Solution overview



Protecting your enterprise from ransomware with HPE and Commvault



Table of contents

2 **Introduction**

2 **Protection and recovery across the stack**

3 **Developing a ransomware protection strategy**

- 1. Harden the protection environment
- 2. Maintain multiple recovery copies
- 3. Isolate and secure backup data
- 4. Detect threats and identify trusted data
- 5. Recover cleanly and rapidly

6 **Summary**

Introduction

As ransomware threats grow more sophisticated, organizations face increasing pressure to protect business-critical data and maintain recovery readiness. At the same time, AI and other data-intensive initiatives are expanding the volume, value, and distribution of enterprise data across data centers, edge, cloud, and SaaS environments. Fragmented protection across this growing data estate can create gaps in visibility, inconsistent policies, and uncertainty about whether critical data can be recovered.

Backup remains a critical line of defense, but backup alone does not guarantee recovery. If attackers compromise production systems and connected backup environments, organizations may be left without a trusted recovery point when they need it most. Effective ransomware resilience requires hardened infrastructure, protected and isolated copies, early threat detection, and the ability to validate and restore clean data rapidly.

Protection and recovery across the stack

HPE provides secure, resilient compute and storage infrastructure for protecting and recovering critical data. Commvault applies intelligent threat detection, policy-driven protection, and clean recovery across hybrid environments. Together, they connect infrastructure resilience with data protection and cyber recovery, helping organizations preserve trusted recovery options, minimize disruption, and restore critical operations with confidence.

97%

of organizations whose data was encrypted were able to recover it. The challenge is no longer whether recovery is possible, but whether organizations can recover cleanly, quickly, and with confidence.[1]

[1] Sophos-state-of-ransomware-2025.pdf

Developing a ransomware protection strategy

Breaches are the new operating condition, and resilience is the new imperative. HPE and Commvault recommend these five core tenets as essential for comprehensive ransomware protection:



1. Harden the protection environment

Security starts at the foundation. That means it's imperative for security to be at the core of the infrastructure.

HPE servers incorporate security capabilities such as silicon root of trust to help protect firmware integrity and strengthen infrastructure security. It allows for the integrity of the firmware to be verifiable at all times and enables restores from the last known clean state in case the firmware is compromised. There are also advanced alerting capabilities if someone attempts to physically access the server hardware by opening the access panel.

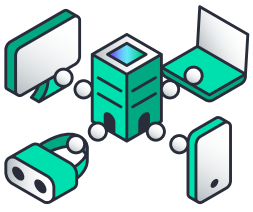
Commvault software is built on a hardened foundation that utilizes the authentication, authorization, and accounting (AAA) security framework:

— **Authentication**—Commvault integrates with secured Lightweight Directory Access Protocol (LDAP)-based directory services and external identity providers through Open Authorization (OAuth) and Security Assertion Markup Language (SAML) protocols. Commvault also supports 2-factor authentication, credential encryption, impersonation, and just-in-time credentials for backup services, certification authentication, and zero trust controls.

— **Authorization**—Fine-grained authorization controls the level of access granted to authenticated users based on their roles and needs.

— **Accounting**—Commvault tracks and audits users' data access and capabilities regularly.

Together, HPE and Commvault provide layered security controls that help reduce vulnerabilities and strengthen protection for critical workloads and backup data.



2. Maintain multiple recovery copies

Multilayered data protection using the 3-2-1-1 rule continues to be crucial. Store three copies of your data on two different media types with one stored off-site and one stored offline. Organizations using both disaster recovery and backup solutions to create a multilayered ransomware defense are able to remediate risks and become operational much faster post-encryption. End-to-end data protection solutions, such as those offered by HPE, let you easily adopt the 3-2-1-1 rule to help keep data secure, and increase application uptime and data availability for your business.

HPE and Commvault help automate protection policies and recovery copies across hybrid environments, reducing the operational complexity of protecting data wherever it resides. When data is backed up, it is also copied automatically to secondary (or tertiary) destinations, as feasible, where Commvault continues to manage it throughout its lifecycle. Commvault helps automate backup policies, secondary copies, and retention management across supported environments, reducing manual effort and helping organizations maintain consistent protection.



3. Isolate and secure backup data

Cybercriminals may target recoverability by encrypting, modifying, or deleting production data and backup copies. In the case of data modification, ransomware changes storage blocks, and backup systems can inadvertently capture and retain the altered, now-encrypted data.

Immutable backups help keep protected data beyond the reach of attackers. Commvault retention and WORM storage controls, combined with immutable capabilities on supported targets such as HPE StoreOnce Systems, help prevent backup data from being encrypted, modified or deleted during its configured retention period. Encryption and layered access controls provide additional protection against unauthorized access and tampering.

An air gap, also called an air wall, is a security measure that protects data from intrusion. The concept is simple: any device that isn't connected to a network cannot be attacked remotely. One of the challenges of on-premises data protection solutions is that they are exposed to the same threat as the rest of your data center. Any backup environment attached to your network can be infected with the same ransomware that corrupted your primary database, preventing you from accessing your backup data at a critical time.

You can avoid this cyber-trap with air-gapped tape backup solutions. Storing offline and off-site copies of data on tape storage, which has no connectivity to public networks, helps ensure that ransomware cannot touch a backup. Create secondary backup copies to tape regularly to help ensure that you have a clean copy of your data.

The ultra-low cost per GB and rapid transportability of HPE Storage Tape provide extra reassurance that you can rapidly recover data if an incident occurs. Storing data offline using tape and LTO media can create the most secure air-gapped protection, providing contingency against both the risk of cybercrime and the disruption caused by natural disasters and plain human error. For organizations seeking cloud-based isolation, Commvault AirGap provides managed, immutable cloud backup storage that helps protect critical backup copies from ransomware and unauthorized modifications.

Commvault MediaAgents integrate with HPE StoreOnce Catalyst and other HPE Storage offerings, including HPE Storage Tape, to provide an end-to-end backup solution capable of leveraging these capabilities to isolate data, separating production data with backup copies and keeping it safe from ransomware attacks. Commvault also provides the ability to configure immutability at the software and/or storage level (locking through layered security controls) and in an air-gap approach (by severing the encrypted tunnel initiated from the isolated site) for data stored on other HPE backup targets and the Commvault Grid platform, providing even more flexibility for how these isolated data backups can be implemented.



4. Detect threats and identify trusted data

Even with the extensive safeguarding measures described previously, you need to detect ransomware attacks as early as possible to reduce their impact and to know which data can be trusted when it's time to recover.

Commvault helps organizations detect ransomware threats early through intelligent monitoring, anomaly detection, and threat scanning. Commvault Threat Scan uses multilayered analysis, including AI-driven detection, to identify potential malware and suspicious activity within protected data, helping organizations identify clean recovery points and reduce the risk of reinfection.

Commvault Threatwise adds another layer of defense through cyber deception technology, using decoys to identify suspicious activity during the early stages of an attack. Together, these capabilities help organizations detect threats sooner and take action before ransomware causes widespread disruption.

With a centralized management interface and dashboards, Commvault provides a single pane of glass to monitor suspicious activity and potential ransomware threats. Automated alerts and workflows help accelerate incident response, enabling IT teams to take action before threats escalate.



5. Recover cleanly and rapidly

When ransomware strikes, recovery is the critical test. Organizations need to restore trusted data quickly to minimize downtime, limit business disruption, and resume operations with confidence. Commvault Synthetic Recovery helps assemble clean recovery data from available backups, while Commvault Cleanroom provides an isolated environment to test and validate recovery before returning workloads to production. Together, these capabilities help organizations reduce the risk of reinfection and restore trusted data with confidence.

For critical applications where minimizing data loss and downtime is essential, HPE Zerto Software provides continuous data protection and orchestrated recovery, supporting recovery points measured in seconds and helping restore operations with minimal disruption. HPE Alletra Storage MP X10000, together with Commvault, provides a scalable, high-performance platform for protecting large enterprise data estates and accelerating backup and restore operations. Commvault IntelliSnap further supports rapid recovery through application-aware snapshots integrated with supported HPE storage systems.

Through complementary protection, recovery, and infrastructure capabilities, HPE and Commvault help organizations restore critical data and resume operations with greater confidence.

Resource

7 tips to defend against ransomware attacks infographic

Visit HPE.com

Summary

As ransomware threats continue to evolve, organizations need a comprehensive approach to protecting critical data and maintaining recovery readiness. From hardened infrastructure and immutable backups to intelligent threat detection and clean recovery, HPE and Commvault deliver complementary capabilities that help strengthen ransomware defenses.

Together, HPE and Commvault help organizations safeguard critical data across hybrid environments, minimize data loss and downtime, and recover with confidence when attacks occur.

Learn more at

HPE.com/us/en/alliance/commvault.html



Chat now

© Copyright 2026 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

a50006409ENW, Rev. 3

HEWLETT PACKARD ENTERPRISE

hpe.com