

## TippingPoint Solutions for Financial Institutions

### DATASHEET



“Senior management was reviewing plans for Sarbanes-Oxley compliance, and the audit firms that were helping in planning suggested that companies would fare better in the SOX audit if they had intrusion prevention systems in place. At the same time we in network security recognized that we needed a way to fully protect our applications against application exploits. We knew of no other way to block spyware and application exploits...”

Once we had the TippingPoint IPS in place, we found spyware on client computers was trying to connect to information collection points outside our organization. When we put in our IPS, the number of spyware connections dropped from more than 130,000 to fewer than 20,000. The IPS simply blocked the connection from the spyware on the client computer trying to phone home.”

*Scott Davis*

*Network Security Group Manager, Enterprise Security  
T. Rowe Price*

In today's financial services industry, collecting and securing personal information about a company's customers, employees and other stakeholders is a daily activity. If the wrong person gains access to this information, stakeholders are at great risk. Data breaches also put financial service firms and their executives at risk for legal action. As consumers and enterprises grow increasingly dependent on electronic banking, federal regulations now mandate the protection of digital financial data, requiring CIOs/CSOs and IT administrators to rethink their network security priorities.

The TippingPoint Intrusion Prevention System (IPS) delivers the most powerful network protection in the world. The TippingPoint IPS is an in-line device that is inserted seamlessly and transparently into the network. As data packets pass through the IPS, they are fully inspected to determine whether they are legitimate or malicious. This instantaneous form of protection is the most effective means of protecting the company from outside-in and inside-out attacks. The TippingPoint IPS gives financial institutions the ability to:

- Secure data flow for Sarbanes-Oxley Section 404 Compliance
- Secure customer and employee data from malicious activities for compliance with Graham-Leach-Bliley
- Implement Service-Oriented-Architecture and Business Process Management to keep up with changing customer behavior with technology that seamlessly integrates with any network

#### Sarbanes – Oxley Compliance

In the wake of information integrity scandals, the US Government enacted the Sarbanes-Oxley Act in 2002. The Sarbanes-Oxley Act (SOX), Section 404 of the legislation, requires the documentation, validation and attestation of controls, including security, around financial and accounting systems and processes.

TippingPoint ensures protection of business-specific files, data center information and network access from unauthorized access, hacking attempts, Denial of Service attacks (DoS), phishing and spyware. To detail the eradicated threats, TippingPoint provides extensive reporting capabilities for

documenting detected and mitigated threats to the system through the TippingPoint Security Management 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. Each system provides at-a-glance review of traffic behavior and mitigated attacks as it responds to network traffic. This comprehensive approach to security ensures the integrity of personal information.

#### Customer Confidentiality Solution

As financial institutions collect personal information from their customers, they must protect the integrity of critical data. The Graham-Leach-Bliley Act of 1999 (GLBA) requires companies legally defined as financial institutions to ensure the security and confidentiality of this data. The FTC also issued the Safeguard rule, which requires financial institutions to have measures in place to protect this type of information.

To assist financial institutions with compliance guidelines specific to GLBA, TippingPoint's Intrusion Prevention Systems provide 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, the TippingPoint IPS protects VoIP infrastructure, routers, switches, DNS and other critical infrastructure from targeted attacks and traffic anomalies. TippingPoint's 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.

### Changing Consumer Behavior

Customers are demanding more network based services, which translates to increases in demand for secure identities. The Federal Trade Commission reports that consumers can become less willing or unwilling to continue to do business with a company if they perceive a risk for identity theft. A 2004 Unisys study discovered that nearly half of U.S. households were willing to switch to financial institutions that offer stronger theft detection and alert services.

Forrester asserts that "current financial services models were built around the needs of older generations of consumers. Firms will need to adjust their offerings to meet the needs of younger consumers." To accomplish this, firms must be flexible and evolving. This points to increased online and network-based banking products and applications as well as increased access to sensitive information and potential vulnerabilities.

To adapt to changing customer demands, financial institutions will require flexible operations. In response, they are moving toward service-oriented architecture (SOA) and business process management (BPM).

### The Importance of a Secure Network

As the financial services industry grows, so does the competitive environment. Organic growth from large financial institutions, international competition, non-traditional financial service businesses like people-to-people lending and large retailers are all impacting the dynamics of the industry and market.

As consumers become more diligent regarding the security of their identity and personal data, security will become a competitive advantage in a market where the value per customer is high, but customer switching cost is low. TippingPoint works constantly and diligently to stay ahead of existing and potential threats to your corporate assets, including financial and customer information, and is committed to remaining the world's leader in network security.

### Service-Oriented Application:

SOA Capability	TippingPoint Benefit
Easily integrate existing applications	As an in-line device, the TippingPoint IPS literally plugs right into your network and is up and running within minutes. The TippingPoint Security Management System (SMS) allows the IT staff to centrally manage and monitor multiple TippingPoint IPS's and report on the health and status of the network's internal and external traffic.
Share customer information across organizations	As a centrally managed, in-line device that operates at both the network core and perimeter, the TippingPoint IPS monitors and protects all internal and external data flow at gigabit speeds. This allows information to be shared across the company without negatively impacting the business.

### Business Process Management:

BPM Capability	TippingPoint Benefit
Adapt business rules in dynamic environments	The SMS enables centralized deployment of system changes rather than machine by machine. Any changes can be made in minutes rather than hours or even days; therefore company responsiveness increases exponentially yielding significant productivity gains, cost savings and improved customer responsiveness.
Automate business processes	As a centrally managed security solution, TippingPoint does not require the countless man hours that typical network disaster responses do. This allows IT staff to perform more value-add activities like building processes to increase the efficiency of business operations.



Headquarters:  
7501B North Capital of Texas Hwy.  
Austin, TX 78731  
+1 512 681 8000  
+1 888 TRUE IPS  
www.tippingpoint.com

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