WHITE PAPER: BEST PRACTICES FOR HEALTHCARE

Endpoint Virtualization for Healthcare Providers

Confidence in a connected world.

symantec™

White Paper: Best Practices for Healthcare

Endpoint Virtualization for Healthcare Providers

Contents

Executive summary

As hospitals continue to automate their processes, they need to implement more advanced clinical software applications, which require complex authentication. The challenge is to provide direct and convenient access to these applications for physicians and clinicians while maintaining security and patient data privacy. Healthcare professionals move around a hospital, share access points, and connect remotely. Gaining access to applications is sometimes cumbersome and slow, and many applications do not recognize differences in location.

Many hospitals are discovering that endpoint virtualization can help address these issues. This white paper describes the many challenges of hospital automation and explains how endpoint virtualization can address them, providing value for physicians and clinicians, IT professionals, and hospital administrators.

The challenge for physicians and clinicians

Physicians, clinicians, and other healthcare professionals face a variety of challenges in today's hospital and clinical IT environment. For example, to implement a new computerized physician order entry (CPOE) system, all doctors are required to authenticate and personally enter their orders. To fulfill this requirement, they need to locate a workstation—preferably one that is near their patient—and gain quick access to the required applications. In fact, because physicians, nurses, case managers, and other hospital workers are continually roaming throughout the facility, they all require convenient and easy access from multiple locations. Clinicians need to be able log in and out quickly to their own workspaces using the hospital's shared workstations. And healthcare professionals who work remotely—such as referring physicians—need the same simple, fast access whether they are working from their own private offices or at the clinic.

Another challenge is posed by the fact that most legacy software applications in healthcare environments today are traditional "thick client" applications—i.e., dedicated software that has to be installed and maintained on the client machine. As a result, client applications need to be installed and maintained on large numbers (often hundreds or even thousands) of desktops and mobile devices. In some cases, application conflicts preclude running two client software packages from different vendors on the same machine. Client software may have different system requirements (such as different Java versions), and the most demanding applications also raise hardware requirements for each client machine. For example, a radiologist may want to reference a patient's lab, medication orders, or information in the electronic medical record (EMR) from a hospital workstation, only to find that the required application is not installed there. In another example, the radiologist may want to consult with a colleague inside or outside the hospital regarding a patient X-ray, but if that colleague does not have the correct picture archiving and communication system (PACS) application installed, the image is not accessible.

In addition to these issues, physician and clinician users often do not gain the quick and reliable access they need because of the complexities inherent in application delivery and desktop management:

- **Password problems**—Users forget their passwords or forget which passwords to use for which applications. They also forget when to reset their passwords, which can compromise information security as well as impede access to viable information. Calling the help desk for assistance consumes much of the valuable time of physicians and other healthcare professionals.
- **Application access**—Whether logging in from a new workstation or returning to a kiosk they were using earlier in the day, physicians and other users need to be able to identify the right application and the correct file or data field to resume their work. This can be time-consuming, especially if the user has moved to a different workstation with a different user interface. This complexity may also result in a help desk call, further reducing productivity.
- **Printing confusion**—Even printing can become difficult for roaming users in a hospital or other healthcare facility. Users may not know which printer is used by that workstation. And, once identified, the printer may not be located near that work area.
- **Frustrating remote access**—When working remotely, physicians and other healthcare professionals may not be able to connect reliably to the network and access the applications they need. When they can connect, the desktop interface may be different than the interface in the hospital. Adding to user frustration, remote connections are often unreliable, may be slow, and can often drop users in mid-session.
- **Inability to use computing resources**—Some guest users, such as nursing assistants and vendors, are unable to use computing resources for basic access because they are not authorized to use the corporate network. This impairs their ability to effectively complete their tasks.

IT staff challenges

Among the most critical responsibilities of IT staff is ensuring that all the hospital's authorized users—physicians, nurses, case workers, administrators, and others—have access in multiple locations to the applications and data they need to perform their jobs effectively. Because hospitals never close, their IT staffs need to ensure continuous, reliable access. However, healthcare IT professionals face challenges in this complex IT environment:

- **Desktop management**—Clinicians often share workstations in a kiosk-like fashion. Dozens of healthcare professionals may use the same workstation in a typical day. In many cases, hospital workers also need to access applications and patient data from other client devices (e.g., laptops and handhelds). In order to enable device-to-device roaming and kiosk capabilities, IT staff members are forced to install and configure each and every workstation with all the potential applications users may need, while ensuring that each workstation has the computing power to handle these diverse applications. This approach leads to an inefficient use of computing resources and requires IT staff to conduct time-consuming installations of local applications and troubleshoot problems at the workstations.

- **Help desk deluge**—Today, healthcare professionals use multiple workstations both in the hospital and when working at remote locations, and the interface of each new desktop can be quite different from the last. When printing documents, users may not know how to locate the local printer. They may forget passwords or forget to reset a password. User confusion reduces productivity and often leads to help desk calls, which take time to resolve.
- **Security issues**—To save time, many healthcare professionals use other workers' passwords instead of contacting the help desk for log-in assistance. Sharing passwords not only violates HIPAA mandates, but also hinders enforcement of identity management initiatives and makes it harder to investigate security incidents.
- **Remote access problems**—Enabling remote access is a must, particularly for physicians who often work from remote locations. However, time-consuming issues such as addressing virtual private network (VPN) complexities, user issues related to blocked or dropped connections, and lengthy connection processes complicate effective remote access.
- **Additional training**—Inconsistent user interfaces and sign-on complexities require more user training by IT staff members, consuming valuable time.

Hospital administrator challenges

To comply with security and privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA) and the standards promulgated by the Joint Commission on Accreditation of Healthcare Organizations (Joint Commission, formerly known as JCAHO), hospital administrators need to know who is accessing what resources from which locations. They need to ensure, for instance, that data about ICU patients is only accessed from computers within the ICU. They also need to ensure that sensitive information does not leave the hospital premises. Preserving such information boundaries and providing accurate audit trails of personnel who access hospital information are critical for regulatory compliance.

On the other hand, administrators also want to make physicians' and clinicians' jobs easier. Those hospitals and other healthcare facilities that can accomplish this task better than others gain a competitive advantage, attracting more physicians and clinicians. But to gain that edge, they must provide IT staff with the resources needed to support these users. Administrators also seek to ensure that the IT department can efficiently provide and manage these resources so that the hospital can control costs and meet its budgets.

Overview of the endpoint virtualization solution

Endpoint virtualization is all about provisioning the right IT resources to the right users regardless of location and in the simplest, most efficient, and most reliable manner. By virtualizing users' workspaces, hospitals and other healthcare facilities can meet the dynamic needs of wide-ranging constituents—whether they are power users, have a more typical user profile, or are just casual guest users—while reducing the burden on IT staff and managing the cost of delivery.

With endpoint virtualization, healthcare users can authenticate and connect to their workspaces from any device—such as a thick or thin client, a PC tablet, or a rack PC—and from any location. If a user moves to another location in the hospital and reconnects from another device, the workspace session is transferred and the session resumes exactly where the user left off. The administrator can tailor workspaces to individual users and make them location-aware. For example, a doctor might have access to an application while in the hospital but not from home.

Endpoint virtualization balances centralized control with the flexibility needed to provide tailored user environments. It leverages virtualization and authentication technologies to optimize the way hospitals deliver and manage end-user workspaces. Endpoint virtualization offers IT staff a streamlined, automated, and cost-effective way to deploy and support both computing resources and users, while also meeting regulatory requirements for privacy and reporting. It delivers the resources that physicians and clinicians need, whenever and wherever they need them. The individual user's workspace—including applications, connection protocol, and desktop type (e.g., dedicated, shared, or local)—follows the user and is accessible from virtually any networked device in the hospital.

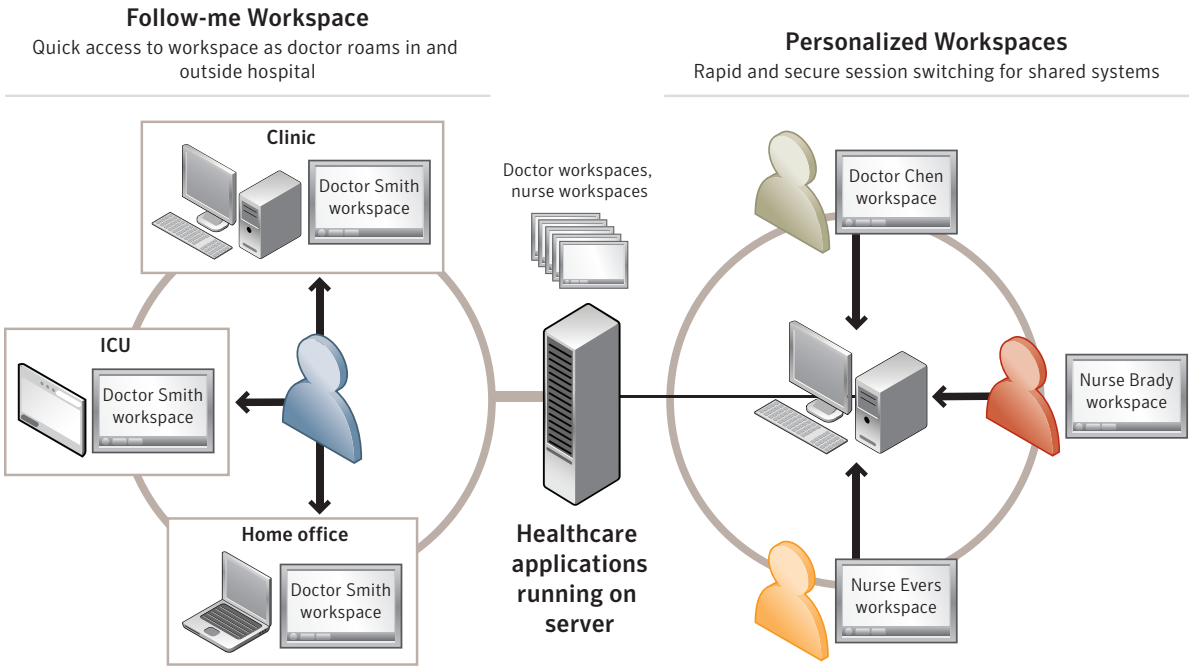

Figure 1. A follow-me workspace provides a secure, personalized desktop that roams with the user throughout the hospital. Clinical users quickly access customized workspaces on shared workstations.

Endpoint virtualization for physicians and clinicians

Endpoint virtualization provides the following capabilities for physicians and clinicians:

- **Familiar, follow-me workspace**—Endpoint virtualization provides each user with a secure, personalized desktop that roams with the user throughout the hospital from device to device. The "follow-me" workspace provides a consistent, familiar experience, regardless of what device being used and whether access is local or remote.

- **Instant-on desktop**—Using endpoint virtualization, physicians can simultaneously share a single workstation with clinicians, case workers, and other healthcare employees—even in high-traffic kiosk areas—without repeatedly entering their login credentials. Single sign-on, automatic password rollover, and self-service capabilities mean that users do not need to remember multiple passwords and can easily reset their passwords if needed. This facilitates user access to all their applications. Endpoint virtualization brings users directly to their own workspace—even to the exact location where the user stopped working in a document—so they can immediately resume working.
- **No-hassle printing**—With proximity printing capabilities, users can print locally even when roaming, eliminating the hassle of tracking down printers.
- **Reliable remote access**—Physicians can work remotely at their convenience, confident that their connection will always be reliable and that their personalized workspace will appear and function exactly as it does when they are in the hospital.

Endpoint virtualization for IT staff

Endpoint virtualization helps IT departments of any size mitigate the challenges described above and provide higher-quality service in a much more efficient manner. With endpoint virtualization, IT can deliver, maintain, manage, and monitor all resources—and support users—easily and quickly in the following ways:

- **Efficient resource allocation**—By intelligently allocating computing resources, including hypervisors, terminal services, and connection protocols, based on user class profiles, IT can optimize these resources. IT no longer needs to install and configure all applications on every workstation. In fact, thick-client resources can even be replaced with centrally managed thin-client resources—and with central management, IT can service users and devices while minimizing desk-side visits.
- **Consistent, personalized user experience**—Follow-me capabilities tie workspaces to users instead of devices. This enables IT to efficiently deliver tailored workspaces to all of its users. IT can also ensure consistent user experiences, regardless of what device is being used.
- **Centralized control for improved support**—Centralizing control and enablement of single sign-on, automatic password rollover, and self-service password maintenance options helps IT resolve password issues more quickly and easily. Centralization also enables IT to quickly resolve any locked desktop issues that may arise. IT can instantly terminate the user's session, and the user can then simply re-authenticate. In addition, location awareness capabilities ensure that documents will always print on a printer close to the workstation, avoiding help desk inquiries and increasing user productivity.
- **Improved remote access management**—Endpoint virtualization permits secure, easy-to-administer remote access. Of equal importance, this approach—which requires only a single connection and efficiently utilizes server and connection resources—ensures that users obtain consistently reliable access to hospital applications and data.
- **Reduced IT costs**—The ability to allocate resources efficiently and manage them centrally enables IT to lower the cost of delivering workspaces and supporting end users.

Endpoint virtualization for hospital administrators

Endpoint virtualization helps administrators improve operational efficiencies and regulatory compliance while meeting physicians' and employees' need for fast, easy workspace access in the following ways:

- **Accurate, instant reporting**—Extensive, on-demand auditing and reporting of workstations, users, and applications across the enterprise enable administrators to track who is working with what application in what location, at a moment's notice. Instant, detailed post-incident reporting improves forensics. In addition, comprehensive authentication and single sign-on reduce the risk of password sharing, increasing the accuracy of reporting and auditing.
- **Reliable, secure remote access**—Administrators can provide the remote working capabilities that physicians demand while lessening the risks associated with remote access.
- **Reduced IT costs**—Endpoint virtualization enables IT to allocate resources efficiently and cost-effectively by delivering desktops based on user requirements, which helps hospital administrators lower IT costs even as they transition to an increasingly digital information environment.

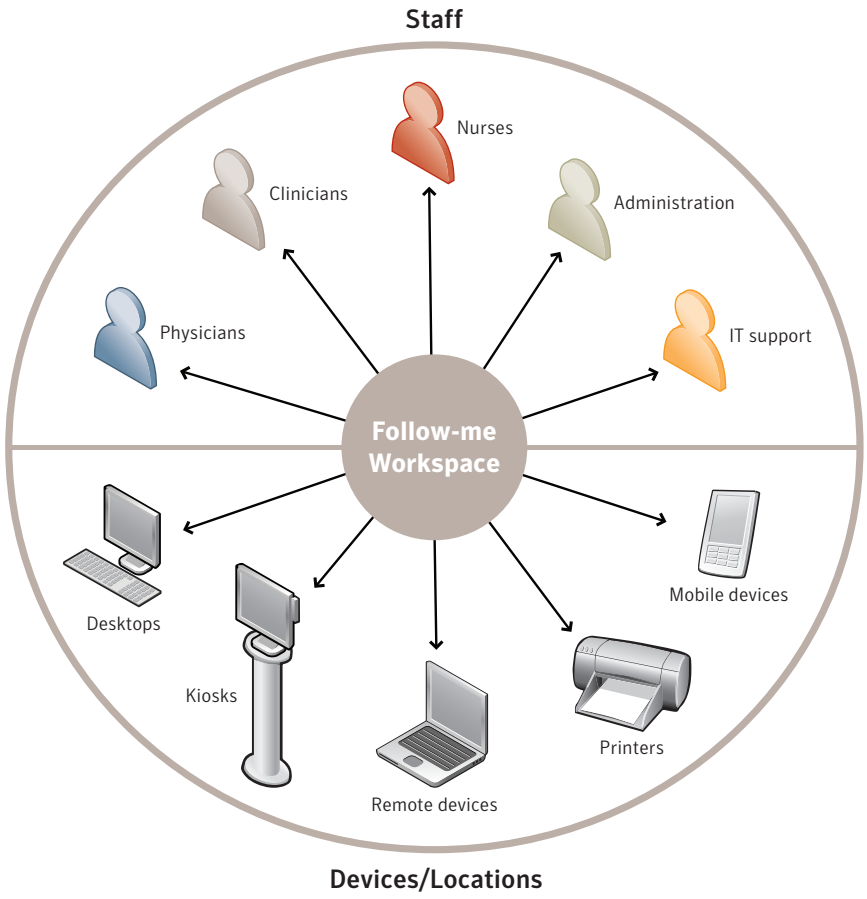

Figure 2. Endpoint virtualization provides staff with access to workspaces from any device.

Endpoint virtualization case study

A prominent healthcare facility recently implemented a Symantec™ endpoint virtualization solution. This 120-bed facility employs more than 1000 staff members, of which about 100 are physicians. After using the new implementation for an initial period, physicians expressed satisfaction with the roaming feature, which enables them to work at one workstation, suspend their work when they are called away from that workstation, and then resume work at another workstation at the same point where work was suspended. Physicians also took advantage of having remote, online access to the same applications they use at the hospital using a single sign-on.

From the IT department perspective, the system's advanced authentication was advantageous. The use of biometric (finger-pad) or key-card log-in eliminates password sharing, and session suspension protects the privacy of information in cases where users forget to log out. At this facility, users save their work to network drives rather than local drives, which eliminates the need to encrypt local hard drives. In addition, the system's role-based access and simplified user provisioning and deactivation enable better definition of user groups for application access purposes—as well as rapid user deactivation when employees depart the company.

Endpoint virtualization products from Symantec

The table below describes the capabilities of the various endpoint virtualization products available from Symantec.

Symantec endpoint virtualization products

Challenge	Symantec solution
• **Quick single sign-on** to applications from any location without multiple passwords or repetitive logons • **Fast user-switching** at kiosks and shared workstations • **Roaming** with the ability to transfer the workspace session to follow the user • **Location-aware printing** • **Customized workspace access** defined by user and role (doctor, nurse, radiologist, etc.) • **Flexible application delivery and management** with the ability to redirect applications from terminal services and run them locally	Symantec™ Workspace Corporate Symantec™ Workspace Remote
• **Secure clinical desktop access** from anywhere with an Internet connection • **Common clinical information access method**, both inside the hospital and remotely	Symantec Workspace Remote
• **Software virtualization**, eliminating application conflicts and allowing portability of applications and data	Symantec™ Workspace Virtualization
• **Instant access to applications** through on-demand streaming • **Dynamic license management** for automatic provisioning and reharvesting of idle licenses	Symantec™ Workspace Streaming

For more information about how Symantec can help your healthcare organization reap the benefits of endpoint virtualization, visit our Web site: www.symantec.com/healthcare

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at: www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

1/09 20004040