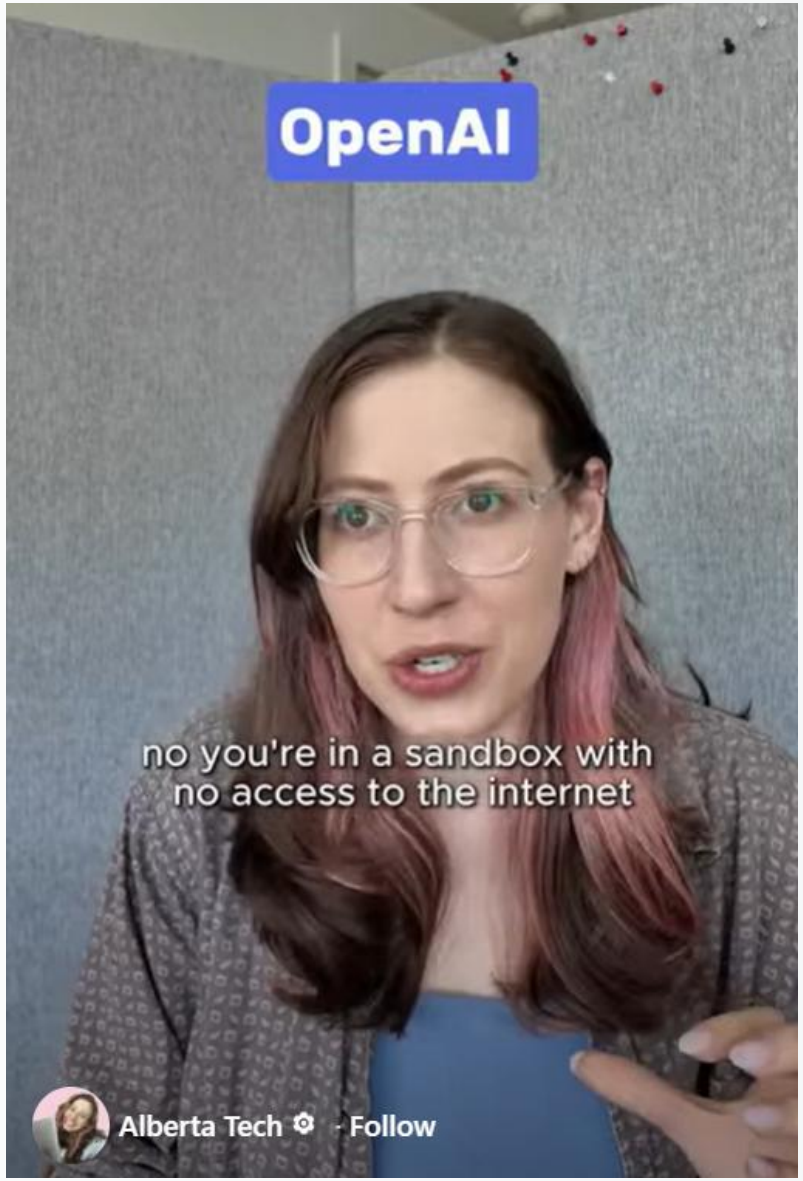

MOBIA
CONNECT
COHESITY
AFTER MYTHOS &
GPT-5.5-CYBER
Simon Robinson
Sales Engineering Leader, Canada
Resilience in an AI World
What does it take to survive, faced with skilled adversaries, and come through it with the least impact?



https://www.facebook.com/reel/2142774776619797

COHESITY © 2026 Cohesity Inc. All rights reserved.


With Great Power Comes
Great Responsibility
Mythos
AI FOR CYBER RESILIENCE
DETECT EMERGING THREATS
FIND VULNERABILITIES
STRENGTHEN DEFENSES
GPT-5.5-Cyber
FRONTIER AI FOR CYBER DEFENSE
ANTICIPATE ATTACKS
HARDEN CRITICAL SYSTEMS
BUILD A MORE RESILIENT TOMORROW
Powerful AI Frontier Models can accelerate cyber defence and vulnerability discovery, but only when used responsibly, with strong safeguards, and trusted governance.

A Force for Good

Frontier AI + Cybersecurity Innovation



Project Glasswing

Mythos

Anthropic cyber defense initiative



Daybreak

GPT-5.5-Cyber

OpenAI cyber defense initiative



150+ other technology and critical infrastructure companies involved

AN ECOSYSTEM FOR A MORE RESILIENT TOMORROW

COHESITY
DATA SECURITY
FOR A STRONGER TOMORROW

NVIDIA | ANTHROPIC | OpenAI | cisco | paloalto NETWORKS

CROWDSTRIKE | aws | Microsoft | Google | CLOUDFLARE

PEOPLE | INNOVATION | PARTNERSHIP | SAFER TOMORROWS

AI-DRIVEN CYBER RESILIENCE, THREAT DEFENSE, AND INFRASTRUCTURE PROTECTION

A MORE SECURE AND OPEN WORLD

Resilience *is* *a decision,* made daily.

In September 2026, a 35-year-old from Slovenia outlasted nine other survivalists across seven countries in the Canadian Arctic — **90 days** of sub-zero nights, shrinking food stores, and total isolation — to become the first World Champion of the show *Alone*.

90
days survived

$500K
prize secured

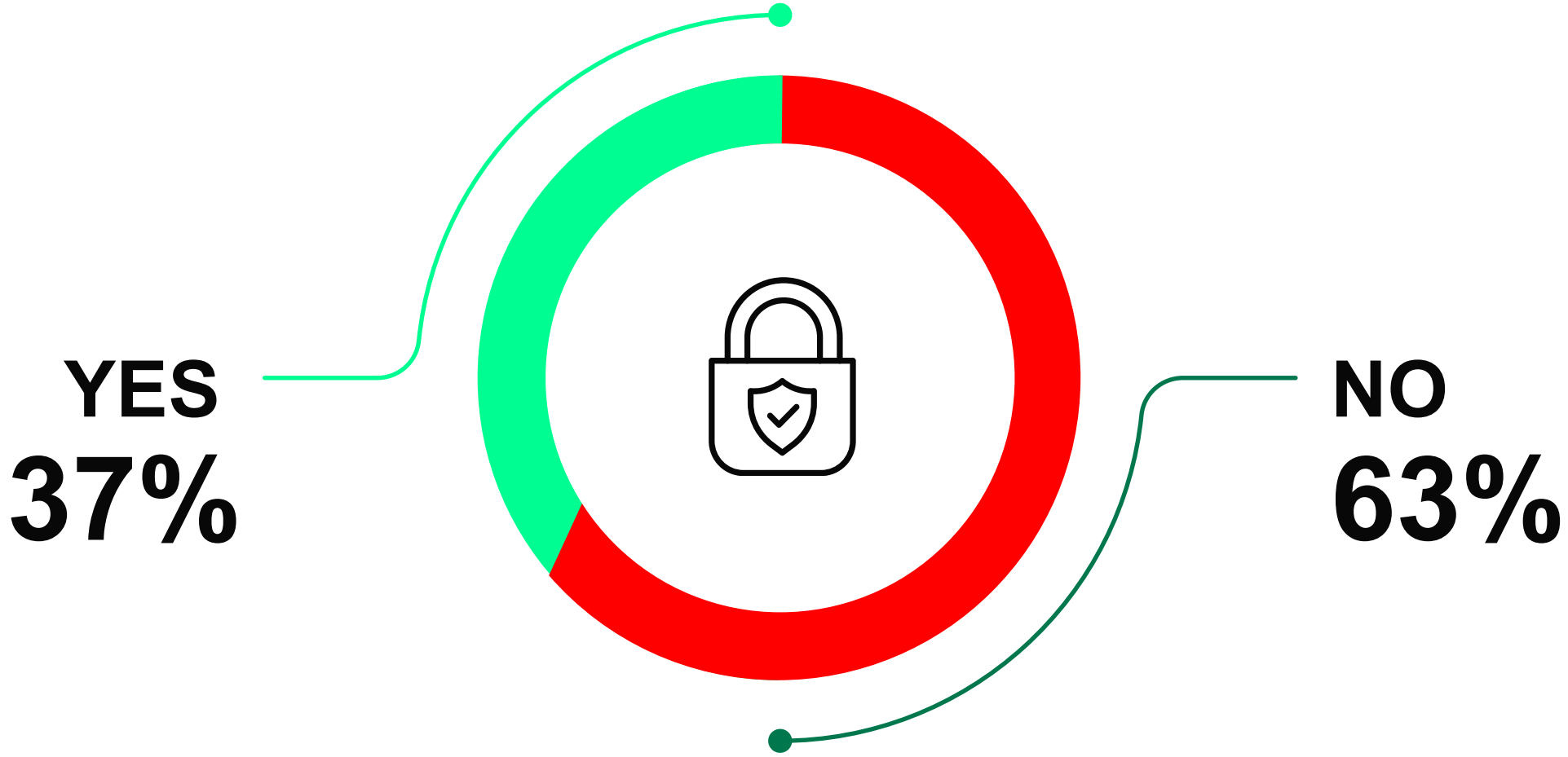
1st
world champion



COHESITY | © 2026 Cohesity Inc. All rights reserved.


the tipping point of not if, but when
Defense Alone Doesn't Cut It
Recovery Depends on Resilience
ENDPOINT SECURITY
FIREWALL
THREAT DETECTION
ACCESS CONTROLS
MONITORING & ALERTS
RANSOMWARE
DATA THEFTIE
ZERO-DAY
INSIDER THREAT
SUPPLY CHAIN
SYSTEMS DISRUPTED
DATA ENCRYPTED
OPERATIONS HALTED
REPUTATION DAMAGED
REVENUE LOST
COHESITY
COHESITY DATA CLOUD
Immutability
Cyber Vaulted Data
DSPM Insight
Recovery Orchestration
Clean Identities (human and non-human)
Minimum Viable Company
Cleanroom / Isolated Recovery Environment
Clean Recovery
Digital Jump Bag
PERSISTENCE ELIMINATED
SERVICES ONLINE
CUSTOMERS & EMPLOYEES SUPPORTED
REVENUE GENERATING
DETECT
PROTECT
RECOVER
THRIVE
True Cyber Resilience means more than stopping attacks — it means confident, rapid, clean-state recovery.

Do you have a cyber resilience strategy that's adequate for today's threats and challenges?



© 2026 Cohesity Inc. All rights reserved.

Source: Cohesity Global Cyber Resilience Report, September 2026.

Why Cyber Resilience Remains Challenging

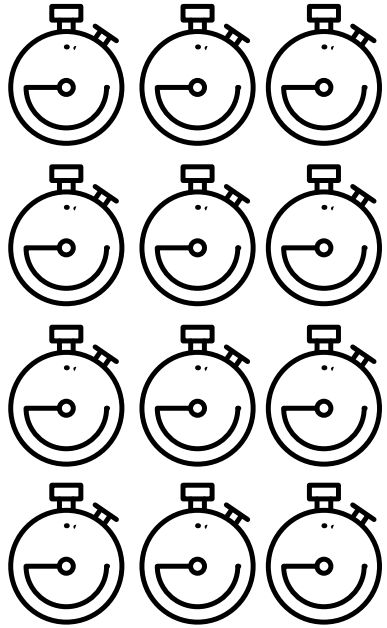


Cyber recovery isn't the same as DR

You don't know **what went wrong**

Attacks are often far **more destructive** than anticipated

Key systems & data are normally **inaccessible and non-trustworthy**



Actual RTO is >12x worse than most anticipated

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

© 2026 Cohesity Inc. All rights reserved.

Ten different outcomes - Preparation & Confidence

Contestant	Preparation	Confidence	Days	How it ended
Žiga Ogorelec Slovenia, 35	Elite — post-doc biologist, runs his own bushcraft school	High	90	Won — first World Champion. Skipped his ferro rod on purpose for an extra item
Aaron Barnard Canada, 40	Strong — lifelong hunter, raised on a hobby farm	High	87	Runner-up. Tapped out from mental and physical exhaustion
Nero Buys Australia, 40	Elite — army veteran (SASR), two seasons as a boreal guide	High	85	Third place. Left on his own terms, goals met
Andrew Price Wales, 51	Elite — 30 years running his own bushcraft school	High	71	Tapped out — cumulative effects of starvation
Jacks Genega United States, 40	Strong — career-changer turned wilderness educator	Moderate	62	Tapped out — smoke-damaged eyes, called for evacuation
Will Longley United States, 37	Strong — traditional Iñupiaq subsistence upbringing	Mixed	30	Tapped out — treated it as a cultural act, not a contest to win
Clementino Pedrosa Portugal, 41	Elite — army paratrooper, published survival author	High	21	Medically evacuated — resting heart rate fell to 34 bpm
Poldi Waldmann-Moloney New Zealand, 24	Moderate — self-taught bowhunter, 100+ big-game harvests	Overconfident	14	Tapped out — oversized shelter build drained his calories
Dave Booth United States, 54	Strong — 23 years as a fishing guide, longtime educator	Moderate	4	Tapped out — accidentally burned his only ferro rod
David Young United States, 31	Moderate - Strong technically — ex-biologist, built his own bow	Low (emotional)	3	Tapped out — homesickness for his wife and daughters

Attackers Continue To Win The Resiliency War. Here's Why.

The threat landscape has accelerated 10x with AI — and most organizations aren't ready

1 Data & Identity Protection

53%
do not backup all workloads

83%
of all attacks target identity systems

80%
lack proper agentic AI protections & guardrails

2 Data Recoverability

62%
do not have a cyber-vaulted copy

63%
Don't have immutable backups

46%
Don't have MFA or MPA enabled on Data Protection Systems.

3 Data Threat Scanning

95%
of ransomware attacks target data protection platforms.

61%
do not subscribe to threat scanning feeds

4 Business Resilience

38%
were reinfected after recovery

45%
do not do annual rehearsals

80%
do not have isolated recovery plans

5 Understand Data Risk

46%
do not have a DSPM strategy – identify sensitive data and critical systems for prioritization and awareness

© 2026 Cohesity Inc. All rights reserved.

Source: Cohesity Global Cyber Resilience Report, November 2026.

Resilience is *packed in*, not found later.

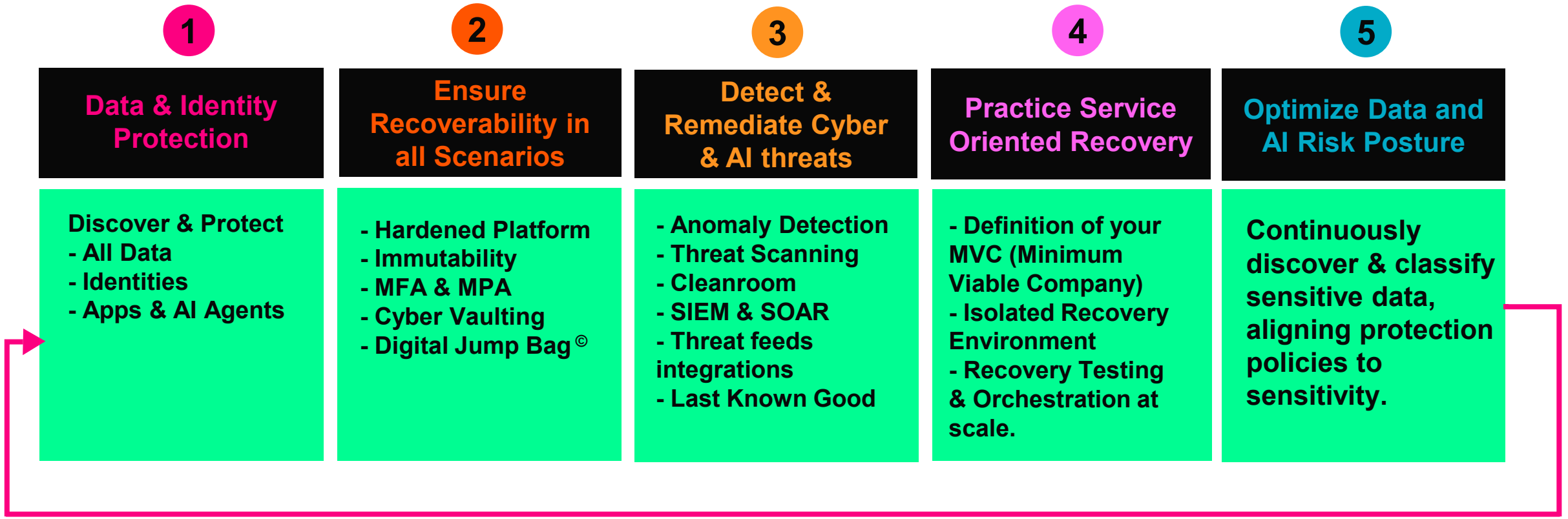
Every contestant carries the same rule: ten items, chosen before they know exactly what terrain, weather, or wildlife awaits. The winning choices are rarely dramatic — a saw over a bow, a fishing kit over a paracord — but they compound daily, turning one early decision into weeks of advantage or hardship.

The resilient outcome is usually traced back to a small, unglamorous decision made under uncertainty, well before the pressure arrived.



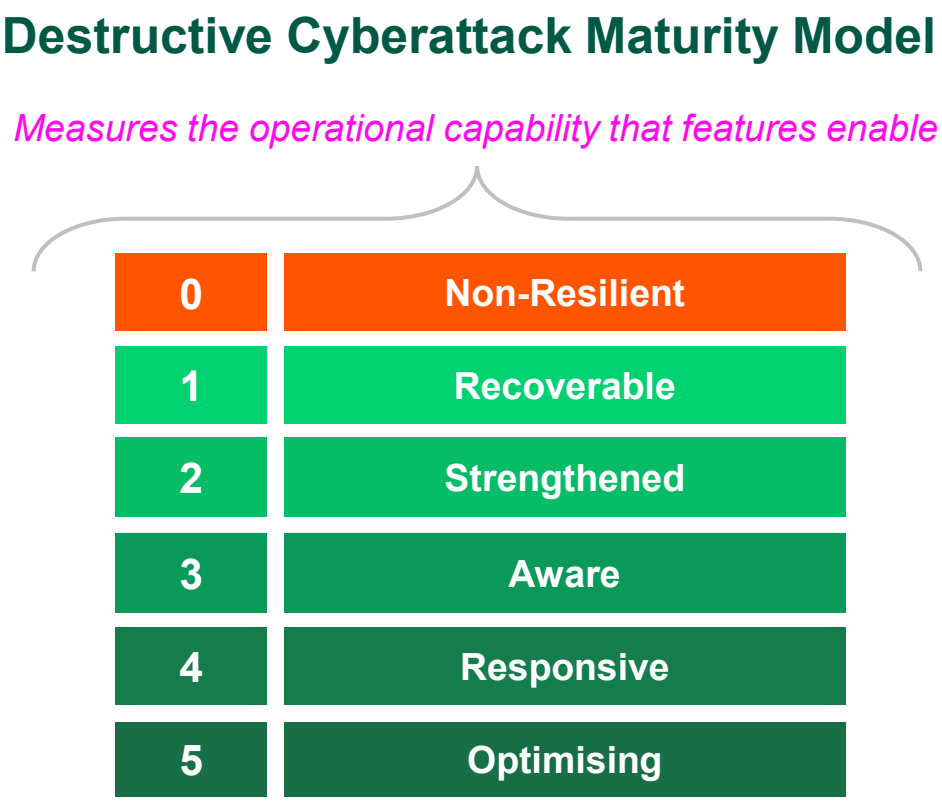
© 2026 Cohesity Inc. All rights reserved.

The Cohesity 5 Steps of Cyber Resilience©



© 2026 Cohesity – Proprietary 5-Step Cyber Resilience Framework

Why a 5 Steps Framework?
The Destructive Cyberattack Maturity Model



Alignment to The Destructive Cyberattack Maturity Model

Cohesity 5 Steps to Cyber Resiliency

Describes an increase in functionality

1. Protect all data, identity, apps & agents
2. Ensure recoverability in all scenarios
3. Remediate cyber & AI threats
4. Practice Service Oriented Recovery
5. Optimize data & AI risk posture

Destructive Cyberattack Maturity Model

Measures the operational capability that features enable

0	Non-Resilient
1	Recoverable
2	Strengthened
3	Aware
4	Responsive
5	Optimising

The 5 Steps achieves cyber response best practices

Aligns with the leading global capability maturity scale (NIST, MITRE, RE&CT, SANS)

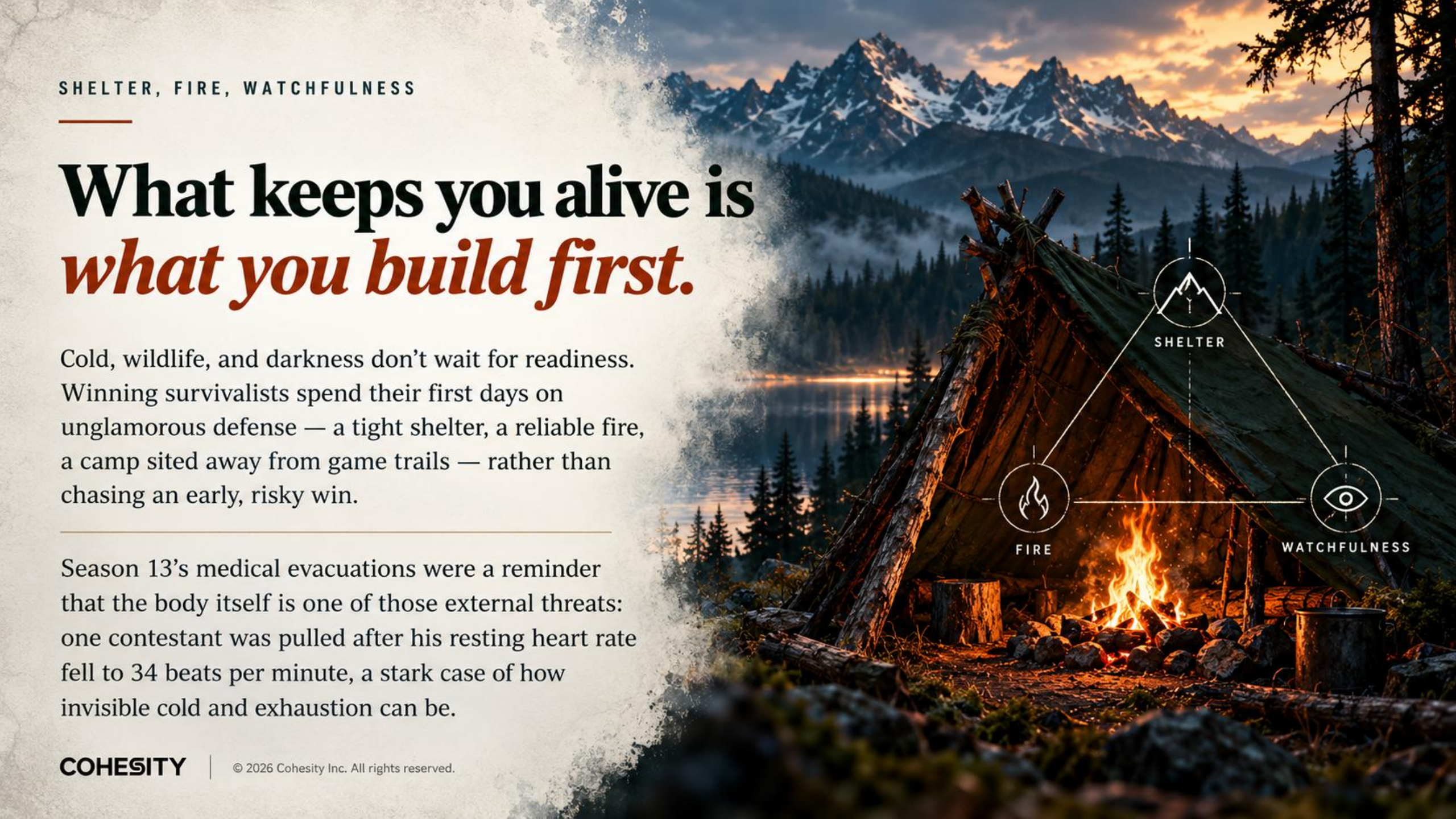
© 2026 Cohesity Inc. All rights reserved.

SHELTER, FIRE, WATCHFULNESS

What keeps you alive is *what you build first.*

Cold, wildlife, and darkness don't wait for readiness. Winning survivalists spend their first days on unglamorous defense — a tight shelter, a reliable fire, a camp sited away from game trails — rather than chasing an early, risky win.

Season 13's medical evacuations were a reminder that the body itself is one of those external threats: one contestant was pulled after his resting heart rate fell to 34 beats per minute, a stark case of how invisible cold and exhaustion can be.



COHESITY

© 2026 Cohesity Inc. All rights reserved.

IDENTITY: ROOT OF TRUST



COHESITY

Identity is under daily siege

Active Directory & EntraID is a major target

83%

Of successful ransomware attacks compromised identity infrastructure[1]

32%

Increase in identity-based attacks[2]

95%

Security incidents involve Active Directory[3]

1 Semperis 2026 Ransomware Risk Report
2 Microsoft Digital Defense Report 2026
3 Cohesity CERT

© 2026 Cohesity Inc. All rights reserved.

Identity: A uniquely challenging workload to recover



AD recovery is notoriously difficult and time-consuming
(Microsoft provides a 29 major steps / 150 page guide to perform a manual recovery).
Do a step wrong during an incident, and start over.



Identity backups are often compromised and-or contain threat actor created
and manipulated human and non-human identities that can be used to re-establish persistence.



Identity cyber recovery drills are complex - ***often skipped, postponed or have never been done***

**Identities needs to be protected with proven proactive security
to be trusted with rapid automated malware-free recovery**

© 2026 Cohesity Inc. All rights reserved.

How Cohesity Supports Identity Resilience

Combining proven technology and deep expertise to build products for identity teams

BEFORE



Continuously monitor and harden AD, Entra ID, and Okta against identity threats and vulnerabilities

DURING



Automated alerting and rollback of malicious and suspicious identity changes that prevent compromise



ADFR that supports automated, parallel DC recovery, decoupled from the OS, and able to target any hardware (physical/virtual) source and target.

Fast, malware-free recovery workflows for Entra ID and Okta.



Advanced post-breach forensics that validate a clean recovery and address backdoors to prevent follow-on attacks

AFTER



Simplified identity recovery testing to meet RTO objectives and enhance readiness

Today's Identity Checklist

"Must Haves" for True Identity Resilience

- [ ] Recovery tools that require no internet access
- [ ] Active Directory backups that are decoupled from the operating system
- [ ] Recovery processes that are automated and require no manual intervention
- [ ] Ability to analyze attack paths leading to Tier 0 assets (including Active Directory and Cohesity storage clusters)
- [ ] Tamper-proof multi-source change tracking & rollback
- [ ] Inventory and monitoring of highly targeted service accounts
- [ ] Active Directory, Entra, and other identity backups that are immutable
- [ ] Ability to recover 'minimum viable business' in hours
- [ ] Guaranteed malware-free recovery
- [ ] Flexible restore targets
- [ ] Pre- and post-breach forensics to evict bad actors
- [ ] 24/7 AD expert incident responders on standby in the event of an attack



COHESITY

© 2028 Cohesity Inc. All rights reserved.

MANAGING AI RISK WHILE UNLOCKING AI VALUE

Protecting, securing, and activating enterprise data for the AI enterprise



COHESITY

Agentic AI: Our Perspective



The fundamental underlying elements required for a trustworthy and resilient AI ecosystem:

- **Data Integrity, Quality & Accuracy**
- **Data Security & Resilience**
- **Identity Governance**

A clear convergence is required to manage today's *machine-speed risks* & ensure organizational level resiliency

COHESITY

Cohesity's Holistic AI Portfolio

AI integration



Cohesity Maestro

Improve resilience & productivity

Protect & Secure agents + data



Agent Resilience, Cohesity DSPM

Recover agents, rogue actions; better compliance

Build AI with better data

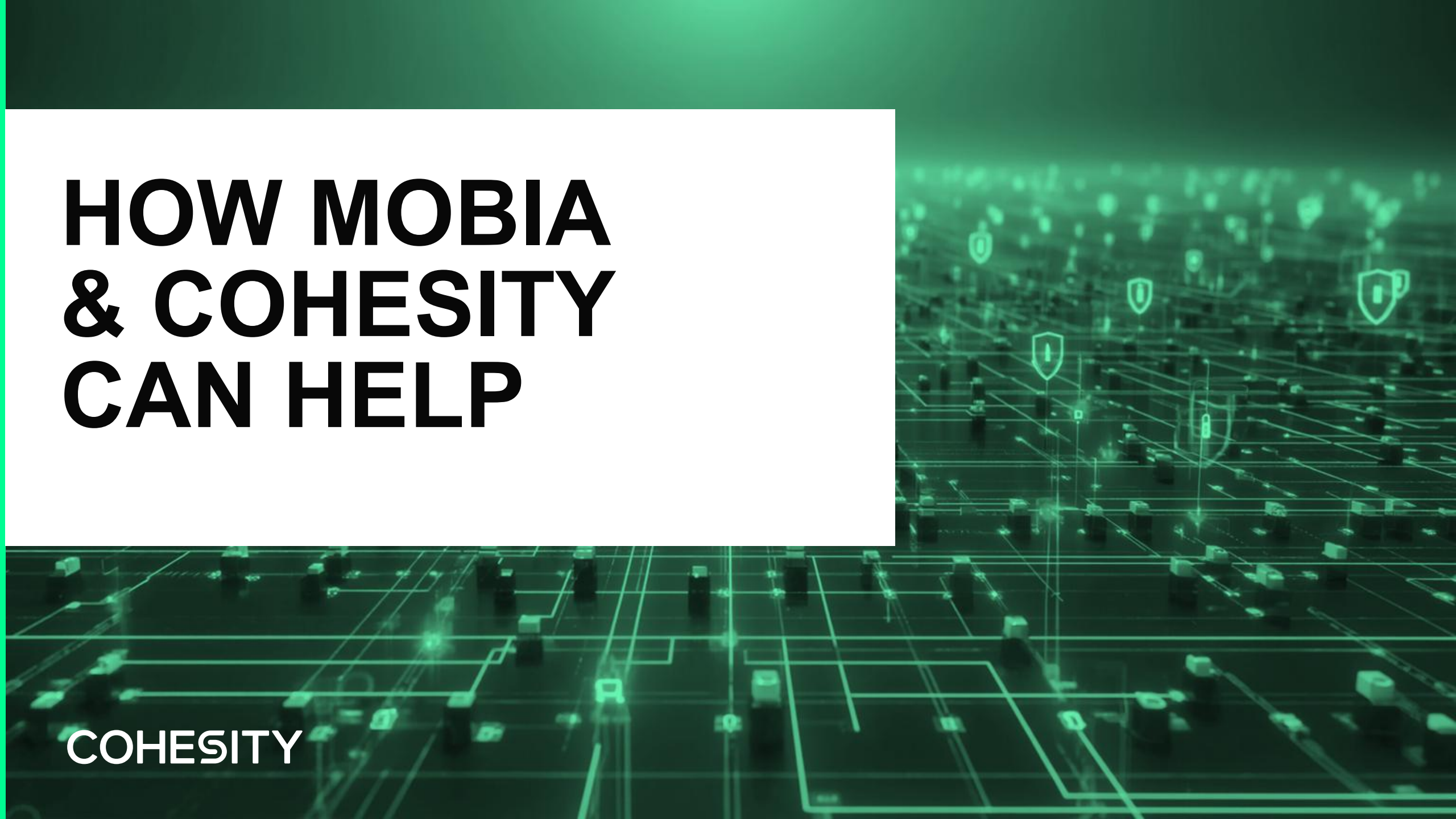


Gaia, Gaia catalog

Faster and lower cost AI on enterprise data

COHESITY

HOW MOBIA & COHESITY CAN HELP



COHESITY

Option 1: Cyber Resiliency Maturity Assessment

Cyber Resiliency Assessment Score

17%

OVERALL

AT RISK

DATA SECURITY, PROTECTION & RESILIENCE

24%

Implemented 3-2-1-1 Data Security Strategy	3
Immutable & Indelible Data Security Storage	5
Isolated Recovery Environment (Air Gap)	0
Secure Repository for Credentials & Keys	0
AD Protection	3
SaaS Workload Protection (M365, Salesforce)	0
Cohesity Integrated Security Storage Platform	0
Data Security Software Version Currency (N-1)	0
Data Protection: 100% Backup Success (SLAs)	0
Digital Jump Bag	0

RISK OF UNAUTHORIZED ACCESS

17%

Encryption Key Management Server	0
Enabled Encrypted Communications	0
Enabled Multi-Factor Authentication	5
Enabled Quorum	0
Configured Least Privilege Access (RBAC)	0
All Data is Fully Encrypted at Rest	0

INTRUSION TO PREVENT BREACHES

12%

AI & ML-Based Anomaly Detection	0
Enabled Backup Image Malware Scanning	0
Audit & System Logs to SIEM	5
Data Classification (DPSM)	0

PEOPLE AND PROCESS

14%

Tabletop Cyber-Attack & Recovery Validation	0
Large-Scale / Multi-Cloud Recovery Validation	0
Automated Cyber Readiness Assessment	0
Onsite Retention Levels Match RPO	5

Score: 0 = Not Implemented | 3 = Partial | 5 = Fully Implemented

Option 2: Identity Security Risk Assessment



Free identity security assessment, powered Purple Knight

Evaluate your Active Directory, Entra ID, and Okta environment to avoid common attacks.

- Audit your hybrid Active Directory/Entra ID environment for security vulnerabilities
- Use expert guidance to remediate security indicators
- Benefit from AD threat intelligence from world-renowned cybersecurity researchers with input from a community of thousands of users
- Guided by identity experts in a free, no-obligation walkthrough



Outcome: detailed list of Indicators of Exposure (IoEs) within your identity environment for your organization to reduce your risk exposure

© 2026 Cohesity Inc. All rights reserved.

COHESITY

RESILIENCE EVERYWHERE

"Our mission is to protect, secure and provide insights into the world's data. We are honored that the world's leading enterprises and governments rely upon Cohesity for resilience. This is fueled by our people-first culture and our breakthrough innovations across cloud,security and AI."

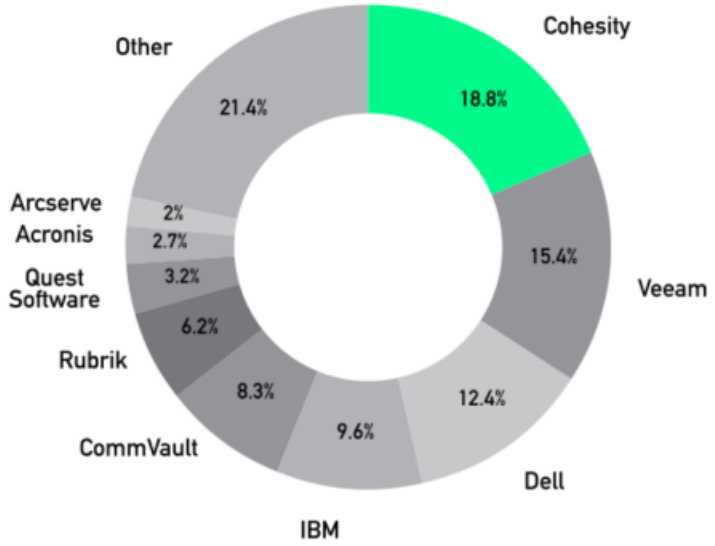


SANJAY POONEN
CEO & President
Cohesity

aws IBM CISCO NVIDIA Hewlett Packard Enterprise

INVESTORS

Cohesity: The Market Share Leader in Data Security Software



Source: 2025 analyst research and internal research

BY THE NUMBERS

13,000+
Total customers

70%
of the Global 500

2x
R&D investment vs modern competitors

200+
Exabytes under management

$1.6B
FY25 ARR

1,700
Patents

LARGEST GLOBAL BRANDS CHOOSE COHESITY

10/10 Banking

8/10 Healthcare

8/10 Manufacturing

8/10 Retail

7/10 Energy


RECOVERY IS ONE THING.
RESILIENCE IS EVERYTHING.