**COHESITY** | **CISCO**

# Automate ransomware response. Accelerate data recovery.

Cohesity DataProtect and Cohesity DataHawk integrated with Cisco XDR

## Key benefits

- Reduce data loss during a ransomware attack
- Accelerate digital forensics, response, and recovery

The threat from cybercriminals is real and growing. Ransomware attacks, in particular, are widespread and cause significant harm. Most leaders now accept that their organization will likely face a cyberattack, but most companies don't have a strong InfoSec strategy to respond effectively. Legacy data management systems, siloed security tools, and a lack of early coordination between Security and IT teams often hinder quick response and recovery, so leading enterprises are adopting a new approach to cyber resilience to prioritize data protection in an adaptive and automated way.

## Minimize data loss through early and rapid response

The powerful combination of Cohesity DataProtect and Cohesity DataHawk with Cisco XDR reduces the time between threat detection and backing up critical data to near zero, thus minimizing data loss and limiting disruption to your business operations. Use early and immutable backup snapshots to help accelerate response and recovery activities.

The **first integration of this kind** in the industry, this solution gives your Security and IT teams the ability to:

**Prioritize the protection of critical data during an attack:** Instantly respond at the very first signs of a ransomware attack to snapshot business-critical data before ransomware spreads laterally through the network. This approach allows you to reduce your recovery point objective (RPO).

**Accelerate digital forensics and clean room recovery:** Preserve potentially infected virtual machines and quickly recover data to a clean room environment to expedite forensics and recovery activities, thus reducing recovery point objectives (RTOs). Analyze the backup snapshots to identify sensitive data and potential pathways for ransomware lateral movement towards crucial data, and take steps to mitigate the incident.

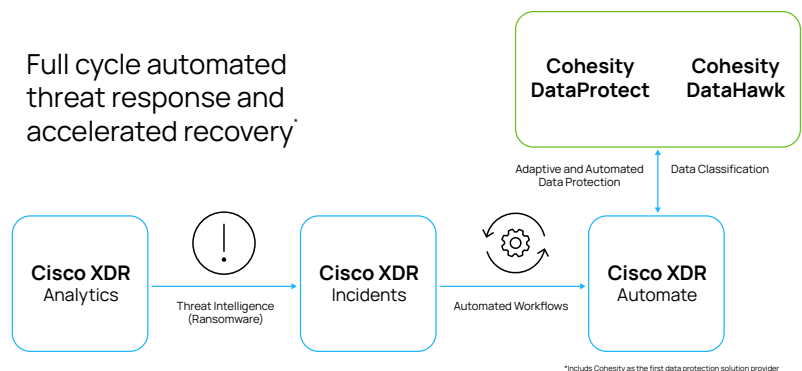Full cycle automated threat response and accelerated recovery[*]

Figure 1: Cohesity and Cisco XDR Integration

## Key solution capabilities

### Adaptive and automated data protection

Enhance cyber resilience by integrating automated data protection into incident response to accelerate response and recovery.

### Classification of sensitive data

Scan critical workloads backed up by Cohesity and monitored by Cisco XDR for threats using Cohesity DataHawk's highly accurate, ML-based engine to classify sensitive data, including personally identifiable information (PII), PCI, and HIPAA.

### Immutable snapshots

Store backed-up data in its secured file system in immutable snapshots that can't be directly accessed or mounted from outside the Cohesity cluster.

### Multilayered protection for snapshots

Stop bad actors and unauthorized applications from modifying or deleting your data, thanks to Zero Trust principles, including granular RBAC, MFA, SSO, immutable snapshots, ML-based ransomware attack detection, and more.

### Proven integrated backup and recovery with Cisco Servers – Unified Computing System (UCS)

Get the fastest possible recovery time by combining the solution with the fast backup and recovery throughput of Cisco UCS® X-Series Modular Systems, certified with Cohesity DataProtect for rapid deployment.

## Simplify security with the Cohesity and Cisco partnership

Customers subscribed to Cohesity DataProtect software and Cisco XDR (Advanced or Premier licensing option) can gain access to the integration at no additional cost. Optional license for Cohesity Data Classification or Datahawk is required for sensitive data classification and visibility. Support options include Cisco Solution Support for primary point-of-contact support.

To learn more, visit **www.cohesity.com/cisco** and the **Cohesity Marketplace**.

COHESITY.com | 1-855-926-4374 | 300 Park Ave., Suite 1700, San Jose, CA 95110                    3000134-001-EN 1-2024