5 STEPS TO CYBER RESILIENCY

Josef Honc, Senior Principal Sales Engineer

COHESITY

Does your organization have a cyber resilience strategy that you believe is adequate for today's threats and challenges?

© 2026 Cohesity Inc. All rights reserved.

Source: Cohesity Global Cyber Resilience Report, November 2025.

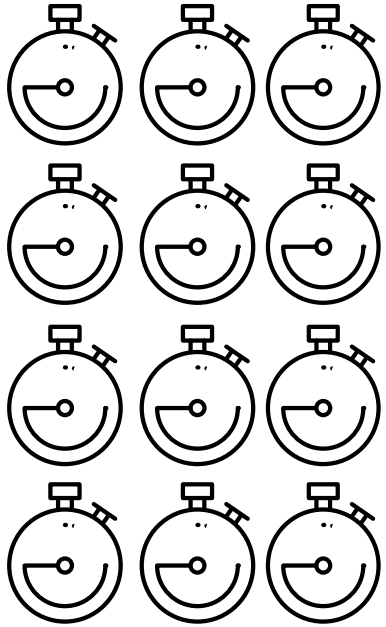
Why cyber resilience remains challenging

You don't know
what went wrong

Cyber recovery isn't
disaster recovery

Attacks are often far
more destructive
than anticipated

Key systems & data
are often inaccessible

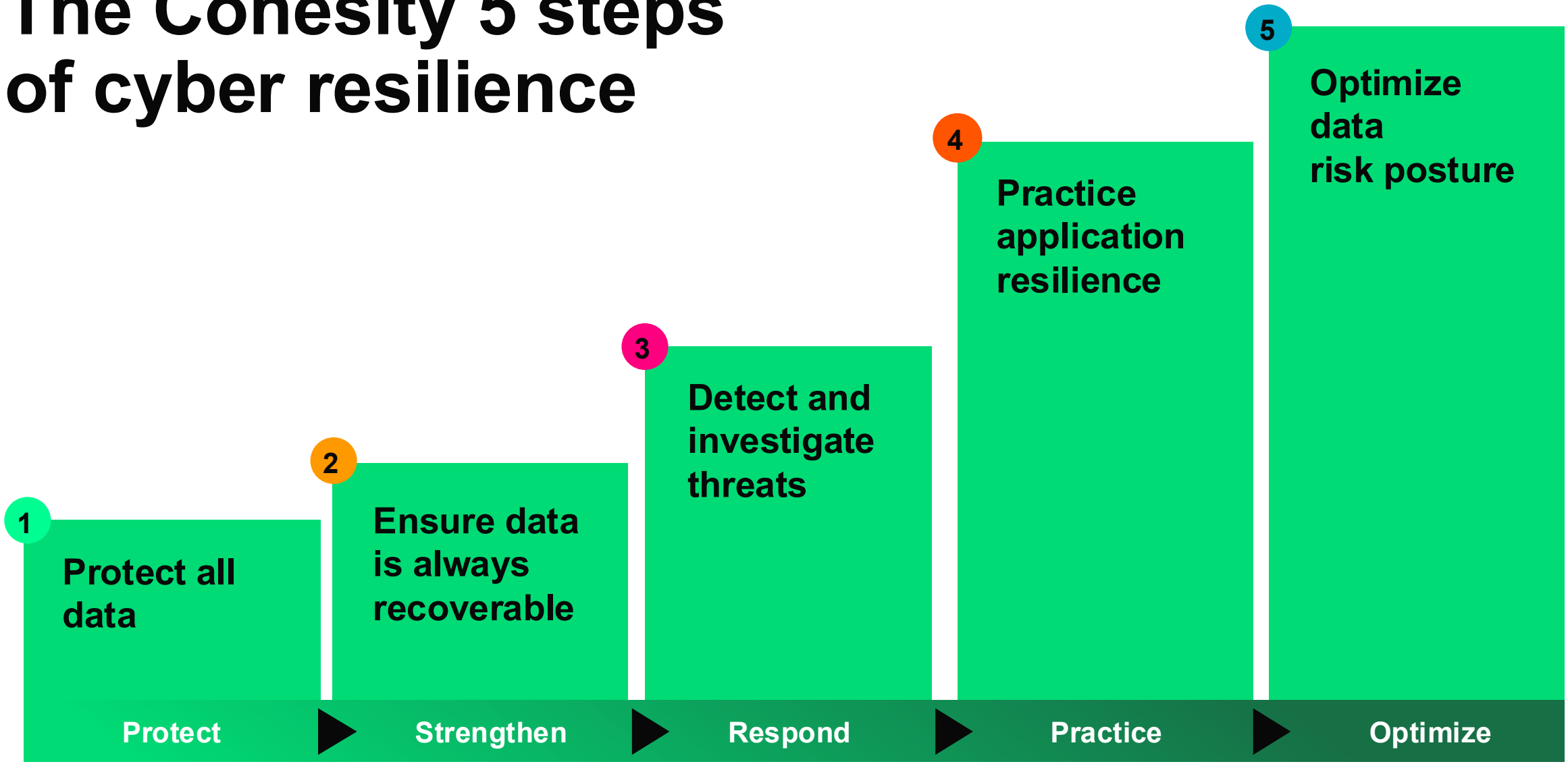


Your actual RTO is 12x worse than anticipated

Without a thorough and proper response, **rapid reinfection can occur.**

COHESITY © 2026 Cohesity Inc. All rights reserved.

The Cohesity 5 steps of cyber resilience



COHESITY © 2026 Cohesity Inc. All rights reserved.

Many opportunities to strengthen capabilities

1 Protect all data

53%
do not backup ALL workloads and data

2 Ensure data is always recoverable

52%
do not have an offsite copy

63%
do not have immutable backups for all data

46%
without MFA

3 Detect and investigate threats

33%
do not perform threat hunting

39%
do not subscribe to threat intelligence feeds

4 Practice application resilience

38%
were reinfected after recovery

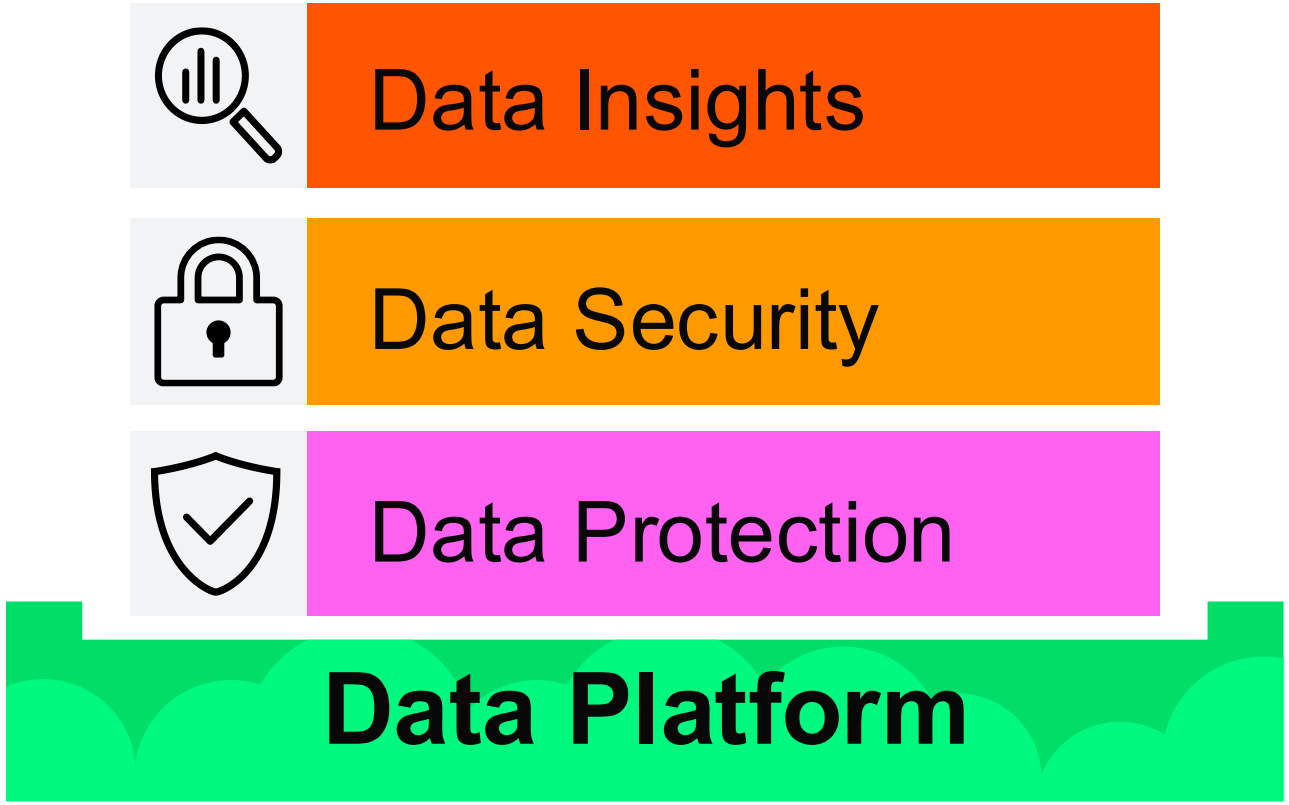
42%
do not do annual rehearsals

5 Optimize data risk posture

46%
do not ID & prioritize sensitive data and systems for backups

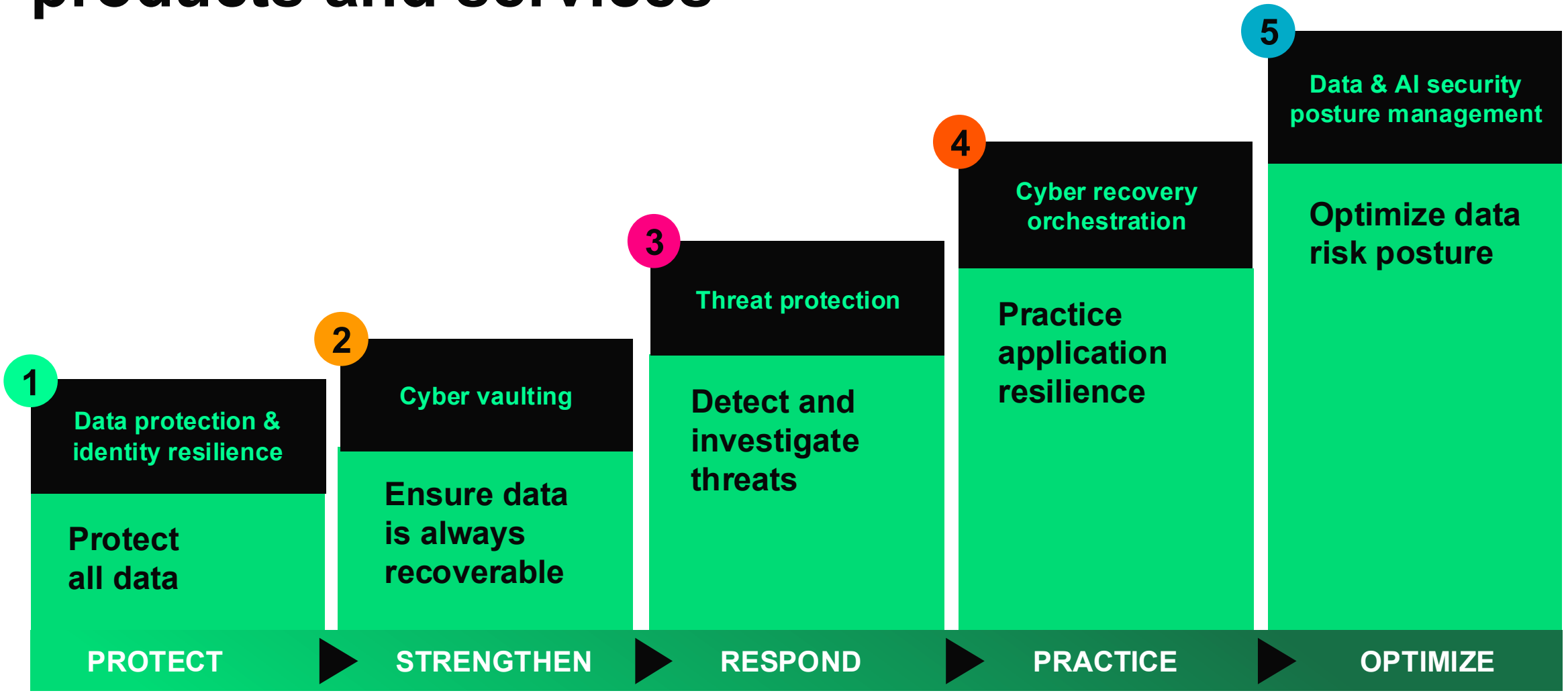
© 2026 Cohesity Inc. All rights reserved.
Source: Cohesity Global Cyber Resilience Report, November 2025.

Cohesity Data Cloud



COHESITY © 2026 Cohesity Inc. All rights reserved.

Cohesity data security products and services



COHESITY © 2026 Cohesity Inc. All rights reserved.

1 PROTECT ALL DATA with global governance

Identify unprotected data – your biggest security risk

Physical servers VMs Containers	Databases NAS Object Storage	Identity SaaS Agents	1000+ data sources

Cohesity Data Cloud

Unified UI + APIs | Common SLAs | Compliance | Reporting | Policies | AI-Powered Operations

Critical Success Factors

Storage Efficiency | Scale-out Performance | Global Search | Flexible Deployment Models | Consistent Licensing

KEY OUTCOMES

- Enhanced security
- Risk reduction
- Improved compliance & governance
- Lower costs & improved ROI
- Increased IT efficiency

COHESITY © 2026 Cohesity Inc. All rights reserved.

Active Directory: A Critical, and Challenging Workload To Protect

Decide and Prepare
Steps 1-5

1 Identify problem and scope
Confirm forest-wide failure symptoms; engage stakeholders.

2 Decide recovery and prep
Commit to forest recovery; stand up isolated recovery network/bubble.

3 Gather credentials
Domain Admin (per domain) plus DSRM passwords; preserve securely.

4 Select trusted backups
Choose last-known-good backups (writable DCs; few days pre-failure).

5 Pick restore DCs
Prefer dedicated, writable DCs; VM with GenID; root DNS/GC as needed.

Outputs:
- Recovery bubble ready
- Trusted backups selected
- Credentials secured

Restore - Bring up root
Steps 6-14

6 Isolate root-domain DC
Disconnect from production network (cable/NIC removal or isolated vNet).

7 Restore AD DS plus SYSVOL
Nonauthoritative AD DS restore plus authoritative SYSVOL on first restored DC.

8 Verify restored DC data
Validate database/system; if damaged, repeat with a different backup.

9 Handle initial sync edge-cases
If needed, set 'Repl Perform Initial Synchronizations'=0 so AD DS is available.

10 Reset privileged accounts
Reset EA/DA/Schema creds; plan trust resets if breach suspected.

11 Plan user password resets
If user creds may be compromised, plan domain-wide password reset.

12 Seize FSMO roles
Seize domain and forest FSMO roles onto restored DCs (root first).

13 Metadata cleanup
Remove metadata for writable DCs not being restored; delete stale DC DNS locator records.

14 DNS role and client settings
Ensure DNS service; root DC uses itself; child domains point to root DNS.

Outputs:
- Root DC restored
- FSMO seized
- Admin creds rotated

Restore - Hygiene and rese
Steps 15-22

15 Purge stale DNS records
Delete NS/SRV for removed DCs; run nltest /dsderegdns as needed.

16 Raise RID pool
Increase available RID pool (e.g., +100,000) to prevent SID reuse issues.

17 Invalidate current RID pool
If system-state restore not used, invalidate to prevent re-issuing old RIDs.

18 Reset DC computer account
Reset recovered DC computer account password twice.

19 Reset krbtgt
Reset krbtgt password twice (and trust passwords as needed).

20 Remove GC on restored DC
If multidomain and DC was GC, clear GC flag to avoid lingering objects.

21 Mitigate gMSA exposure
If using gMSA, replace/recreate as needed (Golden gMSA scenario).

22 Configure time service
On PDC emulator (root), sync time from external time source.

Outputs:
- DNS cleaned
- Kerberos/RIDs reset
- Time service aligned

Reconnect and Validate
Steps 23-27

23 Repeat for all domains
Restore 1 writable DC per domain; recover parent domains before child domains.

24 Reconnect to recovery network
Join restored DCs to a common isolated network for validation/replication.

25 Fix name resolution
Create DNS delegations; configure forwarding and root hints as required

26 Validate replication and health
Run repadmin; create temp connections if needed; dcdiag; verify key events.

27 Add global catalog
Enable GC on root-domain DC; force replication; verify (event 1119/registry).

Outputs:
- Domains restored
- Replication healthy
- GC validated

Redeploy and Cleanup
Steps 28-29

28 Re-baseline backups
Take fresh backups of restored DCs before scaling out recovery.

29 Redeploy and cleanup
Redeploy remaining DCs (clone/reinstall/IFM, RODCs); revert DNS; delete WINS; restore

Outputs:
- Fresh baseline backups
- Remaining DCs redeployed
- Environment cleaned up

© 2025 Cohesity Inc. All rights reserved.

Semperis ADFR: 7-Click Active Directory Forest Recovery

Transform catastrophic AD failures from weeks to minutes

1. Click Recovery
2. Start Forest Recovery
3. List Backup Sets
4. Select Backup Set
5. Select location
6. Review
7. Start Recovery

Up to 90% Faster - Minutes to recover instead of days of manual coordination.

Reduced Reinfection Risk - Controlled validation and reconnection protect against persistent threats.

Automated Orchestration - Consistent execution eliminates human error and configuration mistakes.

Predictable Outcomes - Repeatable workflows deliver reliable recovery every time.

Highlights

- Minutes instead of days to full recovery
- Predictable recovery outcomes
- Guided automation with validation checks
- Consistent, repeatable execution

COHESITY

© 2025 Cohesity Inc. All rights reserved.

2 ENSURE DATA is always recoverable

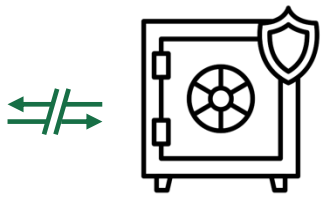
Harden your platform + add a cyber vault

1000+ data sources

On-Prem | Cloud | Agents | SaaS | Edge

Cohesity Data Cloud

Immutability | MFA | Separation of Duties | 3-2-1-1 | Threat Containment | DataLock | REDLab



Cyber Vault

Physical & logical isolation

Critical Success Factors

Backup Restoration Performance | Cyber Vault On-Prem or Cloud | Cyber Vault Key Management & Immutability

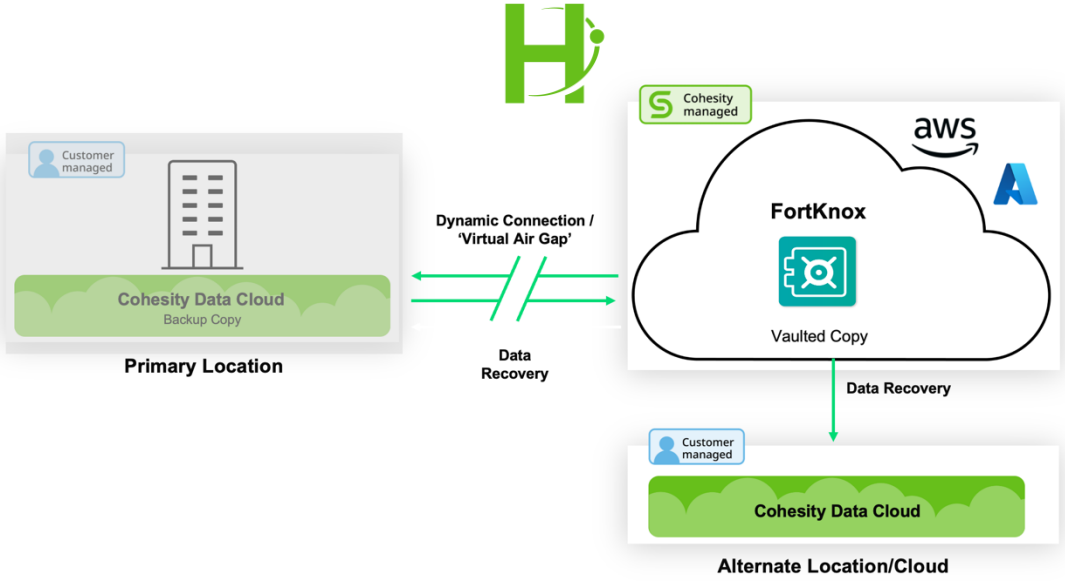
KEY OUTCOMES

- Faster & more secure recovery
- Stronger protection against attacks
- Audit readiness
- Zero trust alignment

COHESITY © 2026 Cohesity Inc. All rights reserved.

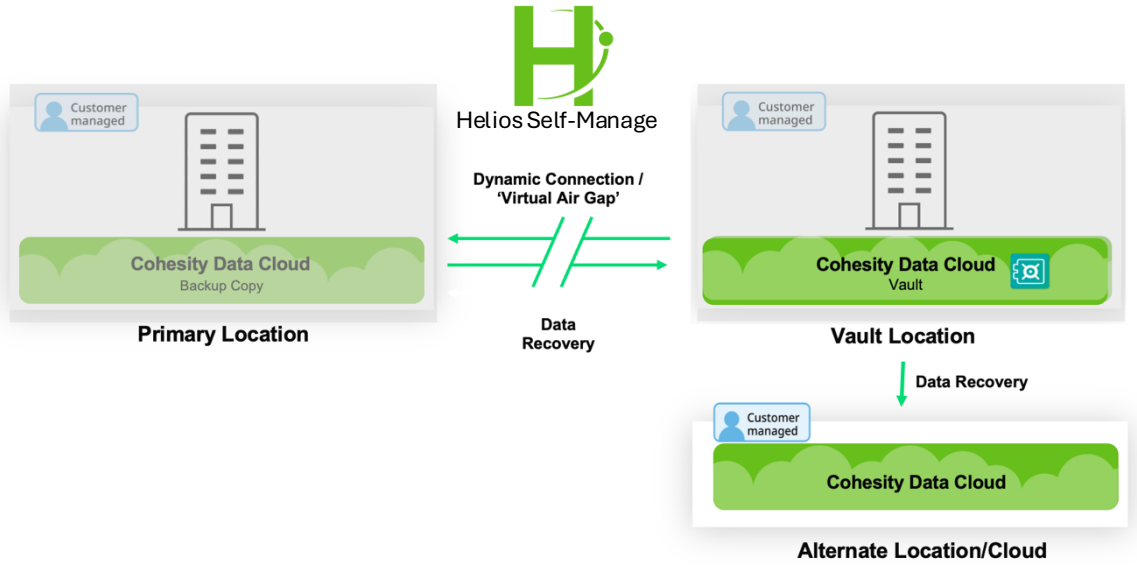
Cohesity FortKnox – deployment models

Fortknox SaaS



- Preferred choice for Cloud-first customers
- No Infrastructure to manage
- Cohesity guarantee for complete data isolation, immutability and air-gapping
- Available for both On-Prem and Cloud-based workloads
- Unlimited Scale
- Vault availability - Cloud region level

Fortknox Self-Managed



- Preferred choice for Dark Site, Fed, Financial customers
- Needs customer hosted infrastructure
- Shared responsibility model - Customer required to follow security best practices
- Available for On-Prem workloads
- Multiple Cohesity clusters may be needed
- Vault availability – Data center level

COHESITY © 2026 Cohesity Inc. All rights reserved.

3 DETECT AND INVESTIGATE threats

Regularly conduct threat scanning & threat hunting

Threat scanning

Threat hunting

Ecosystem integrations
(SIEM/SOAR)

Cohesity Data Cloud

Google Threat Intelligence | YARA Rules | Anomaly Detection | Sophos Malware Scanning | Secure Sandbox Analysis | Hash Index

Critical Success Factors

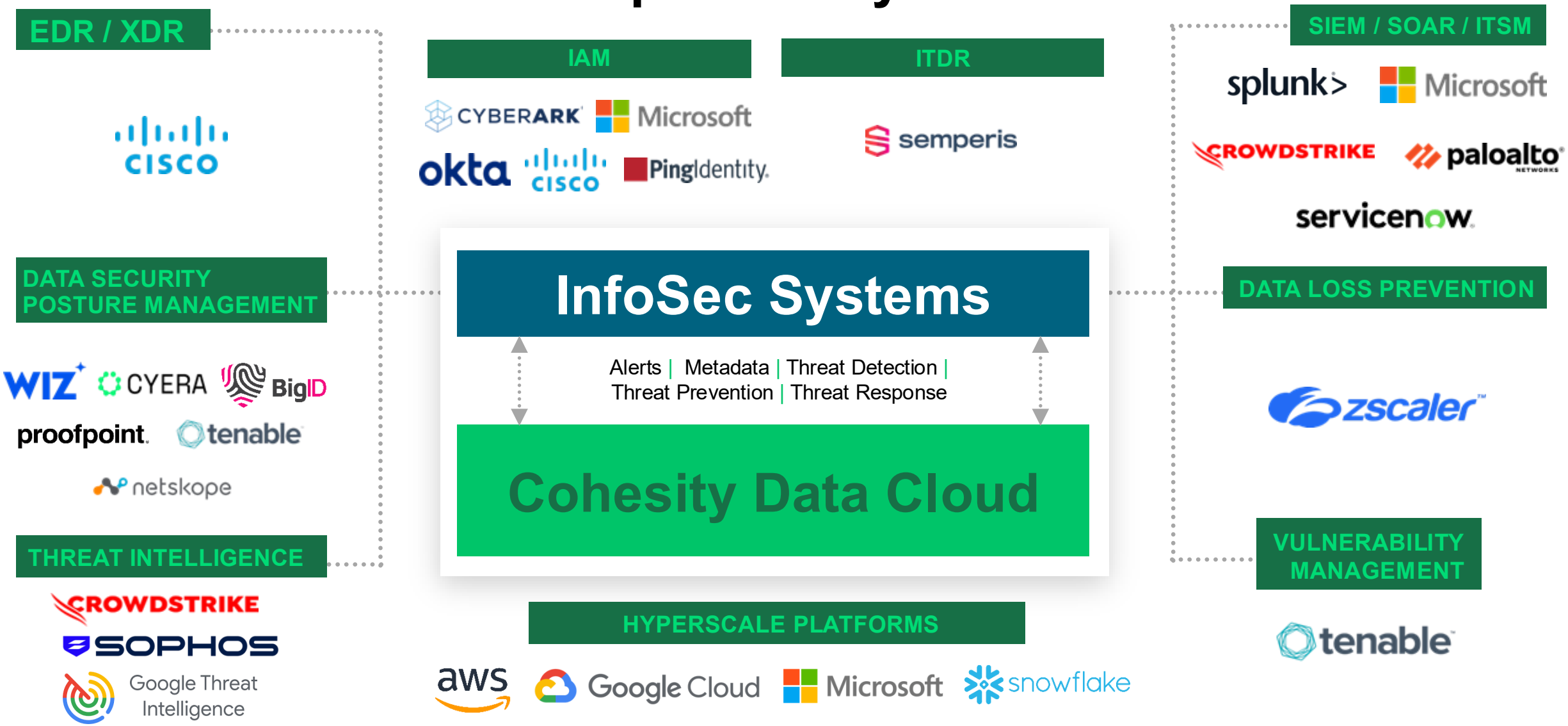
Unlimited Threat Scans | Scheduled & On-Demand Scans
High Performance Scans | Open & Extensible Platform

KEY OUTCOMES

- Early threat detection & mitigation
- Backup integrity assurance
- Faster incident recovery and reduced downtime
- Shared context for IT & InfoSec teams

COHESITY © 2026 Cohesity Inc. All rights reserved.

The Industry's Most Secure & Open Ecosystem



COHESITY © 2025 Cohesity Inc. All rights reserved.

4 PRACTICE APPLICATION RESILIENCE

Automate cyber recovery: initiate, investigate, mitigate

Digital Jump Bag™

Orchestration

Clean Room

Rapid Recovery at Scale

Cohesity Data Cloud

Secure File Storage | Cyber Recovery Orchestration | AD Recovery | Clean Room | Forensic Threat Hunting | IR Ecosystem

Critical Success Factors

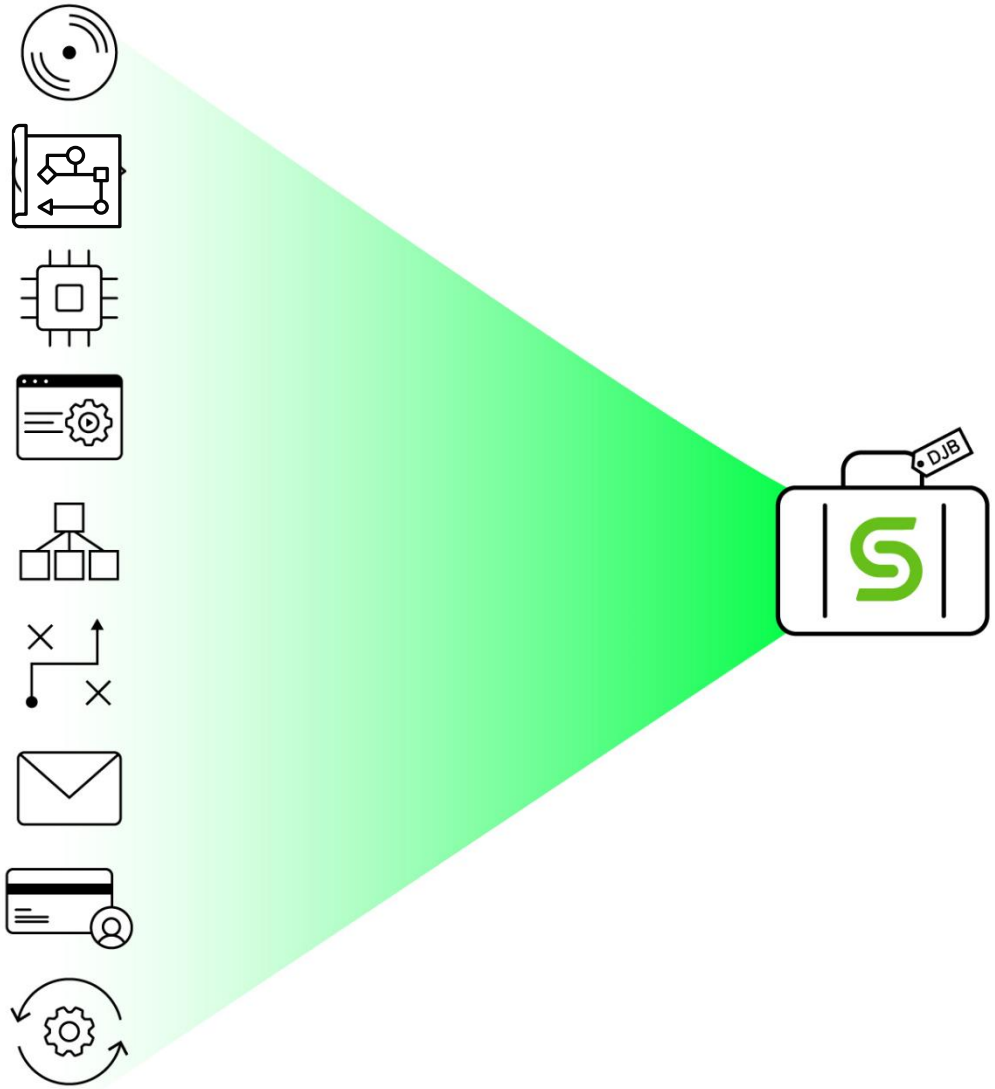
MVRC | Incident Analysis Timeline | Instant Mass Restore | CERT (Cyber Event Response Team)

KEY OUTCOMES

- Faster & safer recovery
- Improved RTO
- Lower risk of re-infection
- Reduced disruption & financial risk

COHESITY © 2026 Cohesity Inc. All rights reserved.

Digital Jump Bag Cheat Sheet



5 OPTIMIZE DATA RISK POSTURE

Reduce your risk from data theft

Assess incident impact

Identify unprotected critical data

Data classification

DSPM
Data discovery & classification

Cohesity Data Cloud

Large Pattern Dictionary | Context Recognition | Name Entity Recognition | Ensemble Learning Models | DSPM Integration

Critical Success Factors

230+ Data Classifiers | Choose the Right DSPM Solution

KEY OUTCOMES

- Enhanced data visibility & classification
- Proactive risk identification & mitigation

COHESITY © 2026 Cohesity Inc. All rights reserved.

OPTIMIZE DATA RISK POSTURE

BEST PRACTICES

Discover and classify data

Align protection with data sensitivity

Configure access/permissions

Manage AI security posture

© 2026 Cohesity Inc. All rights reserved.

THANK YOU

josef.honc@cohesity.com

COHESITY

© 2025 Cohesity, Inc. All rights reserved.
Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, the Helios logo, DataGovern, SiteContinuity, DataHawk, 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.

COHESITY

RESILIENCE EVERYWHERE