Solution Brief

Sophos Integrations: Firewall

Enhance the visibility of your network perimeter

Threat actors continuously target external attack surfaces, probing and exploiting vulnerabilities in cyber defenses. Sophos XDR and MDR integrate seamlessly with Sophos and third-party firewall solutions to analyze security events, monitor incoming and outgoing traffic for signs of malicious behavior, and proactively counter threats early in the attack cycle to safeguard your critical assets from compromise.

Use Cases

1 | EXTEND ATTACK SURFACE VISIBILITY

Desired Outcome: Capture firewall security events to analyze potential exposure or breaches on the network edge.

Solution: The Sophos XDR and MDR Firewall integrations ingest and analyze edge security events caused by external threats, requiring no tuning or training. Detected events undergo a meticulous five-step process to filter noisy alerts, normalize complex telemetry, enrich data with threat intelligence, correlate with data from other security tools, and score to determine the risk.

2 | ENHANCE INCIDENT RESPONSE

Desired Outcome: Identify suspicious activities, such as data exfiltration and malware beaconing, to shorten response time.

Solution: Firewall telemetry empowers you and the Sophos MDR service to accelerate incident prioritization and response. Correlate suspicious network traffic patterns, such as initial access, Command and Control communications, and contextual data from other tools, to automatically generate cases for investigation. Analysts can apply host-based IP blocking and additional actions to neutralize threats.

3 | REDUCE ALERT FATIGUE

Desired Outcome: Offload high-volume alert inspection to Sophos threat experts.

Solution: Network security tools can generate huge volumes of telemetry data. Allocating time to analyze and verify threat activity can be time-consuming, and many organizations lack the resources needed to do so. The Sophos XDR and MDR Firewall integrations ensure security events generated by your firewalls are inspected and reviewed for malicious intent, enabling your team to focus on business enablement.

4 | ADDRESS CYBER INSURANCE AND COMPLIANCE GOALS

Desired Outcome: Incorporate security controls that help meet mandated security posture requirements.

Solution: Storing and inspecting security events is critical to many cyber insurance and compliance frameworks, which encourage using security information and event management (SIEM) tools. The Sophos XDR and MDR Firewall integrations help you address regulatory requirements with comprehensive logging, monitoring, effective threat response against cyberattacks, and validating security posture efforts.

Integrations include

paloalto NETWORKS

FORTINET

cisco

Forcepoint

and more.

Gartner Peer Insights Customers' Choice 2023

A Customers' Choice in the 2023 Gartner®, Voice of the Customer for Managed Detection and Response Services report

FROST & SULLIVAN

A Leader in Frost & Sullivan's 2024 Frost Radar report for Global Managed Detection and Response

To learn more, visit
www.sophos.com/mdr
www.sophos.com/xdr

SOPHOS

2024-07-23 SB-EN (PS)