Secure Healthcare IT Environments and Solve Endpoint Challenges

PROVIDED BY

healthcare innovation
PEOPLE. PROCESS. TECHNOLOGY TRANSFORMATION.

IN COLLABORATION WITH

Quest™ | KACE™

KACE® solutions help healthcare organizations safeguard patient data and automate endpoint management challenges

With the universe of devices being used in the healthcare workplace and constantly shifting business arrangements — such as mergers and acquisitions, the development of accountable care organizations and value-based payment contracts, and the ongoing evolution of health information exchange — healthcare information technology leaders face a dramatically shifting landscape.

Strategies such as mobile device management and enterprise mobility management have evolved to try to meet at least some of the needs of patient care organizations everywhere. But, over time, it has become clear that broader strategies need to be developed and executed as hospitals, medical groups and health systems are more vulnerable than ever before to the potential and actual attacks being launched against them by cybercriminals and others.

Ultimately, unified endpoint management (UEM) is the broader, overall strategy emerging as a successful approach in healthcare as it has been in other industries.

A number of recent white papers, studies and reports speak to the broad issues. They have noted, among other things, that numerous advantages accrue from a UEM strategy through unifying the application of configurations, management profiles, device compliance and data protection; providing a single view of multidevice users; enhancing efficacy of end-user support; and gathering detailed workplace analytics. In addition, developing such a strategy can act as a coordination point to orchestrate the activities of related endpoint technologies, such as identity services and security infrastructure.

However, industry experts also note that one of the limitations of a UEM strategy is that it does not fully account for the true, complete range of tools involved — all computers, internet-of-things (IoT) devices and so on. Looking at the issue from a mobile device-centric standpoint remains limiting. Flexibility in managing any device in the future, and at a granular level, is a huge challenge. Managing servers also stands outside a UEM strategy, while flexibility around all objects and the ability to manage server security remain as major challenges. And the dramatic expansion in the number of devices that will need to be managed in the coming years in healthcare points to challenging problems around security, compliance and costs.

Recent studies and reports also found that the majority of healthcare organizations don't employ software or services to help automate the management and provisioning of unified

communications-enabled devices. Instead, they have found that IT departments spend extensive amounts of time every year with manual troubleshooting and device management.

HIPAA and its connection to endpoint management

One important element in this landscape is the Health Insurance Portability and Accountability Act (HIPAA). Most of its provisions relate to health insurance portability, but a significant number of provisions concern the privacy and security of protected health information (PHI).

Three main rules within HIPAA connect to the handling of patient health information:

- The Privacy Rule details how PHI can be used and disclosed.
- The Security Rule encompasses the necessary standards and safeguards needed to protect electronic PHI at rest and in transit.
- The Breach Notification Rule requires organizations to notify patients and the proper authorities in case of a PHI data breach. The Department of Health and Human Services' Office for Civil Rights has been responsible for the enforcement of HIPAA since 2003.

The American Medical Association provides an in-depth explanation of the Security Rule on its website: "The HIPAA Security Rule requires physicians to protect patients' electronically stored, protected health information (known as "ePHI") by using appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of this information. Essentially, the Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and nontechnical safeguards that covered entities must implement to secure ePHI.

"All covered entities must assess their security risks, even those entities who utilize certified electronic health record (EHR) technology. Those entities must put in place administrative, physical and technical safeguards to maintain compliance with the Security Rule and document every security compliance measure."

Cyberattacks and a unified endpoint security strategy

Cyberattacks are increasing across all industries, and cybercriminals are savvier than ever. While the total number of IT vulnerabilities is decreasing, the number considered critical is on the rise — and so are the number of actual security exploits. In that context, patient care organizations are at greater risk of disruption more than ever, with the very strong potential for

financial and reputational damage. What's more, endpoint updates are more complex and challenging than ever with the proliferation of smartphones, tablets and other devices. Bring-your-own-device (BYOD) programs and IoT technologies further complicate security. Each device connecting to your system increases the number of threats from malware and viruses.

Recent surveys and studies have found clear, persistent dangers around securing healthcare data and managing cybersecurity. According to the Healthcare Information and Management Systems Society's 2019 HIMSS Cybersecurity Survey, "Healthcare data is widely used internally and must be exchanged with a wide variety of entities in order to facilitate the coordination and delivery of care — something that is complex in and of itself, but securing this data, too, adds on an additional layer of complexity."

In that context, healthcare IT managers are working harder and longer to secure their growing endpoint environment against malicious and unintentional attacks alike and are facing more frequent system downtime with loss of data and productivity. Meanwhile, maintaining compliance with security regulations is becoming more complicated, and fines are increasing.

What's needed is an endpoint security strategy that provides IT managers with clear visibility into all the devices connecting into their network, and also provides automated patching and software deployment to ensure that all endpoints are fully protected for in-house as well as remote end users.

It's vital for IT managers to protect their endpoints from a wide range of threats, including unpatched operating systems and applications, out-of-date software and improper security configurations.

Experts weigh in

Even as the threat level intensifies in the current moment, the business activity involving mergers and acquisitions sweeping the industry significantly complicates the management of networks in healthcare organizations. "The ongoing consolidation of patient care organizations is really making all of this considerably more complex," says Ken Galvin, a senior project manager at Quest Software®. "For one thing, if you don't know what you have on your network, you can't manage it, period. As a result, you can't secure it. Is there a Raspberry Pi on a static place on a server? It has to be managed. And not just on a lifecycle level, where you need to repair or retire or replace items, or service them. You need to know what the attack vectors are. In terms of using these devices, you have devices that are ensuring hand hygiene compliance, and those devices are on the network." In all this, Galvin says, after engaging in a very comprehensive inventorying process, moving forward to securitize everything is the next, enormous step in the process.

Jillian Salamon, a pre-sales engineer at Quest®, agrees. One of the core challenges here, she says, is the very breadth of the tools, systems and devices involved. "There was always something known as systems management, which refers to managing traditional endpoints — desktops, laptops, servers," she notes. "As things have progressed, and mobile devices have come into the work environment, customers wanted to be able to manage those types of devices just as with traditional endpoints. So that's the origin of the term 'unified endpoint management' — not having four different products managing endpoints."

The end user's perspective

Justin Wunder, a network specialist at Gilsbar, shares his organization's real-world experience with these issues. Gilsbar is a health and business management organization that partners with larger insurance companies and smaller clients that bridge that gap and make sure that everyone works well together to become a healthier, more efficient business. "I work as a network specialist in the company, so I'm the main middleman between the infrastructure teams and the end users at our organization, to make sure they're up and running and being as efficient as possible," Wunder says.

"Some of the biggest challenges that we had were with patching in security," Wunder notes. "Our company, which is about 500 users strong, mainly uses laptops in case of disaster. So one of the biggest things that we're having issues with is making sure that all the computers are patched and constantly up to date and being secure. Being in a health type of organization, we deal with a lot of personal information. We want to make sure that we are as secure as possible when dealing with our users' information. After implementing KACE, we were able to get our patching up to near 100 percent, making sure that we are being a very secure company, ensuring that all of our own computers were always up to date, always the most secure, and never vulnerable to outside attackers or to losing information. We use it to make sure that we are all in compliance, as well. So we use the inventory systems to make sure that all of our computers are running the proper software and don't have anything that shouldn't be on them. We're able to run a lot of auditing and reports on each individual computer."

Speaking of the Quest® KACE® Systems Deployment Appliance (SDA) features, Wunder notes, "We also use the KACE SDA; it enables us to be able to roll out new computers. That means that if someone's having an issue, we can easily remedy that by just picking up their old computer, using the KACE SDA to image a brand-new computer, and pushing that back out to the users, so they have minimal downtime."

"I find that KACE saves a lot of time at work," he observes, "because if you end up having a really big issue that can be complicated to fix, that can cause you to have hours of downtime. But for us, using the KACE SDA, if someone's having a really big issue, rather than taking six hours to work on that issue, we can instantly just deploy another brand-new computer

right to them that has all of their software that's required for them to do their job — which enables us to get it to them in about 45 minutes to an hour." In all of this, he attests, there is peace of mind: "I know that if I have my patch schedule running every weekend, I don't have to worry or think about anything. And then, once I go home, I can actually relax and enjoy the little things."

Five steps to building a unified endpoint security strategy

Technical experts at Quest have been able to outline for their clients a comprehensive strategy of five core steps for achieving unified endpoint security using the Quest UEM solution supported by the KACE portfolio of products:

- **Step 1:** Automate inventory management and deploy anti-virus software to all endpoints.
- **Step 2:** Automate patch management and vulnerability scanning.
- **Step 3:** Track and manage mobile assets remotely.
- **Step 4:** React quickly to reimage systems when you suspect an endpoint infection.
- **Step 5:** Administer appropriate access rights by restricting user privileges and USB access.

Visibility is key

Quest experts agree: If you don't know what you have on your network, how can you manage it? With the rise in BYOD programs and IoT devices, visibility into your entire connected environment becomes increasingly critical. From computers and servers to routers, printers and more, the KACE Systems Management Appliance (SMA) discovers and helps you manage all hardware and software installed across your network. The KACE SMA provides you with ongoing automated IT inventory management, IT asset management and software asset management capabilities. With robust reporting and alerts for most platforms, you can quickly view all assets and hardware on your network for refresh planning or preparing for an audit. Whether you're running Windows, Mac OS X, Linux, UNIX or Chrome, the KACE SMA gives you detailed oversight of your entire environment from a single console.

Administrative capabilities

You can experience robust security with the KACE SMA. Doing so will help you to automate patch management and deploy patches from one of the largest patch libraries in the industry. Achieve peace of mind by patching and updating your Windows and Mac platforms as well as potentially vulnerable third-party applications, such as Adobe Reader or Oracle Java. Get powerful administrative capabilities, including customizable and automated patch scheduling based on dynamic filtering, and detailed tracking and reporting on the status of patches.

Remotely track and manage mobile assets

It's important to discover and manage mobile assets remotely. The KACE Cloud Mobile Device Manager (MDM) simplifies mobile endpoint management, so you're able to protect your organization's investment in both Android and iOS mobile devices while simplifying device configuration and deployment. Effectively manage your organization's BYOD or corporate-owned mobile device programs all from a single solution, while identifying, remotely inventorying, securing and controlling all devices that access your network. If a mobile device goes missing, you can lock it and wipe its data to ensure company information is safe. Send specific commands to any mobile device that has been registered — and remotely inventory, lock, unlock, erase or factory reset the device or its password. When integrated with the KACE SMA, the KACE Cloud MDM helps streamline your transition to UEM, giving you visibility into the inventory of traditional and mobile devices from the same interface.

Reimage systems and devices

It's important to quickly reimage systems when you suspect an endpoint infection. If you suspect that an endpoint is infected with a virus, don't take any chances — reimage the device. Simplify system imaging and software deployment with the KACE SDA. Eliminate manual processes for building and maintaining gold master images for multiplatform OS imaging and deployments. Make automated deployment, image storage and management easier with access to a centralized deployment library. All system and software deployment assets, including images, scripted installations, drivers, applications and scripts, are found in the deployment library. All images are captured and stored to give you an accurate, comprehensive view, eliminating the need for removable media, such as CDs and DVDs.

Administer appropriate access rights

To avoid security breaches, it's critical that users have the correct level of access to systems containing sensitive corporate data. Without visibility into which endpoints are connecting to the network, administrators can't easily keep track of which systems specific users are

accessing. KACE Privilege Manager addresses the issue by giving users varying levels of local administrator rights on their Windows machines. By default, users get least-privilege rights to access the systems they need, and only specific users get administrator rights. This prevents unauthorized users from accessing sensitive data and possibly spreading malware that could infect that data. Endpoints also include printers, cameras, external drives and other devices that have USB ports in various locations. Left unattended, any of the USB ports in these devices could be exploited to introduce malware into the network. There is also a risk that precious company data will leave the business. Administrators can restrict access to USB ports with KACE Desktop Authority®, which secures USB-equipped endpoint devices. Using a least-privilege approach, administrators can granularly control who accesses which USB ports, and where to block malware and prevent data theft. Maintain the balance between security and user productivity while saving IT resources.

Looking ahead into the future

How will this entire landscape evolve in the coming years? Quest's Ken Galvin says: "Achieving UEM is actually going to become a critical accomplishment for healthcare IT leaders; it will be an essential capability. What's more, integrating mobile device management and client-based management into a single function will be an element in that overall strategy. I will need to be able to look at your computer, your phone, any device you're using, from anywhere."

"More and more, we'll go to cloud-based management," he says. "There will always be those who need on-premises only — for example, a Department of Defense dark network, or a lot of financial institutions. But customers are becoming more and more comfortable with the cloud, and they're being driven that way because they're using so many apps like Slack and Office 365 and OneDrive now. The bottom line will be flexible control. Any set of vendor solutions that doesn't offer IT managers and executives that capability will become far less useful over time."

****

Key takeaways

Strategies such as mobile device management and enterprise mobility management have evolved to try to meet at least some of the needs of patient care organizations around information security. Ultimately, UEM is the broader, overall strategy emerging as a successful approach in healthcare.

- Three of the major HIPAA provisions — the Privacy Rule, the Security Rule and the Breach Notification Rule — concern the privacy and security of PHI.
- Healthcare IT managers are working harder and longer to secure their growing endpoint environment against malicious and unintentional attacks alike, and are facing more frequent system downtime with loss of data and productivity.
- What's needed is an endpoint security strategy that provides IT managers with clear visibility into all the devices connecting into their network, and provides automated patching and software deployment to ensure that all endpoints are fully protected for in-house as well as remote end users.
- Technical experts at Quest have been able to outline for their clients a comprehensive strategy for achieving unified endpoint security using the Quest UEM solution supported by the KACE portfolio of products.
- The Quest experts' recommendations include five steps on automating inventory management and deploying anti-virus software to all endpoints; automating patch management and vulnerability scanning; reacting quickly to reimage systems that might have experienced endpoint infection; tracking and managing mobile assets remotely; and administering appropriate access rights.

Quest experts agree: Achieving unified endpoint management is an essential capability for healthcare IT leaders going forward.

It can be challenging to manage a diverse IT environment with a variety of operating systems, devices and applications. The Quest UEM solution enables you to discover, manage and secure assets across a variety of platforms, from Windows, Macintosh and Linux to iOS, Android and others. Being able to manage multiple platforms from a single solution not only saves time, it also reduces risk because all admin and management tasks are controlled in the same place. When you must manage each platform individually, vulnerabilities increase, and the risk of human error becomes greater.

With the KACE Go Mobile App, you can access the KACE SMA from your Android or iOS mobile device and manage your endpoints effectively across multiple office locations while traveling. Because healthcare organizations manage a lot of sensitive data such as PHI, cybercriminals see your healthcare institution as a prime target. Manual patch management takes a lot of time and increases the risk that vulnerabilities in your environment will go undetected.

The Quest UEM solution enables you to be proactive with patch management and security.

The KACE SMA provides one of the most robust patch libraries in the industry, covering Windows, Macintosh and third-party applications.