Delivering Healthy IT Outcomes

Healthcare professionals depend more and more on IT as a way to provide better patient care. However, their increasing reliance on IT means these systems must be more efficient and responsive than ever, so caregivers can stay focused on the patient.

Protect Patient Data

Electronic Health Records (EHRs) contain some of the most sensitive, personal data organizations access. The data's confidential nature makes healthcare organizations frequent targets for hackers and other cybercriminals. EHRs are shared across medical facilities and healthcare networks, on devices running several applications. Ensuring the IT environment has up-to-date security policies and processes is critical to safeguarding patient data and maintaining compliance with HIPAA and other regulations. But how do you apply security updates successfully without taking devices offline?

A flexible, automated patching solution is critical to reducing the time of exposure to vulnerabilities while operating in an environment of zero tolerance to downtime. Healthcare firms must look to a patching solution that can work with existing tools such as Microsoft SCCM, but also patch quickly the thousands of third-party applications used in healthcare networks. Firms require a patching solution that can separate and prioritize vulnerability patches, while allowing for minor updates and bug fixes to be applied on a schedule of convenience. Finally, these organizations must be able to have the patches applied automatically while employing a staggered schedule that fits the demands of a 24 x 7 healthcare environment.

Enable Appropriate Access

Nurses can log in to 75 or more stations during one shift. With so many sessions, logins must be fast wherever caregivers are working. They need immediate access to the tools, applications, and data to do what they do best—care for patients. Personalization is imperative to enable more time for patient interaction, but also to reduce clinical risk. This means employing a least-privilege access approach across the devices nurses, clinicians, and administrative staff carry and the apps residing on each platform.

Gain Visibility to Devices and Apps

Regional mandates such as the European Union's Mobile Device Regulation (MDR) compel healthcare organizations to have better traceability of medical devices. Still, meeting regulatory requirements such as the MDR and its forthcoming Eudamed database are just some of the reasons visibility is so vital in the healthcare industry.

It happens more often than organizations like to admit—the unauthorized application or device "hand-carried" into healthcare environments. Shadow IT occurs in every industry, but the risks can be significantly higher in healthcare if patient data is compromised. Beyond ensuring compliance, the software that entered through some back door is now another asset to track and support, adding to costs and security risks. What type of asset is it? Who's using it? Where's it located? Were any commitments made around usage, license transferability, or auditing? Gaining visibility into all assets that touch the healthcare network is foundational to manage, secure, and optimize the environment properly. Turn that visibility into further value for your organization when you track asset lifecycles, manage vendor scorecards, and optimize license spend with automated reclamation processes.

Maximize Uptime and Connectivity

Face it. There's no time for downtime in the high-pressure world of healthcare. That includes IT outages from

ivanti

planned or unplanned changes. Your healthcare environment must maintain clinician productivity, with practices that speed the discovery of root causes to issues before they impact clinicians at the point of care.

In addition, effective Change Management processes—incorporated into service management systems—are critical to avoid unnecessary downtime that hinders medical staff, places patients at risk, and hikes the IT organization's workload. These processes help IT teams better control risk, ensure compliance, and protect the availability of critical applications and services during needed IT changes.

Elevate Interoperability

More and more, healthcare CIOs look to consolidate vendors. No doubt there are economies of scale to be realized in purchasing, but a deeper intent resides in system performance, shared workflows, and actionable data. IT leaders look to solutions that solve more than a single challenge.

In many cases, this is a reduced set of vendors that have compatible products easier to use, supporting the broadest range of IT environments. For the best outcomes, they search for systems that can deliver visibility across endpoints, providing real-time insights across the organization's technology estate. This is possible when enterprise service management solutions are truly integrated with security and endpoint management, completing the picture for systems administrators.

Our proven solutions help healthcare organizations worldwide maintain compliance while delivering a better IT experience so caregivers can focus on the patient. Ask how you can achieve healthier IT outcomes with Ivanti.

Learn More
▸ **ivanti.com**
☎ **1 800 982 2130**
✉ **sales@ivanti.com**

Ivanti in Healthcare	
Common Challenges	**Remedies**
Protect Patient Data	▪ Simplify patching across physical and virtual environments ▪ Reduce time to patch by integrating with tools such as vulnerability scanners ▪ Secure apps on legacy systems that don't or can't get patched ▪ Prevent the introduction of unauthorized apps or code ▪ Employ secure configuration management
Enable Appropriate Access	▪ Accelerate login times ▪ Deploy least-privileged access approach across applications and device platforms
Gain Visibility to Devices and Apps	▪ Integrate various data sources (from spreadsheets, inventory sources, and connectors to other systems, etc.) ▪ Normalize and reconciliate this data for single point of truth ▪ Manage asset lifecycles end-to end ▪ Correlate service support and asset data
Maximize Uptime and Connectivity	▪ Improve insight and coordination to IT changes ▪ Better risk visibility and mitigation ▪ Improve governance and compliance ▪ Reduce unplanned outages and downtimes

Elevate Interoperability	▪ Remove dependencies
	  • Use cloud or on-premise
	  • Agnostic support for hardware and OS platforms
	▪ Augment the value and extend the life of connected systems
	▪ Unified reporting
	▪ Real-time insights across estate