Solution Brief

Sophos Integrations: Productivity

Detect abnormal user and device activity

Software as a Service (SaaS) applications offer comprehensive tools through cloud-based management platforms, presenting an evolving attack surface. The Sophos XDR and MDR Productivity integrations work with Microsoft 365 and Google Workspace to enhance visibility into malicious activities, including abnormal behaviors and account compromises.

Use Cases

1 | INCREASE RETURN ON INVESTMENT

Desired Outcome: Leverage your existing tools to achieve superior security outcomes.

Solution: Productivity suites generate valuable telemetry for security analysts. However, accessing and interpreting this data can take considerable time and effort. Integrating your productivity suite with Sophos XDR and MDR allows security analysts to detect and respond to threats with a unified platform.

2 | INVESTIGATE SUSPICIOUS USER ACTIVITY

Desired Outcome: Detect and analyze unusual activity to prevent potential breaches.

Solution: Applications like email and remote file storage can create multiple attack vectors for threat actors to exploit. Integrating productivity telemetry data into Sophos XDR and MDR exposes unauthorized user access patterns that can indicate an attack, such as repeated failed login attempts, suspicious sessions, logins from unidentified IP addresses, and email inbox tampering.

3 | GENERATE BREACH TIMELINES

Desired Outcome: Identify the origin of an attack by adding context to detected security events.

Solution: Constructing breach timelines requires tools capable of tracing an attack's inception. The Sophos XDR and MDR Productivity integrations capture details of user and administrator actions and correlate this information with other detections. Configuration changes, suspicious resource usage, and unusual execution patterns are tracked to help determine the origin of a breach.

4 | DETECT DATA EXFILTRATION AND INSIDER THREATS

Desired Outcome: Track data access and file sharing attempts that may violate company policies and restrictions.

Solution: Productivity tools monitor for sensitive information leaks by tracking data access, detecting user privilege abuse, and providing insights into file sharing. Sophos MDR analysts can respond to threats by disabling user accounts and terminating unauthorized file transfers, and provide expert guidance on enhancing security through policy updates, safeguarding company data, and identifying insider threats.

Microsoft 365

Google Workspace

Productivity integrations are included with Sophos XDR and Sophos MDR subscriptions.

G2 Leader

Named a Leader for XDR and MDR in the Summer 2024 G2 Grid® Reports

Gartner Peer Insights Customers' Choice 2023

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

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

SOPHOS

2024-07-23 SB-EN (PS)