

TippingPoint Healthcare Solution Brief

IPS-Secured Networks

SOLUTION BRIEF – Healthcare



Once defined by open environments and large, interconnected sprawling networks, the healthcare facility today is moving to one of control, confidentiality, integrity and accountability. Conversely, healthcare organizations are also challenged to make information more readily available online or remotely to physicians and patients. 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.

“TippingPoint was the hands down winner. It did better on all our criteria. TippingPoint stops spyware from being installed, blocking several hundred spyware attacks each day. What’s great about it is that it also blocks outgoing traffic attempting to reach the spyware data collection sites. There’s a huge amount of spyware on the Internet and it is a compliance issue as well as a performance issue. TippingPoint is the central tool that makes us confident that our patient information is being protected. It sits on the edge and in the core and protects our network segments.”

Wellstar Health System

“We found the TippingPoint IPS to be the most advanced and mature solution on the market. They’re also easy to manage, and deliver the capacity that we require, all at very competitive costs. Installation was easy. The TippingPoint IPS demands few changes or configurations to our existing network systems, which helps to contain ownership costs. It also protects multiple gigabit links without impacting network performance, making it ideal for organizations as large as ours. Regardless of how rapidly new threats emerge, we’re proactively protecting our healthcare delivery thanks to our TippingPoint IPS. It’s an investment in our patients’ well-being.”

Stockholm Söder Hospital

TippingPoint Customer Base

- 3,500+ worldwide customers
- 10,000+ in-line IPS deployments
- 300+ Fortune 1000 customers

What Specific Security Challenges Do Healthcare Institutions Face?

Securing Patient Medical Information

The volume of patient medical information collected and stored by the healthcare industry grows daily. This presents serious liability issues for healthcare organizations as a public disclosure of a loss or a theft of this private information could seriously impact both the reputation and financial well being of healthcare organizations.

Protecting Increasingly Open Networks

Healthcare networks are increasingly open and interconnected with a variety of external networks and external users exposing these organizations to attacks from networks and devices of questionable or unknown security.

Securing Networks Against An Evolving Threat Landscape

Traditional threats including viruses, worms and Trojans have not gone away; in fact, most of these threats continue to grow in sophistication. In addition, these threats are targeting applications instead of just network devices and operating systems. Unfortunately, most of today’s security solutions such as firewalls, Intrusion Detection Systems (IDS) and anti-virus leave organizations vulnerable to attack.

Network Availability and Performance

Healthcare organizations are relying more and more on communications systems such as Voice over IP (VoIP), video conferencing and wireless infrastructures that create more network complexity and demand. These additional systems further increase the sensitivity of users to network throughput and latency issues.

Security Policy Compliance

Healthcare organizations have to deal with significantly more stringent security policies and increasing regulatory requirements in the face of today’s threats. Organizations need solutions that help them enforce policy and show auditors how the network is protected from the latest threats.

Ensuring Proper Network and Application Access

Healthcare organizations need to keep network resources and applications safe from unauthorized persons and devices. It is also important for audit and compliance purposes to be able to track and report on all user and device access to network resources.

Patching Network and Medical Devices

Another challenge that most healthcare groups deal with is the need to keep pace with application, operating system (OS), and network device software patches. Moreover, for healthcare organizations, this frequently extends to working with equipment vendors to keep critical medical devices patched against possible vulnerabilities.

How TippingPoint Protects Healthcare Networks

Improve Network Reliability and Security

In the face of more sophisticated traditional attacks, increasingly open and exposed networks, and the inability of traditional solutions to meet security and performance requirements, the TippingPoint IPS provides network reliability and security, with:

- (1) automated protection for servers and applications; and
- (2) in-line security for sensitive and private

TippingPoint®

TippingPoint Healthcare Industry Solution Brief

data, including protection against the latest blended threats with thorough and timely network security filters. In addition, the TippingPoint Network Access Control (NAC) solution reduces network vulnerabilities by ensuring only authorized users and devices that meet internal security policies have access to the network.

Minimize IT Staffing Demands

Customers minimize staffing demands with automated in-line protection – eliminating time consuming event follow-up and manual remediation associated with IDS-based solutions.

Improve Efficiency of Patching Programs

TippingPoint's IPS solution allows customers to reduce cost and complexity by eliminating emergency patching for network and medical devices with security filters that provide a virtual patch from zero-day events.

- Virtual Patching – covers software vulnerabilities and zero-day threats, allowing customers to protect assets before patches are deployed, including devices where patches may be infrequent or unavailable

Maintain or Improve Network Performance

Customers can maintain or even improve network performance with line-rate speeds and rate limiting capabilities built into the TippingPoint IPS.

Improve Security Compliance

In the face of more stringent security policies and regulatory demands, TippingPoint's IPS provides automated enforcement of network security policies and reporting to show internal and external auditors how the network is protected from the latest threats. In addition to meeting compliance requirements, customers can have the best security enforcement available for their network.

- Meet internal mandates and regulatory requirements with an easy to use central management system
 - Generate reports for internal requirements and audits

"The TippingPoint system requires very little IT time and resources to administer, yet safeguards our business from attacks that could be potentially very costly. It will pay for itself in no time. Simply put, it just works."

Paragon Biomedical

"Over the past year, the TippingPoint IPS has given us continuous protection against cyber threats improving network performance and minimizing risks. And when an all-out onslaught that has damaged networks around the world comes kicking at your gateway, the TippingPoint IPS has proven it's a terrific security solution. I can't imagine how we could survive without it."

University of Washington Medical

"The only way to keep PHI secure is to know what people are doing on devices that contain it, and the TippingPoint solution gives us that capability. We can now instantly block malicious traffic, music downloads and online gaming, preserving our bandwidth for legitimate, health-critical applications."

Indiana Healthcare System

What is the TippingPoint Solution?

The TippingPoint Intrusion Prevention System is purpose-built for in-line network protection and is specifically designed to deliver network security enforcement with:

- High availability
- Multi-gigabit throughput including 10Gbps solutions with the TippingPoint Core Controller
- Switch-like latency and support for millions of sessions
- Filter accuracy (no false positives)
- Broad filter coverage
 - Vulnerability, exploit and anomaly-based filters
- Timeliness of filter coverage
- Low-touch central management system (manage with current staff)

Filter accuracy, coverage, and timeliness are made possible by the world-renowned DVLabs security research team.

The TippingPoint IPS also provides multiple enforcement functions:

- Blocks malicious traffic flows
- Quarantines non-compliant hosts
- Rate limits non-critical traffic
- Alerts staff of key events
- Redirects designated traffic
- Allows clean traffic to pass unimpeded

The function of the product is based on a simple concept: bad traffic goes in; only good traffic comes out. This provides real-time automatic protection for applications, operating systems, clients, servers, VoIP infrastructure, routers, switches and other assets.

The TippingPoint solution protects networks at the WAN perimeter and inside the network; providing protection of critical Web infrastructure in the DMZ and key assets in the data center. TippingPoint provides security isolation in the core and for key network zones at the aggregation and access layers. By enabling strong protection between network zones, organizations can mitigate the propagation of threats within the network.

The TippingPoint Network Access Control (NAC) solution provides an organization the ability to manage user access and endpoint security which is a critical component to ensuring the overall security and availability of its IT infrastructure. TippingPoint provides an easy to manage, comprehensive NAC solution that provides a means to confirm user and endpoint identity and verify device health prior to granting access to the network and its resources. TippingPoint NAC provides multiple methods of enforcement including 802.1X, DHCP and in-line blocking, allowing customers to centrally manage a combination of the appropriate enforcement types given their network topology and access control priorities.

How TippingPoint Can Help

Over 3,500 TippingPoint customers are already securing their networks with an in-line TippingPoint IPS, and passing security and regulatory audits with flying colors because of its automated in-line policy enforcement. Learn how our customers are protecting their networks with TippingPoint by visiting www.tippingpoint.com, or call TippingPoint directly to speak to a representative about our IPS evaluation program at (888) 878-3477.

TIPPINGPOINT PRODUCT EVALUATION PROGRAM
Evaluate the best security solution for your network
Visit www.tippingpoint.com/eval to qualify

Corporate Headquarters:

7501B North Capital of Texas Hwy.
Austin, Texas 78731 USA
+1 512 681 8000
+1 888 TRUE IPS

European Headquarters:

Herengracht 466, 2nd Floor
1017 CA Amsterdam
The Netherlands
+31 20 521 0450

Asia Pacific Headquarters:

30, Cecil Street, #18-01
Prudential Tower
Singapore 049712
+65 6213 5999

TippingPoint

www.tippingpoint.com