

# TippingPoint Financial Industry Solution Brief

IPS-Secured Networks

SOLUTION BRIEF – Financial Industry



As consumers and enterprises grow increasingly dependent on electronic banking, the opportunities associated with online banking pose increasingly significant risks to financial institutions. These organizations must ensure adequate privacy protection as well as adapt to provide and share information across multiple systems and facilities, monitor and evaluate the security of their information and maximize the value of their information technology resources. In addition, they must comply with legislation that requires the safeguarding of their networks and data.

*"We have a TippingPoint IPS protecting our customer-facing Web applications. We see exploits being blocked by the IPS...some of these would have made it through our firewall and infected production systems. For compliance purposes, we have been able to show internal and external auditors evidence of attacks blocked, reduction in spyware infections and tracking of asset protection."*

T. Rowe Price

*"With TippingPoint, we've increased the protection we provide our customers against identity and electronic theft. TippingPoint's Intrusion Prevention System has been very effective at preventing various viruses, worms and other cyber threats from entering our gateway. It's more proactive than traditional security technologies."*

Nedbank

## TippingPoint Customer Base

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

## What Specific Security Challenges Do Financial Institutions Face?

### High Volume of Online Financial Transactions

The volume of online financial transactions in the financial services industry continues to grow. The financial industry is collecting and storing more and more sensitive information from customers, employees and partners. This presents an attractive target to would-be hackers and criminal organizations who continue to develop new attacks specifically targeting this financial data.

### 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 organizations<sup>1</sup>."

### Financial Fraud

According to the same CSI Survey<sup>1</sup>, financial fraud overtook virus attacks as the source of the greatest financial losses. Virus losses, which had been the leading cause of loss for seven straight years, fell to second place.

### 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. Financial services organizations 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.

### 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 (PCI-DSS), GLBA, SOX, Basel II, FFIEC, etc.)

### Ensure Proper Network and Application Access

Financial institutions 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.

## How TippingPoint Protects Financial Networks

### Improve Network Reliability and Security

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

**TippingPoint**

# TippingPoint Financial Industry Solution Brief

- (1) automated protection for Web servers and applications; and
- (2) in-line security for sensitive and private financial data, including protection against the latest blended threats with thorough and timely network security filters. In addition, the TippingPoint Network Access Control 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

The TippingPoint IPS solution allows customers to reduce cost and complexity by eliminating emergency patches for applications, operating systems and network devices with IPS filters that provide a virtual patch from zero-day events.

- Virtual Patching – covers software vulnerabilities and zero-day threats allowing you to protect assets before patches are deployed

## Maintain or Improve Network Performance

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

## Improve Security Compliance

Finally, in the face of more stringent security policies and regulatory demands, 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.

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

## 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 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.

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, including many financial institutions, 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 financial institution customers are protecting their networks with TippingPoint by visiting [www.tippingpoint.com](http://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](http://www.tippingpoint.com/eval) to qualify



<sup>1</sup> Richardson, Robert. "2007 CSI Computer Crime and Security Survey," October 2007 *Computer Security Institute*. [http://www.gocsi.com/forms/csi\\_survey.html](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:

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**<sup>®</sup>

[www.tippingpoint.com](http://www.tippingpoint.com)