

TippingPoint Higher Education Solution Brief

IPS-Secured Networks

SOLUTION BRIEF – Higher Education



As universities focus on facilitating quality education and academic research, they are faced with the difficult task of maintaining an open door policy for massive loads of network traffic despite the growing demands of providing a stable and secure network environment. Universities must safeguard the integrity and availability of their campus data network, reduce threats to computer systems connected to the network and reduce the likelihood that computers on campus are used to attack other organizations.

"We were struck by how effectively TippingPoint defended against unwanted traffic, as well as its higher throughput and lower latency. We liked the platform's advanced design and technology, which features components like custom ASICs that deliver superior performance over competing devices from other vendors. TippingPoint systems also control traffic by blocking or throttling unwanted file sharing. Moreover, the product was simple to install and easy to manage."

University of Leeds

"Based on our research, we found that the TippingPoint Intrusion Prevention System (IPS) gave us the most complete and most proactive protection of any competitive solution. After contacting TippingPoint, we tried it for 30 days. Once you put an appliance that powerful in front of your servers for a month and see how much malicious traffic it blocks before it gets into your network, you simply can't take it out."

George Washington University

TippingPoint Customer Base

- 3,200+ worldwide customers
- 10,000+ in-line IPS deployments
- 300+ Fortune 1000 customers

What Specific Security Challenges Do Higher Education Institutions Face?

Academic Freedom and Network Security:
One of the greatest challenges for higher education security and IT administrators in the implementation of effective network security, is how to safeguard the network, while keeping network performance and access to services unencumbered and open to the students, faculty and guests that rely on them.

Targeted Attacks

According to the 2007 Computer Security Institute (CSI) Annual Computer Crime and Security Survey, "Almost one-fifth (18 percent) of respondents said they'd suffered a "targeted attack,"...aimed exclusively at their organization...or a small subset of organizations¹."

Time to Patch Vulnerable Systems

Securing applications and keeping operating systems up to date in the face of attacks and frequent patch releases is a daunting task. Schools then are frequently open to attack during the gap between the time that a system vulnerability is discovered, and the time a patch is actually deployed.

End-Point Configuration

Security client applications like anti-virus meant to help protect the network from viruses and worms, and other malicious traffic, may or may not be installed by students, and client systems may not be properly configured or patched,

enabling malicious traffic to sneak into the network.

Peer-to-Peer File Sharing and Social Networking Abuses

More than any other industry, colleges and universities are vulnerable to compromises in productivity and privacy from malicious software, peer-to-peer file sharing that includes downloads of copyrighted songs and movies as well as social networking threats. These abuses can raise legal issues and bog down network performance.

Inadequate Traditional Protection

Traditional network security (Firewalls, Intrusion Detection Systems (IDS), Anti-Virus, etc.) does not provide adequate security in the face of new targeted threats and more sophisticated versions of old threats (worms, viruses, etc.). Technologies such as IDS, which rely on reactive, high-touch models, lack the automated enforcement required to adequately protect today's networks. Many customers realize the need for in-line enforcement, but are afraid of the impact it might have on network performance.

Internal Mandates and Regulatory Requirements

Internal Security Policies have become more stringent along with audit compliance requirements – driven by security, privacy, regulatory and legal concerns (including Payment Card Industry-Data Security Standard

TippingPoint

TippingPoint Higher Education Solution Brief

(PCI-DSS), Family Educational Rights and Privacy Act, FERPA, Health Insurance Portability and Accountability Act (HIPAA), etc.)

How TippingPoint Protects Higher Education Networks

Improve Network Reliability and Security

As colleges and universities focus on maintaining their increasingly open networks in the face of more targeted attacks, more sophisticated traditional attacks, and the inability of traditional solutions to meet their security and performance requirements, the TippingPoint IPS provides the network reliability and security required to provide (1) automated protection for servers, applications and critical university data; and (2) in-line security for sensitive and private student, faculty and administrative information, including protection against the latest blended threats with thorough and timely network security filters.

Minimize IT Staffing Demands

Universities can minimize staffing demands with automated in-line protection, eliminating time consuming event follow-up and manual remediation efforts associated with IDS-based solutions. In addition, the TippingPoint Security Management System provides easy to use management and reporting capabilities so IT organizations can easily set-up and manage an entire IPS deployment with little to no impact on IT time demands.

Maintain or Improve Network Performance

Universities can maintain or even improve network performance using the rate limiting capabilities built in to the TippingPoint IPS to restrict bandwidth usage from students' peer-to-peer applications.

Improve Efficiency of Patching Programs

The TippingPoint IPS solution allows university

IT organizations to reduce cost and complexity by eliminating emergency patching with IPS filters that provide a virtual patch protecting applications, operating systems and network devices including servers from zero-day events.

- Virtual Patching – covers software vulnerabilities and zero-day threats protecting assets before patches are deployed

Improve Security Compliance

Finally, in the face of more stringent security policies and regulatory demands on university IT systems, the TippingPoint 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, TippingPoint provides the best security enforcement available for networks.

How TippingPoint Performs In-line Policy Enforcement

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
- 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 DV Labs 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.

How TippingPoint Can Help

Over 3,200 TippingPoint customers, including hundreds of education customers, are already securing their networks with an in-line TippingPoint IPS, and passing security audits with flying colors because of its automated in-line policy enforcement. Learn how our education 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 for 30 days
Visit www.tippingpoint.com/eval to qualify



¹ Richardson, Robert. "2007 CSI Computer Crime and Security Survey," October 2007 *Computer Security Institute*. http://www.gocsi.com/forms/csi_survey.html

Corporate Headquarters:

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

European Headquarters:

World Trade Centre Amsterdam
Zuidplein 36, H-Toren
1077XV Amsterdam
The Netherlands
+31 20 799 7629

Asia Pacific Headquarters:

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