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



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



Named a Leader in XDR in the G2 Summer 2024 Reports



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

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.

