

Sarbanes-Oxley Compliance Using Intrusion Prevention

DATASHEET



In response to a significant number of corporate and accounting scandals, the U.S. Congress enacted sweeping new corporate governance legislation known as the Sarbanes-Oxley Act of 2002 (SOX). By drawing a direct enforceable relationship between senior corporate management and the integrity and quality of their companies' financial statements, today's CEOs and CFOs are now held personally responsible for the accuracy of their company's financial data. Section 404 of the Sarbanes-Oxley Act specifically addresses the flow and integrity of financial data and provides three broad, open interpretation compliance requirements.

One point is clear: all financial data flows through the network, leaving it vulnerable to malicious activity and potential identity theft. To ensure the integrity of data to stockholders, customers and employees, the following three questions must be addressed and sufficiently answered:

- How are you protecting and auditing the flow and integrity of your financial data?
- Are you maintaining a secure internal control system to protect the integrity of your data?
- Have you enlisted the services of a veritable evaluation firm confirm your system's security?

Integrating TippingPoint's globally-acclaimed Intrusion Prevention System (IPS) into your network addresses the three main requirements of SOX compliance and protecting critical financial information. TippingPoint provides comprehensive protection by:

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

Comprehensive Network Security

Officers and board members of public companies have a responsibility to provide accurate information and act in the best interests of the stockholders and customers. The amount of information under management is vast and growing. Access to data must be restricted according to the user's role.

TippingPoint's IPS enforces security by preventing unauthorized access to data sources at the network level. The system detects and prevents malicious traffic, including virus and worm outbreaks that often contain Trojans with further hidden attacks. The system employs its Threat Suppression Engine to scan and block traffic if determined to be malicious in real-time.

Evergreen Protection

The protection of a network and critical company information requires constant updates for emerging threats. Hackers continue to evolve their attacks and methods for cracking systems and crashing networks. To best protect the network, especially critical financial data, from external and internal malicious traffic, continual updates are necessary.

Digital Vaccine® is TippingPoint's filter update service. The Digital Vaccine team creates vaccines to address specific exploits, but also creates vaccines for potential attack permutations to protect TippingPoint customer networks from Zero-Day threats. Digital Vaccines are delivered weekly automatically, or as needed when critical threats strike.

Robust Reporting and Threat Analysis

SOX requires that public companies be audited by a veritable third party. The auditor must offer an opinion regarding whether the public company is able to adequately protect and track the flow of financial information. With no uniform government compliance checklist, network reporting must be able to adapt to a particular auditor checklists. Therefore, the reporting and tracking capabilities of the network is essential to compliance.

TippingPoint provides extensive reporting capabilities via:

- TippingPoint Local Security Manager (LSM) – The LSM is embedded in every TippingPoint IPS. The LSM is a Web GUI management application that provides administration, configuration and reporting capabilities in an easy-to-use, secure Web interface.
- TippingPoint Security Management System (SMS) – The SMS is a hardened appliance 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. It provides a scalable, policy-based operational model for large-scale IPS deployments

Using the reporting and event log features, companies can conduct risk analysis of their network traffic, infrastructure, and attempted access attempts. Customized reports provide details on blocked and successful attacks against the system by category of attack, range of time, and other factors including specific filters, devices and segments.

To provide further enhancements to reporting, data from the SMS can be exported into formats for legacy reporting applications. Reports can also be sent to executive and administrative staff in PDF format. Scheduled reports provide additional options for e-mailing results to specific individuals for continuous updates.

TippingPoint Sarbanes-Oxley Compliance Checklist

SOX created the Public Company Accounting Oversight Board (PCAOB) to oversee the auditing of companies subject to securities laws in order to protect the interests of investors and further the public interest. In addition, the Office of Internal Oversight and Performance Assurance (IOPA) conducts internal performance reviews and real-time quality assurance of PCAOB programs to ensure efficiency, effectiveness and integrity of those activities. PCAOB acknowledges that there isn't a one size fits all approach to compliance. The following checklist demonstrates how TippingPoint provides solutions in-line with the widely used COBIT Checklist of Best Practices for SOX compliance.

TippingPoint Sarbanes-Oxley Compliance Checklist

Sarbanes-Oxley Section 404 Compliance Requirement	TippingPoint Intrusion Prevention System (IPS) Solution
Ensure Systems Security	TippingPoint's comprehensive approach to security ensures reliable protection from internal and external cyber attacks; protection of critical network infrastructure from targeted attacks and traffic anomalies; and preservation of valuable network bandwidth susceptible to non-mission critical applications.
Develop and Maintain Policies and Procedures	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.
Manage Changes	The TippingPoint SMS provides the ability to generate and deploy numerous policies to multiple TippingPoint systems through an intuitive policy management user interface. Granular role-based user administration and authentication mechanisms are supported and user access levels are defined on a per device, per segment, per profile and global basis.
Manage Third-Party Services	TippingPoint supports an open Web Service API for database access to allow third party integration and access. TippingPoint's Quarantine Protection allows the IPS and SMS systems to interact with external systems and applications to aid in the remediation process.
Manage Performance and Capacity	TippingPoint's rate limiting functionality provides a means for monitoring and enforcing bandwidth utilization. Traffic rate-limiting can be employed for dynamic protection in the event of worm outbreaks, denial of service attacks or for controlling bandwidth consumption by non-critical applications while assuring availability for critical applications.
Ensure Continuous Service	The TippingPoint IPS operates in-line in the network, blocking malicious and unwanted traffic, while allowing good traffic to pass unimpeded. TippingPoint optimizes the performance of good traffic by continually cleansing the network and prioritizing mission-critical applications.
Educate and Train Users	TippingPoint's training experts provides comprehensive, collaborative training designed to provide hands-on experience either at TippingPoint's Training Headquarters or onsite at customer facilities. Curriculum includes emerging security trends, implementation planning and advanced troubleshooting and diagnostics.
Assist and Advise Customers	TippingPoint engineers help customers manage the installation of TippingPoint devices from start to finish, including the physical installation and connection of the TippingPoint equipment, configuration of relevant parameters and any/all advanced features, and connectivity testing of the installation. In addition, TippingPoint provides recommendations for network management and future growth.
Manage the Configuration	Network parameters as well as TippingPoint system and filter behaviors can be viewed, assessed and tuned from one interface. Revision control and granular auditing of all configuration changes made to TippingPoint devices or security policies are very extensible and open for integration into third party systems.
Manage Problems and Incidents	The TippingPoint SMS provides enterprise-wide reporting and trend analysis for multiple TippingPoint IPS deployments. The SMS dashboard provides an overview of current performance for all TippingPoint systems in the network, including notifications of updates and potential problems that may need attention. TippingPoint is able to integrate into any third party Security Information Management (SIM) vendor or trouble ticketing application in support of fully automated remediation and incident handling procedures as well.
Manage Data	The global vision of the TippingPoint SMS allows for the continuous analysis of system logs and network management information for immediate cyber attack containment, perpetrator location and identification, and damage mitigation. All event data automatically logs to system files in the SMS. Off-box data retention is available for compiled and stored log information.



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