Solution Brief

Sophos Integrations: Email

Monitor inboxes for email threats targeting users

Phishing attacks can have significant impacts on businesses, ranging from financial losses and compromised data to reputational damage and operational disruption. Sophos XDR and MDR integrate with Sophos and third-party email tools to detect and analyze email-based threats such as business email compromise (BEC), credential harvesting, and malicious payload deliveries, to ensure a robust defense against one of the most common cyberattack vectors.

Use Cases

1 | IDENTIFY SUSPICIOUS EMAIL BEHAVIOR

Desired Outcome: Detect and investigate malicious activity across user inboxes to prevent threat outbreaks.

Solution: Once an account is compromised, adversaries use persistence mechanisms to maintain access for continued attacks. Sophos XDR and MDR Email integrations ingest security alerts, quickly identifying common signs of account compromise such as users exceeding sending limits, modification of email forwarding rules, and other inbox manipulation attempts designed to harvest credentials and data.

2 | NEUTRALIZE MALICIOUS CONTENT

Desired Outcome: Inspect all delivered content and respond quickly to confirmed threats.

Solution: Attackers bypass security controls by delivering emails with 'safe' content that mutates post-delivery. If successful, attackers can gain unauthorized access to your users' devices to exploit and propagate malware. Integrating email solutions with Sophos XDR and MDR enables prompt host-based response, deleting artifacts and blocking risky IP addresses and domains.

3 | ACCELERATE POSTURE IMPROVEMENTS

Desired Outcome: Discover threat sources so you can harden security and reduce the attack surface.

Solution: According to Sophos' 2024 State of Ransomware report, "email-based approaches were identified as the root cause of attack by 34% of respondents." Integrating email solutions with Sophos XDR and MDR identifies spam and phishing attempts indicating unauthorized access by imposters – crucial for tuning security controls, identifying the root cause of attacks, and ultimately preventing breaches.

4 | CORRELATE DATA BETWEEN SECURITY SOURCES

Desired Outcome: Increase visibility across your security ecosystem with a unified detection and response platform.

Solution: A comprehensive cybersecurity strategy involves a unified platform to monitor your entire ecosystem. Sophos integrates email telemetry with data from other security products and automatically maps detections to the MITRE ATT&CK framework to correlate events and provide a broad view of the attack lifecycle. Maximize the ROI on your existing tool investments by integrating them with Sophos XDR and Sophos MDR.

Integrations include

Microsoft

Google Workspace

proofpoint.

mimecast

and more.

kuppingercole ANALYSTS

Sophos Email recognized as a Product Leader, Market Leader, and Market Champion by analyst firm KuppingerCole.

vb June 2024 VERIFIED SPAM + virusbtn.com

Sophos Email is the only solution to block all malware and phishing samples in the 2024 VBSpam test.

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

SOPHOS

2024-07-23 SB-EN (PS)