mal-intencionados, o Sophos NDR identifica:

- Dispositivos sem proteção – o Sophos NDR identifica os dispositivos legítimos sem proteção que poderiam ser usados como pontos de entrada para ataques cibernéticos.
- Ativos ilegítimos – além de monitorar o tráfego de dispositivos sem proteção, o Sophos NDR identifica dispositivos não autorizados que se comunicam com a rede.
- Sensores IoT e OT – os dispositivos de Internet das Coisas (IoT) e tecnologia operacional (OT) são um desafio para o monitoramento de ameaças, porque muitos desses dispositivos são incompatíveis com agentes de proteção de endpoint. O Sophos NDR monitora dados de dispositivos IoT e OT para detectar tentativas de invasão.
- Ataques de dia zero – o Sophos NDR tem um processo patenteado de detecção de servidores C2 de dia zero usados pelos invasores baseado em padrões encontrados no tamanho de sessão, direção e tempo entre chegadas.
- Ameaças internas – o Sophos NDR oferece visibilidade de fluxos de tráfego na rede e exfiltração de dados que podem parecer “normais”, inicialmente.

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. A tabela abaixodescreve os requisitos de sistema do Sophos NDR.

Requisitos de sistema do Sophos NDR

Taxa de transferência da rede	1 Gb/s	5 Gb/s	10 Gb/s
CPU	4	8	16
RAM	16 GB	32 GB	64 GB
Armazenamento	160 GB	320 GB	640 GB
Faixa de usuários prevista*	Até 2.000	Até 10.000	Até 30.000

*Varia de acordo com a organização.

Saiba mais sobre o 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
linktr.ee/sninformatica

Brazil
-
-

22-11-15 DS-PTBR (DD)