Solution Brief: Protect, Recover and Secure Clinical Data

MITIGATE RANSOMWARE ATTACKS WITH COMMVAULT® BACKUP AND RECOVERY

QUICK FACTS

Ransomware is the leading threat for today’s healthcare organization. In fact, 75% of hospitals in the U.S. report that they could have been hit with ransomware in the last year.¹ The fastest way to regain access to your critical files following a ransomware attack is to have a reliable backup of your data. Without a comprehensive backup strategy, consequences can be serious. With an effective backup solution, healthcare organizations can eliminate the ransom entirely, and avoid business disruption.

By maintaining a secure, regularly scheduled backup of your organization’s laptops, you can easily recover from a ransomware attack. Consider endpoint data backups as insurance in the event that all of your other endpoint security tools have failed. Without a secure copy, your only other option is to pay the criminal’s ransom price and pray they’re honest enough to provide you the keys to get your data back.

¹ Healthcare IT News, “More than half of hospitals hit with ransomware in last 12 months,” April 7, 2016

Commvault’s efficient, streamlined approach to endpoint data protection reduces IT burden, improves end-user productivity and keeps your corporate data protected — no matter where it lives.
COMMVAULT EHR DATA PROTECTION

With the extraordinary amount of Personal Health Information (PHI) being created and stored in electronic medical records, healthcare organizations rely on Commvault technology to augment or replace legacy data protection solutions to capture, protect and backup EHR data such as Epic and MEDITECH EHR systems.

Commvault delivers an integrated, automated data protection approach that provides a single, complete view of all your stored data no matter where it is—on-premises or in the cloud. This allows you to:

- Backup databases, files, applications, endpoints and VMs with maximum efficiency according to data type and recovery profile
- Integrate hardware snapshots
- Optimize storage with deduplication
- Rapidly recover data, whenever you need to, and leverage reports to continually improve your backup and recovery processes

Commvault backup and recovery, doesn’t stop at file servers and storage arrays. Even business files stored in third-party file sharing applications can be protected in a secure, searchable and centralized virtual repository. Commvault enables the data created and stored on laptops, desktops and more, to be accessible anytime, anywhere — with a self-service recovery portal accessible from any web browser or mobile device.

In addition, Commvault software monitors, alerts, and locks down managed data paths. Check files are placed in special locations, with services that monitor for any changes. If the check files are altered, alerts and notifications are launched so that you can investigate, or react by taking systems off the network before they hop, and further infect other systems in your infrastructure. However to protect against ransomware, it is critical to have a dual backup configuration, where only one system is connected at a time. With access to two recovery sites, systems can easily be restored with data from the offline system.

STANDARDS-BASED APPROACH MINIMIZES RISK

The CSC 10.4 standard is a collection of the Critical Security Controls recommendations by the Center for Internet Security related to data recovery. The CIS Critical Security Controls are based in the real-world knowledge of actual attacks and effective defenses and reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals); with every role (threat responders and analysts, policy-makers, auditors, etc.); and within many sectors (government, finance, academia, security) who have banded together to create, adopt, and support the controls. Specifically, section 10.4 of the CSC standard is:

Ensure that key systems have at least one backup destination that is not continuously addressable through operating system calls. This will mitigate the risk of attacks like CryptoLocker

Crypto-ransomware impacted 300,000 systems in 2015²

50% of U.S. hospitals were not sure if they could detect an attack⁴

CryptoWall version 3 threat resulted in more than $325 M in damages worldwide³

⁴ Healthcare IT News, “More than half of hospitals hit with ransomware in last 12 months,” April 7, 2016
4 Ways to Protect and Recover from Ransomware Attacks

Learn the best practices for maintaining access to clinical data to ensure quality care and how to protect and recover from ransomware attacks with confidence.

COMMVAULT ENDPOINT DATA PROTECTION

The easiest targets for ransomware are laptops and desktops, as users do not always have the connectivity to backup files and data to your corporate server. Commvault’s efficient, streamlined approach to endpoint data protection reduces IT burden, improves end-user productivity and keeps your corporate data protected — no matter where it lives. Commvault software creates and stores data on laptops, desktops and more, to be accessible anytime, anywhere — with a self-service recovery portal accessible from any web browser or mobile device. If any system is impacted by ransomware, it can easily be wiped clean and rebuilt to minimize damage.

Commvault Endpoint Data Protection provides reliable, efficient backup and recovery for your enterprise laptops and other endpoints. It provides data copy protection on Mac, Linux and Windows systems by providing automated incremental PC backups of endpoint data to an encrypted virtual storage repository that is managed in your secure data center or Commvault’s cloud service. The intelligent backup scheduling engine seeks the most efficient time to perform backup jobs based on things such as network bandwidth and CPU availability, so there’s little to no disruption in user productivity. And users can immediately access and download their protected files from the backup storage location from any device, including mobile devices, while a full data copy restore is in process on new hardware.

Key features of Commvault Endpoint Data Protection include:

• Seamless, efficient backup from any endpoint. Commvault software protects data value with automatic encryption and backs up mobile data to a centralized virtual repository. Should a laptop be lost or stolen, its work data is already safe in the central data store, and encrypted data keeps it safe from data breaches. Commvault software is so efficient your end-users won’t even know it’s running. Backup processes consume minimal device resources so there are no slowdowns or interruptions, meaning your users stay fully productive at all times. And with features such as client-side deduplication and automated backup schedules, backups happen only when they need to — with only the data that has changed since the last backup being sent to your server. This

which seek to encrypt or damage data on all addressable data shares, including backup destinations.

Because the Commvault architecture meets the CSC 10.4 standard, it will alternate copies used to maintain persistent copies of the data in other locations. This is particularly important in the protection against ransomware. With ransomware, hackers access your file servers and encrypt the data. And if they can find access paths to any online backup sets, they can potentially delete the attached backup pool. Commvault enables copy separation, using different Commvault Server (called CommServe®) Media Agents, different sites, and the old standby offline media so that you can minimize risk. By restricting the attack to the client server, you can simply recover the front-end systems from the secondary backup in the Commvault ContentStore.
keeps network bandwidth requirements low, allowing backups to run even over low-speed mobile or cellular networks.

- **Reduced IT workload with self-service file recovery.** With self-service search and restore through a web portal or mobile app, your end-users get anywhere, anytime access to backed-up data, reducing the number of requests sent to your helpdesk. Commvault software’s intuitive visual interface lets users navigate and preview protected files — including multiple versions of the same file — to quickly find exactly what they need. Users can also restore their own files to any device regardless of where it originated, without IT involvement.

- **One view of all your corporate data.** Commvault software automatically detects new endpoints as they’re added to your network to ensure they stay protected and secure. From one centralized console, you can easily check the backup status of a specific laptop, manage access to critical files and more. With Commvault, you get a higher level of control and visibility when it comes to endpoint data protection. The process is safe and secure for end-users, who access their data in virtual private clouds through a web portal, mobile app or natively in Windows Explorer.

---

**COMMVAULT DISASTER RECOVERY**

To further protect against ransomware attacks, Commvault offers multiple options to protect your backup databases. Commvault provides centralized management and administration for your backups, thus to ensure availability, it is essential that you plan and build a disaster recovery process to protect both the CommServe® database and host. Multiple disaster recovery strategies are available:

- **Running Disaster Recovery Backups.** By default, the Commvault software runs Disaster Recovery (DR) backup jobs to protect your production database. The DR backups include the CommServe database and Workflow Engine. In this method, the databases are backed up to a disk media and moved to a tape media periodically. In the event of an actual disaster, you can use these backed up database dumps from the remote media to recover the CommServe database on the same or new host.

- **Building a Standby CommServe Host.** As CommServe functionality is critical to CommCell operations, you can assign a dedicated computer as a standby or passive CommServe host, install the CommServe software and stage the CommServe database for easier activation of the CommServe host. The databases and logs on the active or production CommServe host are replicated to the standby host at regular intervals. When the active CommServe host goes offline, you can immediately fail over the CommServe functionality and resume CommCell operations on the standby CommServe host.

- **Building a Standby CommServe Host for Disaster Recovery.** You can reduce the downtime to recover your CommServe database by assigning a dedicated computer host with preconfigured software as an alternate or standby CommServe host. As CommServe functionality
is critical to CommCell operations, you can assign a computer as the standby CommServe host, install the CommServe software, and replicate the production (active) CommServe databases to the standby host periodically. For this method, the Microsoft SQL Server Agent is used to back up the database and transaction logs from the production CommServe host and restore in standby mode to the standby CommServe host. The database is restored when you first set up the standby CommServe host and transaction logs are restored every time you perform the transaction log backup on the production CommServe host.

▶ SECURE PHI FOR THE BEST POSSIBLE PATIENT CARE

Guarding information from ransomware attacks is a top priority for healthcare organizations as they work to avoid the loss of availability to critical information and EHR systems. Equally, securing PHI and maintaining compliance with industry regulations is critical to delivering the best possible patient care.

Commvault delivers a unified, integrated, automated data protection platform that provides a single, complete view of all your data – wherever it resides – on-premises, off-premises, or in the cloud. And you can quickly recover and leverage your data when needed – regardless of how it was protected or where it resides. From snapshots, to backup, replication, archive, eDiscovery, and more, Commvault provides the flexibility to protect and recover your data in multiple ways to best meet regulatory and governance requirements, SLA's, and business needs.

▶ RESOURCES

1 commvault.it/2ahJzvf

To learn more about how Commvault® will help you intelligently manage your healthcare data, visit commvault.com/healthcare.