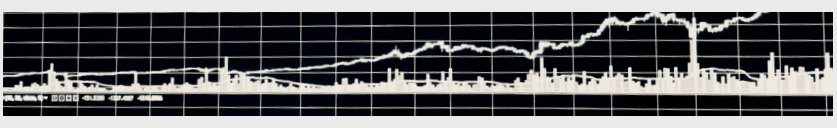
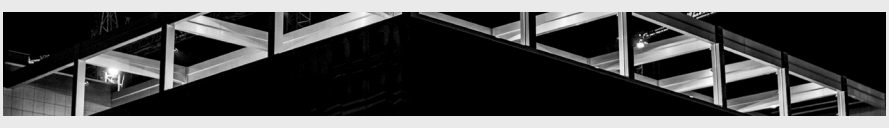
THE IDENTITY RESILIENCE HEALTH CHECK





Modern identity threats move fast – exploiting misconfigurations, escalating privileges, and disrupting access to critical systems. True resilience demands visibility, control, and rapid recovery across the attack lifecycle.

Use this health check to identify what's missing – and what to require from your identity resilience strategy:

1 UNIFY IDENTITY VISIBILITY

Centralize Visibility Across Multi-IdP Environments

Today's fragmented identity landscape demands centralized visibility across platforms.

Implement a single solution that unifies visibility across your identity providers (IdPs), like Active Directory (AD), Entra ID, and Okta. This approach helps simplify operations across hybrid identity environments and maintain consistent policy enforcement, governance, and recovery across providers.

→ Fragmented visibility creates exploitable blind spots.

A unified view helps reduce risk, enforce consistent controls, and give teams the visibility needed to protect and recover identity infrastructure at scale.

2 ASSESS RISK

Know Your Identity Risk Surface

Continuous assessment is essential to uncover misconfigurations, excessive privileges, and hidden attack paths before they are exploited.

A solution that proactively identifies and prioritizes identity risks helps enable you to focus on the exposures that matter most and remediate them before they can be exploited.

→ Unaddressed identity risk compounds over time.

Understanding your risk surface allows you to help reduce exposure before it's exploited – helping limit opportunities for privilege escalation, lateral movement, and widespread compromise.

3 MONITOR CONTINUOUSLY

Detect Identity Threats Early

Identity attacks often leverage valid credentials, allowing them to blend in with normal activity and evade traditional detection.

Implement continuous monitoring and alerting for identity changes, privilege escalations, and anomalous behavior – paired with context to identify what's truly risky.

→ Identity-based attacks hide in plain sight.

Early detection helps reduce dwell time and enable faster responses before threats spread. Solutions that surface high-risk changes and enable immediate action directly from alerts help reduce risk and accelerate response.

4 REMEDIATE QUICKLY

Contain Threats Before They Escalate

Verify your solution helps offer precise, rapid remediation, including instant rollback of malicious or unauthorized changes to a known-good state.

→ Manual recovery is slow, error-prone, and risks reinfection.

Rapid rollback helps restore trusted configurations and reduces lingering risks from unauthorized changes.

5 RECOVER WITH CONFIDENCE

Quickly Restore Identity Infrastructure to a Trusted State

Identity systems are foundational to business operations, and to cyber recovery. If compromised, users can't authenticate, applications fail, and operations can come to a halt.

Look for automated recovery capabilities that can help restore identity systems – from individual objects to full AD forest recovery – using clean, isolated backups and orchestrated workflows.

→ Without trusted identity control, business halts.

Fast, reliable recovery can help minimize downtime and prevent reinfection from compromised elements.

A solution that integrates identity recovery with broader cyber recovery efforts can help further accelerate full business restoration, providing a unified platform to restore identity alongside your critical enterprise workloads.

6 TEST AND VALIDATE READINESS

Prove Recovery Before It's Needed

Establish a consistent testing cadence to help validate identity recovery processes. Use isolated testing environments to help deliver confidence that recovery plans, workflows, and clean restore points are always ready.

→ Untested recovery introduces uncertainty and risk.

Regular testing helps increase confidence that identity systems can be restored to a trusted state quickly and reliably when an attack occurs.

COMMVAULT CLOUD IDENTITY RESILIENCE

A unified platform that brings together risk assessment, real-time auditing and anomaly detection, and automated recovery, designed to allow you to protect and restore identity with confidence.

Find out how Commvault Cloud can help your organization build identity resilience.