COHESITY



HOW TO BUILD YOUR MINIMUM VIABLE COMPANY (MVC)

Strengthen your cyber resilience and prove you can recover before the next attack.

INTRODUCTION

1. WHY ORGANIZATIONS ARE SHIFTING TO AN MVC

When a cyberattack takes a business down, there's pressure to get everything back at once. It rarely goes to plan: Three in four organizations (76%) still missed their recovery time objective, and on average, recovery took nearly twice as long as their RTO.[1]

A lack of focus is slowing recovery. That's why more organizations are rethinking how they plan for recovery.

Instead of trying to bring everything back at once, they're building a Minimum Viable Company (MVC): the operational capability to restore their most critical services to a trusted state when systems, identities, and documentation are untrustworthy or unavailable. When a destructive attack happens, they'll know which services to bring back first and how to recover them without risking reinfection from compromised systems.

An MVC helps ensure you can stay financially, operationally, and strategically viable during a disruption. You keep serving customers, processing payments, and meeting obligations, even while large parts of the environment are still untrusted.

The bottom line: Defining and operationalizing your MVC before a severe disruption is the most effective way to strengthen cyber resilience.

What's changed? 3 factors driving MVC adoption

Three shifts have made recovery riskier without an MVC.

1. Attacks are more disruptive than ever.

Cyberattacks rarely stay confined to IT systems or focus only on stealing data. In fact, 86% of the major incidents Unit 42 responded to in 2024 caused operational downtime, reputational damage, or financial loss, according to a 2025 report.[2] And the damage doesn't end when systems come back online. Until you know the root cause and how far the attacker reached, you can't assume anything you restored is trusted. Proving that takes time: You have to investigate, remediate, and validate the system before it goes back into production. You can't do that for everything at once. **Someone has to decide in advance what comes back first.**

2. Attackers go after your backups (your last line of defense).

Attackers now target the backup tier, deleting backups and disabling protective infrastructure. In a 2024 Sophos survey of organizations hit by ransomware, 94% said attackers tried to compromise their backups, and 57% of those attempts succeeded.[3] That means the resources and tools you need to respond to threats and rebuild critical services must live in a secure, isolated location. **An MVC gives you the ability to recover from a trusted foundation, out of an attacker's reach.**

3. Regulators expect proof of recovery.

Under rules such as the Digital Operational Resilience Act (DORA) and Network and Information Security Directive 2 (NIS2), regulators expect proof of operational resilience, and boards are holding leaders accountable for downtime and compliance exposure. **You need to demonstrate how your most critical services can come back. An MVC provides that proof.**

The urgency of building your MVC

Defining your MVC is the most important cyber resilience decision you'll make before an attack. Yet only 22% have formally documented and tested an MVC.[1]

If your organization is one of the other 78%, the time to begin building your MVC is now, well before a crisis happens. How you define, build, and operationalize your MVC determines whether your business stays viable during a destructive cyberattack. This eBook shows you how to get it right.

2. DEFINE YOUR MVC: WHAT COMES BACK AND WHAT IT RUNS ON



Begin by deciding what belongs in your MVC. Knowing which services are critical is the input, not the capability. Without the ability to bring them back to a trusted state, you have a spreadsheet, not a capability. Most organizations already know their essential services. The hard part is proving they can trust what they bring back.

Take a top-down approach: Rather than starting with a list of workloads, apps, servers, or systems to restore (bottom-up), start by selecting a handful of critical services necessary to keep the business running. That's not yet standard practice: More than three-quarters of IT and security decision-makers say their plans focus more on restoring systems than on maintaining critical operations and serving customers during recovery.[1]

4 core service categories your MVC must preserve

What makes a service critical? It's a candidate for your MVC when it falls into one of the four categories in the graphic. Be selective about what you include, because the definition of "critical" often expands during a disruption, when everything feels urgent.

The four categories tell you where to look; your impact tolerance tells you what makes the cut. Impact tolerance is the maximum disruption your organization can absorb, usually measured in time and severity. If losing a service would push you past that threshold, it belongs in your MVC. And the faster it would breach that tolerance, the sooner it needs to come back.

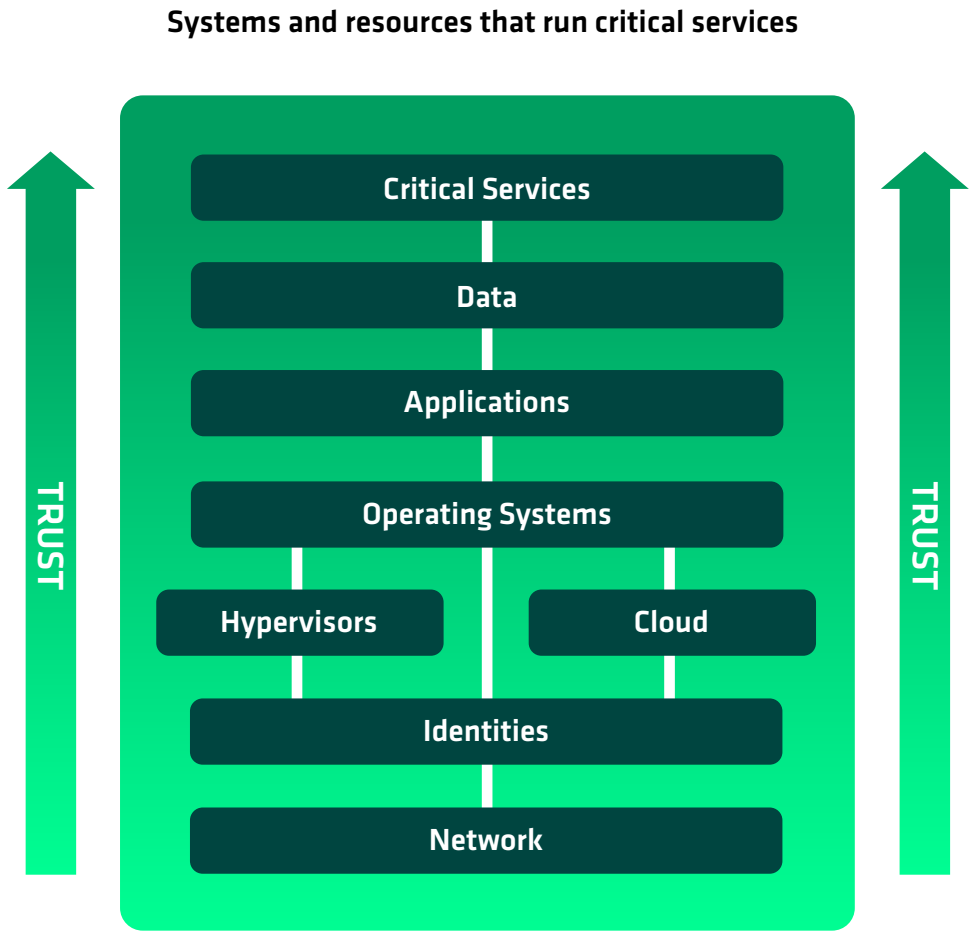


Map what each service depends on

Next, map the dependencies for your critical services. These services run on layers of systems and resources: the network, the identities that control access, hypervisors and cloud, operating systems, applications, and the data itself.

Your map will show you what needs to be trusted before the service can be.

Build your map carefully, because dependencies stay hidden until you need them. Among organizations hit by a material cyberattack, 61% found moderate to significant gaps in how their plans accounted for dependencies.[1]



3. WHAT IT TAKES TO DELIVER YOUR MVC

3 pillars of your cyber resilience

After you've defined your critical services, a natural question follows: What foundational systems and resources do you need to bring them back? Backups ultimately make recovery possible, but your MVC rests on three pillars that work together:

1. PEOPLE

a named owner with the authority and budget to enforce your MVC, plus clear roles for response and recovery, including who declares a system trusted

2. PROCESSES

a defined and well-rehearsed recovery process, automated wherever possible to increase efficiency

3. TECHNOLOGY

the trusted assets and secure environment you need to recover foundational infrastructure



5 technology essentials

The third pillar, technology, needs further unpacking. Your MVC must incorporate these five essential components to bring back critical services.

1. Identity resilience

Every critical service runs on identity, so you'll need trusted user and admin access back from day one. If you restore identity systems while they're still compromised, every service above them inherits the compromise, along with any access an attacker left behind. Treat identity as foundational to recovery and bring it back to a trusted state before you restore data.

Yet 68% of organizations hit by a material cyberattack don't always test identity systems afterward to confirm attacker persistence and access are gone.[1]

2. Digital jump bag™

A digital jump bag™ is a secure, pre-prepared repository of trusted communications, collaboration, and investigation tools and documentation used for initiating incident response when production is unavailable.

Think forensic and log analysis tools, identity recovery tooling, contact lists, insurance policies, and incident playbooks. **Pack it in advance, keep it reachable in minutes, and store it outside the blast radius of your primary environment.**

WHY IDENTITY COMES BACK FIRST

Identity sits behind most cyberattacks. Once attackers compromise your identity services, your entire business can grind to a halt. That's why many ransomware operations target identity infrastructure first.

You can restore your data, applications, and systems, but nothing is usable until identity comes back. Even your recovery tools can require identity to authenticate. Identity is the recovery bottleneck, and that's why it's the foundation of your MVC. It needs to be restored first, fast, and clean.

Once attackers compromise identity, they often leave mechanisms of persistence that can survive a restore. So restoring your identity services alone isn't enough. If identity is restored in a compromised or untrusted state, every dependent service becomes equally untrustworthy and vulnerable to reinfection. They need to come back malware-free and bring back trusted access.

When production is compromised, your jump bag lets you start recovery from a known-good foundation. It also keeps the contacts you'll need within reach: 59% of organizations hit by a material cyberattack were slowed by difficulty reaching third parties or suppliers or by difficulty getting information about their systems.[1]

3. Cyber vaulting and immutable backups

Attackers now target backups to increase the odds of a ransom payment. Cyber vaulting keeps the digital jump bag™, applications, and data your MVC depends on in an air-gapped, immutable vault that's isolated from your backup tier. Even if attackers compromise your backups, you still have a protected, golden copy they can't alter or delete, so you can recover, even in a worst-case scenario.

4. Clean room

If you recover without investigating and addressing the root cause, you risk reinfection and a doom loop: attack, recover, reinfect. Each pass prolongs your downtime and compounds your losses.

A clean room breaks the loop. It gives your team four stages to follow (prepare, investigate, remediate, and mitigate) in isolation, where the attacker can't interfere. You can recover and clean a system to keep its state and recent data, or rebuild it from the vaulted, immutable images and restore your latest scanned data. You recover once, and your business owners get the evidence to decide when each service is trusted enough to run.

5. Networks

In a destructive attack, the network is part of your untrusted infrastructure. It's essential to rebuild segmented connectivity without reopening exposure. Every service you restore depends on the network under it: DNS, connectivity to identity and backup systems, even door access controls.

WHAT SURVIVES WHEN EVERYTHING ELSE IS UNTRUSTED? YOUR CYBER VAULT.

When attackers hit, the recovery plan, the contact list, and the network configuration often sit in systems that are now encrypted.

A cyber vault keeps what you need to start incident response in an isolated, immutable environment or clean room: your digital jump bag, identity systems, application data, configurations, and installation images. If production and backup systems are compromised, the vault is the protected starting point for rebuilding your MVC.

With cyber vaulting, teams can recover vaulted snapshots and digital jump bag assets into a clean room, investigate and validate them, and then restore critical services in the sequence the business has defined.

If the network configuration was changed by the attacker, or never backed up, teams end up rebuilding it from memory mid-incident, and every other recovery step waits on it. Vault known-good network configurations ahead of time, and rebuild from them rather than restoring whatever was running.

4. HOW TO OPERATIONALIZE YOUR MVC

Defining your MVC and putting the essentials in place help get you ready. Operationalizing it keeps you resilient as threats evolve and your business changes.

The Cohesity 5 Steps of Cyber Resilience© framework is our approach to building and strengthening cyber resilience. We developed it from our work supporting thousands of organizations through response and recovery. This framework gives you the structure to build, validate, and optimize your MVC.

Once you've decided which services are critical, the 5 Steps help you build resilience for those services. Practice them regularly, and your MVC becomes a capability you know how to re-create after a disruption.



Cohesity 5 Steps of Cyber Resilience©

The table below shows how the 5 Steps map to your MVC, including where the technology essentials like the digital jump bag™ fit in.



What it does for your MVC	Protects the foundation of your MVC: identity, critical apps, and data, with backups for every critical service	Keeps a prepared jump bag and your MVC data isolated in an immutable cyber vault, so you can recover in the worst case	Gives you governance through the clean room: evidence of root cause and attack surface, and validation before the business runs on anything	Automates jump bag and clean room workflows, so rehearsals are affordable enough to run often and recovery is efficient	Tracks changes to critical services and sensitive data, so your MVC stays within risk tolerance as the business changes
Key actions	Protect jump bag contents (contact lists, known-good configurations, license keys), identity systems, and critical apps and data	Keep the jump bag, critical apps, and data recoverable	Detect and remediate threats against your MVC foundation, before and after an incident	Validate that your MVC foundation comes back first, and threat-free, in a controlled environment	Assess critical applications and sensitive data continuously to keep pace with AI risk
How Cohesity helps	Digital jump bag™, identity resilience, data protection, Cohesity CERT consulting	Platform security, Cohesity FortKnox	Threat Protection	Digital jump bag™, Cohesity Clean Room, identity resilience, data protection, Cohesity RecoveryAgent	Cohesity DSPM, powered by Cyera

Tip: Start with one service

Pick one critical service, assess it across the 5 Steps, and close the gaps you find.
That service becomes the blueprint for the rest of your MVC.

6 questions your MVC must answer

Use these questions to test your readiness:

1. Which critical services come back in the first wave, in ranked order?
2. Do infrastructure, security, and the business share one definition of "trusted"?
3. Who owns the MVC, with the authority and budget to enforce it?
4. Can you recover identity to a trusted state before restoring data?
5. Where is your jump bag, and when was it last updated?
6. Whose sign-off does a system need before it returns to production?

If any of these questions are hard to answer with confidence, you've found a gap to close first.

5. GET GUIDANCE WHEN BUILDING YOUR MVC

An MVC only matters if it works on the day you need it, and the middle of an attack is the worst time to find out it doesn't. Here's how we help you get it right.

The Cohesity CERT (Cyber Event Response Team) MVC Advisory Engagement helps you discover, design, and prove the capability to restore your most critical services. Our cyber resilience consultants have helped hundreds of organizations investigate, contain, and recover from destructive cyberattacks, and they bring that experience to building your MVC.

We combine hands-on advisory with automated discovery that captures your identities, applications, cloud services, networks, middleware, and data stores from more than 70 sources. **You decide what belongs in your MVC based on what's actually running in your environment.**



The Cohesity Six-Phase MVC Methodology

We take you from discovery through design to proof in six phases.

01 MVC scoping and planning

02 Critical service selection and mapping

03 Digital jump bag development

04 Clean room design and recovery environment planning

05 Recovery workflow and playbook development

06 Cyber recovery simulation and validation

Here's what our service delivers:

- **Recovery confidence:** Move from "we think we can recover" to proof that your most critical services come back trusted and operational.
- **Reduced business impact:** Limit the damage of an attack by restoring trust in your critical services within your impact tolerance.
- **Audit-ready evidence:** Show your board and regulators the documented playbooks and simulation results.
- **Repeatable methodology:** Scale from one critical service to the rest of your MVC.



Hear how leading organizations define their MVC

The on-demand webinar **"Prove you can recover data and restore trust: The Minimum Viable Company"** features Cohesity CERT cyber resilience consultants. Learn the executive decisions and operating model shifts that make an MVC real.

WATCH THE WEBINAR

Sources

[1]Cohesity, Global Cyber Resilience Report, September 2026.
[2]Palo Alto Networks Unit 42, 2025 Global Incident Response Report, February 2025.
[3]Sophos, The Impact of Compromised Backups on Ransomware Outcomes, March 2024.

© 2026 Cohesity, Inc. All rights reserved.

Cohesity, the Cohesity Logo, and other Cohesity Marks are trademarks of Cohesity, Inc. or its affiliates in the US and/or internationally. Other names may be trademarks of their respective owners. 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

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

6100037-001-EN 11-2026

