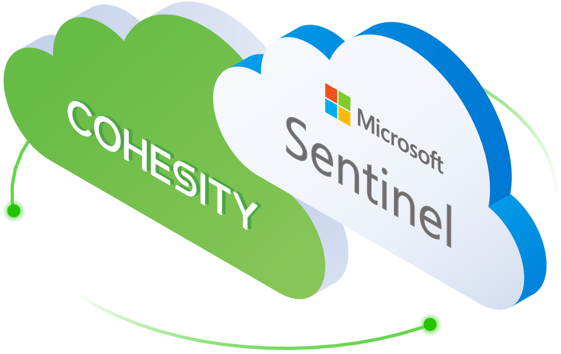
COHESITY | Microsoft

SOLUTION BRIEF

Boost Your Cyber Resilience With New Integrated Solution



Key Benefits

- Faster time to threat detection and investigation
- Rapid recovery with operational simplicity
- Strengthened IT, security, and operations team collaboration

Ransomware attacks have increased exponentially, causing billions in losses and putting lives at risk while damaging trust and reputations. As cybercriminals get more inventive, they're not only locking up production systems but also destroying backups and stealing sensitive data. This leaves your enterprise with no option but to pay a ransom. Your organization can do more to defend your data by fortifying data security defenses and responses with the integrated Cohesity and Microsoft Sentinel solution that tears down the silos between your IT and security operations teams. The result: faster time to discovery, investigation, and recovery from ransomware attacks.

The coupling of the Cohesity security and data management platform with Sentinel, which detects and aggregates security events before orchestrating threat response, delivers intelligent backup data security analytics to your enterprise. The integrated solution brings data-driven insights from your ITOps and SecOps organizations together, boosting the teamwork required to most effectively assess an attack's scope and quickly remediate the threat.

Gap Puts Businesses and Security Postures at Risk

The first annual State of Data Security and Management report[1] from Cohesity reveals that despite more than four in five (81%) IT and security operations decision-makers believing they should jointly share responsibility for their organization's data security strategy, many of these teams are failing to effectively collaborate to address growing cyber threats. Of respondents believing collaboration is weak between IT and security teams, nearly half agree their enterprise is more exposed to cyber threats as a result. A full 40% of all surveyed said collaboration between the two groups had remained the same even in light of increased cyber attacks, likely due to not addressing technology complexity, siloed visibility, and slow remediation. Closing the gap between IT and security operations would have big advantages. A full 83% percent of all respondents agreed that if security and IT collaborated more closely, their organization would be better prepared to recover from cyber threats including ransomware attacks.

> "Solve your business's most important problems with confidence by ensuring your security incident and event management (SIEM) system expands as threats to your data evolve." – PWC[2]

[1] Based on the 2022 survey, commissioned by Cohesity and conducted by Censuswide, of more than 2,000 IT and security decision-makers (split nearly 50/50 between the two groups).

[2] PWC & Microsoft Security Perspective, 2022.

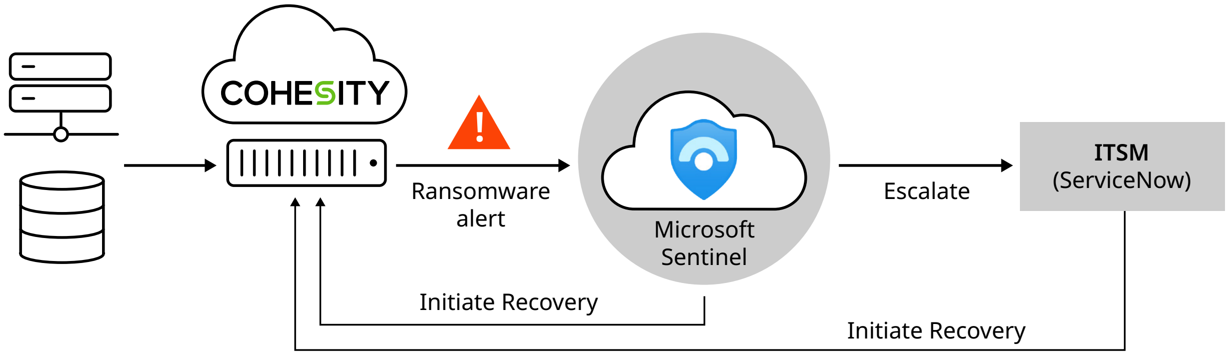


Figure 1: Closed-loop ransomware detection and remediation with integrated Cohesity and Microsoft Sentinel

Security and IT Operations. *United.*

The Cohesity and Microsoft Sentinel integration is an efficient, risk-reducing solution that saves your organization valuable time and money. It automatically sends Cohesity ransomware alerts for data directly from Cohesity to Sentinel, where they can be logged and opened as security incidents. Within the Sentinel console, your security analysts can investigate the incidents as ransomware detection events, and as needed, initiate a snapshot recovery directly from Sentinel or via ServiceNow, escalate the incident or dismiss the alert.

Cohesity's pre-built, data protection workflows in Sentinel unite security and IT teams for collaborative investigation and remediation. You create any number of workflows by extending and integrating Cohesity workflows with other tools in the Sentinel ecosystem. For example, in the event of a cybersecurity attack, you can speed up incident response by automatically opening a ticket in ServiceNow to trigger broader team coordination via a workflow and orchestrating the initiation of data recovery when needed.

Accelerate Ransomware Detection, Investigation, and Response

Cohesity Data Cloud and Cohesity DataProtect seamlessly work with Microsoft Sentinel to both accelerate how your enterprise discovers, investigates, and recovers from ransomware attacks and to improve the collaboration of IT, security, and operations teams.

Unified Threat Visibility

- Gain early insights through the Sentinel console into potential cyberattacks on your data and minimize the blast radius of ransomware
- View ransomware incidents through the lens of AI-powered forensics and anomaly scanning on Cohesity backups—all with complete visibility in Sentinel

Enriched Investigation

- Triage and take action fast on risk insights in backup data—complementing existing threat intelligence for users, apps, servers, and devices—from inside of Sentinel
- Automate and speed security and IT operations collaboration through pre-built and custom playbooks

Rapid Response

- Speed incident response and remediation, including restoring to a clean backup snapshot, directly from Sentinel or via ServiceNow integration with Sentinel
- Avoid reinfecting production systems with a clean restore

To learn more, visit Cohesity Marketplace.