Health IT Needs Consistency and Resiliency

Provide workers and customers with anywhere, anytime availability of highly secure and compliant applications and workspaces.

Medical professionals are tasked with getting things done faster and more efficiently.

Time to service, patient satisfaction, and asset utilization rates are critical for healthcare providers competing in a rapidly changing market. Getting high marks rests in part with the provider's ability to ensure that its staff always has immediate access to whatever tools it requires to address patient needs.

For instance, clinical locations such as exam rooms, ERs, ORs, and nurse stations now often utilize a single endpoint device that serves multiple purposes. Since every provider attending to a patient within each of these environments has a specific job, it's common for each provider to leverage a different set of applications. A progressive healthcare network will recognize this diversity and ensure that with a few key strokes, it's possible to pull up a familiar, personalized environment that allows the technology to serve as a tool rather than an impediment.

Optimal bedside care also depends on availability of the right tools, and health organizations are increasingly relying on mobile technology that affords providers with immediate access to electronic health records (EHRs) for historical information (i.e., meds, previous treatments, sensitivities, etc.) as well as the ability to review test results (EKG, MRI, blood work, etc.), all without ever leaving the patient's side.

Hewlett Packard Enterprise

vmware®

CIO Strategic Marketing Services

Failure has dire consequences

Effectively mobilizing the medical team without putting the healthcare organization at risk starts with centralizing the delivery of the desktop applications. Of course, in doing so, organizations need to protect against falling prey to a network outage or component failure that could cause significant downtime or outage of client devices. Also, in an ER or critical care environment, mobile devices can easily leave the building, resulting in noncompliance with HIPAA HITECH requirements to keep patient data safe.

A progressive healthcare network will ensure that with a few key strokes, it's possible to pull up a familiar, personalized environment that allows the technology to serve as a tool rather than an impediment.

Additionally, healthcare providers are under constant pressure to remove costs, especially from an infrastructure perspective. Clinical computing in particular is a significant cost line item when considering the traditional tech refresh budget. Typically, healthcare organizations go through a 15% to 20% annual refresh of endpoints, whether they are handheld devices or desktop units. When tens of thousands of endpoints exist systemwide, even a 10% to 20% savings is significant.

Whether it's the outpatient, physician office environment, or the inpatient hospital environment, medical professionals are tasked with getting things done faster and more efficiently. Providing a consistent application experience is an important aspect in maximizing productivity and accuracy.

Security is also an ongoing issue, with highly sophisticated hackers increasingly targeting healthcare organizations with ransomware as a means to hold patient data hostage until the provider pays a set fee. The WannaCry ransomware that targeted around 300,000 machines in 150 countries is a prime example. Some of the victimized hospitals in the U.K. had to cancel outpatient appointments because they no longer had access to crucial patient records. Unfortunately, many of these healthcare organizations had no choice but to pay the ransom.

At the same time, mergers and acquisitions have naturally become commonplace as healthcare organizations seek new efficiencies. And as organizations merge, the expectation is that physicians will be able to easily cross boundaries from one provider to the acquiring provider. Unfortunately, those boundaries are very difficult to navigate—especially from an IT perspective. After all, in many instances healthcare providers have spent decades building complex legacy systems that have difficulty interweaving with other applications.

With each merger, the size of the distributed workforce continues to grow in size and complexity, encompassing more remote clinics, hospitals, urgent care centers, and primary care providers. As provider networks merge, there's a growing need to deliver a common, standardized set of applications capable of serving the needs of the entire merged workforce without spending months of integration work. IT is also faced with the growing need to gain staff acceptance as it rolls out new scalable solutions across an array of platforms.

Ensuring high availability and resiliency

Effectively addressing cost, security, consistency, and workspace efficiency starts with embracing a foundational infrastructure that furnishes healthcare providers with anywhere, anytime availability of highly secure and compliant applications and workspaces. This is where the VMware AlwaysOn Digital Workspace solution thrives.

Security is an ongoing issue, with highly sophisticated hackers increasingly targeting healthcare organizations with ransomware as a means to hold patient data hostage until the provider pays a set fee.

By combining VMware's Cloud Pod Architecture utilizing VMware's AlwaysOn Digital Workspace solution with HPE Proliant DL380 servers and HPE StoreVirtual VSA software, organizations gain access to a powerful virtual desktop-based workspace. This solution can play a pivotal role in developing new capabilities for health professionals who want to leverage centralized technology while striving to improve patient care.

Enabling a HIPAA HITECH-compliant, "follow me" virtual desktop. When lives are on the line, the importance of clinical workflow efficiencies takes center stage. The "follow me" virtual desktop empowers physicians or other medical professionals to maintain a constant work environment regardless of device. The key here is that the experience for the physician always remains the same, whether it's from home, an in-facility workstation, or a mobile device. For instance, from home a physician can tee up patient information based on who they are seeing throughout the day, lock their virtual desktops, and instantly pick up the applications in exactly the same state. Easy access without having to constantly navigate through desktop clutter remains intact the entire shift. The significance compounds quickly considering many medical professionals turn to their device repeatedly throughout the day—whether it's to check for potential med-based reactions before ordering a script within an emergency environment, or to look up test results during a follow-up office visit

Continuous availability for nonstop care. No healthcare environment can afford to suffer through a four-hour outage caused by a server crash. AlwaysOn addresses this by providing an architecture that has built-in, ultra-high availability—a true hallmark of the offering. The solution also has essential end-to-end redundancy. AlwaysOn architecture uses a number of complementary components to provide a variety of highly available services. Specifically, AlwaysOn leverages HPE StoreVirtual storage resilience within both a cluster and multisite design. This configuration provides automatic failover for individual servers as well as instances of management software within the solution stack.

Easy, cost-effective service expansion across extended affiliated provider groups. As healthcare organizations expand, especially through mergers and acquisitions, it translates to a large group of people IT needs to add to the mix. This architecture affords seamless support for local and remote locations with high levels of service and continuity of operations. It also reduces unnecessary outages or disruption in service from failed software updates or device hardware failure. In terms of cost-effectiveness, the centralized nature of the AlwaysOn Digital Workspace enables the use of lower-cost endpoints like tablets rather than costly desktops.

Keeping data away from threats

Communication between a client device and the VMware Horizon Virtual Desktop Infrastructure (VDI) is based on VMware's adaptive Blast Extreme protocol that is designed to ensure great user experience across varying network conditions—especially those with low bandwidth, high latency, and high packet loss. Blast is designed for real-time streaming of the graphical user interface (GUI) without including any data content when communicating to the user device. Therefore, traditional data protection measures, such as endpoint encryption, are not necessary. Similarly, loss of the end-user device is no longer a security issue because no data is locally stored or cached.

With AlwaysOn most of the end-user compute experience runs within the data center. AlwaysOn uses client virtualization to provide users with a real-time stream of the GUI—not actual data transmission. This substantially reduces the attack surface, controlling access to sensitive information on end users' devices as well as desktops common in the traditional healthcare setting, while keeping data safe in the data center.

AlwaysOn uses client virtualization to provide users with a real-time stream of the GUI—not actual data transmission.

This approach protects sensitive applications and restricts data by keeping everything centralized within the data center. IT can immediately apply software updates and security patches to protect the edge from malware or cyberthreats. This is crucial in eliminating zero-day vulnerabilities. It also provides policy- and role-based access control with a complete audit trail—logging and reporting to help ensure compliance. AlwaysOn also reduces risk by tracking, locking, and remote wiping devices that are compromised or lost.

Furthermore, VMware Identity Manager, which fully leverages the existing Active Directory environment, provides the core authentication and entitlement functionality. This user authentication process ensures that data never leaves the data center. This capability spans on-premises, remote, and mobile use cases across any device (running Windows, iOS, Android, or OS X). With multiple levels of access controls available, customers can tailor their authentication models in a variety of forms that best suit their business requirements.

The AlwaysOn Point of Care solution is compatible with most of the top anti-virus protection platforms, such as Trend Micro, McAfee, Symantec, and Sophos. These platforms are capable of running their services in VMware vSphere hypervisors, thereby offloading that task from the virtual desktops, which yields higher capacity and better user experience.

HPE & VMware: Alliance for healthcare transformation

Drawing on over 16 years of partnership, engineering, and joint investment, the alliance between HPE and VMware provides its clients with comprehensive solutions that benefit from HPE serving as the one end-to-end support provider. As industry leaders, HPE and VMware are constantly collaborating to revolutionize virtualization economics and efficiencies for the client.

For instance, HPE management tools are designed to work with VMware to enable the best managed VMware environment, with key integrations for HPE OneView, to allow the richness of management data provided through ESXi.

Together, HPE and VMware have a proven track record of addressing key business challenges for IT organizations by improving cybersecurity, supporting transformation initiatives, lowering cost, and increasing automation.

For more information, please read our white paper: HPE Reference Configuration for building a VMware AlwaysOn Digital Workspace with HPE ProLiant DL380 Gen9 servers