Healthcare Data Security Challenges

Healthcare organizations face security challenges regarding potential data breaches or penalties, or public ire about their carelessness for exposing personal information. It is imperative that healthcare organizations tighten their security to avoid facing these negative consequences.

A growing challenge for even the best-prepared organizations is the task of securing protected health information (PHI). This can refer to demographic information, medical history, test and lab results, and any other data a healthcare professional collects to identify an individual and help determine appropriate treatment.

An immense amount of data held within healthcare organizations requires protection. This data includes claims requests, PHI, and medical records. Balancing security needs with health care professionals' need for quick access to data and applications is a key focus area for IT professionals.

Distributed or mobile security will continue to be a renewed priority for many organizations. Furthermore, the need for enhanced security that does not inhibit end user productivity is becoming an increasingly important requirement for IT security in organizations.

Private Cloud Computing in the Healthcare Industry: Why It Works

Infrastructure security and private cloud[1] computing are continually evolving to meet the growing security requirements of heavily regulated industries like healthcare. Legitimate cloud service providers have strict security protocols designed to comply with different regulatory mandates.

While privacy concerns have kept many healthcare organizations from migrating to a private cloud computing solution, the cloud offers major benefits to providers:

- **Security:** Healthcare and medical data management professionals are concerned about space, costs, records accessibility, and regulatory compliance. Storing medical records on a compliant cloud system eliminates physical theft, the most common type of large data breach. Effective security includes ensuring data is encrypted and securely backed up, verifying data can be easily recovered, and using permission-based data access.
- **Scalability:** Unlike onsite hardware infrastructure, companies can easily scale their cloud storage solution to manage ever growing patient data. Generally, healthcare service providers must keep records for at least six years. Considering the volume of patient data, the likelihood of this requirement overwhelming any onsite IT infrastructure is inevitable.
- **Mobility:** The increasing demand for physicians' time often means they only have the opportunity to review patient records and tests or do research during evening hours. In the past, this meant being stuck in the office after hours. With private cloud computing solutions, patient information is readily available at any time, anywhere.
- **Cost Reduction:** The adoption of private cloud computing solutions results in cost savings for healthcare organizations. For example, the patient doesn't have to pay for the same test twice when they go to different doctors or specialists or if the test results are lost. Better hardware utilization means more efficient power use, and the centralized deployment of applications and desktops reduces the IT staff's workload, which increases the overall cost savings.

Build a Private Cloud Computing Solution with Parallels Remote Application Server

While private cloud computing solutions provide efficient, scalable, and reliable systems, their full potential lies with the virtualization of applications, desktops, files, and folders that can be delivered to various devices. Through centralized application management, data storage, and maintenance, IT gains more control and can remotely ensure a strict separation between corporate and personal data.

Parallels Remote Application Server enables medical and paramedical staff to work securely from anywhere and from virtually any device. Parallels Remote Application Server is a well-known solution for virtual application and desktop delivery. It offers the required flexibility to build any private cloud computing infrastructure, since it can work at the same time with VDI and Microsoft Remote Desktop Services. To limit the risks of data leakages, access rules can be enforced and data can be segregated in restricted silos to reinforce the division between the different virtual applications. Parallels Remote Application Server deploys critical software security that is updated centrally for all users at once, reducing the application's downtime. In addition, Parallels Remote Application Server supports continuous availability, resource-based load balancing, and universal printing. These features allow healthcare organizations to complete any task with ease.

[1] A private cloud is a particular model of cloud computing that involves a distinct and secure cloud- based environment in which only the specified client can operate.

How Parallels Remote Application Server Increases a Healthcare Organization's Security

Parallels Remote Application Server adds tools and features to increase data security without compromising the advantages of private cloud computing.

Advanced Filtering–Parallels Remote Application Server sits on top of Active Directory and offers advanced filtering options that prevent illegitimate user access. Filtering rules allow administrators to restrict access to sensitive data, such as cardholder details, by user or group, MAC address, IP address, and several other criteria.

Logon–Parallels Remote Application Server offers two modes, private and public, to log users on to the virtual application and desktop. With the private logon, the user data can be kept on the device, while with the public logon, no user data can be retained on the device. This increases the security of shared workstations or tablets.

Data Segregation–Parallels Remote Application Server can create an unlimited number of farms and sites. A farm is a group of servers used to deliver applications to users, and a site is a group of farms; however, any site has an independent activity directory. No data can be shared between sites, guaranteeing perfect data segregation when needed.

Desktop Replacement–Parallels Remote Application Server offers the capability to replace the desktop of the Windows machine, transforming it into a secure pseudo thin client. The IT administrator can decide which applications are allowed to run locally based on security requirements. For maximum security, the administrator can block any local operation or any operation that needs to be executed remotely on the server.

Limitation for Copy and Paste–In order to avoid any unwanted data leakage from applications and the desktop, paste and copy on the clipboard can be disabled.

Higher Security–All data is kept on the server side with centralized security and backup management. Only mouse clicks, keyboard keystrokes, and desktop/application screenshots are transmitted to and from the client device, thus preventing data leakages, viruses, Trojans, and other vulnerabilities on clients.

Smart Card Authentication–Parallels Remote Application Server makes it easy to use a smart card to authenticate users on a virtual application. While the redirection of virtual desktops and applications can be complicated, Parallels Remote Application Server increases security, allowing IT managers to use this technology when needed.

Two-Factor Authentication–Parallels Remote Application Server second-level authentication provides a high level of protection via different types of security tokens for two-factor authentication. Users are required to authenticate through two successive stages to access the application list. The second level of authentication can be provided by DualShield, SafeNet, or a RADIUS server.

SSL Certificate/Encryption–Parallels Remote Application Server Secure Client Gateway acts as a proxy between the Parallels Client software running on client devices and Parallels Remote Application Server. The gateway encrypts the communications using SSL. Each Parallels Remote Application Server Secure Client Gateway has its own certificate, which should be added to Trusted Root Authorities on the client side to avoid security warnings.

No Data Saved Locally–Parallels Remote Application Server supports private cloud computing by allowing healthcare organizations to maintain complete control over their virtual resources. Remote Application Server can eliminate the risk of data saved locally, while it allows access to corporate assets only on the servers, enforcing HIPPA compliance.

Conclusion

Parallels Remote Application Server improves patient care and security; in fact, the solution was awarded the prestigious Govies Security Award three years in a row. Parallels Remote Application Server has also been chosen by hundreds of healthcare organizations for its reliability, ease of use, and cost-effectiveness. Caregivers and staff enjoy real-time access to virtualized applications from any device, including zero and thin clients, mobile workstations, and other endpoints.

Customer Stories

"Using our Remote Application Server solution allows us to grow up rather than out."

— Chris Worth, Intuitive Medical, Abilene Diagnostic

"Parallels Remote Application Server is easy to deploy and easy to manage. Our number one benefit is having the ability to provide access to selected applications based on user group needs."

— Mariusz Mazek, Norwegian American Hospital

"With the implementation of Parallels Remote Application Server, we solved the performance and connectivity problems on our network and servers, improving the user experience significantly."

— Juan Rosa, IT Manager, Bay Dermatology