Protecting your enterprise from ransomware with HPE and Commvault

Contents

Introduction 2
Developing a ransomware protection strategy 2
1. A hardened, secure environment 2
2. Multiple data copies help ensure recoverability 3
3. Isolate backup data 3
4. Intelligent monitoring and alerting 4
5. Increased backup frequency and rapid recoverability 4
Summary 4

Introduction

With new strains of ransomware and other malware threats on the rise and data continuing to grow from core to edge to cloud, your enterprise and data are more at risk than ever. Today, ransomware attacks are at an all-time high and the numbers are growing at a staggering rate. According to Cybersecurity Ventures,[1] global cybercrime costs are expected to reach $10.5 trillion annually by 2025, up from $3 trillion in 2015. It means the growth rate is 15% per year—more than enough to keep your chief information security officer (CISO) up at night. These threats span all industries with high-profile events affecting healthcare providers, government, education, financial institutions—the list goes on and on. In this fast-morphing environment, organizations must act quickly to protect business-critical data.

Data protection is a crucial line of defense against ransomware. Secure backup copies of critical business data and applications allow companies to roll back in time to recover applications and data before the point of ransomware infection. Although many data protection solutions in the market promise to address backup and recovery, most of them provide only partial protection. Legacy solutions are not immune to ransomware once data center systems are impacted.

Hewlett Packard Enterprise and Commvault have combined to provide customers with unified data protection solutions. The solutions keep customer data safe from ransomware attacks by reducing downtime, driving down recovery-time objectives (RTOs) and recovery-point objectives (RPOs), improving alerting and reporting, and enhancing overall business continuity.

Developing a ransomware protection strategy

Attacks happen. It's not a matter of if, but when. If cybercriminals believe your data has value, they'll continue to exploit vulnerabilities and find innovative ways to encrypt critical data. It means that investing in recovery is just as critical as prevention. Including data protection in your cybersecurity framework is a requirement for cyber-resilience.

HPE and Commvault recommend these five core tenets as essential for comprehensive ransomware protection:

1. A hardened, secure environment

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

HPE offers the most secure industry-standard servers in the world[2] including a silicon root of trust built into the hardware. It allows for the integrity of the firmware to be verifiable at all times and enables restores from the last known good state in case the firmware is somehow 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 OAuth and 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.

With security deeply ingrained in the solution from the hardware components through the software, Commvault and HPE help ensure that their joint data management solution is fully hardened and resistant to malware that could impact the workloads being backed up or the backup data being stored.

[1] cybersecurityventures.com/cybersecurity-almanac-2022/
[2] hpe.com/us/en/solutions/infrastructure-security.html

2. Multiple data copies help ensure recoverability

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 (DR) and backup solutions to create an impenetrable multilayered 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 to keep data secure, and increase application uptime and data availability for your business. HPE and Commvault allow you to automate the creation and management of these extra copies of data through policies that can be applied to any data sets within your environment, whether on-premises or on the cloud. When data is backed up, it is also copied automatically to secondary (or tertiary) destinations where Commvault continues to manage it throughout its lifecycle. Once the data expires or is obsolete, it is deleted from all locations and the space is reclaimed. This automation saves your backup administrator from having to perform manual tasks and helps eliminate the possibility of data being unnoticed and being left inadvertently unprotected.

3. Isolate backup data

Cybercriminals usually attempt three insidious techniques to try and force a ransom payment: encrypting, modifying, or deleting an organization's data. In the case of data modification, ransomware changes storage blocks, and your backup system ends up backing up the altered, now-encrypted files.

Immutable backups keep backed-up data out of reach, effectively erecting a wall against ransomware attacks. Commvault Compliance lock and WORM storage controls keep retention locked in and apply object lock controls on cloud, and on-premises backup targets like HPE StoreOnce Systems. Protocols such as HPE StoreOnce Catalyst ensure that you can configure immutability for data backups so that they can't be encrypted, modified, or deleted. These solutions completely isolate data wherever it lives to prevent it from being tampered with, intentionally or unintentionally. Secure by design, these solutions make backup images invisible and inaccessible to ransomware and malware threats, ensuring backups are not compromised.

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 ransomware 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 StoreEver 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.

Commvault media agents integrate with HPE StoreOnce Catalyst and other HPE Storage offerings, including HPE StoreEver 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 HyperScale X platform, providing even more flexibility for how these isolated data backups can be implemented.

4. Intelligent monitoring and alerting

Even with the extensive safeguarding measures described previously, you must be able to detect ransomware attacks as quickly as possible and alert the appropriate personnel, so you can reduce its impact.

Commvault provides several advanced methods to detect new ransomware attacks. Scanning files for anomalies is aided by machine learning that uses historical data to differentiate between legitimate activities and ones that might raise suspicion. Another method involves mimicking a hidden file that is enticing for hackers. Commvault monitors this file for signature changes or other activity that would indicate an attempt to infiltrate the environment.

With a centralized management interface and dashboard capabilities, Commvault provides a single pane of glass for your IT team to watch these anomalies or indications of a possible attack. When an attack is identified, real-time alerts can be sent to critical individuals, and integrated ticketing systems or workflows can be triggered to make sure your response begins immediately.

5. Increased backup frequency and rapid recoverability

Attacks do happen, and fast. While it's important to employ the 3-2-1-1 rule to protect you from data loss, it's every bit as critical to prepare for fast recovery. The longer your business waits to be operational again, the deeper the damages.

In the event of an actual attack, recovery is the make-or-break step. Once you've identified your environment has been compromised and you know which systems have been affected, you need to confidently recover the data from one of your backup copies. You also need to do this as quickly as possible, so you can mitigate downtime and resume business operations. Data protection solutions with global protection policy and automation help provide predictable and rapid recovery, mitigating system downtime, business disruptions, and revenue loss.

Deep integration between Commvault software and HPE storage portfolio allows you to reduce your RTOs and recover your affected data quickly. IntelliSnap technology combines a broad range of application awareness with the snapshot engine for HPE primary storage arrays including HPE Alletra, HPE Primera, HPE Nimble Storage, and HPE XP7 to provide fast, reliable recovery of file systems and complex applications.

Summary

At a time when ransomware attacks are increasing exponentially, it is essential for organizations to plan and implement a strong data protection strategy that protects and enables them to recover quickly if their data is compromised. By implementing these steps, you can start protecting your organization's data against damaging ransomware attacks. When you are in control of your business data, you are no longer vulnerable to the hacker's demands. As the threat landscape continues to evolve, more enterprises will need to modernize their data protection edge to cloud to keep their data secure from any cyberattacks. HPE and Commvault combine to provide integrated, enterprise-class data management solutions that address the core pillars of ransomware protection as described previously and can provide customers the assurance that their data is safe, secure, and recoverable, so their business can remain operational no matter what cyberattacks are thrown their way.

Resource

5 tips to defend against ransomware attacks infographic

Learn more at

hpe.com/us/en/storage/data-protection-solutions.html

hpe.com/us/en/solutions/infrastructure-security.html

commvault.com/hpe

a50006409ENW