Cohesity Integrations with the Data Security Alliance

Cyber resilience requires a seamless and orchestrated approach across the cybersecurity solutions you may already have in place today. This is the impetus behind the Data Security Alliance. Cohesity drove the creation of the Alliance to unify data security and data management with cybersecurity to improve your cyber resiliency. Our goal is to deliver technical integrations and architectures, as well as best practices and thought leadership through market education and awareness activities.

Cohesity collaborates with your security vendors to deliver technical integrations that bridge enterprise IT and security. These integrations share context and enable new automated workflows to help mature cyber threat defenses and accelerate response and recovery in the event of a cyberattack.

Simplified Secure Access	Vulnerability Scanning	Automated Ransomware Response
Minimize business risk by securing and controlling access to your Cohesity clusters.	Avoid re-injecting known vulnerabilities back into production by scanning backup data proactively or during incident recovery.	Accelerate ransomware recovery by enriching SOC visibility into active threats and deploying automated playbooks in one location.

Use cases enabled through direct integrations with the industry's ONLY Data Security Alliance

Supported Security Integrations

Alliance partner / solution	Use case	Integration benefits	Related links
Microsoft Sentinel	Automated ransomware response	• Automatically pushes Cohesity anomaly alerts* to Microsoft Sentinel to enable correlation and investigation within a single location. • Allows security analysts to investigate ransomware detection incidents on the Sentinel console, and if needed, initiate a snapshot recovery directly from Microsoft Sentinel or via ServiceNow, escalate the incident, or dismiss the alert.	Boost Your Cyber Resilience With New Integrated Solution Deployment guide
Cisco SecureX	Automated ransomware response	• Automatically pushes Cohesity anomaly alerts* directly to Cisco SecureX. • Allows security and IT teams to restore a specified backed-up object from its latest clean snapshot or ignore a specified ransomware alert.	Fight Ransomware Attacks With Integrated Cohesity and Cisco SecureX
Palo Alto Networks Cortex XSOAR	Automated ransomware response	• Automatically pushes Cohesity anomaly alerts* directly to Cortex XSOAR. • Allows security and IT teams to restore a specified backed-up object from its latest clean snapshot or ignore a specified ransomware alert.	Automated Response and Recovery from Ransomware
Crowdstrike LogScale	Automated ransomware response	• Automatically pushes Cohesity anomaly alerts* directly to Falcon LogScale. • Automates response workflows such as initiating a snapshot recovery directly from Falcon Logscale or via ServiceNow, escalating the incident, or dismissing the alert.	Ransomware Protection and Recovery Available in the coming months
Tenable	Vulnerability scanning	• Powers Cohesity's CyberScan app. • Scans backup data on Cohesity Data Cloud immediately or on schedule to ensure that no known vulnerabilities get injected into the production environment during a restore operation. • Provides a global view of all cyber exposure within your production environment through a security dashboard.	Counter Ransomware Attacks with Cohesity Deployment guide
ServiceNow	Automated ransomware response	• Automatically pushes Cohesity anomaly alerts[2] directly to ServiceNow. • Allows security and IT teams to restore a specified backed-up object from its latest clean snapshot or ignore a specified ransomware alert.	Available in the coming months
Splunk	Automated ransomware response	• Collects alerts and audit logs from Cohesity Data Cloud and integrates these with Splunk Enterprise to enrich security and operational intelligence and improve data management.	Available in the coming months
BigID	Automated ransomware response	• Powers Cohesity DataHawk's ML/NLP-based data classification to identify sensitive and regulated data. • Identifies compromised data and maps this data set against built-in and custom patterns per classification task. • Reports the patterns matched (e.g. phone number pattern) and associated file names in Cohesity's Security Center AntiRansomware interface.	Cohesity DataHawk

Alliance partner / solution	Use case	Integration benefits	Related links
Okta	Simplified secure access	• Enables single sign-on (SSO) access to Cohesity cluster. • Allows users to sign in to the Cohesity cluster via the Okta sign-in page or the Cohesity login page.	Integration with Okta for Single Sign-On Capabilities
CyberArk	Simplified secure access	• Secures privileged accounts on the Cohesity platform by vaulting the credentials and automating the password rotation. • Initiates secure and controlled sessions to Cohesity cluster and IPMI interfaces and records all privileged access activity during the session.	Secured Identity and Privileged Access for Your Data Deployment guide

Preview of Select Upcoming Security Integrations By Use Case

Sensitive data loss prevention	Automated ransomware response
netskope zscaler™	CISCO CROWDSTRIKE

* Cohesity's Anomaly Detection finds unusual patterns such as sudden change rates in files written, files read, and logical size in the backup data that do not conform to the expected behavior. It leverages the Unsupervised Machine Learning technique to identify any abnormal changes in backup data by getting telemetry data and signals.

Visit the Cohesity Marketplace for more information about these and other Cohesity integrations

COHESITY