COMMVAULT®

Healthcare Data Security Solutions

KEY BENEFITS

With the extraordinary amount of protected health information (PHI) being created and stored in electronic medical records, healthcare organizations are increasingly leveraging Commvault's industry leading data management platform to capture, protect and backup data across the enterprise. Commvault provides healthcare organizations with solutions that offer continuous availability of clinical data while guarding PHI from unauthorized access by cyber threats, including:

- Network security
- User security
- Endpoint data security
- Media security
- Data encryption
- Ransomware alerts

With an integrated, automated data protection approach, Commvault provides a single, complete view of all your stored data no matter where it resides — on-premises, in the cloud, or both.

Commvault enables healthcare organizations to secure protected health information (PHI) and maintain access to clinical data, ensuring quality of care.

INTRODUCTION

Hospitals are hit with 88% of all ransomware attacks.[1] The Ponemon Institute study[2] calculated that healthcare organizations incurred the highest average cost of $355 per lost or stolen record, compared to the average global cost per record across all organizations surveyed at $158. In addition, hospitals were the target of 88% of all ransomware attacks.[1]

Providing always-available access to clinical data is critical to delivering high quality patient care. However, cyber threats and privacy breaches that result in HIPAA violations top the list of healthcare IT security risks, posing a serious threat to clinical data availability. And according to a report from KPMG,[3] 81% of healthcare executives surveyed said that their IT security has been compromised at least once in the past two years.

Healthcare IT must balance data access and interoperability with securing protected health information to maintain compliance with HIPAA and other government regulations — not to mention preserve the trust of their patients. Although there is no single vendor that covers the complete spectrum of data security, there are many security technologies that healthcare organizations can implement to increase readiness and minimize the regulatory consequences of a data breaches.

Solution Brief: Protect, Recover and Secure Clinical Data

The fastest way to regain access to your critical files following a ransomware attack is to have a reliable backup of your data.

READ NOW

PDF commvau.lt/2agPXQ7

COMMVAULT® HEALTHCARE DATA SECURITY SOLUTIONS

Commvault® software provides comprehensive enterprise-class security including full multi-tenancy support across all of its solutions, such as enterprise data protection and recovery, endpoint protection, file sharing, as well as data and application archiving. Healthcare organizations using Commvault software can be confident that healthcare data is secure, private and protected, whether hosted on-premises or in the cloud. Commvault solutions, when used in conjunction with a comprehensive compliance plan, have a robust set of features, including encryption, access controls, data integrity controls and other security features that can help satisfy HIPAA requirements and other regulations.

Here are six key areas where Commvault solutions can enhance data security within the healthcare organization:

NETWORK SECURITY

Preventing cybercriminals from infiltrating the network is the first line of prevention. With Commvault software, hardware components, user devices, and storage media are interconnected to form a network to ensure that the Commvault instance is secure.

- **Encrypted challenge and reply.** All network communications between Commvault software components use encrypted challenge and reply to validate the components involved.

[1] commvau.lt/2j8v67N [2] commvau.lt/2kCqlCz [3] commvau.lt/2lWPY28

- **Client security certificates.** Authenticates client communications by confirming the identity of clients attempting to establish connections between systems. In the event a client is lost or compromised, certificates can be revoked to deny further communication.
- **Firewall.** Commvault software components can be configured to use authorized ports and connection routes through the firewall to communicate and perform data management operations such as backup, restore, spam prevention, etc.
- **Third-party port mapping.** Map ports between source and destination computers to listen for incoming connections. Multiplex ports to reduce the number of ports open and reduce the attack envelope.

USER SECURITY

The next line of defense is user security. Commvault software builds extensible credentials into its infrastructure, providing clinicians with a secure environment to access and share critical data to support quality patient care.

- **Role-based access control.** Increases the flexibility of user security by enabling the administrator to align task authorization to business needs rather than to technology considerations.
- **Auditing and session management.** Commvault Audit Trail allows administrators to track every user's data access and software actions. Audit reports and alerts can be configured to monitor and flag unauthorized login attempts and attempts to view or destroy data.
- **Integration with directory services.** Integration with external directory services allows administrators to manage a single set of users.
- **Two-factor authentication.** Add an extra level of security to Commvault software logon requirements.

ENDPOINT DATA SECURITY

The clinical data used to support patient care is increasingly created on – and accessed by – growing numbers and types of devices. Commvault software protects this growing universe of devices with protection, security, and search capabilities that proactively protect PHI against unauthorized access and data breaches.

- **Secure file sharing.** Authorized end users can access and share their protected files and email in protected storage by using remote devices such as smart phones, tablets or laptops.
- **Privacy and client locking.** Client locking prevents unauthorized access to a lost or compromised client's protected data.
- **Data loss prevention.** Schedule periodic encryption of files to prevent unauthorized access if mobile devices are lost or stolen. As an option, laptops can be tracked so that data can be erased.
- **Erase data.** Permanently erase any data from protected storage copied to it by a backup or archive operation. This may be necessary to meet compliance requirements to remove all or inadvertent copies of original data.
- **PHI detection.** Commvault software can detect PHI and automatically move it to a secure location.

MEDIA SECURITY

Healthcare organizations create terabytes of sensitive patient data every year, including patient records, reports and medical images. This data must be retained in accordance with HIPAA and other regulations, in some cases for many years. Commvault software prevents unrecognized processes from corrupting storage systems. Media passwords are used to prevent unauthorized access to non-encrypted data residing on removable media when using external recovery tools to restore data. This ensures that only the originating, licensed software can recover data written by that software. For more granular security, different media passwords can be specified for different data content, i.e., patient data versus business data. This allows for the compartmentalization of data so that one compromised password does not expose all data.

DATA ENCRYPTION

Storage encryption and key management secures data, and upholds the integrity and confidentiality of PHI and business data. Supporting the Key Management Interoperability Protocol, Commvault works closely with a growing list of key management vendors to allow healthcare IT to efficiently and securely manage and store cryptographic keys and policies — across the key management lifecycle.

- **Software.** Commvault software supports FIPS-140-1 and FIPS-140-2 approved encryption of data in transit (source to media) and data at rest (on media). For data encryption in transit, the location of where the encryption takes place is flexible – at source or destination.
- **Hardware.** Commvault software supports tape devices and inline hardware encryption devices.
- **Key Management.** Commvault software supports the Key Management Interoperability Protocol and allows for the key storage to be in a separate physical location than the data storage.

RANSOMWARE ALERTS

The number of ransomware incidents targeting healthcare is on the rise. When a successful attack occurs, healthcare organizations lose access to critical electronic files, potentially compromising patient care. To protect against ransomware, it is critical to have a dual backup configuration, where only one is system is connected at a time. With access to two recovery sites, systems can easily be restored with data from the offline system.

Commvault software protects backup data from malware like ransomware by disallowing interference with the data by any process that is not explicitly recognized by Commvault. Stopping interaction with the underlying library data paths through a custom driver does this.

Case Study: University of Rochester Medical Center

Commvault helped enhance patient care with improved management of electronic medical records and research data.

READ NOW

PDF commvau.lt/2mxbbEe

In addition, Commvault software provides a monitoring mechanism that alerts administrators to malware activity, allowing them to take proactive measures to lock down managed data paths, and protect the infrastructure. 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 so you can investigate, or react by taking systems off the network before they hop and further infect other systems in your infrastructure.

SUMMARY

The protection of healthcare data has never been more important. This is why approximately 2,000 healthcare organizations across the world trust Commvault to protect their most critical data. Commvault offers a comprehensive set of security features and tools that play a key role in a comprehensive data protection strategy and help ensure that data is kept private, secure from unauthorized users, and available to support the delivery of care and drive organizational decisions. Only Commvault provides a single solution for keeping all data across the healthcare enterprise — clinical and business data alike — fully protected and accessible.

▶ Only Commvault provides a single solution for keeping all your healthcare enterprise data — clinical and business data alike — fully protected and accessible. Read more at commvault.com/healthcare.