Solution Brief

Sophos Integrations: Network

Detect anomalies your firewall can't see

Threat actors evolve their methods to compromise networks. Unprotected devices are prime targets for malicious activities, increasing the risk of authenticated user impersonation and encouraging lateral movement and misuse of privileges. Sophos XDR and MDR integrations gather telemetry from your network detection tools, identifying compromised devices and enhancing response capabilities to thwart breaches.

Use Cases

1 | DISCOVER UNPROTECTED DEVICES

Desired Outcome: Identify rogue and unprotected devices on your network that attackers could use as a foothold for attacks.

Solution: Devices such as mobile phones, IoT equipment, smart TVs, and endpoints with outdated operating systems, may evade traditional security controls. Sophos XDR and MDR solutions integrate seamlessly with Sophos and third-party network detection and response (NDR) solutions, enabling security teams to identify unknown and unauthorized devices that threat actors could abuse.

2 | MONITOR INTERNAL NETWORK TRAFFIC

Desired Outcome: Inspect east-west traffic for anomalies and staging tools designed to deliver malware.

Solution: Firewalls effectively block unauthorized inbound and outbound network traffic, but detecting an attacker who has breached an unprotected device can be exceptionally challenging. Sophos MDR analysts meticulously review alerts from your network security tools, including unusual activity, anomalous connections, and suspicious file downloads, accurately identifying genuine threats.

3 | ACCELERATE RESPONSE TIME

Desired Outcome: Respond to sophisticated threats at the network level by identifying Indicators of Compromise (IoCs) that might not be visible to an endpoint.

Solution: Sophos XDR and MDR integrate with network security tools and actively observe network traffic, enhancing your ability to respond to potential threats and minimize security incidents. Analyzing encrypted traffic provides visibility of anomalies that would traditionally evade detection. Respond to threats with host-based mitigation to block adversaries from communicating with protected devices.

4 | CORRELATE BEHAVIOR ACROSS THE ECOSYSTEM

Desired Outcome: Provide additional context to security events detected by endpoints and other security controls.

Solution: Effective cybersecurity requires correlating data across attack surfaces to understand the relationship of threat indicators. Sophos XDR and MDR ingest telemetry from endpoint, firewall, network, email, productivity, cloud, identity, and backup technologies, streamlining security management into a unified platform, enabling analysts to measure risk and resolve threat activity with a single pane of glass.

Integrations include

DARKTRACE

THINKST CANARY

Skyhigh Security

Cisco Umbrella

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

IDC

A Leader in the 2024 IDC MarketScape for Worldwide Managed Detection and Response

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

Gartner, Voice of the Customer for Managed Detection and Response Services, 28 July 2023. The Gartner Peer Insights Logo is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences with the vendors listed on the platform, should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

IDC MarketScape: Worldwide Managed Detection and Response (MDR) 2024 Vendor Assessment (doc #US49006922, April 2024).

SOPHOS

2024-07-23 SB-EN (PS)