Solution Brief

Sophos NDR

Critical Visibility Deep Inside Your Network

Sophos Network Detection and Response is available for both Sophos MDR and Sophos XDR to detect malicious network activity deep inside the network that endpoints and firewalls can't see. Sophos NDR continuously analyzes traffic for suspicious patterns, including unusual activity originating from unknown or unmanaged devices, rogue assets, new zero-day C2 servers, and unexpected data movement.

Use Cases

1 | CRITICAL VISIBILITY

Desired Outcome: Gain critical visibility into network activity that other products can't see

Solution: Sophos NDR works together with your managed endpoints and firewalls to monitor network activity for suspicious and malicious patterns that your endpoints and firewalls cannot see. It detects abnormal traffic flows from unmanaged systems and IoT devices, rogue assets, insider threats, previously unseen zero-day attacks, and unusual patterns deep within the network.

2 | EARLY DETECTION

Desired Outcome: Five independent detection engines work in real time to identify threats sooner

Solution: Sophos NDR includes five independent detection engines that work together in real time to quickly detect suspicious or malicious traffic, with technologies like deep learning, deep packet inspection, encrypted payload analysis, domain name analysis, and powerful analytics. Our unique analysis provides only high-value alerts that ensure you're not wading through excessive noise.

3 | AUTOMATIC RESPONSE

Desired Outcome: Automatically stop active adversaries and threats dead in their tracks

Solution: Sophos cross-product automation between Sophos NDR, Sophos XDR, Sophos MDR, and Sophos Firewall provides immediate response to stop active threats dead in their tracks. When Sophos NDR identifies an indicator of compromise, active threat, or adversary, analysts are immediately alerted and can instantly push a threat feed to Sophos Firewall to trigger an automated response to isolate the compromised host.

4 | MANAGED THROUGH A SINGLE CONSOLE

Desired Outcome: Spend less time managing your network security

Solution: With Sophos Central, you get a single cloud management platform for all of your Sophos products, including NDR, XDR, endpoints, Firewalls, and much more. You get rich and powerful tools that leverage our deep data lake for cross-product threat hunting, managing an early response, and reporting and auditing. This ultimately means you're spending less time managing your network security.

Identify Unprotected and Rogue Assets

Reveal Unusual Data Movement and Insider Threats

Detect Previously Unseen Zero-Day Attacks

Learn more and trial Sophos NDR
sophos.com/ndr

2023-11-06 DS-EN (MP)

SOPHOS