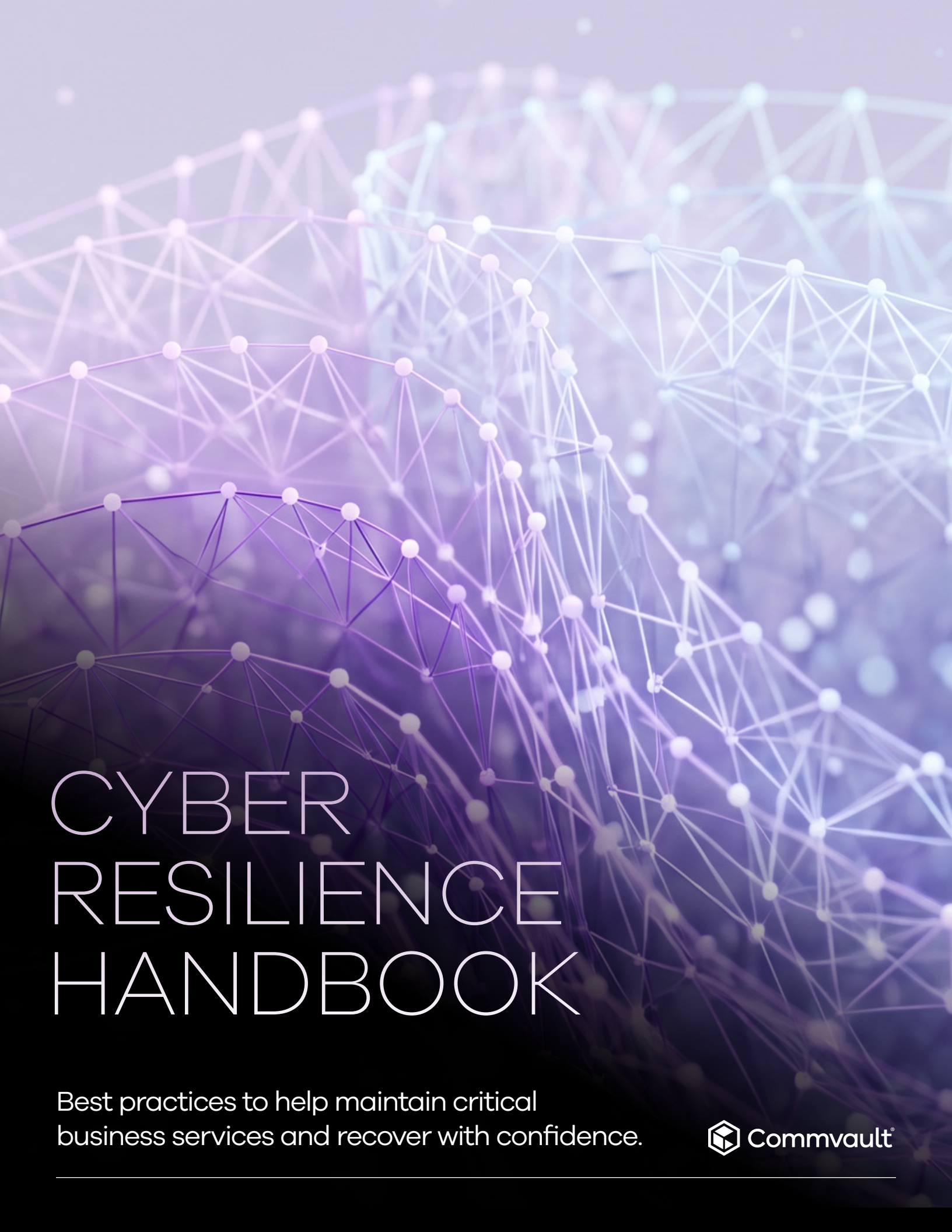

CYBER RESILIENCE HANDBOOK

Best practices to help maintain critical business services and recover with confidence.

Commvault®

OVERVIEW

Being prepared for cyber disruption is crucial in an environment where AI-powered threats, identity compromise, cloud complexity, and increasingly interconnected technology ecosystems are changing the speed, nature, and impact of cyberattacks.

Cyber resilience often requires more than protecting data or restoring systems after an attack. Organizations need to understand which critical business services must continue, what those services depend on, and how teams across the organization will work together to maintain or restore them when disruption occurs.

That starts with defining minimum viability: the minimum level of trusted business operations an organization must be able to maintain or restore during a cyber incident. This means understanding not only critical data and applications, but also the people, identities, infrastructure, AI-enabled services, business processes, and third-party dependencies required to deliver essential services.

57.7% OF RESPONDENTS IN A RECENT IDC SURVEY HAVE NOT DEFINED THEIR MINIMUM VIABLE BUSINESS[1]

However, knowing what must remain viable is only part of being cyber-ready. Organizations also need the operational capability to act when those services are threatened.

This is where ResOps (resilience operations) can come into play. ResOps helps bring together security operations, identity, recovery, infrastructure, cloud operations, business continuity, and business stakeholders around a shared objective: maintaining or restoring trusted business services.

Rather than treating incident response, business continuity, and cyber recovery as isolated activities, ResOps helps teams coordinate priorities, decisions, and recovery actions around what the business needs most.

Cyber recovery is a critical part of that capability. Effective recovery strategies help organizations restore trusted identities, applications, infrastructure, and data following an incident while minimizing downtime and disruption to business operations. Recovery plans should establish not simply what can be recovered, but what must be recovered first, in what sequence, and how teams will validate that the resulting business service can be trusted and safely returned to operation.

Confidence in recovery cannot begin when an attack occurs. Organizations should continuously protect recovery capabilities, monitor threats and dependencies, validate clean recovery points, exercise recovery processes, and confirm that the people and technology required to deliver minimum viability are ready when needed.

1 Resilience Operations: The Discipline That Make Readiness Provable, IDC

A MATURE CYBER RESILIENCE STRATEGY THEREFORE CONNECTS FOUR IDEAS:

- **Minimum viability** defines the critical business services and operating capabilities that must be maintained or restored.
- **ResOps** coordinates the people, processes, decisions, and technologies required to maintain or restore them.
- **Cyber recovery** helps restore trusted identities, applications, infrastructure, and data in business-priority order.
- **Continuous recoverability** provides confidence that those capabilities will work when they are needed.

Regulatory requirements such as GDPR, HIPAA, DORA, and SOCI reinforce the need for detailed cybersecurity, resilience, disaster recovery, and business continuity planning. But the objective extends beyond compliance. A well-designed cyber resilience strategy can help reduce data loss, protect critical information, and limit business disruption. It also can help give customers, stakeholders, and regulators confidence that the organization can continue delivering its most important services even when its technology environment is under attack.

The five steps that follow – **Identify, Protect, Respond, Recover,** and **Monitor** – provide a practical framework for putting that strategy into action.

STEP #01

IDENTIFY

A key principle of any strategy is deep visibility into the environment and an understanding of which apps, systems, and data are needed to deliver minimum viability in the face of outages and cyberattacks.

Commvault® Cloud helps you discover, classify, and monitor sensitive data across all your data stores. The classification of data can then trigger protection policies and help guide organizations toward what is most critical and what requires a different level of protection.

Once you know about the things that must be protected, you can instrument the environment with threat detection, anomaly detection, and early-warning mechanisms to alert security teams to threats in your networks before they cause damage.

You also need a layered approach when it comes to finding and stopping malware, ransomware, and other data corruption vectors. Data should be inspected at all points in its lifecycle to find corrupted data so you can restore it to a clean point in time.

TO SUPPORT IDENTIFY, THE COMMVAULT CLOUD PLATFORM IS DESIGNED TO INCLUDE:

- A unified, comprehensive view of data, workloads, and dependencies across multi-cloud environments from a single data protection platform.
- Data Posture 360 capabilities, which are designed to discover and classify sensitive data – enabling you to better understand and protect your data.
- Threat Scan, which leverages AI to help identify, analyze, and quarantine suspicious files; detect newly encrypted files, and search for Indicators of Compromise (IOC).
- Integrated vulnerability assessment, identity change, and anomaly detection to help track risks across users, groups, and policies in Active Directory (AD).

STEP #02

PROTECT

Protection must be multi-layered. Attackers increasingly target not only production data, but also identities, cloud environments, AI-enabled systems, and the recovery infrastructure organizations rely on to restore operations.

Start with the data. Best practice dictates that organizations follow the 3-2-1 rule: three copies of data, on two types of media or platforms, with one copy that cannot be altered. Backups should be immutable and indelible, with appropriate isolation or air-gapping to help protect recovery copies from ransomware and other threats.

Identity is equally critical. Authentication should follow zero-trust principles and include multi-factor authentication and, where appropriate, multi-person authorization. Identity systems should be securely configured, backed up, and monitored for suspicious changes.

Protection also should extend to cloud and AI-enabled environments, and the third-party services critical business operations depend on. Organizations should monitor for configuration drift, protect sensitive AI data and services, and account for dependencies on cloud, SaaS, AI, and other providers in resilience planning.

Finally, protect the ability to recover. The infrastructure, identities, access paths, and recovery environments teams will need during an incident are themselves critical assets. Keeping those capabilities secure and ready helps teams coordinate effectively and restore trusted business services when protection fails.

TO SUPPORT PROTECT, THE COMMVAULT CLOUD PLATFORM IS DESIGNED TO INCLUDE:

- Unified data protection across multi-cloud, hybrid, on-prem, and edge data.
- AI-enabled, real-time insights to help enhance data protection and resiliency.
- Commvault AirGap to offer a layer of air-gapped, immutable, indelible data protection.
- Adaptive Fabric, a unique architecture that helps automatically spin up and down compute resources to scale resilience operations.
- VaultOS™ operating system to help deliver protected, optimized, hardened deployments.
- Intuitive data governance to help reduce risks.
- Model Context Protocol (MCP) server to help provide a policy-based bridge between enterprise systems and generative AI assistants.

STEP #03

RESPOND

No technology will serve you well in a silo. That's why Commvault Cloud is designed to integrate with security information and event management (SIEM) software and security orchestration, automation, and remediation (SOAR) platforms.

This allows for context sharing between Commvault Cloud and other security tools to better detect security events, data integrity issues, and anomalous activities.

Whether you're using the Palo Alto Networks XSOAR platform, Splunk SIEM, Microsoft Sentinel, or another tool, Commvault Cloud's threat and anomaly detection is a force multiplier in building cyber resilience and improving incident response.

When Commvault Cloud finds suspicious files or receives an anomaly alert from an integration, that file can be quickly quarantined from your production data and a copy sent to a Sandbox for detonation and analysis to determine if it is malicious.

TO SUPPORT RESPOND, THE COMMVAULT CLOUD PLATFORM IS DESIGNED TO INCLUDE:

- Security ecosystem integrations with SIEM and SOAR technologies to share IOCs and events between systems.
- Threat intelligence integrations and the ability to search for specific IOCs to help enable fast, targeted threat hunting.
- Sandbox integrations to enable inspection and detonation of suspicious files.

STEP #04

RECOVER

When it comes time to recover from a cyberattack or other disruption, the goal should not simply be to restore data and systems – it should be to restore trusted business operations.

Your minimum viability requirements should guide what comes back first. Recovery plans should account for the identities, applications, infrastructure, data, and other dependencies required to restore critical business services in the right sequence. Identity may need to come first so users, applications, and services can authenticate securely as recovery proceeds.

Recovery also requires confidence that what you restore is clean. Data and systems should be validated against known-clean recovery points to reduce the risk of reinfection, with the flexibility to restore applications and workloads to alternate infrastructure or cloud environments when necessary.

The worst time to discover that a recovery plan doesn't work is during an attack. Regular exercises should validate not only data and application recovery, but also identity recovery, critical business services, and the people and processes required to maintain minimum viability. Moving toward continuous validation can help provide greater confidence that recovery capabilities are ready when needed.

Effective recovery is a coordinated operation. Security, identity, infrastructure, cloud, recovery, and business teams should understand what must be restored, in what order, and when a recovered service can be trusted and returned to operation.

Finally, preserve affected data and systems as needed for forensic investigation, incident response, law enforcement, cyber insurers, or other stakeholders.

TO SUPPORT RECOVER, THE COMMVAULT CLOUD PLATFORM IS DESIGNED TO INCLUDE:

- Cleanroom for recovery testing, validation, and forensics.
- Threat Scan and Synthetic Recovery™ to help validate that files being recovered are clean and free of malware, ransomware, and corruption.
- Cloud Rewind to help rebuild applications across different clouds, from code to data.
- AD recovery for identity continuity even in the face of a cyberattack.
- Adaptive Fabric for fast, cloud-scale recovery.
- Cleanpoint validation to provide a known clean point in time for you to restore to.

STEP #05

MONITOR

All your planning and readiness only works if you have instrumented your environment to alert security operations and IT teams to anomalies or events across your infrastructure.

Monitoring for threats that have infiltrated your organization and are attempting to evade detection is critical to minimizing the damage they can cause. This is increasingly important as attackers use AI to accelerate attacks and develop new techniques designed to evade traditional detection. The earlier you identify suspicious activity, the sooner you can investigate, contain the threat, and begin restoring affected services.

The challenge with monitoring is that many cyber tools trigger hundreds or thousands of alerts, creating a lot of noise from false positives. AI-assisted detection and analysis can help teams identify meaningful signals and focus investigations, while human oversight remains important for validating findings and response actions.

Production and backup data should be monitored continuously for changes, anomalies, malware, and other IOCs. You also should monitor identity and recovery environments for changes that could affect their ability to maintain minimum viability or recover trusted business services.

You also may benefit from consolidating all monitoring, including threats and anomalies detected by Commvault, into a single platform – in most cases, a SIEM or SOAR tool that is continuously monitored by security operations personnel and used to coordinate investigations and response.

TO SUPPORT MONITOR, THE COMMVAULT CLOUD PLATFORM IS DESIGNED TO INCLUDE:

- Threatwise™ software for detection of attackers performing reconnaissance and traps that provide high-fidelity alerts of a breach.
- Threat Scan to help with continuous scanning of backup data and files for malware and encryption.
- Threat Scan Predict to help discover zero-day or AI-driven polymorphic attacks.
- Security ecosystem integrations to even greater levels of threat intelligence from third-party providers.

SUMMARY

Cyber resilience depends on knowing what your business needs to keep operating – and being ready to protect, respond, and recover when disruption occurs.

01

Identify what you need for minimum viability, including the systems, apps, and data that are critical for your business to operate.

02

Invest in advanced protection, detection, and monitoring tools to enhance your organization's ability to quickly detect and respond to cyber threats.

03

Develop and maintain an up-to-date incident response plan, outlining clear roles, responsibilities, and procedures to follow in the event of a breach.

04

Run full tests to validate you've covered multiple scenarios and can recover trusted business services – and continuously validate that you can do it again.

05

Monitor your systems and backups so that you have confidence they're clean and ready when they're needed.

To see how Commvault Cloud can help with the technology piece of the cyber readiness puzzle, **request a demo and consultation** with our readiness and recovery experts.