Solution Brief

Sophos Integrations: Endpoint Protection

Detect malicious activity on non-Sophos endpoints

Threat actors exploit deficiencies in endpoint security controls, leading to ransomware attacks affecting businesses of all sizes and industries. Sophos XDR and MDR offer superior protection with Sophos Endpoint and include integrations with third-party endpoint solutions at no additional cost. The integration ingests telemetry and provides comprehensive EDR capabilities for your existing endpoint protection solution to swiftly detect and respond to cyber threats, enhancing overall defenses.

Use Cases

1 | INCREASE VISIBILITY ACROSS ENDPOINTS

Desired Outcome: Gain insights into device behavior from detailed endpoint telemetry, discovering suspicious activity and enabling in-depth forensic analysis.

Solution: Endpoint protection platforms aim to prevent malicious behavior, but without robust threat intelligence and response capabilities, vulnerabilities can lead to successful attacks. Sophos XDR and MDR go beyond event notification, automatically collecting and analyzing telemetry from files, processes, users, and network activities around the clock to provide maximum visibility of threats.

2 | STRENGTHEN DEFENSE AGAINST ADMIN OVERSIGHTS

Desired Outcome: Reduce blind spots caused by misconfigurations in your security stack.

Solution: Implementing and keeping pace with best practices can be challenging, and configuration mistakes can occur quickly. Sophos XDR complements endpoint protection platforms by capturing telemetry about health and performance. This information can detect and remediate security posture issues, such as outdated software or policy misconfigurations, allowing you to address them before an attacker strikes.

3 | ACTION-ORIENTED THREAT RESPONSE

Desired Outcome: Verify adversary behavior through human-led investigation and execute responses to disrupt attackers.

Solution: Sophos MDR analysts proactively hunt for potential adversary activity based on data collected from your endpoint solution. Our experts rigorously triage, investigate, and remediate each case to validate and neutralize malicious activity. Effective response actions like artifact removal, process termination, user disabling, and more, eliminate threats from the environment.

4 | CORRELATE DATA ACROSS MULTIPLE TOOLS

Desired Outcome: Collect and analyze telemetry from multiple security tools to detect multi-stage threats.

Solution: Managing endpoint, firewall, network, cloud, identity, and email security controls can be complex. Sophos provides a comprehensive view of threat alerts across all key attack surfaces. Our unified detection and response platform normalizes data, correlates attributes, and analyzes behavior across your entire security stack, aiding in effective threat management and risk reduction.

Integrations include

Microsoft

CROWDSTRIKE

SentinelOne

TREND MICRO

and more.

Gartner

A Leader in the 2023 Magic Quadrant for Endpoint Protection Platforms for 14 consecutive reports

IDC

A Leader in the 2024 IDC MarketScape for Worldwide Modern Endpoint Security for both Small and Midsize Businesses

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

Gartner Magic Quadrant ™ for Endpoint Protection Platforms, Evgeny Mirolyubov, Max Taggett, Franz Hinner, Nikul Patel, 31st December 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, Magic Quadrant and PEER INSIGHTS are registered trademarks of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

IDC MarketScape: Worldwide Modern Endpoint Security for Midsize Businesses (Doc #US50521323, February 2024). IDC MarketScape: Worldwide Modern Endpoint Security for Small Businesses (Doc #US50521424, March 2024).

SOPHOS

2024-07-23 SB-EN (PS)