WHITE PAPER

COMMVAULT

Proactive Data Protection from Tomorrow's Cyberthreats

How to combat the growing complexity of cyberthreats!

Table of Contents

CONTENTS

WHITE PAPER

COMMVAULT

Executive Summary

Cyberthreats look different today. From supply chain attacks to 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 protection missteps in today's cyber era and how proactive data protection keeps business data safe from an ever-changing threat landscape.

DATA PROTECTION 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 a redefined look at data protection.

Rather than leaving you flatfooted, this redefined 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 data protection strategy. The result is mismatched SLAs, over-reliance on native capabilities, and workloads improperly covered, or worse, wholly left behind. For effective protection, modern businesses need comprehensive coverage that uniformly and fluidly protects across on-prem, cloud, and SaaS investments without sacrifice.

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 data protection in a box, myopically applying the technology.

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

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

PROACTIVE, LAYERED DATA PROTECTION

Layered protection, 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 data protection, 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 conventional data protection approaches, which are reactionary and only come into play after damage occurs, Commvault 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]

Secure

Proven data protection 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 data protection 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 data protection service. 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 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 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 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 is the gold standard, providing best-in-class security with leading identity security providers. Using a just-in-time schema, Commvault securely stores credentials outside of backup environments and applies intelligent privilege controls to reduce the risk of exposure.

Defend

Cyberthreats are sophisticated (and successful). Why wait for data to be compromised to recover? With patented early warning, end-to-end observability, and robust monitoring baked-in, Commvault proactively safeguards production and backup data so businesses can respond, limit exposure, and minimize the need to recover.

- **Early warning:** Using patented cyber deception technology, Commvault surfaces unknown and zero-day threats early in production environments. By intercepting active threats during discovery, recon, and lateral movement, Commvault 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.

[3] ESG Impact Study,2023

- **Detection:** Complete visibility means better data decisions. Commvault 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 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.

Recover

Hybrid IT isn't an interim state. It's a way of life for today's organizations. Whether journeying to the cloud, repatriating environments back on-prem, or tackling new mergers and acquisitions, data is in new places – which all need protecting. With ubiquitous recovery across workloads Commvault helps companies improve business continuity and decrease costs in the face of evolving cyberthreats.

- **Broadest coverage:** Commvault offers the broadest coverage of on-premises, SaaS, and cloud-native workloads from a single pane of glass for the highest level of business continuity across enterprise data. With unmatched cloud, software, or appliance delivery models, coupled with proprietary and bring-your-own storage options, businesses of every size get optimized cost and performance to keep data safe and recoverable from threats. Commvault data protection adapts to your business and easily meets evolving needs without risking expensive data loss due to gaps in coverage.

- **Rapid recovery:** Cyber defense doesn't happen without cyber recovery. Commvault's flexible recovery controls rapidly restore data to eliminate downtime and maintain business operations. 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 solutions can instantiate the systems needed only when facing mass recovery incidents – without dedicating costly standby infrastructure.

- **SLA compliance:** Meet internal and external regulatory standards. With Commvault, 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 data protection from Commvault? **See how Commvault** safeguards your organizational data from advanced threats while fortifying your cyber response strategy.