Sophos Network Detection and Response (NDR)

Continuously monitoring and analyzing network traffic to identify rogue assets, unprotected devices, insider threats, and zero-day attacks.

Why NDR

- NDR detects malicious network activity deep inside the network that endpoints and firewalls can't see
- NDR analyzes traffic deep inside the network and is an essential part of a defense-in-depth strategy
- It detects activity originating from unknown or unmanaged devices, rogue assets, new zero-day C2 servers, and unusual data movement

Sophos NDR Overview

- Sophos NDR is an add-on to Sophos MDR and Sophos XDR
- Works perfectly with Sophos Firewall to provide the ultimate in detection and response
- Alerts are passed instantly to Sophos MDR and XDR analysts for investigation and response with Sophos Firewall's Active Threat Response
- Deployed as a virtual appliance that connects to a physical or virtual switch on the corporate network

Priced Per Users + Servers

10,000 users
\+ 1,000 servers
= 11,000 NDR Users and Servers

Priced lower than point NDR solutions

Virtual appliance software included in the subscription

Volume discounting built-in

Why Choose Sophos NDR

- Full integration with Sophos MDR, XDR, and Firewall for the ultimate in detection and response
- Five different detection engines deliver maximum network threat visibility
- A unique, patented machine learning approach that identifies malware in encrypted traffic
- Domain Generation Algorithm (DGA) detection that doesn't require additional threat intel
- Powerful risk analytics detect abnormal activity and identify patterns that warrant further investigation

Sophos NDR: Delivering Superior Cybersecurity Outcomes

Sophos NDR elevates protection by detecting threats and malicious activity other products miss:

- Rogue devices - unauthorized, potentially malicious devices communicating across the network
- Unprotected devices – legitimate devices that can be used as an entry point
- Insider threats – spot abnormal traffic and data movement from those on the inside
- Zero-day attacks - detect server C2 attempts based on patterns found in the session packets
- IoT and OT threats (e.g., medical devices, point of sale machines) – monitor data from these devices

When combined with other security telemetry, Sophos NDR enables analysts to paint a complete picture of the attack, enabling a faster, deeper response.

Example scenario:

1. Sophos NDR detects a device communicating on the internal network
2. Endpoint protection has no known device under management

INSIGHT: Unmanaged device communicating on network

MDR ACTION: investigate if internal user policy violation or malicious adversary

Discovery Questions

- Do you have any current network traffic monitoring solution (e.g. Darktrace, Security Onion, Thinkst Canary?)
- Do you currently have any laptops or other devices without endpoint protection? For example: in a lab, POS terminals, or IoT devices?
- Do you monitor network traffic behind your firewall?
- How are you monitoring internal user behavior?
- How are you monitoring "normal" data movement?
- Do you do regular asset discovery across your network?
- Are you able to identify new systems or rogue systems on the network?
- Do you have any visibility into encrypted traffic on your network? Are you currently able to determine if this traffic is malicious?

23-11-06 -DA-[MP]

SOPHOS