Solution Brief

Sophos Integrations: Cloud

Detect cloud misconfigurations and malicious behavior

Public cloud environments are expansive, intricate, and continually evolving. Threat actors exploit this complexity to access valuable company data and resources. Sophos XDR and MDR Cloud integrations mitigate potential damage to business operations by improving visibility, contextualizing cloud alerts, and strengthening resilience against attacks on your public cloud environments.

Use cases

1 | ANALYZE RISKY AND MALICIOUS BEHAVIOR

Desired outcome: Identify insider threats and high-risk user behavior that could indicate a compromised account.

Solution: Cloud telemetry captures user activities, such as logins, asset and file access, and administrative actions. The Sophos XDR and MDR Cloud integrations help identify anomalous user behaviors, potential insider threats, and malicious activity.

2 | DETECT AND PRIORITIZE CLOUD MISCONFIGURATIONS

Desired outcome: Identify and provide remediation steps for cloud misconfigurations across all major cloud providers.

Solution: Simple misconfigurations in cloud consoles can lead to breaches.

Cloud integrations provide insight into security weaknesses such as Identity Access Management roles with overprivileged policies, newly created root users, or publicly visible API gateways.

3 | IDENTIFY POTENTIAL ATTACK PATHS

Desired outcome: Map potential routes to critical business data (e.g. PII, PCI, PHI) and identify where to mitigate that risk.

Solution: Cloud technology integrations provide Sophos XDR and MDR with increased visibility into how an attacker could exploit a chain of individual risks to breach your public cloud environment. Armed with that knowledge, you can remediate those attack paths.

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 using a single pane of glass.

Integrations include:

orca security

+ Integrate with AWS, Azure and GCP with Sophos Cloud Optix

G2 Leader

Named a Leader for XDR and MDR in the Winter 2025 G2 Grid® reports

Gartner Peer Insights Customers' Choice 2024

A Customers' Choice in the 2024 Gartner® Voice of the Customer report for Managed Detection and Response Services

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

SOPHOS

2025-02-05 SB-EN (PS)