Commvault

WHITE PAPER

Proactive defense from tomorrow's cyberthreats.

How to combat the growing complexity of cyberthreats!

Commvault

Table of Contents

WHITE PAPER

Commvault

Executive summary

Cyberthreats look different today. From supply chain attacks to AI-powered ransomware-as-a-service toolkits, bad actors are developing new, sophisticated methods that lower the barrier to entry, effectively mine for vulnerabilities, silently bypass perimeter defenses, and compromise their targets faster. To effectively safeguard your business (and data) from emerging threats, today's organizations must think like an attacker, adopting strategies and proactive methodologies that insulate assets from current and future threat vectors.

In this whitepaper, we uncover the common data security missteps in today's cyber era and how proactive defense keeps business data safe from an ever-changing threat landscape.

DATA SECURITY MISSTEPS

The threats

Traditional cyberattacks revolve around data encryption. Commonly called ransomware, their primary objective is to encrypt your data and demand a monetary payout in exchange for restoring access.

Conventional backup and recovery solutions offered businesses a way out. Often referred to as a last line of defense, conventional backup solutions enable organizations to independently restore their data post-attack to avoid lofty ransoms. Understanding this, bad actors evolved their approaches in ways that conventional tools can't combat. The problem? Most businesses didn't notice.

> **Today, 83% of ransomware attacks involve some form of data leakage, exfiltration, theft, or damage.[1]**

From leaking trade secrets to selling sensitive data on the dark web and everything in between, today's cyberthreats are purposefully designed to silently bypass perimeter defenses and inflict pain – in ways that recovery alone can't counteract. Contrary to conventional thinking, tackling this new age of cyberthreats starts with total cyber resilience.

Rather than leaving you flatfooted, this proactive approach picks up where conventional security tools leave off – instilling data resiliency from a new vector of threat – with equal parts identification, defense, and recovery.

The workloads

It's not only how data is being exploited that's changed – it's also where that data lives. Today's businesses have a lot of ground to cover. From multi-generational systems sitting in data centers to modern cloud-delivered solutions, data is more fragmented than ever. And it's not slowing down.

> **In fact, 87% of organizations run multi-cloud environments, with 44% running applications siloed on different clouds.[2]**

This creates one simple challenge: the more places your data lives, the more places you need to protect.

As digital transformation and cloud adoption initiatives continue to accelerate, more data protection blind spots emerge. From neglected workloads to patchwork methodologies, most organizations enlist a deluge of approaches and tools to round out their cyber resilience strategy. The result is mismatched SLAs, over-reliance on native capabilities, and workloads improperly covered, or worse, wholly left behind. For effective data security, modern businesses need comprehensive coverage that uniformly and fluidly protects across on-prem, cloud, and SaaS investments without sacrifice.

1 ComputerWeekly.com, Backups 'no longer effective' for stopping ransomware attacks, February 2022
2 Flexera, 2023 State of the Cloud Report, March 2023

The thinking

As cyberthreats become more frequent and sophisticated, preventing, responding to, and recovering from an attack has become (and rightfully so) a critical focal point within the organizational landscape. Yet, despite increased visibility, data protection is still commonly miscategorized by many. It's often viewed as the transactional process of nightly backups. This flawed thinking puts cyber protection in a box, myopically applying the technology.

While routine backups are part of the game, it's paramount that organizations recognize the irreplaceable and broader role cyber resilience plays within modern cybersecurity strategies. Whether monitoring threats, controlling data access, or rapidly recovering data, cyber resilience sits at a pivotal juncture in the attack lifecycle to contain breaches, limit exposure windows, and drive business continuity.

PROACTIVE, LAYERED DEFENSE

Layered defense, also known as defense in depth, is the practice of implementing multiple tools and measures to protect against a wide range of threats. Each layer has a specific function, working in unison for the multi-faceted protection of customer environments. Commvault applies this principle to cyber resilience, uniquely delivering the right breadth of detection, security, and recovery capabilities to actively secure and defend data while ensuring its recoverability broadly across production and backup environments. Unlike traditional solutions, which are reactionary and only come into play after damage occurs, Commvault® Cloud proactively meets threats head-on to minimize damage, preserve data integrity, and drive stronger business continuity – proven to deliver over a $1 million dollar ransomware benefit across a three year period.[3]

Security

Proven cyber resilience starts at its core. Commvault sets the bar by meeting the most stringent confidentiality, accessibility, and availability protocols for enterprise businesses and government agencies and remains the only cyber resilience vendor to achieve FedRAMP High status (alongside other industry-recognized standards such as ISO 27001, SOC2 Type II, CJIS, and more).

- **Proven architecture:** At an architectural level, Commvault delivers a robust and durable framework across our entire cyber resilience platform. Hardened immutability prevents tampering, alerting, or the destruction of data – while zero-trust authentication and access protocols prevent unwarranted access and lateral movement. Physical and virtual air gaps isolate backup copies in a separate security domain, with data encryption at rest and in transit. This ensures cyber breaches impacting target workloads and environments can't also infect backup copies.
- **User control:** At the end-user level, Commvault Cloud delivers a multitude of tools to prevent misuse. Automated workloads guide users along best practices, while compliance locks, multi-authorization workflows, policy management controls, and more prohibit rogue and accidental actions on data and recoveries. Commvault Cloud continuously monitors backups, providing admins with organic recommendations to further harden and improve the security posture of backup environments.
- **Security integrations:** At the platform level, Commvault Cloud delivers robust integrations with leading SIEM and SOAR platforms. Knowing data protection is a team sport, these bi-directional integrations orchestrate actions that increase visibility into incidents, accelerate response times, and automate countermeasures for additional layers of security. On the credentialing front, Commvault Cloud is the gold standard, providing best-in-class security with leading identity security providers. Using a just-in-time schema, Commvault Cloud securely stores credentials outside of backup environments and applies intelligent privilege controls to reduce the risk of exposure.

 ESG Impact Study,2023

Intelligence

Ransomware is a multi-billion-dollar, global business, and today, AI makes it exponentially more insidious. Go beyond the backup to proactively stop ransomware in its tracks. Commvault® Cloud, powered by Metallic® AI, provides layered defense — minimizing the impact of cyberattacks with early warning and cyber deception, while accelerating recovery with comprehensive threat scanning, remediation, intelligent quarantining, clean recovery validation, and unparalleled recovery speeds.

- **Early warning:** Using patented cyber deception technology, Commvault Cloud surfaces unknown and zero-day threats early in production environments. By intercepting active threats during discovery, recon, and lateral movement, Commvault Cloud uniquely defends and diverts attacks on data and backup infrastructure to kickstart remediation efforts before bad actors reach their targets and it's time to recover.
- **Detection:** Complete visibility means better data decisions. Commvault Cloud provides end-to-end detection and forensics for proactive visibility into datasets. Detailed forensic analysis tools provide validated and sanitized points of recovery and prevent future incidents while simultaneously discovering, quarantining, and deleting sensitive datasets to prevent cyber exposure and potential data exfiltration.
- **Scanning & monitoring:** Data should always be accurate, complete, and reliable. With detailed monitoring baked-in, Commvault Cloud actively surveys backup environments for latent risk, suspicious files, and unwarranted activities impacting data and its recoverability. Robust scanning analyzes datasets to identify encrypted, corrupted, or suspicious files - to remove malware, ensure clean recoveries, and prevent reinfection. Built-in AI-powered anomaly detection and behavior monitoring surfaces insider threats, corrupt data, and malware lurking in datasets to intelligently provide pre-event recovery points. Additionally, AI-driven threat prediction helps find zero day and polymorphic malware threats (or AI-driven malware) that have already impacted backup content so you can quarantine and recover data cleanly while avoiding reinfection during recovery.

Recovery

Businesses must assume they will be breached. It's imperative that recovery is at the heart of their cybersecurity posture. Commvault Cloud secures the recovery—ensuring that data can be restored from anywhere to anywhere, rapidly, reliably, and at massive scale. This ensures your data is secure and available wherever it lives, with powerful AI-driven automation to verify clean recovery points and unparalleled scaling to recover data faster than the competition at the lowest TCO.

- **Cyber recovery:** Cyber defense doesn't happen without cyber recovery. Commvault Cloud's flexible recovery controls rapidly restore data to eliminate downtime and maintain business operations allowing for any to any recovery across platforms and locations. Businesses get full-fidelity and flexible recovery options to recall individual datasets or entire environments with speed, precision, and scale. Coupled with trusted warm disaster recovery capabilities, Commvault Cloud solutions can instantiate the systems needed only when facing mass recovery incidents – without dedicating costly standby infrastructure.
- **Cloudburst recovery and cleanrooms:** Commvault Cloud offers an unfair advantage against cyber attacks with Cloudburst Recovery by combining infrastructure-as-code and cloud scaling to ensure fast, predictable, and reliable cyber recovery at scale. And ensure your data is always safe, clean, and recoverable from a guaranteed malware-free cloud environment with cleanrooms.
- **SLA compliance:** Meet internal and external regulatory standards. With Commvault Cloud, businesses can eliminate disparate and niche solutions for standardized SLAs and compliance across entire data estates. Achieve extended retention and exceed data recovery objectives for unrivaled SLA compliance when facing data loss, while integrated archival and eDiscovery capabilities support the fulfillment of legal and regulatory needs.

Want to learn more about proactive defense from Commvault? See how **Commvault Cloud** safeguards your organizational data from advanced threats while fortifying your cyber response strategy.