COHESITY | aws

SOLUTION BRIEF

Improve Your Cyber Resilience

Key Benefits

- Protect all your data (cloud-native SaaS, and on-premises) with a defense-in-depth security framework
- Quickly discover and respond to intrusions, anomalies, and inconsistent behaviors
- Reduce downtime and data loss with rapid recovery at any scale

Data is at the center of every organization. From home, remote, and branch office locations to on-premises data centers and cloud provider environments, a variety of systems and applications generate and touch data. Given the dependence of digital businesses on data—no matter where it resides—data is an attractive target for cybercriminals.

Cohesity empowers you to protect your data and business reputation. Cohesity Cloud Services, a portfolio of SaaS data security and data management offerings hosted in Amazon Web Services (AWS), effectively counters ransomware attacks and helps your organization avoid paying the ransom. Imbued with defense-in-depth security principles, the joint Cohesity and AWS solution features protect your mission-critical data against ransomware, quickly detect anomalous activity and suspicious behavior, and predictably recover your data in case of an attack.

Protect. Detect. Recover with Cohesity and AWS

By 2031, ransomware will cost victims $265 billion annually, according to Cybersecurity Ventures, and cybercriminals will attack a business, consumer, or device every 2 seconds. Better protect, detect, and recover your data with Cohesity and AWS.

Protect

Cohesity and AWS safeguard your cloud-native, SaaS, and on-prem data against internal and external threats with a multilayered data security architecture.

Immutable snapshots – All backup snapshots, by default, are stored in an immutable state within the Cohesity-managed environment hosted in AWS. This means that no user or application can overwrite the backed up data. For all AWS-supported services (EC2, RDS, and S3), Cohesity also can create an isolated/air-gapped copy stored in a separate tenant.

Object Lock – As an additional layer of protection, AWS Object Lock places a time-bound lock on the backup snapshot stored in the Cohesity-managed backup as a service or cyber vault as a service environment. Even in the case of compromised user credentials, these backup snapshots cannot be deleted or modified.

Data encryption – Cohesity features software-based FIPS-validated, AES-256 standard encryption for your data in flight and at rest. This cryptographic module validated by the U.S. National Institute of Standards and Technology (NIST) at the Federal Information Processing Standards (FIPS) 140-2 Level 1 standard is trusted worldwide. The Cohesity platform is SOC 2 Type II certified in the Security, Availability, and Confidentiality Trust Services Categories.

Cyber vaulting – Cohesity also delivers a SaaS-based data isolation and recovery solution that improves your cyber resiliency with an immutable copy of data in a Cohesity-managed cloud vault via a virtual air-gap. Cohesity FortKnox, hosted in AWS, provides an additional layer of security against ransomware and other cybersecurity threats by delivering both data and operational isolation. Unlike traditionally complex, costly, and time-consuming approaches to data isolation, FortKnox dramatically simplifies operations and lowers your costs with a fully-managed cloud service. It also helps you prepare for and recover confidently from attacks with ML-based anomaly detection and quick, granular recovery back to the source or an alternate location.

Strict access controls – Lost or stolen credentials are a preferred way for cybercriminals to exploit your data. Cohesity's architecture and data security capabilities mitigate against the risk posed by weak user passwords and insider threats by stopping unauthorized users from impacting your business. The Cohesity in AWS solution supports:

- Multi-factor authentication (MFA), requiring anyone accessing the Cohesity platform to authenticate using multiple factors, such as something you have (i.e., your mobile device, one-time password token, smart card, etc.) and something you know (i.e., your password, PIN). Cohesity supports native MFA or third-party MFA providers such as Ping, Duo, Okta, and more.
- Granular role-based access control (RBAC), helping to stop unauthorized access while enabling you to grant users appropriate privileges to perform their duties.
- Quorum, requiring any critical changes, including root-level changes, to be authorized by two individuals, making your data and the Cohesity platform secure. No single user or compromised credential can impact the most sensitive operations. Additionally, unlike alternative solutions, Cohesity doesn't have a service back door built into the platform for cybercriminals to exploit.

Detect

As cybercriminals continue to strengthen and modify their approaches, Cohesity makes it easier for your organization to detect intrusions, anomalies, and inconsistent behavior.

Cohesity and AWS provide multiple cloud services delivering comprehensive data security capabilities to discover and respond to cyber incidents. Jointly, Cohesity and AWS leverage artificial intelligence/machine learning (AI/ML) to detect user and data anomalies that could indicate an emerging attack; utilize threat intelligence to ensure your protected-data is malware free; and with data classification, enable you to determine the exposure of sensitive and private information should an attack occur.

User behavior anomalies – With Cohesity data security and data management, you can review data access and logs in your unstructured data for unusual data activity. You or your administrators can easily search audit logs to determine who is creating, modifying, accessing, or deleting files in a manner that does not support typical operations. This provides security teams with insights into behavior that could indicate a ransomware attack or other malicious activity.

Threat detection – Cohesity threat detection capabilities combine threat intelligence with platform scanning to detect threats and malware. This can help your organization identify indicators of compromise (IOCs) that could indicate an emerging attack.

Data classification – With data proliferation—growing data locations, volumes, and source types—your organization needs automation to track the most critical and sensitive information. Cohesity DataHawk, hosted in AWS, automates data classification so you can discover and classify data to identify potentially sensitive data exposure from attacks. It uses AI-based classification to illuminate sensitive data location and classification. Predefined policies can also help your organization meet global and regional requirements for GDPR, CCPA, HIPAA, and other regulations, and you can employ100+ predefined patterns to create policies tuned to your specific needs.

Recover

Cybersecurity breaches, internal and external, do happen and fast. That's why your recovery has to be predictable and rapid. Cohesity and AWS jointly speed the process of getting back your ransomed data and applications—at scale.

ML-driven recovery recommendations – Cohesity can help accelerate your data recovery after an anomaly is detected by advanced ML by recommending a clean copy of data to restore. This removes guesswork and aids you in making informed decisions.

Global search – Irrespective of data type or location, Cohesity's unified, global wild-card-based search helps you locate and rapidly recover data. All data that lands on Cohesity is indexed, making it easy and fast to locate across environments and initiate the recovery.

Fully hydrated snapshots – Once your recovery data is identified, Cohesity in AWS delivers rapid recovery at scale using Cohesity's unique architectural capabilities, including storing all your backup data in ready-to-use, fully hydrated snapshots. This means your data can be near-instantly recovered when needed to any point in time and location—no stitching required.

Learn more at Cohesity

COHESITY