Unisys Stealth Security for Healthcare

Securely Protect PHI *and* your Healthcare Investments

Patient Personal Health Information (PHI) is the most critical, valuable and sensitive data moving through the healthcare system today. The ultimate goals of today's healthcare system is to securely link all related information to each patient within and across systems. Patient trust, safety and concern are the new vulnerabilities. The increasing onslaught of sophisticated cyber attacks and alarming data breaches have moved the protection and maintenance of PHI integrity high up on the global agenda.

Increasing Pressures All Around

Healthcare Executives are under intense pressure to protect their organizations from DDoS, insider threats, lost laptops and smart devices, compromised BYOD and other risks that jeopardize the security of highly sensitive patient information. In addition:

- Regulations like HIPAA, HITECH, ACA (Affordable Care Act) and Meaningful Use are driving tightened security and controls, further squeezing limited budgets;
- Mobile, cloud, social media, and other disruptive technologies are being integrated into organizations faster than they can be safeguarded;
- Aggressive cost-cutting agendas are degrading security programs at a time when threats and data breaches are escalating.
- Patient privacy has become a major driver of patient/consumer trust and loyalty, making any breach both a public relations nightmare and a financial disaster.

HIGHLIGHTS

- **Segment your data center based on users.** Define and control access to the sensitive information you are entrusted to protect.
- **Go undetectable – conceal communication endpoints.** Make servers, devices, and other communication endpoints undetectable.
- **Secure data in motion.** AES-256 encryption and patented key management secures data in motion.
- **Reduce reliance on physical infrastructure for security.** Consolidate physical networks and reduce costs.
- **Quickly respond to the needs of your business.** Easily update security access privileges through Active Directory.

A *Truly* Innovative Approach

Unisys Stealth™ software-based security makes data communication endpoints undetectable to unauthorized users and protected data-in-motion across any network. Stealth helps reduce the attack surface, increase data protection and simplify management. Healthcare executives therefore no longer need to balance the traditional tradeoff between cost and risk – they can increase security and reduce costs.

Unisys Stealth brings unprecedented security to healthcare providers and payers and to the patients they are entrusted to protect.

- **Strengthen security** by making communication endpoints, such as laptops and servers, undetectable to all unauthorized parties inside or outside the enterprise
- **Reduce costs** by decreasing reliance on traditional physical IT infrastructure
- **Simplify security management** and enhance agility and control with the ability to easily scale to emerging needs and adapt to change

How Can Healthcare Organizations Use Stealth?

Leading healthcare providers and payers can implement Unisys Stealth across their healthcare systems to help them protect what matters most.

Compartmentalize the data center and reclassify sensitive patient data based on need-to-know access.

- Consumerization of IT, cloud computing, and breach attempts are driving healthcare executives to segment their networks and data centers.
- Unisys Stealth is designed to securely micro segment data centers and protect data and systems by cloaking strategic assets.

Confidently embrace mobility – improve patient experience while strengthening security.

- The proliferation of mobile devices is unstoppable. The chance of malware attack is high. Already, 46% of organizations allowing BYOD (Bring Your Own Device) have had a data breach attributed to employee devices accessing the network.[1]
- Unisys Stealth(mobile) provides a comprehensive, innovative approach to mobile security – security follows the user, not the device, so your sensitive data is protected from inside and outside your enterprise.

Ensure only the right personnel have remote access to sensitive patient information.

- Stealth is designed to cloak endpoints from users or devices except those who are pre-identified as part of a secure Community of Interest (COI).
- You can manage access to sensitive information by establishing COIs and restricting members on a need-to-know basis up and down the global supply chain.

Get more leverage from the cloud

- Stealth-protected servers or virtual machines are cloaked from other tenants in the cloud and from hackers attempting to infiltrate the cloud.
- This enables you to confidently deploy sensitive workloads in the cloud and take advantage of the associated cost savings.

For more information, please contact:

stealth@unisys.com

www.unisys.com/stealth

[1] Decisive Analytics, Mobile Consumerization Trends & Perceptions - IT Executive and CEO Survey, 2012

STEALTH™

Printed in the United States of America 04/16 16-0185