Virtual Desktop Management in Healthcare
A Case Study

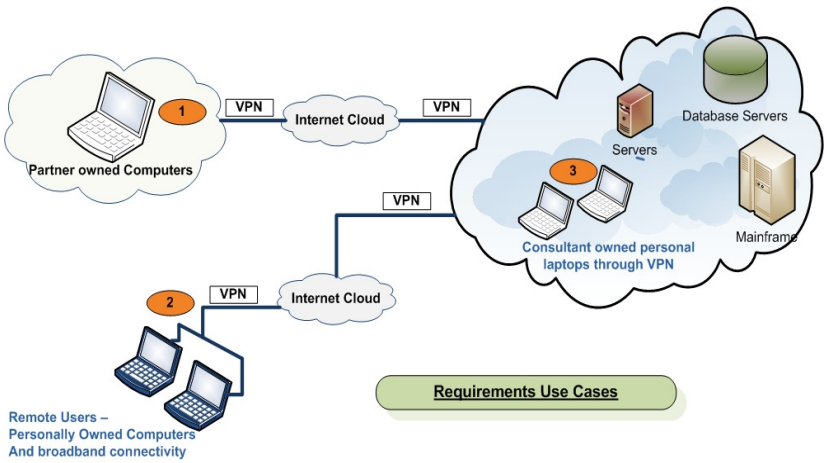
In early 2008, the newly appointed head of security for a large health services provider had a dilemma. Nearly 30% of all corporate users, who needed access to applications and data, were connecting from un-trusted machines. He knew this exposure could lead to significant compliance infractions with HIPAA, the body of regulation that all healthcare organizations have to meet.

This case study documents the experiences of a real-life organization, how they approached the problem, and the steps they followed to select the best-fit solution.

The Challenge

With thousands of physicians working from medical centers across the country, it was crucial for the company that users stayed secure while remotely accessing the patient information and company restricted data. Due to the cost and delays in procuring corporate laptops, about 30% of the users were working on personal machines or non-enterprise machines to access the Patient Healthcare Information (PHI) of their patients' files. This was creating risks of data loss and violation of national health care standards. These at-risk users fell into one of two categories:

- Healthcare professionals connecting to the corporate network from home or another partner facility using non-enterprise owned computers;
- Consultants accessing the corporate network from their non-enterprise owned laptops.



Executive Summary

***Industry**: Healthcare*

***Customer Profile**: A large health care provider with thousands of employees working from medical and non-medical facilities daily.*

***Situation**: 30% of users were accessing patient information using personal machines which led to increased exposure to data leakage and potential HIPAA violations.*

***Selected Solution**: MokaFive's Virtual Desktop Solution gave users flexibility to connect using personal machines while providing IT with a secure and efficient management solution.*

Key Features:

- Corporate data and applications remain secure and isolated from a personal host computer

- Ability to work online or offline with full access to all applications and files

- Corporate Virtual Desktop can be carried on a USB stick

- Users can rejuvenate an ailing laptop on their own

- Users can choose PC or Mac

- IT can remotely terminate stolen or lost laptops

In both cases, unauthorized individuals could access the residual traces of data left on these PCs by virtue of application use, which in turn could result in HIPAA violations. In addition, there was no mechanism or methodology in place to audit individuals when they remote accessed the HIPAA-related information on the corporate network. With their current technology, the organization appeared to be left with two options: (a) encrypt all non-company owned computers, or (b) provide employees with company-owned laptops.

A Vision

Desktop virtualization, however, seemed to offer a new set of choices. After some research, the Head of Security developed the following vision for remote users and for the Information Technology (IT) organization.

- IT would provide a corporate Virtual Desktop, within which all company applications and utilities would be encapsulated and controlled.
- Employees would have the ability to use the corporate Virtual Desktop in any location – at home, at a partner hospital, at a clinic. Users would have easier access to corporate files from anywhere in a secure manner.
- Contractors could use the corporate Virtual Desktop on their own machines to securely access a selected set of corporate data and applications without compromising security of corporate proprietary data.
- IT would manage the corporate Virtual Desktop centrally. They would be able to send updates, adjust policies, and revoke or terminate a Virtual Desktop instance if it were lost or stolen. In turn, this would protect company information from leakage while keeping personal files separate.

The Requirements

An evaluation team was formed, which included key stakeholders from IT enterprise architecture, senior management, security, compliance, account management, as well as the medical staff. After discussing possible options, the team prioritized the

High Level Requirements

Flexibility

- ☐ Virtual Desktops run off portable USB drives
- ☐ Virtual Desktops function offline (ie, when server connection is unavailable) for travelling users
- ☐ Supports Windows and Mac hosts

Infrastructure

- ☐ Efficiently imports standard desktop images to a Virtual Desktop
- ☐ Integrates with enterprise-specific domain joining tools such as Active Directory
- ☐ Supports major VPN clients
- ☐ Supports a major, enterprise-class VM hypervisor with seamless integration

Manageability

- ☐ Provides centralized control for providing, revoking and suspending Virtual Desktop access
- ☐ Supports standard corporate patch management and anti-virus tools

Scalability

- ☐ Supports efficient deployment of Virtual Desktops to thousands of enterprise users

Security

- ☐ Supports hardware- or software-based encryption
- ☐ Controls copying and transferring of data between guest and host, including copy-and-paste and screen scraping
- ☐ Audits all files leaving the Virtual Desktop, if allowed
- ☐ Restricts copying of Virtual Desktop from one host to another
- ☐ Centrally revokes Virtual Desktop usage based on schedule or login frequency

Usability

- ☐ Performs with user-acceptable performance on typical host machines
- ☐ Provides users with a straightforward Virtual Desktop initial setup
- ☐ Supports user-initiated reset of Virtual Desktop environment

requirements. These would enable them to decide on the best solution to meet both IT's management needs as well as users' flexibility requirements.

Evaluation Process

From the analysis of the available technologies, the evaluation team found 4 categories of solutions:

- Server hosted desktop (VDI)
- Encrypted laptops
- Client-hosted virtual desktops
- Remote access solutions

The evaluation team structured the process into 2 phases: a high-level solution comparison, and an on-site proof of concept.

Phase 1: High-level Solution Comparison

The team talked with analysts and reviewed available literature on the relative pros and cons of the four solutions categories.

Solution Comparison

Category	Pros	Cons
VDI	✓ Easy deployment of new desktops ✓ Centrally managed	✓ Requires a large amount of data center space ✓ Desktop is inaccessible if working offline ✓ No USB peripherals permitted
Encrypted Laptop	✓ Easily administrated	✓ High capital costs
Client-Hosted Virtual Desktops	✓ Flexible ✓ Cost effective	✓ Relatively new technology
Remote Access Solutions	✓ Very Flexible ✓ Cost effective	✓ No way to ensure host security & isolation ✓ Causes compliance issues

Virtual Desktop Infrastructure (VDI)

Implementing server side VDI was an attractive hosted virtual desktop option. However, the team determined that VDI would require a large amount of data center space, with heavy power requirements and capital to deploy. In addition, VDI would not support their offline usage requirements.

Encrypted Laptops

Providing enterprise-owned laptops to remote users would meet their requirements, but it would require a large capital investment and greatly increase their operating expenses. They estimated that this option would require a substantial capital outlay for hardware, software licenses and support staff head count.

Client-Hosted Virtual Desktop Solution

Client-Hosted Virtual Desktop, despite it's relative nascence, seemed to offered a flexible solution while satisfying requirements for providing a secure environment for users to access compliance critical data from their personally owned computing device of choice (Windows and Mac).

Remote Access Solution

With Remote Access solutions (GoToMyPC.com, PCAnywhere, etc), a remote user could access his/her own corporate computer from any available computer with a connection to the Internet. While Remote Access solutions were appealing, they suffered from variable performance depending on the network connection, and did

not allow for shared PCs. For example, a remote user would not be able to access a workstation currently in use by a colleague.

Phase 2: Proof-of-Concept (POC)

The evaluation team conducted research to see which vendors were the most mature and viable. The team reviewed analyst recommendations, and researched the companies and solutions using the Internet. Four prospective products were selected: Kidaro (now Microsoft), MokaFive, Sentillions vThere and VMware Ace. During the POC, each vendor was asked to carry out the following:

1. **Set up environment and create a corporate Virtual Desktop:** Each vendor was given the copy of the desktop image and any needed hardware. The vendors were expected to create the Virtual Desktop image and document the image creation process. The members of the evaluation team were involved in verifying and approving the Virtual Desktop.

2. **Package regional applications:** Each vendor was given regional application requirements and expected to package region-specific virtual images.

3. **Create the deployment model:** Each vendor was tasked with creating a deployable package that could be distributed to the end user through down-loadable link, DVD or USB. The vendors were not only asked to demonstrate how the provisioning would be scalable for tens of thousands of users, but also were asked to institute a simple and fast first time setup process.

4. **User testing:** More than 50 technical and business users from each region were asked to test their region-specific virtual images from each vendor.

The results of the POC were aggregated and summarized for IT management. A summary of the findings is represented in the following table.

Proof-of-Concept Result Summary

● = Good ◐ = Fair ○ = Poor

Requirement		Kidaro	Moka5	vThere	VMware
Flexibility	Virtual Desktops run off portable USB drives	○	●	○	○
	Virtual Desktops function offline (ie, when server connection is unavailable) for traveling users	●	●	●	●
	Supports Windows and Mac hosts	○	●	○	●
Infrastructure	Efficiently imports standard desktop images to a Virtual Desktop	●	●	●	○
	Integrates with enterprise-specific domain joining tools such as Active Directory	●	●	●	●
	Supports major VPN clients	●	●	●	◐
	Supports a major enterprise-class VM hypervisor with seamless integration	●	●	●	●
Manageability	Provides centralized control for providing, revoking and suspending Virtual Desktop access	●	●	●	●
	Supports corporate standard patch management, and anti-virus tools	●	●	◐	○
Scalability	Supports efficient deployment of Virtual Desktops to thousands of enterprise users	●	●	◐	◐
Security	Support for hardware or software-based encryption	◐	●	◐	◐
	Controls copying and transferring data between guest and host, including copy-and-paste and screen scraping	●	●	●	●
	Audits all files leaving the Virtual Desktop, if allowed	●	●	●	●
	Restricts copying of Virtual Desktop from one host to another	●	●	●	○
	Centrally revokes Virtual Desktop usage based on schedule or login frequency	●	●	●	●
Usability	Performs with user-acceptable performance on typical host machines	◐	●	◐	○
	Provides users with a straightforward Virtual Desktop initial setup	◐	●	◐	○
	Supports user-initiated reset of Virtual Desktop environment	●	●	●	●
Total		◔	●	◔	◐

The Outcome

MokaFive was selected as the vendor of choice. The company addressed all "must have" requirements and most of the "high priority" requirements related to HIPAA. Although desktop virtualization was a nascent and evolving market, MokaFive appeared to have had the most focus on enterprise customer requirements, and could satisfactorily meet their needs. In addition, MokaFive had solid financial backing, which was important for a long-term relationship and support.

Summary

MokaFive's Virtual Desktop Solution demonstrated the most user flexibility while providing IT with the most secure and efficient management solution.

- Corporate data and applications are secure and isolated from a personal host computer
- Ability to work online or offline with full access to all applications and files
- Corporate Virtual Desktop can be kept on a USB stick that is easy to transport
- Users can rejuvenate an ailing laptop on their own
- Users can choose PC or Mac
- IT can remotely terminate stolen or lost laptops

About WaveStrong Inc.

Founded in 2001, WaveStrong, Inc. has been a value added partner providing quality professional services in the areas of information security and risk management including customized integrations, complete enterprise deployments, strategy and risk advisory services, and training and maintenance to a wide range of businesses and educational institutions both in commercial and government sectors. Based in Pleasanton, California, WaveStrong Inc. serves customers in US and Canada. For more information, please visit URL: http://www.wavestrong.com, Main Tel: (800) 920-0603 or Technical Sales: (206)331-2935.