

## Securing Critical Data and IT Infrastructure in Healthcare Environments

## General Healthcare Security Trends

Healthcare organizations are in the midst of a complete turn around in regard to information security and privacy. A few years back, a medical facility was a very open environment. Hospitals had large sprawling networks that interconnected to other hospitals and clinics. In some cases, connections were also established to medical colleges and research organizations. It was not uncommon for interns or medical students to browse through medical records, and little to no consent was considered surrounding privacy.

Times have changed. Through the onslaught of regulations and privacy liability, healthcare organizations are changing course. Where before the typical healthcare facility could be considered an open environment, today's healthcare facility is moving to one of control, confidentiality, integrity, and accountability.

Conversely, healthcare organizations are also challenged to make information more available to physicians and patients. Patients want to access their medical data online. Physicians want immediate access to lab reports and diagnosis – at times from remote parts of the world. More and more medical devices are also being connected to large healthcare networks, often with exposed commercial operating systems that control them.

The seemingly paradoxical demand in healthcare organizations today is increased *availability and security*. Without a defined security architecture in place this would truly be impossible.

## TippingPoint Addresses Healthcare Concerns

TippingPoint provides the solution to both availability and security with the TippingPoint IPS. TippingPoint is the industry's leading Intrusion Prevention System (IPS), unrivaled in security, performance, high availability, and ease-of-use. Unlike passive-mode Intrusion Detection Systems, the TippingPoint IPS operates in-line in the network, blocking malicious and unwanted traffic, while allowing good traffic to pass unimpeded. As the only Intrusion Prevention System to receive the NSS Gold Award, SC Magazine Best Buy and Common Criteria certification, among many other awards, TippingPoint is the defining benchmark for network-based intrusion prevention.

Only a short time ago, Intrusion Prevention Systems were considered leading-edge technology – not ready for prime time. But very quickly, network-based IPS devices have proven their value throughout thousands of organizations. IPS has rapidly become an accepted standard and is considered a “best-practice” in the eyes of healthcare organizations trying to comply with industry mandates such as HIPAA, Sarbanes-Oxley, and FDA CFR Part 11. TippingPoint's TippingPoint IPS also protects medical systems from medical device manufacturers that often go un-patched due to FDA regulation concerns.

Through a robust Intrusion Prevention reference architecture as detailed in this whitepaper, TippingPoint provides healthcare organizations the means to ensure a high level of security and privacy of patient information while providing legitimate access to data and high availability.

## HIPAA Security & Privacy

The primary driver for security in healthcare environments is the Health Insurance Portability and Accountability Act of 1996 - Public Law 104-191 (HIPAA). Congress enacted this regulation with a focus on healthcare reform. The legislation gives authority and requires the United States Department of Health and Human Services (HHS) to develop standards and requirements for maintaining and transmitting health information, including the privacy thereof.<sup>1</sup>

Overall, HIPAA is aimed to improve the efficiency of healthcare data and processing through the standardization of administrative and financial data transactions, while protecting the privacy and integrity of patient information.

The HIPAA regulation includes specific sections on privacy and security:

- **Privacy** — These standards require the protection of patient data from inappropriate and unauthorized disclosure or use<sup>2</sup>
- **Security** — These standards require the safeguarding of patient data from unauthorized access. The security safeguards fall into three categories (as defined by the regulation):<sup>3</sup>
  - **Administrative Safeguards** — Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information
  - **Physical Safeguards** — Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion
  - **Technical Safeguards** — Technology and the policy and procedures for its use that protect electronic protected health information and control access to it

The HIPAA regulation impacts providers, healthplans, and healthcare clearinghouses. Many large organizations that are self-insured fall under HIPAA compliance as well.

Failure to comply with the HIPAA privacy and security standards results in both civil and criminal penalties. The penalties for non-compliance range from \$100 to \$250,000 with up to ten years imprisonment time per infraction. These penalties do not take into account the loss of confidence in providers, investors, customers, and other institutions and companies in the healthcare industry. The first criminal prosecution and conviction under the HIPAA privacy rule occurred in *US v. Richard W. Gibson* in August of 2004.<sup>4</sup>

### TipingPoint's Solution for HIPAA

Integrating TipingPoint into a healthcare network addresses many of the HIPAA requirements for securing protected health information. The TipingPoint IPS protects by:

- Protecting against unauthorized access to the network and malicious attacks against networked equipment and medical systems
- Providing constant vigilance against emerging vulnerabilities
- Provides detailed reporting options for reviewing network behavior and blocked attacks

### TipingPoint: Protecting Access and Traffic

Healthcare organizations manage vast amounts of data ranging from personal medical records to insurance claims. Access to data must be restricted according to the user's role. The TipingPoint IPS enforces security by preventing unauthorized access to PHI at the network level. The system detects and prevents malicious traffic, including virus and worm outbreaks, which often contain Trojans with further hidden attacks that exploit PHI from within. All attempts to access the network are verified and mitigated if considered malicious or false. The system employs a sophisticated engine to scan and block access and potential threats in network traffic through the Threat Suppression Engine. This protection keeps information confidential and access secure.

TipingPoint's custom hardware Threat Suppression Engine (TSE) is the underlying technology that has revolutionized network protection. Through a

Safeguard elements are either required or addressable. *Required* elements are mandatory, and covered entities must implement them. *Addressable* elements are somewhat discretionary, but the covered entity is required to justify its position or implement a reasonable alternative. For a delineation of elements, see the Appendix.

*"We believe TipingPoint's Intrusion Prevention System meets HIPAA requirements to deploy 'best practice' security solutions. TipingPoint is a best-of-breed product. Our number one benefit to using the system is peace of mind."*

Bonnie Norman, System Security Engineer at WellStar Health System.

combination of pipelined and massively parallel processing hardware, the TSE is able to perform thousands of checks on each packet flow simultaneously. The TSE architecture utilizes custom ASICs, a 20 Gbps backplane and high performance network processors to perform total packet flow inspection at Layers 2-7. Parallel processing ensures that packet flows continue to move through the IPS with an average latency of less than 150 microseconds, independent of the number of filters that are applied.

If any of the filters identifies the packet and its associated flow as malicious, it is dropped or rate shaped along with any subsequent packets belonging to the same flow. TSE hardware acceleration is a competitive advantage, and is critical for IPS functionality. Traditional software and appliance solutions must check filters serially, consequently sacrificing performance and greatly increasing latency as more filters are activated.

### **TipingPoint: Updating Protection**

The protection of a network requires constant updates for emerging threats. Despite the laws against cyber crimes, hackers continue to evolve their attacks and methods for cracking systems and crashing networks. To best protect a network's traffic, access, and services – especially in the sensitive area of medical data and devices – healthcare providers and related businesses need continual updates to protect against new vulnerabilities and potential risks.

TipingPoint provides a filter update service called Digital Vaccine™ to protect against these threats. Vaccines are created not only to address specific exploits, but also potential attack permutations, protecting customers from Zero-Day threats. Digital Vaccines are delivered to customers every week, or immediately when critical vulnerabilities emerge, and can be deployed automatically with no user interaction required to IPS devices. The Security Management System provides enhanced management of Digital Vaccines packages, downloading and updating devices across networks.

### **TipingPoint: Reporting Performance and Threats**

At any time, federal organizations can investigate a healthcare organization to determine if systems adhere to regulations. Failure to provide clear documentation of protection and statistical analysis of detected and mitigated attacks can incur fines by the federal guidelines. Healthcare organizations also need to have clear reports on threats for reviewing network performance, attack behavior against their systems, and accurate details of possible vulnerabilities.

TipingPoint provides extensive reporting capabilities through the IPS devices and SMS. Using the reporting and event log features, companies can conduct risk analysis of the network, devices, and attempted access. Customized reports provide details on blocked and successful attacks against the system by category of attack, ranges of time, and other factors including specific filters, devices, and segments.

To provide further enhancements to reporting, SMS data can export into formats for third party reporting applications, like Crystal Reports. SMS reports can also be sent via PDF to executive or administrative staff. Scheduled reports provide additional options for emailing results to specific contacts to keep a continual record of system performance and network behavior.

## **Protection of Medical Devices**

As healthcare organizations face increasing regulatory compliance and general liability demands around information security and privacy, a unique challenge has emerged for medical device security.

Over the last several years, medical devices have moved to commercial operating systems and network connectivity. While this change has facilitated device access, reporting, and integration into the healthcare organization's network, the move has come at a great cost. These devices are critically exposed because of software vulnerabilities, and thus often remain vulnerable to virus, worm, or even worse – the malicious hacker attack.

The challenge is that these systems cannot be hardened and maintained through normal IT security processes. The FDA regulates the manufacturing process of medical devices, and changes to the system – including patches – can affect the integrity and operations of the device. All medical devices require a rigid validation process to

make sure the device operates according to specification. Failure to follow this process results in FDA penalties, but worse it can lead to death of patients in some cases. This has recently received a lot of attention in the trade press as Network World has devoted several articles to this challenge.<sup>5</sup>

The FDA provides an overview of Section 510(k) for device manufacturers at <http://www.fda.gov/cdrh/510k.html>. This overview details the Premarket Notification process, also called PMN or 510(k). PMN requires medical device manufacturers to notify the FDA 90 days in advance if a device is new or being modified “to the extent that its safety or effectiveness could be affected”.

Caught between the FDA and medical device manufacturers, hospitals and healthcare facilities are looking for answers to solve this problem. A few organizations have provided guidance on this topic:

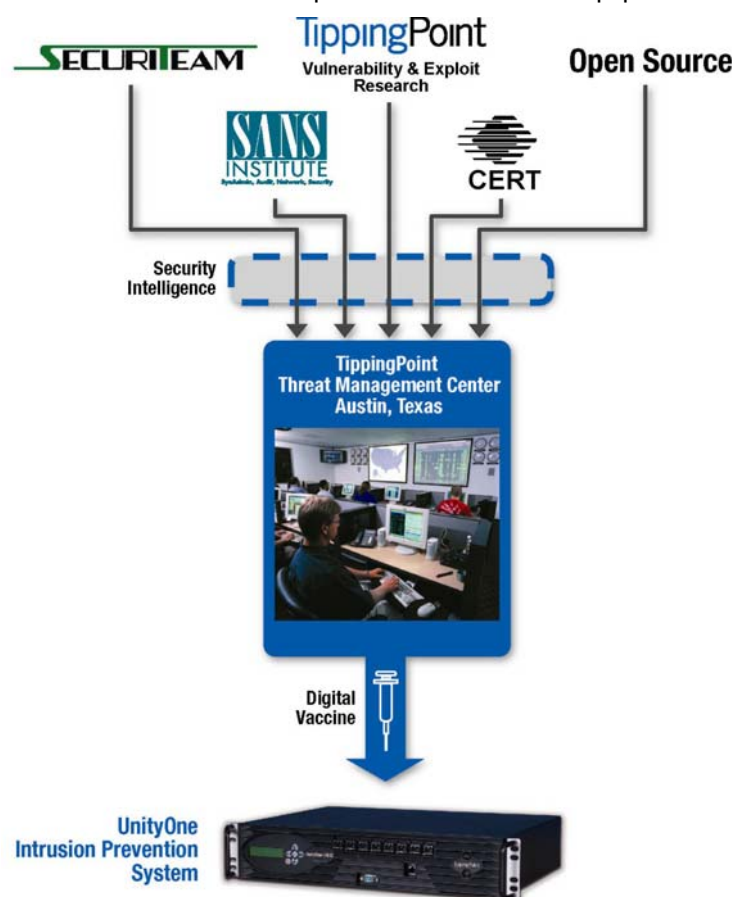
- The US Air Force – Air Force Communications Agency Certificate of Networkiness (AFA CON)
- The US Veterans Administration – Medical Device Isolation Architecture Guide<sup>6</sup>
- The National Electrical Manufacturers Association – Security & Privacy Committee<sup>7</sup>

### TippingPoint’s Solution for Medical Devices

With the sensitivity of networked medical equipment, any attack against a network can have devastating affects. The TippingPoint system provides a complete solution, including specific filter protection for underlying operating systems of medical devices. Additional categories of filters in the TippingPoint IPS provide enhanced protection against malicious attacks that can cripple network services and accesses required for this medical equipment.

The TippingPoint IPS also provides continual updates for network protection. TippingPoint is the primary author of the SANS @RISK email newsletter, containing the latest information on new and existing network security vulnerabilities, with a subscriber base of nearly 300,000 network security professionals worldwide. Coordinated by the SANS Institute and delivered every Thursday, the SANS @RISK newsletter summarizes newly discovered vulnerabilities, details their impact, and informs of actions large organizations have taken to protect their users. The SANS @RISK newsletter is available for free at: <http://www.sans.org/newsletters/risk/>

In providing the vulnerability analysis for SANS every week, the TippingPoint security team simultaneously develops new attack filters to address the vulnerabilities and incorporates these filters into Digital Vaccines. Vaccines are created to protect vulnerabilities to protect against all potential attack permutations rather than specific exploits. Digital Vaccines are delivered to customers every week, or immediately when critical vulnerabilities emerge, and can be deployed automatically with no user interaction required.



A recent filter package is summarized below:

- **Application Protection: Attack Protection - Vulnerabilities** (602 Total) — Operating System (Microsoft, Linux, Unix etc.), Application (MSSQL, MS-Exchange, IIS, Oracle, Lotus Notes etc.), Protocols (HTTP, SNMP, SMB, RPC, SMTP, POP, IMAP, SSH, FTP, HTTP)

- **Application Protection: Attack Protection - Exploits** (456 Total) — MS-Blaster, Slammer, Welchia, Sobig, BugBear, Nimda, Code Red etc.
- **Application Protection: Reconnaissance** (Probes, Scans, Sweeps - 306 Total) — Fingerprinting activity with comprehensive directional support for scans, sweeps, probes
- **Application Protection: Security Policy** (136 Total) — Policy based on whether organizations allow or deny (i.e. root access to Telnet, multi-session FTP, covert channel communications, ICMP options, application-specific access permissions)
- **Application Protection: Informational** (48 Total) — Basic network protocol activity (directory traversals, ICMP, login attempts, FTP commands etc.)
- **Infrastructure Protection: DDOS** (User Defined) — SYN Floods and Established Connection Floods/Process Table Attacks, Connections per Second Attacks, Amplifier and Reflector Attacks
- **Infrastructure Protection: Network Equipment** (21 Total) — Protecting network infrastructure (i.e. Cisco routers/switches etc.) from IP based DOS attacks
- **Infrastructure Protection: Traffic Normalization** (30 Total) — Cleaning the network from invalid resource consuming “trash packets” (IP/TCP/UDP/ICMP/ARP) to make the network run more efficiently
- **Infrastructure Protection: Traffic Threshold** (User-Defined) — Bandwidth-shaping to detect and manage traffic patterns that vary from the norm
- **Performance Protection: Misuse & Abuse** (Peer to Peer - 95 Total) — Over 98% of all P2P protocols can be tracked, rate-limited, or blocked (uni-directionally or bi-directionally)
- **Performance Protection: Traffic Management** (User Defined) — Security Rate-Shaping filters (user defined) for any IP/TCP/UDP/ICMP application or protocol by IP address, CIDR block/subnet, segment, or any filter in the system

## FDA 21 Code of Federal Regulation Part 11

The regulation FDA 21 CFR part 11 establishes requirements for the acceptance of electronic records and signatures – in lieu of paper records and handwritten signatures – in FDA regulated manufacturing processes.

The FDA regulates the manufacturing processes of industries such as bio-medical, pharmaceutical, personal care products, medical devices, and the food and beverage industry. FDA oversight requires organizations in these industries to document and acknowledge conditions and events at stages of the manufacturing process to ensure adherence to defined manufacturing procedures and to provide for consistent and manufactured products. Records must be reviewed, securely archived, and available for review by the FDA.

This regulation was introduced to provide for more accurate, timely, and streamlined processing of electronic records as opposed to the time consuming manual physical record process. The final rule was published in March 1997, and went into effect that same year. Enforcement of the rule began in 2000.

### TippingPoint’s Solution for FDA 21

TippingPoint provides a solution to protect against these access and security issues, ensuring the proper authorization of network users, data transfer, and traffic security. The TippingPoint IPS provides a powerful tool to maintain a “Closed Systems” for healthcare provider institutions (except those conducting research, like an academic medical center). For these organizations, the IPS provides integrity and extensive protection from unauthorized access and hacking. Through network isolation using a network IPS strategy and deployment, a regulated organization can ensure that the closed environment is sealed and secured.

## Sarbanes-Oxley Act

The Sarbanes-Oxley Act (SOX) requires the documentation, validation and attestation of controls, including security, around the financial and accounting systems and process according to Section 404 of the legislation. Furthermore, Section 409 requires the disclosure of any event with a material impact on the financial statements. In this age of digitally stored data and the importance of confidential personal information, a major breach of client data could directly impact a healthcare organization’s financial performance. Publicly traded healthcare organizations need to keep extensive records and documentation of internal controls to comply with the Sarbanes-Oxley Act.

SOX compliance alone requires an increase in spending over the next year in the public sector/health care vertical by 53%.<sup>8</sup> These healthcare organizations include government institutions that currently are not regulated by SOX. As a result, the percentage of actual healthcare organizations increasing security as a result of SOX could be much higher.

### **TippingPoint's Solution for Sarbanes-Oxley Act**

The protection of records requires secure access by specific, authorized users. As with FDA 21 CFR part 11, the TippingPoint IPS ensures protection of business-specific files, data center information, and network access from unauthorized access, hacking attempts, and Denial of Service attacks (DoS). The "Closed System" approach for the TippingPoint IPS tracks all network access attempts through verification of the access. In a segmental deployment, the IPS devices scan access requests for potential malicious activity. If encountered, the access is denied without risking possible hacking of confidential records or sensitive files.

However, access attempts and hacking are not the only threats to file storage integrity. Protecting networks against all attacks requires intensive scanning and detection against all network traffic. TippingPoint performs comprehensive total packet flow inspection through Layer 7 to continually cleanse Internet and Intranet traffic and accurately eradicate attacks (worms, viruses, Trojans, blended threats, DoS, DDoS, Backdoors, Walk-in Worms, Bandwidth Hijacking) before damage occurs. TippingPoint protects network infrastructure by blocking attacks against routers, switches, DNS and other infrastructure equipment.

To detail the eradicated threats, the TippingPoint system provides extensive reporting capabilities for documenting detected and mitigated threats to the system. The detailed analysis enables organizations to detail the integrity of network security for confidential records and sensitive internal services, including external connections to insurance data centers and university networks. Each system provides at-a-glance review of traffic behavior and mitigated attacks as it responds to network traffic. The LSM local client provides administration and monitoring capabilities for audit logs, system logs, and packet traces as well as graphical reports according to filter, attack, and elapsed time.

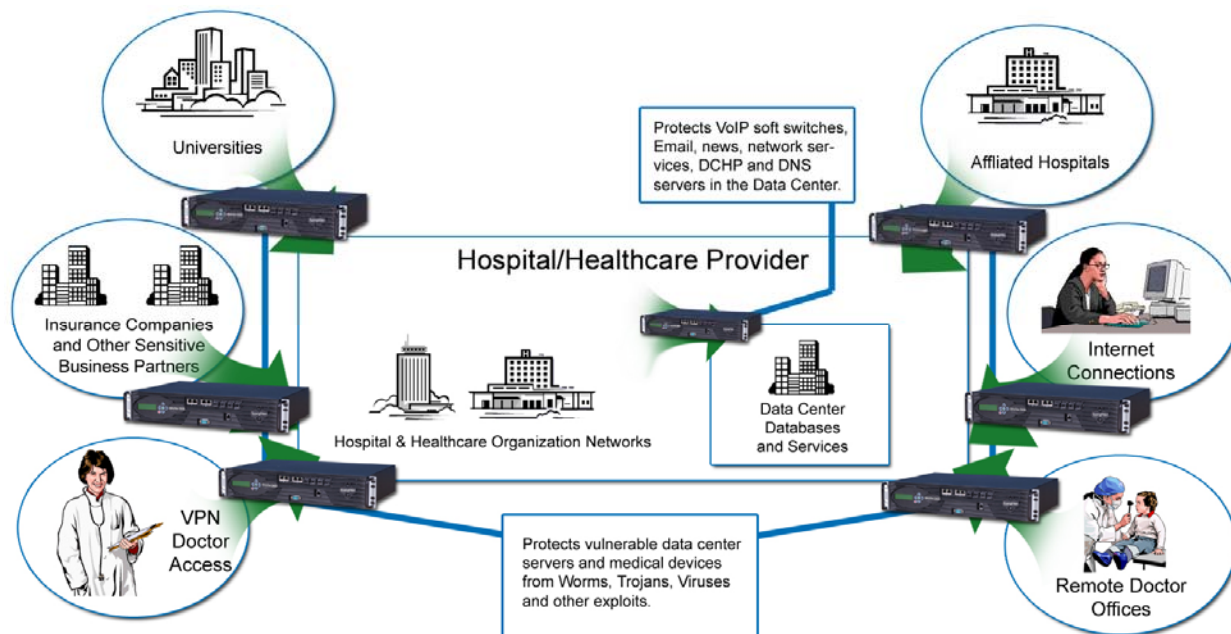
For enhanced reporting, the SMS details the security performance, traffic behavior, and malicious attacks through ad hoc and scheduled reports across deployments of multiple IPS devices. Results of these reports can be emailed and exported in HTML, PDF, and delimited files (csv) by comma or tab formats. Delimited files can be loaded into other programs for review such as Crystal Reports and Microsoft Excel.

### **The TippingPoint Solution**

Tippingpoint is the industry's leading Intrusion Prevention System (IPS), unrivaled in security, performance, High Availability and ease-of-use. TippingPoint's solution provides statistical, protocol and application anomaly protection to protect against traffic surges, buffer overflows, unknown attacks and unknown vulnerabilities. TippingPoint delivers traffic normalization to eliminate malformed or illegal packets, and performs TCP reassembly and IP defragmentation, thus increasing network bandwidth and protecting against evasion techniques. TippingPoint can also act as an access control firewall that can replace CPU intensive router and switch access control lists. Additionally, by rate limiting or blocking unwanted traffic, TippingPoint conserves bandwidth and server capacity to provide complete application protection.

## Intrusion Prevention Reference Architecture

Healthcare organizations must provide absolute security for their network connections to protect services, equipment, and general access. If traditional perimeter protection mechanisms such as firewalls are circumvented, or if any part of the network exists outside of the protection, network security can be compromised and civil and criminal charges can result. The TippingPoint IPS is designed to protect traditional perimeter locations as well as higher speed internal segments.



*TippingPoint provides inline protection for all connections to your network and data centers. TippingPoint's solution provides segmentation of your network, containment of internal attacks, and protects against external threats through Internet connections, VPN, and other services and networked equipment.*

To provide centralized management for updating, configuring, and monitoring IPS devices, TippingPoint offers the Security Manager System™ (SMS). The SMS is a hardened appliance that provides global vision and control for multiple TippingPoint systems. The SMS is responsible for discovering, monitoring, configuring, diagnosing and reporting for TippingPoint systems deployed throughout an organization. The solution is a rack mountable appliance that features a state-of-the-art secure Java client interface that enables "big picture" analysis with trending reports, correlation and real-time graphs on traffic statistics, filtered attacks, network hosts and services, and TippingPoint IPS inventory and health.

A very effective component of the SMS is the SMS dashboard. The dashboard provides at-a-glance monitors and launches capabilities into targeted management applications. The SMS dashboard displays an overview of current performance for all TippingPoint systems in the network, including notifications of updates and potential problems that may need attention.

## Proactive Network Security: IPS vs IDS

Intrusion *Detection* Systems, by definition, only detect and do not block unwanted traffic. Intrusion Prevention Systems detect and prevent attacks. The TippingPoint IPS operates in-line in the network, blocking malicious and unwanted traffic, while allowing legitimate traffic to pass unimpeded. In fact, TippingPoint optimizes the performance of good traffic by continually cleansing the network and prioritizing applications that are mission critical. TippingPoint's high performance and extraordinary intrusion prevention accuracy have redefined network security, and fundamentally changed the way people protect their organization.

No longer is it necessary to clean up after cyber attacks have compromised your servers and workstations. No more ad-hoc and emergency patching. No more out of control, rogue applications like Peer-to-Peer and Instant Messaging running rampant throughout the network. Denial-of-Service attacks that choke Internet connections or crash mission critical applications are a thing of the past. TippingPoint solutions continuously decrease IT security cost by eliminating ad-hoc patching and alert response, and continuously increase IT productivity and profitability through bandwidth savings and protection of critical applications.

## **Characteristics of a High Speed IPS**

Blocking cyber-attacks at multi-gigabit speeds with extremely low latency requires purpose-built hardware, and only TippingPoint has taken such a revolutionary architectural approach needed for true Intrusion Prevention. Traditional software and appliance solutions operate on general-purpose hardware and processors and are simply unable to perform without degrading network performance. Through rigorous third party testing, TippingPoint has demonstrated Intrusion Prevention at multi-gigabit speeds, with extraordinary attack prevention accuracy. TippingPoint is proven in the industry as the most secure, highest performing platform for Intrusion Prevention.

TippingPoint provides Application Protection, Performance Protection, and Infrastructure Protection at gigabit speeds through total packet inspection. Application Protection capabilities provide fast, accurate, reliable protection from internal and external cyber attacks. Through its Infrastructure Protection capabilities, TippingPoint protects routers, switches, DNS and other critical infrastructure from targeted attacks and traffic anomalies. TippingPoint Performance Protection capabilities enable customers to throttle non-mission critical applications that hijack valuable bandwidth and IT resources, thereby aligning network resources and business-critical application performance.

This breakthrough technology dramatically improves the efficiency of network security and control with the following capabilities:

- 50 Mbps to 5.0 Gbps Switch-Like Performance
- Low Latency of less than 150 microseconds
- 2,000,000 Concurrent Sessions
- Precise Filter Accuracy for Vulnerability-Based Filters and Traffic Identification
- 100% Intrusion Prevention Against Emerging Malicious Attacks
- Advanced DoS/DDoS Protection
- Automated In-Service Filter Updates with Digital Vaccine
- High Availability Configurations
- Highly Scalable Security System and Management

The TippingPoint IPS is deployed seamlessly into the network with no IP address or MAC address, and immediately begins filtering out malicious and unwanted traffic. Incorporating TippingPoint into LAN/WAN architectures provides complete protection against internal and external threats. The extremely high speed and low latency capabilities of the TippingPoint IPS enable deployment at the network edge or core, protecting from external as well as internal threats. TippingPoint enables traffic shaping to support critical applications and infrastructure, as well as provides attack isolation and network discovery of vulnerable devices.

## **ROI for IPS in Healthcare**

With TippingPoint, malicious traffic is automatically blocked before damage is done. To Mr. Moore of the University of Texas Health Center of Houston, the most beneficial aspect of the TippingPoint implementation is “the capability to not only see what is going on, but also to be able to do something about it.”

Return on investment (ROI) can be calculated several different ways. ROI calculations should be different for each organization, and are dependent on external forces and formula variations.

In this case, a very basic formula for ROI on intrusion prevention is:

$$\text{(REPAIR TIME X ATTACKS BLOCKED X WAGES)} = \text{ROI}$$

Mr. Moore estimates the following numbers apply to his network environment:

1. Time to patch a system: ~20 minutes
2. Time to fix an infected workstation: ~2 hours
3. Average administrator's hourly wage: \$25 per hour
4. Estimated cost saving of the TippingPoint IPS: tens to hundreds of thousands of dollars

Given Mr. Moore's conservative estimate of preventing ~3000 actual infections to-date, the above numbers give a saving of \$150,000. After implementing the TippingPoint Intrusion Prevention System, the center has blocked an average of 100,000 attacks per month. Mr. Moore reports the university has also blocked many millions (~5) of virus-infected e-mails, which as a minimum, equate to spam. Using his extremely conservative \$0.05 of wasted productivity per spam e-mail a user has to deal with, those saving equal \$250,000.

Total immediate savings from implementing TippingPoint comes to \$400,000.

## Customer Case Study

The vision of WellStar Health System is to deliver world-class healthcare through their hospitals, physicians and services. WellStar Health System includes Cobb, Douglas, Kennestone, Paulding and Windy Hill hospitals; WellStar Physicians Group; Urgent Care Centers; Health Place; Homecare; Hospice; Atherton Place; and WellStar Foundation. For more information, call 770-956-STAR or visit [www.wellstar.org](http://www.wellstar.org).

WellStar Health System, Georgia's largest non-academic healthcare organization with more than 10,000 employees, deployed TippingPoint Intrusion Prevention Systems to protect their electronic medical records, patient data, and corporate assets. In order to prepare for the April 2005 security compliance deadline for the Health Insurance Portability and Accountability Act (HIPAA), WellStar Health System evaluated several security products. TippingPoint's IPS was the most effective at securing the organization, and required less management.

TippingPoint systems are deployed at WellStar Health System on the perimeter as well as internally. On average, TippingPoint blocks approximately 8,700 attacks per week. In addition to protecting the network, TippingPoint also assists with compliance and shows "best business practices" in the event of an audit. Like other healthcare organizations, WellStar Health System is audited to achieve accreditation or to show compliance in various departments.

"Network security is part of every audit," remarks Bonnie Norman, System Security Engineer at WellStar Health System. "Prior to TippingPoint, we did as much manually to protect our organization as we could. We set our firewall to block everything and had anti-virus products. When we turned on the TippingPoint IPS, we immediately saw malicious traffic that we didn't realize was on our network, including the Netsky virus. TippingPoint showed us where the infections were, and helped us clean up our network. As part of compliance, we have to prove eradication. TippingPoint eliminates malicious traffic daily so that our network is secure."

## Conclusion

Healthcare organizations face a significant dilemma regarding the security of networked services, data centers, and equipment while providing authorized clients, physicians, and patients with confidential information.

TippingPoint provides the answer in a single system. The TippingPoint IPS is an easy, affordable, and scalable solution, equipped with a broad range of protection mechanisms for detecting and eliminating threats against networked devices, data centers, connected business partners, and confidential information.

Network threats continue to evolve and increase in sophistication. The flexibility of the TippingPoint platform offers state-of-the-art protection against current unauthorized access and malicious attacks and the power to protect against future ones.

## Appendix

This section maps healthcare related regulations to network Intrusion Prevention Systems. Safeguard elements are either required or addressable. *Required* elements are mandatory, and covered entities must implement them. *Addressable* elements are somewhat discretionary, but the covered entity is required to justify its position or implement a reasonable alternative.

### HIPAA Privacy Regulation

1	<p>164.530 (c)(2)(ii) <i>Administrative requirements. Standard: Safeguards</i></p> <p><b>Reference:</b> “A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure. “</p> <p><b>Solution:</b> The privacy rule for HIPAA empowers the security rule. The privacy rule does not detail the specific requirements for information security; it leaves that determination to the security rule. However, the rule does call for reasonably safeguarding protected health information. In general, network IPS is a strong solution in preventing unauthorized access to PHI at the network level. Of particular concern are the recent malicious virus and worm outbreaks – these often contain a Trojan horse in which, once infected, could lead to the exposure of PHI via a remote attacker getting access to the system.</p>
---	--

### HIPAA Security Regulation

1	<p>164.306 (a)(1)(2) <i>Security standards: General rules.</i></p> <p><b>Reference:</b> “(a) <i>General requirements. Covered entities must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.. “</i></p> <p><b>Solution:</b> IPS helps meet this requirement for network security since it may detect the unauthorized access attempts on web servers, applications etc. Reasonably anticipated threats is a growing and expanding world – only through active as opposed to passive security technologies can healthcare organizations provide adequate defenses to PHI.</p>
2	<p><b>164.308(a)(1)(ii)(A). Risk Analysis (Required)</b></p> <p><b>Reference:</b> “<i>Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and the availability of electronic protected health information held by the covered entity. “</i></p> <p><b>Solution:</b> If a company conducts a risk analysis, it determines the risks of network access, if the network has been or may become compromised, and possible vulnerabilities exposed based on the current implemented network protection protocols. IPS is a component to help understand these inherent risks, providing critical information and continuous risk analysis through detection and protection reporting and monitoring logs for events and system resources.</p>

3	<p><b>164.308(a)(1)(ii)(B). Risk Management (Required)</b></p> <p><b>Reference:</b> <i>“Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a). “</i></p> <p><b>Solution:</b> Network IPS is definitely a component to help reduce network risks and vulnerabilities to a reasonable and appropriate level. Companies such as banks and government have implemented IPS solutions to provide reasonable and appropriate protection measures for their networks as they use other forms of protection to protect assets and customers, such as surveillance equipment and armed guards. Without these security measures, the companies are responsible to their customers and government entities for successful crimes against their systems. Cyber crimes are as liable as criminal acts perpetrated by theft and assault to persons in a company building. For example, healthcare organization buildings in the vicinity may have guards and bulletproof glass to protect customers and employees. If one of these buildings does not, and an incident occurs, that organization may be held liable for not having adequate protection. This concept applies for IPS protection, a theory that has a supported case with <i>T.J. Hooper, 60 F.2d. 737 (2d Cir. 1932)</i>. In this case, a tugboat’s cargo was lost due to a storm. The tugboat did not have a radio on board, which would have alerted the captain to an approaching storm – it was not standard practice for tugs to have radios at this time. However, Judge Learned Hand held the tugboat liable for failing to use technology that was available and in common use in other environments.</p>
4	<p><b>164.308(a)(1)(ii)(A). Risk Analysis (Required)</b></p> <p><b>Reference:</b> <i>“Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. “</i></p> <p><b>Solution:</b> IPS solutions provide detection and alerting capabilities to inform network administrators when incidents occur, hackers try to illegally access the network, and malicious traffic is detected.</p>
5	<p><b>164.308(a)(1)(ii)(D). Information system activity review (Required)</b></p> <p><b>Reference:</b> <i>“Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. “</i></p> <p><b>Solution:</b> IPS helps meet this requirement for network security as it detects unauthorized access attempts at the network level aimed at web servers, applications, and databases that store PHI.</p>
6	<p><b>164.308(a)(5)(ii)(B). Security awareness and training (Addressable)</b></p> <p><b>Reference:</b> <i>“Procedures for guarding against, detecting, and reporting malicious software.”</i></p> <p><b>Solution:</b> IPS is effective at detecting, guarding and reporting on malicious software attacks carried out over the network. Several organizations have seen network IPS as an effective strategy to block known and unknown network worms and viruses.</p>
7	<p><b>164.308(a)(6)(ii). Response and Reporting (Required)</b></p> <p><b>Reference:</b> <i>“Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.”</i></p> <p><b>Solution:</b> IPS helps meet this requirement for network security as it detects unauthorized access attempts at the network level aimed at web servers, applications, and databases that store PHI.</p>

8	<b>164.312(a)(1). Access control</b>
	<b>Reference:</b> <i>“Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).”</i>
	<b>Solution:</b> Network IPS effectively enforces network access control policies for devices and helps meet this requirement.
9	<b>164.312(b) Audit controls</b>
	<b>Reference:</b> <i>“Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. “</i>
	<b>Solution:</b> IPS helps meet this requirement for network security as it detects unauthorized access attempts at the network level aimed at web servers, applications, and databases that store PHI.
10	<b>164.312(c)(2) Mechanism to authenticate electronic protected health information (Addressable)</b>
	<b>Reference:</b> <i>“Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.</i>
	<b>Solution:</b> IPS helps meet this requirement for network security as it detects unauthorized access attempts at the network level aimed at web servers, applications, and databases that store PHI.
11	<b>164.312(e)(1) Transmission security</b>
	<b>Reference:</b> <i>“Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and the availability of electronic protected health information held by the covered entity. “</i>
	<b>Solution:</b> IPS helps meet this requirement for network security as it detects unauthorized access attempts at the network level aimed at web servers, applications, and databases that store PHI.
12	<b>164.312(e)(2)(i) Integrity controls (Addressable)</b>
	<b>Reference:</b> <i>“Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. “</i>
	<b>Solution:</b> IPS helps meet this requirement for network security as it detects unauthorized access attempts at the network level aimed at web servers, applications, and databases that store PHI.

## FDA 21 CFR 11

1	<p data-bbox="269 243 675 268"><b>11.10 Controls for closed systems.</b></p> <p data-bbox="269 289 1382 407"><b>Reference:</b> <i>“Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine.”</i></p> <p data-bbox="269 428 1414 516"><b>Solution:</b> The TippingPoint IPS solution is an effective way to segment a network to provide a closed system. Through network isolation via a network IPS strategy and deployment, a regulated entity can make sure that the closed environment is sealed and secured.</p> <p data-bbox="269 548 1406 636">The FDA defines a closed system as: <i>“Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.”</i></p>
2	<p data-bbox="269 655 686 680"><b>11.30 Controls for open systems.</b></p> <p data-bbox="269 701 1414 911"><b>Reference:</b> <i>“Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.”</i></p> <p data-bbox="269 932 1349 1020"><b>Solution:</b> IPS helps meet this requirement from a network security perspective by detecting unauthorized access attempts at the network level aimed at web servers, applications, and databases that store electronic records governed by the FDA.</p> <p data-bbox="269 1052 1406 1140">The FDA defines an open system as: <i>“Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.”</i></p>

## Sarbanes-Oxley Act

1	<p><i>Section 404 Compliance</i></p> <p><b>Requirement:</b> <i>Section 404 of SOX requires the documentation and validation that appropriate controls are in place to establish the integrity/accuracy of the financial/accounting processes.</i></p> <p><b>Solution:</b> SOX is not prescriptive in its IT requirements, leaving many details to be determined. The primary driver of controls comes from best practices driven by the large auditing firms.</p> <p>Specifically, SOX focuses on the control and integrity of the accounting/financial processes of an organization. The aim is the integrity and accuracy of the financial statements. The rule does not directly focus on perimeter controls. In fact, the Public Company Oversight Board has made very narrow rulings limiting the scope of SOX control around accounting systems and processes. This extends beyond financial ERP systems though. At one insurance company they have felt the pressure to protect 1000s of Excel spreadsheets in the controller's office that feed information into the accounting systems and processes.</p> <p>Network IPS solutions safeguard accounting systems and processes similar to medical devices. The difference for these systems is that TippingPoint protects without limiting accessibility of the financial systems to business units. The solution provides improved security and control throughout the organization, protecting external and internal perimeters and business partner connections.</p> <p>Today, based on what auditors are looking for, the hot security technologies for 404 include configuration/change management, audit trail/event monitoring, patch management, identity management and access control.</p>
2	<p><i>Section 409 Compliance</i></p> <p><b>Requirement:</b> <i>Section 409 requires that organizations disclose events that may have a material impact on the financial statements of a publicly traded company.</i></p> <p><b>Solution:</b> Most attention for SOX has focused on 404 and very little has been given to section 409. This section requires that organizations disclose events that have a material financial impact on the organization.</p> <p>Network IPS provides security for this section by providing intensive protection against malicious traffic. Major virus and worm attacks can and do have significant, but not always material, impact on an organization. Weak security around business partner relationships, or breaches in privacy and security compliance can also have a significant impact, especially in stolen intellectual property.</p> <p>TippingPoint demonstrates complete protection of internal and external perimeters against these incidents. The solution detects and prevents unauthorized access and malicious traffic, ensuring the protection of partner connections, intellectual property, and systems and services such as data centers and internal workstations from threats.</p>

<sup>1</sup> [http://thomas.loc.gov/cgi-bin/toGPO/http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104\\_cong\\_public\\_laws&docid=f:publ191.104.pdf](http://thomas.loc.gov/cgi-bin/toGPO/http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ191.104.pdf)

<sup>2</sup> <http://www.hhs.gov/ocr/hipaa/privrulepd.pdf>

<sup>3</sup> <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf>

<sup>4</sup> [http://www.usdoj.gov/usao/waw/press\\_room/2004/aug/gibson.htm](http://www.usdoj.gov/usao/waw/press_room/2004/aug/gibson.htm)

<sup>5</sup> <http://www.nwfusion.com/news/2004/070504hospitalpatch.html>

<sup>6</sup> [http://www.nwfusion.com/news/2004/VA\\_VLAN\\_Guide\\_040430.pdf](http://www.nwfusion.com/news/2004/VA_VLAN_Guide_040430.pdf)

<sup>7</sup> <http://medical.nema.org/>

<sup>8</sup> Forrester survey, 2004