COHESITY

PLATFORM SECURITY POCKET GUIDE

Cohesity has built a **multilayered data security architecture** to combat not just the ransomware 3.0 threat, but to help our customers achieve specific outcomes as it relates to data protection, **compliance, operational Resilience**, **defense against sophisticated attacks** and **aggressive variants of ransomware**. This architecture offers Cohesity's customers with a **highly resilient platform** that ensures **confidentiality, availability,** and **integrity** of the data.

This pocket guide provides overview of different **Cyber Resilience** capabilities built into **Cohesity platform** aligning with industry leading cybersecurity framework, such as **NIST** and **PICERL**.

Cohesity Cyber Resilience Capabilities

For more details, see the links under each feature on page 2.

1 Data Protection

- Encryption
- Immutability
- Fault Tolerance
- Logical Air Gap

2 Zero Trust-User Level

- Secure User Access
- Multi Factor Authentication (MFA)
- Password Management
- Quorum
- Granular RBAC
- No Support Backdoor
- Secure Shell
- Split Key

3 Zero Trust-Platform Level

- Firewall Profiles and Ports
- Key Management
- Session Management
- Secret-based APIs
- Certificate Management
- Protect Files & Views
- NTP Synchronization

4 Detection & Response

- Near Real Time Threat Detection
- Data Classification
- Antivirus/Malware Scan
- Cyber Scan (Vulnerability Scan)

5 Security Integration

- Threat Management
- Data Security Posture Management
- Vulnerability Management
- Identity Management
- Credential Vault (PIM/PAM)
- Data Masque (PII Masking)

6 Recovery@Scale

- Restore
- Global Search
- Cyber Vaulting & Resilience

7 Compliance & Certifications

- Global Compliance
- Third-party Certification

Learn more at :

- Cohesity Trust Center
- Cohesity Support
- Cohesity Resources

Send us your feedback!

COHESITY

PLATFORM SECURITY POCKET GUIDE

Encryption

- Data at Rest — AES 256 GCM, FIPS-approved
- Data in transit —TLS 1.2,TLS 1.3
- Replication Encryption — AES-256-GCM
- Intra-node — Mutual TLS (mTLS) on by default

Immutability

- By design **SpanFS** is immutable —No overwrites
- **Data Lock** — time-bound, WORM lock
- Incremental-forever object-locked archiving
- NTP Time Synchronization and shift resistance

Fault Tolerance

- **Highly Resilient Hardware** — Disk, Nodes, Chassis, Rack, Network, Power Supply & Fan
- **Highly Resilient Software** — Erasure Coding (EC) / Replication Factor
- Non-disruptive upgrade to avoid missed backups

Logical Air Gap

- Backup—written to Internal View
- Append only & WORM lock
- Clone the View before recovery
- No external access via SMB/NFS

Secure User Access

- **Supported users** — Local, Active Directory, Single Sign-on
- **User Types** — UI, Console, API, Secure Shell

Password Management

- Secure **policy-driven** password Management
- Set password complexity requirements
- Define the **account lockout** policy

Multi Factor Authentication (MFA)

- All users and Groups
- **TOTP, Email**
- Integration with major auth providers (Okta, Duo, Google, Microsoft)

Granular RBAC

- Assign least privileges to users
- Build your own custom or select one of **8 default roles**
- **100+** out-of-the-box role privileges

Quorum

- Protect sensitive operations with multi-user approvals
- **Predefined** templates to identify the privileged operations

Split Key

- Dual Control Authentication with **Challenge-Response Code** for IPMI console, Host shell access

Secure Shell

- **Restricts SSH access** to the host operating system shell
- Allows admins to run only the iris_cli commands and view logs via SSH

No Service Backdoor

- **On-demand assistance** to customers
- SSH reverse tunnel with the Teleport support server on TCP port 443

Data Protection

Near Real -Time Threat Detection

- Perform threat detection scans that look for ransomware and other threats using Indicators of Compromise (IOC) with 110K threat rules
- Understand the user behavior by searching audit trails in near real-time
- Posture Advisor to improve get insights and assess risk
- Real-time ML-based detection to detect anomalies and risky user behaviours

Data Classification

- Automated discovery and classification of sensitive data for security and compliance
- Out the box 200+ production grade, AI/ML based patterns
- Predefined policies & custom policies for data classification based on specific use cases
- Natural-Language Processing (NLP): detect names, addresses, birthdates, and passwords

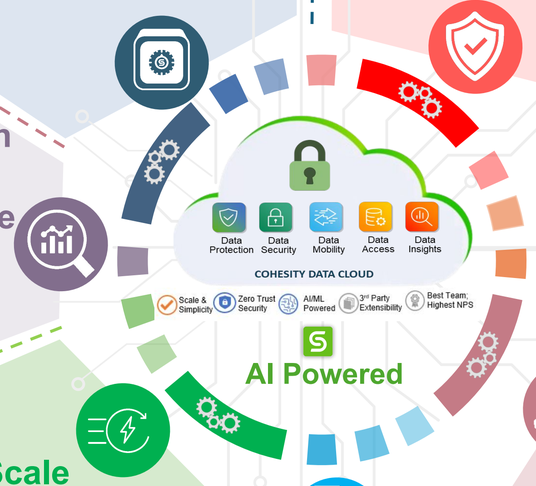
CyberScan

- Scan, identify, analyze the vulnerability and reduces risks.
- On Demand and Scheduled Scans

Antivirus/Malware scan

- Scan the file and detect threats and take required actions
- Register external Antivirus software
- Install the Antivirus App from the Cohesity Marketplace

Detection & Response



Zero Trust-User Level

Platform Level

Key Management

- Cohesity managed Internal KMS
- **KMIP compliant external KMS** with Auto failover
- Supported Vendors—Thales, Fortanix, Entrust, Vormetric DSM, HashiCorp, IBM SGKLM, AWS KMS)

Firewall Profiles and Ports

- Manage Incoming and outgoing traffic of the Cohesity cluster
- 9+ application-based firewall profiles
- Custom firewall profile

Certificate Management

- Supports X.509 certificates in PEM format
- PKI infrastructure - Cluster CA managing agent certs and renewal

Session Management

- Set Absolute and Inactivity timeout for Cohesity interfaces (GUI,CLI & SSH)

Secret-based APIs

- Secure operations while interfacing with Cohesity clusters

NTP Synchronization

- Time-Shift Immunity: NTP change slewing
- Ensures all Cohesity cluster I/O operations are in time sync to prevent time-based attacks

Protect Files & Views

- Secure and restrict the access on the Cohesity Views
- Support for NFS, SMB, and S3 mount paths

Recovery@Scale

Restore

- Accelerate recovery with Instant access @scale—VMs, NAS shares, DBs, volumes
- Parallelized restore of large objects, proxyless
- Instant clean room recovery

Global Search

- Assist with investigation of cyber event
  - Global File and Folder Search
  - Active Directory Protection and Comparison
- Google-like wild-card search
  - Within data and metadata
  - Across all clusters and locations
  - Across all protected sources
  - Can specify the directory path

Cyber Vaulting & Resilience

- Modernize the 3-2-1 rule with SaaS data isolation
- Cohesity FortKnox (quorum, object lock, etc)
- SaaS Cyber Vaulting

Regulatory Compliance & Certifications

Global Compliance

Comply with Industry and international standards such as —

- Common Criteria (CC) Evaluation Assurance Level 2 (EAL2+)
- FedRAMP Moderate Authorized.
- FIPS 140-2 Level 1 validation (AES 256-bit encryption)
  SEC 17a4(f) & CFTC 1.31(c)-(d) (WORM
- Trade Agreements Act (TAA)
- Authorization to Operate (ATO)
- DoDIN APL Certification

Third-Party Certification

Data Security standard certified by independent third-party auditors

- ISO 27001
- SOC 2 Type II
- Regular penetration tests by qualified third-party assessors
- Payment Card Industry (PCI DSS)
- General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act (HIPAA) guidelines

Security Integration

Threat Management (SIEM/SOAR)

- Accelerate response and recovery with automated playbooks.
- **Supported Vendors—**
  - Cisco XDR
  - Palo Alto Networks XSOAR
  - Microsoft Sentinel
  - Crowdstrike Falcon Logscale
  - IBM QRadar

Data Security Posture Management

- Identify any gaps in the protection of sensitive cloud data assets
- **Supported Vendors—**
  - Normalyze, Wiz, Cyera, Dasera
  - Zscaler, Netskope* - Stop the Unauthorized Exfiltration of Sensitive Data

Vulnerability Management

- Flexible Scan Policy
- Cyberscan powered by Tenable.io
- Cohesity Clam AV
- External ICAP-based malware scanner

Identity Management

- **Single Sign on** with SAML v2 support & OpenID Connect
- Supported vendors—Okta, Duo, Ping, and Microsoft Entra ID (supports SAML v2)

Credential Vault (PIM/PAM)

- Manage Privileged Credentials of cluster (UI, IPMI)
- Isolate & Monitor Session
- Partnered with CyberArk

Data Masque (PII Masking)

- Anonymize data to safely feed analytics/dev/test workflows
- Secure SHA-512 salted hashing to support irreversible data masking
- YAML rulesets generation
- UUID mask pattern
- Wildcard character support for keywords
- Custom keywords

*** (coming soon)**

Learn more at :

- Cohesity Trust Center
- Cohesity Support
- Cohesity Resources

Send us your feedback!