COHESITY

SOLUTION BRIEF

Cyber Resilience Security Framework – Going Beyond Zero Trust

Key Benefits

- Enable, build, and keep pace with critical Zero Trust cybersecurity
- Automated cybersecurity analytics for detection, response, & recovery of cybersecurity events
- Open API for 3rd party security tools and analytics, run cyber security apps directly on the platform
- Future proof; a purpose-built software-defined platform for multi-cloud hyper-scale deployments

Cyber resilience refers to an entity's ability to continuously deliver the intended outcomes, despite adverse cyber events. The concept essentially brings the areas of information security (and zero trust principles), business continuity, and organizational resilience together. A critical component to any security framework that aims to achieve a level of cyber resilience is ensuring that the security framework is aligned with Zero Trust principles of "never trust, always verify," which means that devices should not be trusted by default, even if they are connected to a managed corporate network such as the corporate LAN and even if they were previously verified. There are three key components in a zero trust architecture: user/application authentication, device authentication, and trust (don't trust). A cyber resilience security strategy and framework defines security throughout your IT systems and environments to prevent threat actors from accessing your most valuable resource: your data. One of the weakest links in many organizations' security strategy is how their data is organized, protected, and managed. It includes Zero Trust principles of "never trust, always verify" but does not stop there.

Many organizations still have unstructured data, with disparate policies that are inconsistently implemented. These conditions create an attractive attack surface with many attack vectors primed for exploitation by ransomware and cybersecurity criminals. These challenges are compounded with systems getting more distributed and complex with cloud, and more frequently, multicloud.

A successful cyber resilient security approach helps the government successfully keep data secure, detects and defends against cyber attacks, while also delivering on mission objectives. Government organizations are increasingly dependent on properly optimized, simplified, and protected data. A cyber resilient security framework that informs and delivers a security posture that enables the ability to continuously deliver the government's intended outcomes, despite adverse cyber events.

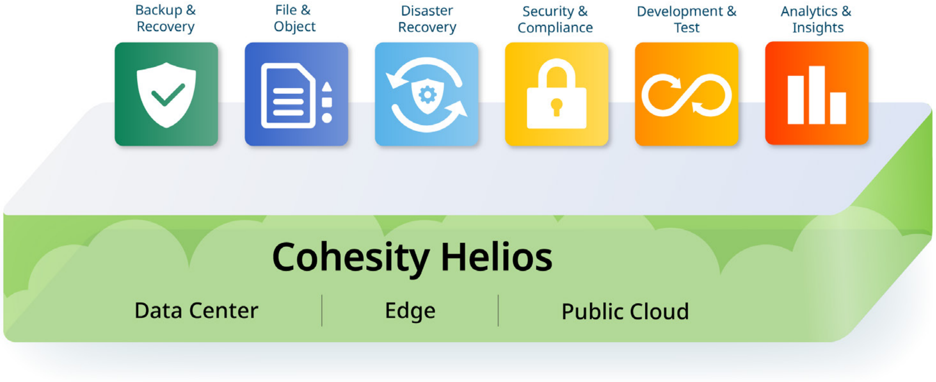


Figure 1. Cohesity Helios is your single data protection platform with reach into all topology areas enabling key critical cyber security functions in the most efficient and cost-effective way available in the industry.

This security approach must also be ready to perform at hyperscale, on-prem, and with multiple simultaneous private and public clouds. Cohesity DataProtect can do all of this for you and more, enabling your organization to achieve a level of cyber resilience by closing many security gaps including those driven by a Zero Trust strategy of systems access, while also keeping your data management operation tuned and automated. This protects the organization by reducing cyber risk, lowering costs, and driving operational efficiencies.

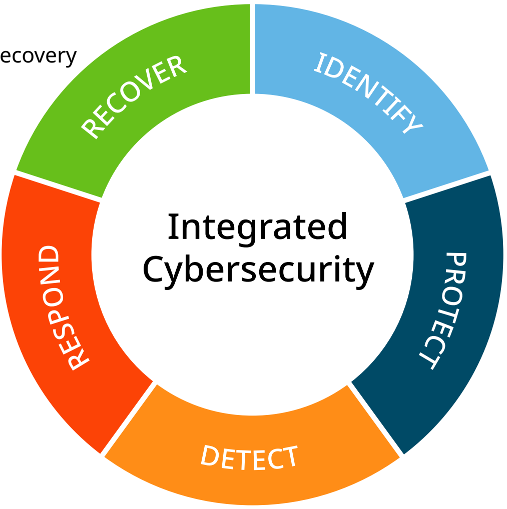
Cohesity Helios is a market-leading multicloud platform that dramatically simplifies how organizations protect and manage their data. Helios aligns and supports NIST, NSA, and DISA security frameworks by providing security capabilities for Data, Applications, Workloads, Devices, Visibility, Analytics, Automation, and Orchestration. Helios is purpose-built to run smart data analysis tools alongside your data at the edge, core, and cloud. These capabilities enable instant backup and recovery, automated disaster recovery orchestration, proactive machine learning-based anomaly detection, ransomware recovery, anti-virus, data classification, auto-indexing with full-text search, data deduplication and compression, quality of service management, data encryption in flight and at rest, immutable data stores, data replication, data storage, data cloning, data masking, and more.

Simultaneously designed to work at the edge, in your data center, and multicloud environments, and with additional onboard tools providing lightning-fast remediation of CMI spills, PHI and PII incidents, and similar events, Cohesity enables your agency to protect, detect and recover from cybersecurity attacks - recover fast and greatly reduce the impact of a ransomware attack. Cohesity capabilities offer a multilayered Cyber Resilience protection approach helping achieve a more comprehensive security posture that goes beyond a Zero Trust Framework.

Cohesity's Comprehensive Cybersecurity Framework

Recover
- Instant recovery at scale for VMs
- Non-disruptive instant large DB recovery
- Recover anywhere to any point
- Machine-driven clean snapshot recommendation

Identify
- Global visibility across environments
- Security advisor
- Cyber vulnerability scan



Respond
- Restore anywhere for forensics
- Built-in auditing and reporting
- Granular active directory comparison

Protect
- Immutable snapshots
- Immutable file system
- Encryption inflight and at rest
- WORM
- Test recoverability multi factor authorization
- Granular RBA
- No service backdoor
- Whitelisting

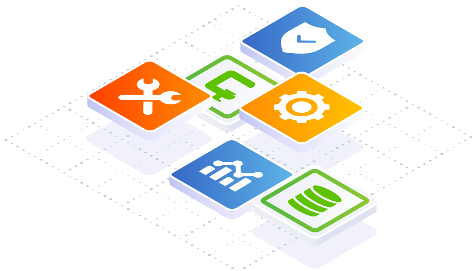
Detect
- Machine learning-based anomaly detection
- Deep visibility of affected objects and sources
- Realtime notifications and alerts

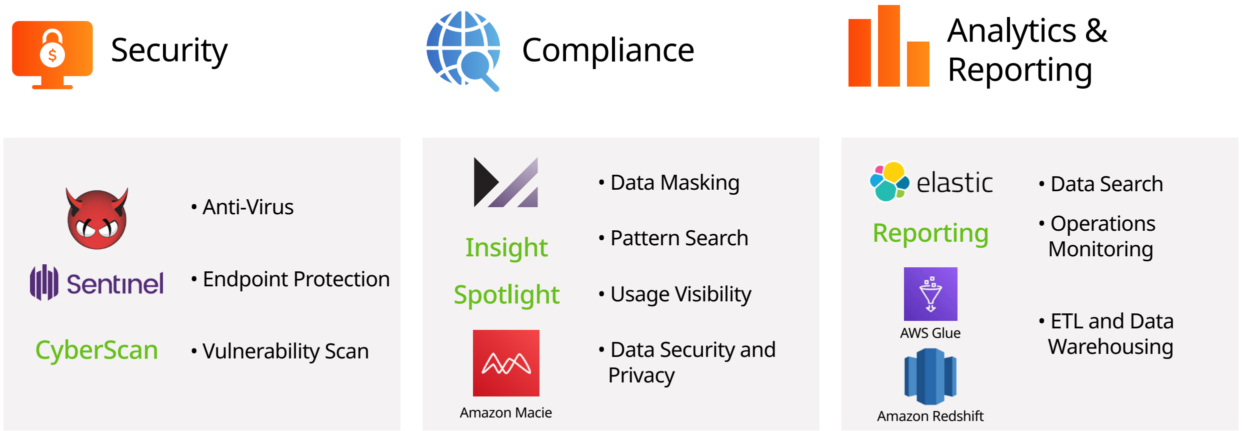
Figure 2. Cohesity's comprehensive cybersecurity framework supports NIST, NSA & DISA Zero Trust Architectures

Feature	Benefit	Description
Zero Trust Hardening	Highly secure – configure once, securely deploy across locations	Accelerating data mobilization, Cohesity can be securely configured and right-sized once then redeployed as the same secure environment anywhere from the cloud to on-prem or the edge reducing deployment time from weeks to hours
Automated Discovery, Baselining & Analytics	Automated the discovery and baseline production system data for Ransomware detection and remediation. Capture production environment elements for historical analysis.	Cohesity performs data analytics co-resident with data storage and can expand use cases enabling Federal organizations to keep pace with future Zero Trust cybersecurity challenges. This presents the most efficient analytics security, performance, business optimization, and operational efficiencies - Cohesity CDP (continuous data protection)
Future Security Capabilities	Cohesity Helios is an application framework and robust extensible API	Cohesity Helios provides an excellent method to quickly onboard new security capabilities to protect against emerging threats.
Improved data analytics and application mobility	Fast access to trends in data for better decision making	Cohesity empowers field-based teams to fully leverage the platform's compute capability to process data analytics in the field and make results readily available. Cohesity Marketplace apps enable rapid search, email forensics, e-discovery, tagging, and help streamline compliance. As a result, teams working with different applications across the many nodes and echelons of the tactical and higher-level networks are better informed.
Software-Defined	Consolidate multiple workloads onto a common data platform. Reduce cost and risk for on-prem and multi-cloud.	Cohesity's software-defined hyper-converged data management platform consolidates multiple point products and converges a range of data services, which helps to reduce that attack surface. The disaggregated architecture integrates easily with leading infrastructure as code and other 3rd party solutions. The net result is the ability to quickly scale up or scale down on demand achieving linear scale to performance objectives for a very broad set of DoD use cases, in additional cybersecurity Zero Trust Architecture.
Standards compliant	Government Certified solution for peace of mind	The joint solution features comprehensive technical controls and certifications: • FIPS 140-2 Level 2 Validated • TAA compliant • Federal Information Security Management Act (FISMA) Compliance | Authorities to Operate (ATOs) on DoD networks • WORM Compliant – SEC 17a-4f certification • Strong multi-factor, certificate (PIV/CAC)-based authentication • Common Criteria: EAL 2+ • SOC 2 Type 2 • (DoDIN) Approved Products List (APL) • Native cloud integrations with all leading FedRAMP clouds
Includes integrated vendor suites	Cohesity's hyperscale platform is architected to consolidate multiple point-product capabilities onto a common data platform.	3rd party capabilities can be integrated onto your Cohesity platform, which reduces costs and creates transformational efficiencies for the government; a highly functional data platform, Helios consolidates multiple data sets, data types, and workloads onto a common platform for more efficient cybersecurity work that can be done in one place.
SIEM Event data storage	Cohesity provides efficient and effective long-term storage of SEIM event data.	Cohesity integrates with leading SEIM vendors providing industry-leading dedupe and compression of log and event data to drive maximum capacity efficiency - lowering operating costs and streamlining Zero Trust and cybersecurity operations for other tools and platforms.
Low operational overhead		To accommodate the variable skills of federal operators, the solution can be pre-configured with the right data and simply stood up. As missions and requirements change, authorized personnel can easily and quickly modify automated policies.

Cohesity App Marketplace

Cohesity developed and third party





Security

CyberScan
- Anti-Virus
- Endpoint Protection
- Vulnerability Scan

Compliance

Insight
Spotlight
- Data Masking
- Pattern Search
- Usage Visibility
- Data Security and Privacy

Analytics & Reporting

Reporting
- Data Search
- Operations Monitoring
- ETL and Data Warehousing

Figure 3. Run your favorite data analytics and security applications (such as Splunk, Tenable, ClamAV, and more) on the same Cohesity platform that stores, indexes, and backs up your data

Trusted Across the Government

To learn more, visit www.cohesity.com/solutions/industry/government

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.