Solution Brief

Sophos Integrations: Backup and Recovery

Monitor threats that target critical backup data

Threat actors attempt to disable backup solutions before executing ransomware attacks, recognizing that backups can hamper their extortion attempts. Detecting this malicious behavior is crucial. It allows you to intervene before critical data is compromised. Sophos XDR and MDR Backup and Recovery integrations extend visibility into this type of adversary activity to increase your resilience against ransomware attacks, minimizing potential damage to your business operations.

Use Cases

1 | IMPROVE BACKUP THREAT VISIBILITY

Desired Outcome: Identify threats designed to affect your business contingency plans.

Solution: When you use the Backup and Recovery integrations, attempts to manipulate backup procedures and delete backup repositories can be identified - tactics frequently used by attackers to hinder recovery post-breach. Anomalies such as unexpected data deletion, disabling multi-factor authentication, and password changes, may indicate malicious activity requiring rapid investigation and remediation.

2 | STRENGTHEN BUSINESS CONTINUITY

Desired Outcome: Reduce downtime by strengthening your security posture.

Solution: Once backups are disabled, attackers will move to encrypt your environment and disrupt critical infrastructure. Sophos Backup and Recovery integrations provide early visibility into these attacks, enabling investigation of suspicious activity and minimizing operational downtime. Consistent and effective backups ensure data availability for seamless recovery, supporting ongoing business continuity.

3 | FORTIFY COMPLIANCE AND INSURANCE REQUIREMENTS

Desired Outcome: Align with regulatory frameworks associated with data protection and disaster recovery strategies.

Solution: Backups are crucial to comply with various data protection regulations, such as PCI-DSS and HIPAA. Sophos Backup and Recovery integrations monitor security events in real time and retain data for 90 to 365 days, ensuring accessible forensic details in case of a cyber incident. Sophos can help implement effective mitigation strategies, reducing the risk of expensive cyber insurance claims.

4 | ACCELERATE INCIDENT RESPONSE TIME

Desired Outcome: Combat threat actors by implementing strategies to disrupt their activities.

Solution: Sophos MDR prioritizes real-time incident response and engages in hands-on mitigation. Our experts conduct root cause analysis, hunt down threat actors, and terminate their access, preventing successful attacks and bolstering your incident response plan.

Integrations include

veeam

Acronis

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)