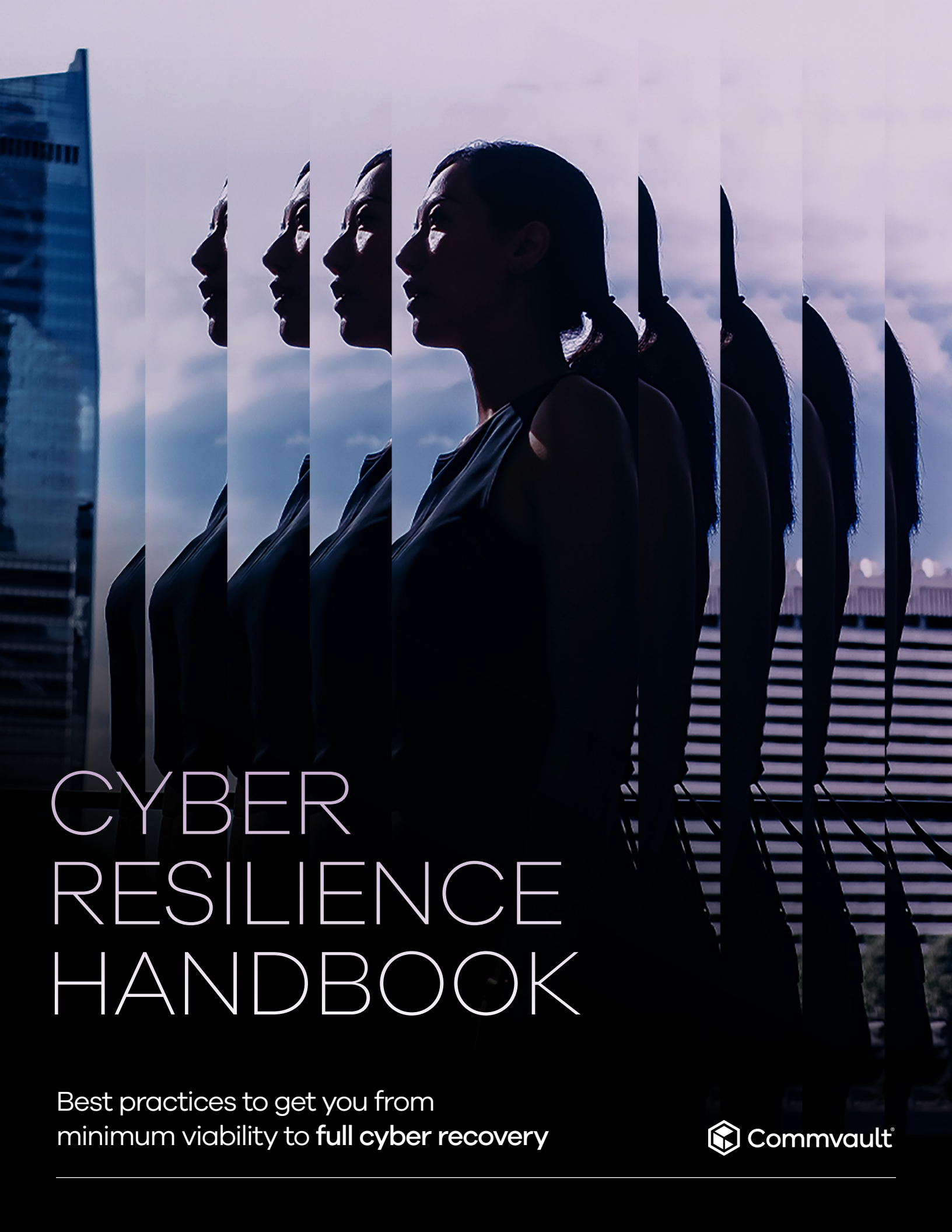

CYBER RESILIENCE HANDBOOK

Best practices to get you from minimum viability to **full cyber recovery**

Commvault®

OVERVIEW

Being prepared for cyber recovery is crucial in today's digital age, where AI-powered cyber threats are increasingly sophisticated and pervasive.

Effective cyber recovery strategies are key to combatting those threats and enabling your business to quickly restore critical systems and data following a cyber incident – minimizing downtime, and mitigating the impact on business operations. By being cyber ready, companies demonstrate to customers, stakeholders, and regulatory bodies that they are serious about protecting sensitive data and the systems that deliver on their commitments to customers.

The first step to building a cyber readiness plan is to identify the mission critical people, processes, systems, and data that are necessary to operate – this is your **minimum viability**.

For most businesses, this includes:

- Executive and operational management.
- An understanding of roles and responsibilities during a recovery.
- The technical ability to restore critical systems, like enterprise identity (Active Directory [AD]), communications channels (email, chat, collaboration tools), and applications that support your mission-critical activities (for example, trading platforms for a financial services company, or electronic medical records for healthcare enterprises).
- The ability to prepare and validate that data, apps, and infrastructure are clean and ready to be recovered and restored from backup.

Beyond compliance mandates (like GDPR, HIPAA, DORA, or SOCI) that require detailed cybersecurity, resilience, disaster recovery, and business continuity plans in place, a well-structured cyber recovery plan reduces the risk of data loss, helping safeguard critical information such as customer details, proprietary data, and intellectual property. In the event of a cyberattack, having a rapid recovery mechanism helps in quickly restoring minimum viable operations and getting systems back online fast.

BOTH COMMVAULT AND GIGAOM UNDERSCORE THE CRITICAL NEED FOR COMPREHENSIVE CYBER RECOVERY STRATEGIES.

Read on to learn about the core components necessary to be ready for a cyberattack – and see how Commvault Cloud delivers the tools to help you succeed, including AI-enabled insights to help you prioritized what to bring back first to maintain operations.

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.

With Commvault Cloud, that includes the ability to 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.

THE COMMVAULT CLOUD PLATFORM INCLUDES:

- A unified, comprehensive view of data, workloads, and dependencies across multi-cloud environments, all from a single data protection platform.
- Intelligent mapping to reveal what's mission-critical, what's vulnerable, and what must be recovered first.
- 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 AD.

STEP #02

PROTECT

To be ready for an inevitable attack, you must protect your data from the actions of attackers, malicious insiders, and even misconfigurations or outages.

This protection is multi-faceted and must take into account the data itself, identity, and configurations. Beginning with the data, best practice dictates that organizations follow the 3-2-1 rule: three copies of data, on two types of media (or on two different platforms), and one copy that's impossible to alter. Duplicating data for the first two steps is straightforward, but the third is a bit more challenging. You need a mechanism to make the data immutable and indelible to protect it from unilateral changes or deletions. This is especially important for two reasons – the majority of ransomware has mechanisms to tamper with backups, and insider threats are real.

You need to validate that your infrastructure (both cloud and backup) is configured according to zero-trust principles. There should be mechanisms in place that check configurations and report and alert on changes or "drift."

Authentication should also follow zero-trust principles and include multi-factor and multi-person authorization, depending on access levels and what actions are being performed. On top of that, any mechanism you have in place for validating identity, such as AD or Entra ID, should also be configured, backed up, and monitored for changes like additions, deletions, or elevation of privileges.

Any data, configuration, or control plane should be backed up to allow for restoration in the event of a security incident, and the backups should be isolated and air-gapped to help reduce the likelihood of attackers finding the backups during reconnaissance or their being deleted or encrypted by malware or ransomware.

THE COMMVAULT CLOUD PLATFORM INCLUDES:

- Unified data protection across multi-cloud, hybrid, on-prem, and edge data.
- AI-enabled, real-time insights to enhance data protection and resiliency.
- Adaptive Fabric, a unique architecture that can 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 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 integrates 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 automatically quarantined from your production data and a copy sent to a Sandbox for detonation and analysis to determine if it is malicious.

COMMVAULT CLOUD PLATFORM CAPABILITIES THAT HELP YOU RESPOND TO THREATS FASTER:

- 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 data, whether from a disaster or a cyberattack, you need a plan that has been practiced and documented; clean, complete data; flexibility of restore targets; the ability to restore everything from the data to the app that uses it; and *speed*.

The worst time to realize your recovery plan isn't going to work is when you're staring down an attack. Conducting regular tests of both minimum viability and full recovery plans is crucial for knowing you can recover when needed, and helps the teams performing the recovery know what is required of them. These tests or practices of the recovery process should check data integrity and be capable of restoring data and rebuilding applications to a new environment.

Portability is important for testing and recovery, as an attack or outage may require you to move entire workloads to a new and different environment. This could mean simply switching accounts or could be as drastic as moving from on prem to the cloud, or to a different cloud entirely – so your recovery needs to be hybrid and flexible.

We already discussed the need for scanning and monitoring of data for anomalies, malware, and other defects. When it comes time to restore, it's important to do one final check of the data to validate that it's clean, ready to restore, and not going to simply reinfect your environment.

Finally, following a recovery, you'll need to keep a copy of the data and systems that were affected by the attack to provide to third-party investigation and incident response teams, law enforcement, cyber insurers, or other interested parties. This forensic copy should be kept separate from your production environment and preserved as is for your investigations. This can help in reverse-engineering malware, identifying the attacker, and identifying techniques and procedures to be prepared for in the future.

COMMVAULT CLOUD PRODUCTS THAT HELP YOU RECOVER:

- Cleanroom Recovery 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 rebuild applications across different clouds, from code to data.
- AD recovery for identity continuity even in the face of a cyberattack.

COMMVAULT CLOUD PLATFORM CAPABILITIES:

- Adaptive Fabric for fast, cloud-scale recovery that's available when you need it.
- 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. The earlier you are aware of them, the sooner you can evict them and restore affected data.

The challenge with monitoring is that many cyber tools trigger hundreds or thousands of alerts, creating a lot of noise from false positives. This leads security operations teams down investigation paths to nowhere, causing burnout and alert fatigue – and taking time away from investigations of real threats. Tuning systems to alert only for true attacks is critical to helping teams focus and find real threats.

Production and backup data should be monitored continuously for changes, anomalies, and malware to help find threats sooner, minimize the risk of additional infection, and restore to known-clean data. This includes the ability to look at behaviors of files, not just the content, so that you can detect never-before-seen attacks.

You also can 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.

COMMVAULT CLOUD PRODUCTS THAT ENABLE CONTINUOUS MONITORING:

- Threatwise™ software for detection of attackers performing reconnaissance and traps that provide high-fidelity alerts of a breach.
- Threat Scan for continuous scanning of backup data and files for malware and encryption.
- Threat Scan Predict to discover zero-day or AI-driven polymorphic attacks.

COMMVAULT CLOUD PLATFORM CAPABILITIES:

- Security ecosystem integrations to add even greater levels of threat intelligence from third-party providers.

SUMMARY

In summation, you need to be aware of the risks that your data presents to your organization.

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 completely.

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.