Cohesity and Microsoft Sentinel

Smarter, faster threat detection and response

Overview

Security teams today face escalating pressures from ransomware, insider threats, and data exfiltration attempts that are not only targeting production systems, but also secondary data. While many organizations may see backups as a last line of defense, they are a tremendous source of intelligence, especially when it comes to threat detection and response. Threat signals and intelligence from secondary data can be used to investigate and remediate threats, adding more intelligence to SIEM and SOAR solutions.

According to Microsoft, over 70% of organizations now operate hybrid or multicloud environments, making centralized visibility a persistent challenge. Cohesity Data Cloud integrates with Microsoft Sentinel to change that equation. By seamlessly feeding Cohesity threat and anomaly alerts directly into Sentinel, organizations gain full visibility across their data. This helps CISOs, SecOps, and ITOps teams correlate data protection signals with their broader security telemetry. The result: faster time to discovery, investigation, and recovery from ransomware attacks.

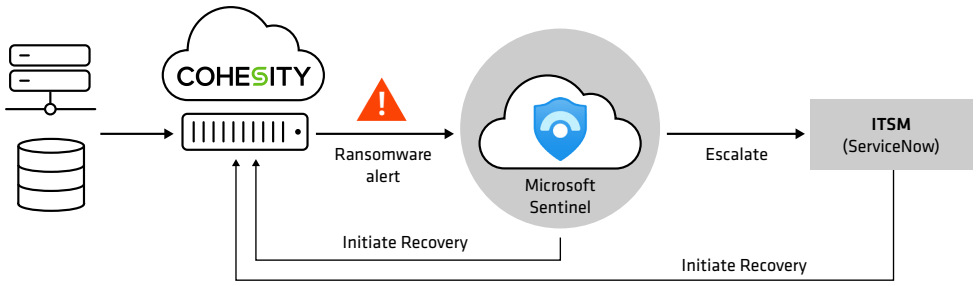

Figure 1: Integrate threat signals from secondary data protected by Cohesity to Microsoft Sentinel to boost security posture.

Key Benefits

- Unified visibility
- Accelerated investigation
- Automate recovery workflows
- Reduce data risk
- Increase operational efficiency
- Meet compliance needs

Key use cases

The Cohesity and Microsoft Sentinel integration is an efficient, risk-reducing integration that strengthens cyber resilience while also enhancing operational efficiency and cost savings. The integration enables the following key use cases:

1. Unified threat visibility

Gain proactive insights through the Sentinel console into potential cyberattacks occurring across your data estate and minimize the blast radius of ransomware. Feed threat intelligence and alerts from AI-powered forensics and anomaly scanning capabilities on data protected by Cohesity into Sentinel.

2. Intelligent threat detection and response

Triage and act quickly on risk insights from secondary data—complementing existing threat intel for users, apps, servers, and devices—from inside Sentinel. The integration empowers security teams to quickly identify and respond to security incidents.

3. Streamline incident management and cyber recovery

Anomalous events detected in Microsoft Sentinel can trigger automated responses within Cohesity, such as initiating data restores to a clean snapshot or creating the ServiceNow ITSM Incident, etc. Automate and speed security and IT operations collaboration through pre-built and custom playbooks. This automation accelerates incident response and minimizes the impact of security incidents so that you can avoid reinfecting production systems with a clean restore.

4. Data governance and compliance

Organizations are tasked with gathering all infrastructure logs in one centralized location. Adhere to regulatory standards by leveraging the combined capabilities of both platforms in showing end-to-end data integrity and protection status.

Unite threat visibility and recovery

Cohesity and Microsoft Sentinel redfine how organizations detect, respond to, and recover from cyber threats. By bridging data protection and threat intelligence, this integration leverages the secondary datasets as a tremendous source of effective active security signals. With automated response workflows, unified visibility, and intelligent threat detection and response, security teams can act faster and with greater precision—stopping threats before they spread and recover with confidence when they do. The result is stronger cyber resilience, reduced operational complexity, and integrated defenses that keep pace with today's relentless attacks.

Learn more at https://marketplace.cohesity.com/app-details/microsoft-sentinel

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

3000100-002-EN 11-2025