Cohesity Advanced Threat Protection

Elevate your cyber resilience with intelligent threat defense

Today's threat response needs more than just backups

Ransomware and malware remain the most punishing cyber risks of 2025: exploited software vulnerabilities ignite **32%** of incidents, while malicious email (**19%**) and phishing (**18%**) round out the top entry points; when attackers break through, half of all cases still end in data encryption and **28%** add data-theft extortion. The mean cost of recovery without the ransom is **US $1.53M** (sophos 2025). At the same time, the proliferation of zero-day exploits shows how quickly adversaries can outpace signature-based defenses (The Hacker News, Microsoft). With only **54%** of victims able to restore from backups and attackers now actively targeting backup data, enterprises must augment perimeter controls with a data-centric layer that continuously scans immutable backup copies for hidden Indicators of Compromise, exposes dormant threats early, and pinpoints clean recovery points precisely the gap Cohesity threat protection is built to close.

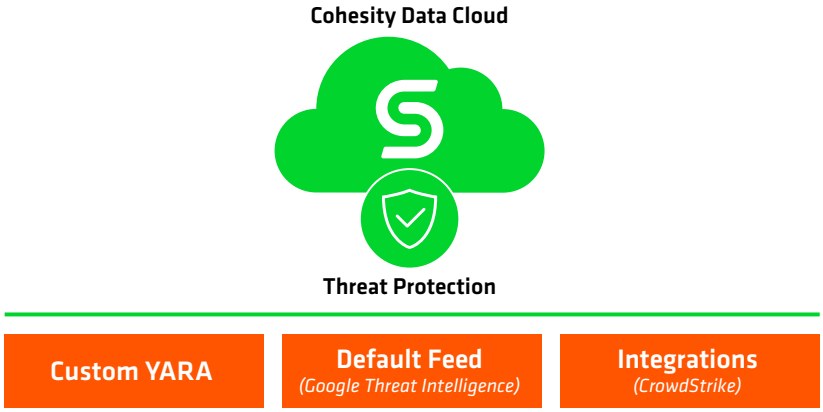
Integrated threat defense for your backup data

In a landscape where ransomware and advanced threats relentlessly target corporate data. Cohesity delivers integrated threat defense by fusing backup, security, and recovery into a single solution. Cohesity continuously detects threats, accelerates incident response, and pinpoints clean recovery points across all protected workloads. Powered by Google Threat Intelligence feeds and augmented with bring-your-own CrowdStrike Falcon intelligence, Cohesity surfaces Indicators of Compromise by scanning immutable backup copies, enabling security and IT teams to spot dormant threats early, accelerate triage, and shut down lateral movement. With unified detection, response, and rapid recovery in one platform, Cohesity fortifies cyber resilience, streamlines operations, and lets organizations rebound with confidence.

Cohesity threat protection unifies threat detection, accelerating incident response, and clean-point recovery on the same Cohesity Data Cloud platform that already backs up and consolidates your data. The feature allows scanning immutable backup snapshots, leaving production workloads untouched while ingesting curated threat-intelligence feeds from Google Threat Intelligence and bring your own CrowdStrike Falcon intelligence to uncover IOCs and infections in secondary data. With support to bring your own YARA rules, Cohesity threat protection becomes a single platform for both proactive and reactive defense. In peacetime, you can continuously scan immutable backups to detect dormant IOCs before they spread. During an incident, you can scan historical snapshots to trace the point of entry and highlight verified, clean recovery points.

Key Benefits

- **Detect zero-day vulnerabilities:** Continuously refreshed threat feeds expose zero-day exploits that may slip past the primary security tools.
- **Snapshot analysis on a timeline:** Hunt specific ransomware strains across multiple historical snapshots to trace the infection path and pinpoint the root cause.
- **One-click threat hunting:** Trigger on-demand ad-hoc scans to accelerate investigations.
- **Unified security and recovery operations:** A single dashboard plus SIEM/SOAR integrations consolidating alerts, posture metrics, and forensic evidence, reducing tool sprawl and mean time to respond.



Key capabilities

- **Broad workload coverage**: Supports scanning VMware, Nutanix AHV, and NetApp VMs; Generic, NetApp, and Isilon NAS shares; Cohesity SmartFiles; and physical servers with file-based protection
- **Multi-source threat intelligence**: Leverages built-in Google Threat Intelligence, plus custom YARA rules and external feeds such as CrowdStrike Falcon.
- **Flexible scheduling**: Scan protected objects at a regular cadence to match business needs.
- **SIEM/SOAR ready**: Streams IOC hits and alerts to your existing security stack for consolidated, end-to-end incident management.
- **Smart scanning controls**: Let you cap scans by file size and IOC match thresholds to balance depth with performance.
- **Automated anomaly response**: Triggers full threat scans automatically whenever Cohesity's Anomaly Detection flags unusual change rates, ensuring hidden infection is caught to assist with investigation and response.

Threat protection should not be an afterthought

Ransomware, zero-day exploits, and data-theft extortion remain the fastest-growing business risks. Traditional perimeter controls alone can't keep pace.

How Cohesity threat protection helps

- **One unified platform** combines backup, threat detection, and clean-point recovery, eliminating tool sprawl and hand-offs.
- **IOC scanning on immutable snapshots** surfaces dormant malware and zero-days that primary defenses miss, without touching production.
- **Google + CrowdStrike intelligence and custom YARA rules** give you real-time feeds and tailored threat hunts in one place.
- **Accelerated Incident Response** quickly identifies infection free copies and orchestrates large-scale restores, slashing downtime and preventing reinfection.

Cohesity threat protection is a single investment that hardens cyber-resilience, trims response times, and turns every snapshot into a security asset, not a liability. With unified detection, response, and rapid recovery in one platform, Cohesity adds a data-centric defense layer that continuously inspects your backups so you can spot threats sooner, contain them faster, and recover with certainty.

Learn more at Cohesity.com

COHESITY

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

3000173-001-EN 7-2025