COMMVAULT

SOLUTION BRIEF

What is Zero Loss Strategy?

Introduction

The cybersecurity reports and statistics make one thing clear: it's highly likely you will experience a cyberattack. However, how that impacts your company depends on your confidence in answering:

- Are your organization and employees prepared for a cyberattack?
- Do your teams know their roles, and will they work together?
- Who has the authority/decision-making power to make time-sensitive decisions such as shutting down servers or networks?
- As an executive, are your business leaders in sync, and how will you keep them informed?
- How many different business units and partners are involved in an incident response plan?

Protecting your organization against ransomware is like gambling in a casino.
"If you gamble long enough, you're certainly going to lose."
Scott Adams | Creator of the Dilbert comic strip

Data security is vital to protecting your organization from a ransomware attack. You need a data protection solution that can keep up with the evolving needs of your organization and ensure you are able to restore your data quickly to resume business operations if you do get hit with a cyberattack. Why? Successful restores are critical to your survival, whether you pay a ransom or not. Based on 35% of data remaining encrypted after the ransom was paid,[1] you still depend on your ability to restore your files successfully.

To mitigate the impact of ransomware attacks, organizations require a solution that expands beyond zero trust principles. Commvault introduces a Zero Loss Strategy that is built on multilayered security for consistent and automated ransomware protection and recovery processes. It helps mitigate the impact of data sprawl and protects workloads with flexible recovery options. With Commvault, you have the broadest workload and application protection, and rapid recovery across cloud and storage platforms through a unified customer experience.

1 Sophos, The State of Ransomware 2021, April 2021.

COMMVAULT

SOLUTION BRIEF

Zero Loss Strategy

Zero Loss Strategy is designed to help you better plan, manage, and reduce the impact of ransomware and cyberattacks. It is a strategy for your organization to incorporate and is built on zero trust principles and implemented through our multilayered security framework to help you remain vigilant against bad actors. The foundational areas of Zero Loss Strategy are:

- **End-To-End Data Visibility.** With a single management platform, identify business-critical and sensitive data, reduce your attack surface, and minimize risk exposure. Easily set and manage data protection policies through an intuitive interface and protect your data with encryption, immutability, and air-gap backup copies for complete ransomware protection.
- **Broadest Workload Protection.** Actively monitor your data and leave no workload behind. Commvault supports the industry's broadest workload coverage from SaaS applications to endpoints, databases, virtual machines, containers, and more for complete ransomware protection. Expand your workload functionality while reducing multiple tools and point products, minimizing complexity and cost through a scalable approach.
- **Faster Business Response.** Speed and accuracy are essential to respond to a ransomware attack effectively. Accelerate your recovery through our single management console with scalable, automated workflows, consistent processes, and flexible restore options. Eliminate complex manual tasks and staff frustration caused by using multiple point products and tape backups. A common console and unified customer experience that spans all your data – regardless of location – further accelerates response.

Zero Trust Principles. Using a multilayered security framework and zero trust principles, Commvault protects your data and environment through secure user accounts, access controls, and leading key management systems integration. In addition, centralized management and monitoring of real-time events and activities and integration with leading security tools help provide complete ransomware protection and recovery.

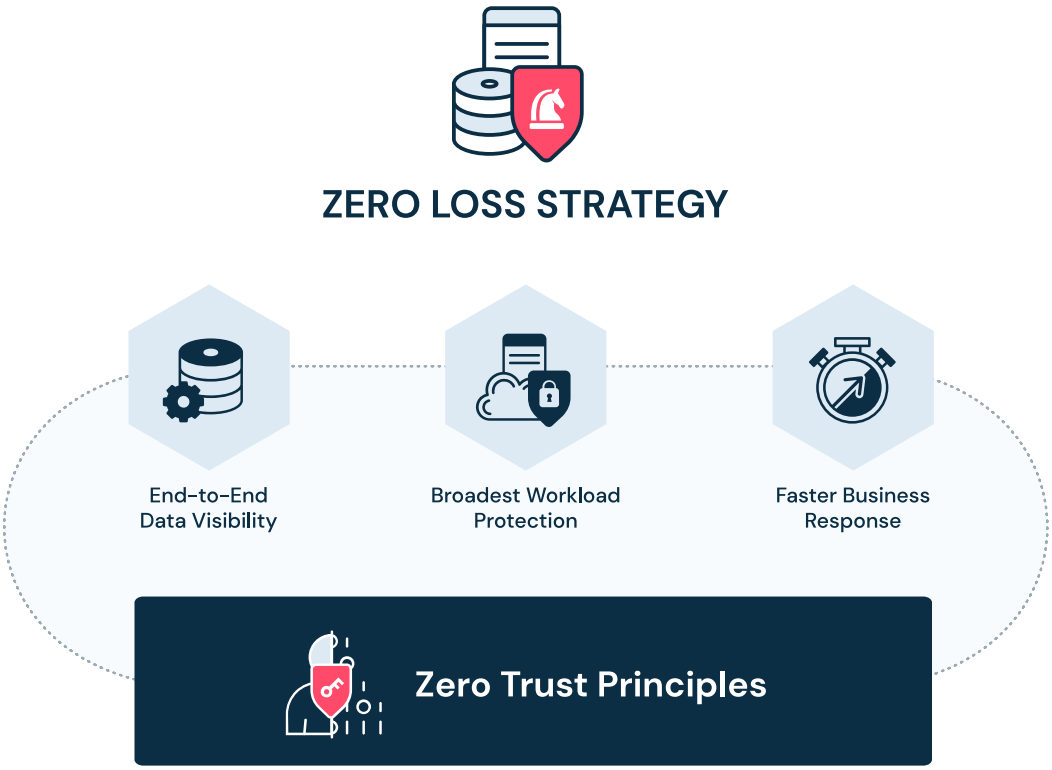


Figure 1: Zero Loss Strategy comprises foundational areas that build upon zero trust principles.

COMMVAULT

SOLUTION BRIEF

END-TO-END DATA VISIBILITY TO BETTER PROTECT YOUR DATA

You can't protect what you can't see. You need to have visibility to all your data, whether it resides in the cloud, edge, or on-premises.

You need to catch threats for ransomware protection before they impact your data. With Commvault, you gain the best end-to-end data visibility to identify business-critical and sensitive data, reduce your attack surface, and minimize risk exposure for data loss. Only Commvault can continuously monitor abnormal activity in backup and live data environments. Easily view ransomware or suspicious activities through the security dashboard, set and manage data policies through our intuitive interface to protect your data with encryption, immutability, and air-gapped backup copies. With a threat monitoring framework that uses machine learning for anomaly detection and honeypot technology, you receive early warning alerts of suspected malicious activity for faster response.

With Commvault data protection and management, you gain:

- **Centralized management** to easily view ransomware or suspicious activities through a security dashboard.
- The ability to **identify business-critical and sensitive data and protect** it with the appropriate policies, reducing the risk of data compromise or leakage.
- **Live monitoring** for early detection of abnormal activity in backup and live data environments.
- **Early warning alerts** through a threat monitoring framework that uses machine learning for anomaly detection and honeypot technology.
- **Rapid identification of exposed or breached data,** including support evidence gathering and audits to address compliance needs that follow a major breach.

Know your vitals: Security Health Assessment Dashboard

Through our single console, Commvault Command Center™, you can easily monitor your security health with our Security Health Assessment Dashboard. The dashboard allows organizations to identify, assess, mitigate, and monitor security controls within the Commvault data protection environment (Figure 2). The dashboard identifies available controls and provides scoring and remarks to help you assess risks properly and continuously monitor your security posture.

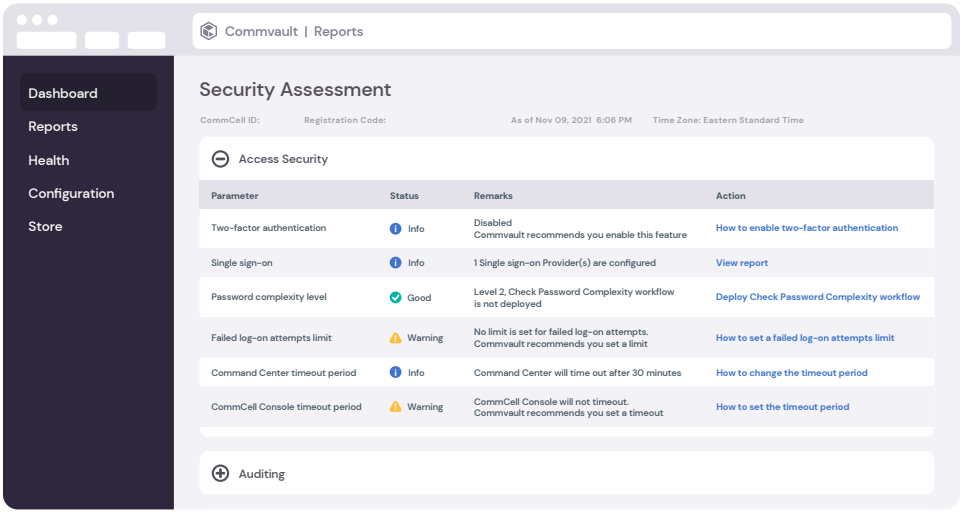


Figure 2 – Commvault Security Health Assessment Dashboard.

> **"The way this ransomware came in bypassed our visibility, but the Commvault software was vigilant, monitoring our backups every night. It saw the encrypted files first and flagged the activity for alert."**
>
> Don Wisdom, Sr. Director of infrastructure Operations
> State of Colorado

COMMVAULT

SOLUTION BRIEF

BROADEST WORKLOAD PROTECTION TO REDUCE THE ATTACK SURFACE

With a business environment that is constantly changing and cyberthreats expanding, you need a solution that automates and scales data protection, facilitates migration, and enables flexible management. With a single solution to manage and protect all data as it's moved, managed, and used across workloads, you can eliminate data fragmentation and reduce the attack surface.

Many organizations find that their data protection strategy can't easily expand to cover modern and hybrid cloud use cases. Next-generation workloads, including cloud-native applications like Kubernetes and SaaS, were adopted in response to the shift to working from home. Moving to these workloads can be daunting, but having a solution that protects your data throughout this transformation will give you peace of mind. What's needed is an overarching data management and protection solution that supports the entire diverse technology stack, including data and workloads from prior, current, and future generations.

"Commvault provides granular and comprehensive protection of a broad range of workloads regardless of whether they are hosted on-premises or public cloud IaaS and PaaS."

Gartner, Critical Capabilities for Enterprise Backup & Recovery Software Solutions | Read

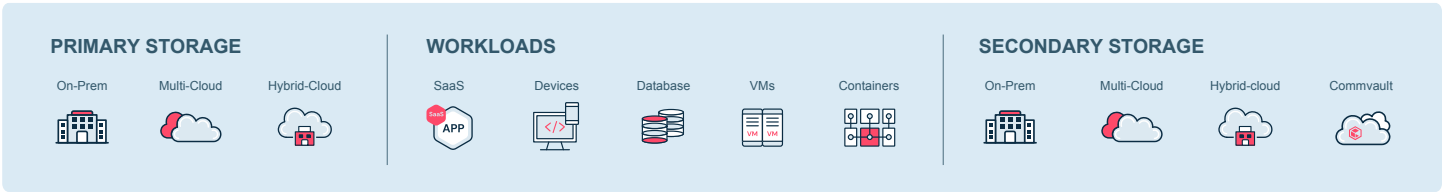
Thanks to unmatched workload coverage, Commvault reduces more of your attack surface than anyone else by eliminating gaps in your protection, detection, and recovery strategy with support for on-premises, cloud, and SaaS applications. In the unfortunate event your organization does get hit with a ransomware attack, with Commvault, you have the flexibility to restore your workload to any target. In addition, you don't have to add more complexity when migrating to or simply adding new workloads and applications. Commvault covers your data with:

- Exceptional workload support across on-premises, cloud, and SaaS applications.
- Native integration with cloud, applications, and databases.
- Flexible and consistent service levels to protect all your workloads.
- Industry-leading support for legacy applications, mainframes, modern applications, and containers.
- The ability to restore any workload to any target, cloud, or on premises.

"The simplicity and scalability of Commvault and Metallic™ solutions empower us to protect diverse workloads via a single pane of glass without deploying multiple applications."

David Ben-Eli, System IT Infrastructure Manager | Harel Insurance

INDUSTRY'S BROADEST WORKLOAD COVERAGE



FASTER BUSINESS RESPONSE WITH CYBER RECOVERY

Speed and accuracy are essential to responding to a ransomware attack. It takes the average organization 22 days to recover from a ransomware attack.[2] But you don't have three weeks. Your CEO and board of directors measure your ransomware recovery plans and return to business operations in days, not weeks.

Security-conscious organizations trust Commvault for data recovery and to get their business back up and running in no time. Commvault ensures you have clean backup copies to avoid business interruptions and minimize risk by automatically isolating suspected files, preventing backup copies from retiring, and protecting your proprietary applications. In addition, Commvault Ransomware Services provides the resources and expertise to accelerate returning to normal business operations after a data loss event through your environment's proper design, implementation, and support.

Commvault helps with faster restores through:

- Operational efficiencies that consolidate data management through a single user interface.
- Quickly bringing the cloud into your security strategy. The Metallic™ Cloud Storage Service makes it simple to adopt air-gapped cloud storage.
- Streamlining recovery operations through machine-learning-driven automation and orchestrated workflows.
- Avoiding ransomware file reinfections by helping you surgically delete suspicious or unnecessary files to ensure a clean and secure recovery. Quickly isolate suspected backup copies or restore them to a safe location.
- Consistent recovery processes across all data and workloads with automated restore to on-premises, cloud, or wherever the data is needed.

"If we had not already converted to Commvault, we probably would have been weeks trying to get everything back. We were able to do it in 12 hours."

Steve Davidek, Information Technology Manager | City of Sparks

ZERO TRUST PRINCIPLES: TRUST, BUT VERIFY

Organizations need to follow zero trust principles to ensure cyberthreats do not have unlimited access within their networks. It is fundamental to every organization's proper cyber hygiene.

Commvault supports the core zero trust principle of trust, but verify. Built on zero trust principles and a multilayered security framework, Commvault uses these as the foundation for you to incorporate a Zero Loss Strategy, which the other three areas build upon.

2 Stastica, Joseph Johnson, Average duration of downtime after a ransomware attack from 1st quarter 2020 to 3rd quarter 2021, November 2021.

Commvault provides multiple layers of authentication controls to stop malicious actors, insider threats, and even unintentional accidents from deleting backup data. Based on your user role within the Commvault environment, multi-factor controls restrict and block potentially dangerous actions and require elevated authorization. Our Security Health Assessment Dashboard provides continuous awareness when locks, alerts, and controls are not applied or disabled. This includes any new feature sets that become available in the future that Commvault may recommend.

In addition, Commvault provides additional layers of data protection:

- Integration with detection, analytics, and security response tools such as Security Incident Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR).
- Easy implementation of a 3-2-1 data protection model for greater resiliency and recoverability.
- Maintain strict access controls and secure user data access and controls with Multi-Factor Authentication options.
- Overall attack surface reduction by isolating networks and data management using multitenancy functionality.
- Securely air gapping of your backup copies to easily isolate and segment storage targets from public networks to mitigate lateral threat movement.

"Thanks to the encryption and security feature with Commvault, it gives us confidence that our backup copies are in a complete locked state and cannot be touched in the event of ransomware attacks."

Sachin Jain, CIO & CISO | Evalueserve

Conclusion

Organizations must remain vigilant and on top of their ransomware game. Zero Loss Strategy with a multilayered framework helps:

- Ensure data integrity through end-to-end data visibility that helps identify threats before they happen.
- Minimize complexity and easily scale with the industry's broadest workload protection.
- Save valuable time and recover quickly with certainty through our single management platform.
- Implement a Zero Loss Strategy to continuously plan, identify, and monitor data across any workload, with a faster response time and flexible restore options to fight ransomware.

Learn more about Zero Loss Strategy. Visit **commvault.com/ransomware >**