

Healthcare organizations today face an unprecedented set of vulnerabilities, compliance requirements and risks when it comes to securing their online networks and protecting patient data. With the extension of the reactive patient data requirements in HIPAA to the more preventative security requirements in the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act, organizations are now required to take broader and more stringent steps to protect against data breaches while at the same time sharing patient data more easily amongst those parties authorized to view it.

Meanwhile, with billions of federal government dollars set aside to facilitate the move towards electronic medical records (EMRs), and with hospitals moving towards unprecedented connectivity of their various IT systems, never before have there been so much data on – and so many potential attack vectors into – healthcare networks.

### **Evolving Security Risks in Healthcare**

The HITECH Act, signed into law as part of the 2009 stimulus bill, requires that patients be notified when there is a breach in their protected health information, as well as that breaches involving more than 500 individuals be reported in prominent media outlets. Additionally, the Act broadens responsibilities to related organizations that use electronic health records (EHRs) from the principal healthcare organization, requiring that they also provide patients who request it with an expanded accounting of disclosures.

A third new privacy and security requirement in the HITECH Act provides for much more aggressive privacy and security compliance monitoring and enforcement, with fines ranging from \$100 to \$1,500,000 for a single violation, and also enables a state's Attorney General to pursue civil actions on behalf of residents for HIPAA privacy and security violations, with damages ranging from \$100 to \$25,000 per violation.

Add to this equation the need for many healthcare organizations to meet security requirements outlined in the Federal Information Security Management Act (FISMA), and the Payment Card Industry (PCI) Data Security Standard, and a broad range of organizations in the healthcare industry now face constant risk for significant public exposure as well as stiff fines for any security breach or leakage.

The latest medical devices and many new EMR software systems have moved to commercial operating systems in order to provide easier network connectivity and interoperability with available monitoring and reporting tools. However, these devices now share the same vulnerabilities that traditional network and server infrastructures are susceptible to, such as viruses, trojans, worms, application and resource attacks, and Distributed Denial-of-Service



***The Conficker worm found its way into nearly 300 MRI machines and other hospital equipment connected to the Internet throughout the United States and around the world.***

(DDoS) attacks. To make matters worse, patches for these vulnerabilities are few and far between because the FDA regulates any changes to medical devices or systems be submitted 90-days before any machine can be patched, leaving these systems exposed to attacks.

For example, the San Jose Mercury News reported that the Conficker worm, which created a massive botnet (a collection of infected zombie computers that are programmed to call into a command center for instructions on how to spread malware and spam), has found its way into nearly 300 MRI machines and other hospital equipment connected to the Internet throughout the United States and around the world.

This alarming discovery has hospital administrators concerned that the Conficker worm will threaten hospital operations and pose a serious risk to the security of patients' records.

### **Protecting Healthcare Networks**

Healthcare IT administrators tasked with security and availability concerns rely on technology to help them achieve their business objectives. In the realm of network security, Intrusion Prevention System (IPS) solutions have rapidly become a

requirement for building secure network infrastructure. Implementing the proper IPS solution is considered a “best-practice” in the eyes of healthcare IT administrators trying to comply with the latest regulations affecting healthcare. An IPS must be employed to protect healthcare organizations in two critical areas:

- Protection of infrastructure used to store and transfer patient data across networks
- Defense of medical systems that are vulnerable to remote exploits of commercial or open-source operating systems and applications – these can range from actual devices used for patient care such as MRI machines, to the 100+ certified EMR systems (with more on the way) in use today

If these systems are left unprotected, vulnerabilities may be exploited to allow attackers to:

- Steal confidential documents not intended for their eyes
- Execute commands on the server host machine, allowing them to modify the system
- Gain information about the provider or insurance company computer that will allow them to break into the system and steal private information, such as patient records
- Cause disruptions to normal hospital operations, including the use of critical medical devices

### Customer Example

Healthcare organizations throughout the world depend on Top Layer's IPS 5500 network intrusion prevention solution for the highest levels of network security. By reducing the risk that computers become compromised, the IPS 5500 helps healthcare organizations achieve the level of protection of client information that their customers expect.

Leading healthcare providers such as the Miller School of Medicine in Miami, FL leverage the Top Layer IPS solution to protect the integrity of their network and meet the strict compliance requirements that all healthcare providers face. The IPS 5500 enables the Miller School of Medicine to protect critical data infrastructure used to store and transfer patient and confidential data across the network providing the organization with a much higher level of overall security.

The net result is a higher level of protection of patient and critical medical device protection while at the same time reducing IT operating expenditures.



### Getting the Right Network Protection for Healthcare

Top Layer is the leader for Intrusion Prevention System (IPS) solutions for healthcare organizations facing the security challenges discussed above. The Top Layer IPS 5500 delivers the right protection, performance and reliability to provide healthcare organizations the confidence to ensure secure infrastructure for handling patient data, while providing proper availability in order to ensure compliance. The Top Layer IPS 5500 secures critical IT infrastructure by preventing undesired access, protecting against malicious content that exposes private data, and stopping rate-based attacks, all crucial elements in fulfilling the expanding government compliance requirements and patient expectations in healthcare.

Combined with a defense-in-depth strategy, Top Layer's IPS 5500 intrusion prevention system provides healthcare organizations with:

- Reduced risk of data breach or service outage
- Increased network bandwidth availability
- Increased network performance
- Continuation of transaction flow even in the face of brute force DDoS attacks

As security threats and related compliance requirements both evolve, healthcare organizations require security solutions that can address their complex and ever changing needs. The Top Layer IPS 5500 is the only solution that can deliver the right protection, performance, and reliability to provide a secure and reliable network for healthcare institutions, their partners, and their patients.

**For more information on Top Layer Security and its award winning IPS  
Call +1.978.212.1500 or visit our website at [www.TopLayer.com](http://www.TopLayer.com)**

### About Top Layer

Top Layer is a leading provider of Network Intrusion Prevention Systems (IPS) that reduce organizations' risks and losses by protecting critical online assets against cyber threats. Its family of high performance IPS provides the most advanced protection against known and zero-day threats at maximum throughput rates. Top Layer is headquartered in Massachusetts, USA, with Global Sales and Support throughout North America, Europe, Asia, and Japan.

Rev 1.0 01-Oct © 2009. Top Layer Networks, Inc. All Rights Reserved. Attack Mitigator, TopInspect, TopMSS, and ProtectionCluster are trademarks of Top Layer. SecureWatch, Top Layer, and Top Layer Networks are registered trademarks of Top Layer.

**Top  
Layer<sup>™</sup>  
Security**