

SOLUTION BRIEF



SARBANES OXLEY COMPLIANCE



Double NSS Award

Sarbanes-Oxley and the Need for Intrusion Prevention System (IPS) Solutions

Introduction

The Enterprise IT landscape was forever changed with the passing of the Sarbanes-Oxley (SOX) Act in 2002. SOX was enacted for the purpose of reforming the reporting, governance, and disclosure of public company financial statement and records. The U.S. Congress passed this act in order to better ensure accuracy and restore trust in the financial statements given to the government and investors following a series of high-profile accounting scandals.

The act requires that key officers of public companies attest to the integrity of their financial controls. Currently, almost all of the financial controls, including transaction handling, accounting ledgers and other financial systems – including links with third party providers, such as corporate banks, trading exchanges and clearing systems – are computer-based. Since IT underlies the business of recording and reporting all financial activity, a lack of control over IT security implies a lack of control over the organization's financial reports, in direct violation of Sarbanes-Oxley section 404. Control of IT systems integrity is therefore required in order to maintain financial reporting integrity.

From a security perspective, any breach in security can lead to compromising resources and information – including those covered by the standards implicit in section 404's mandates. This section of Sarbanes-Oxley carries with it the mandate to properly secure IT enterprise-wide in an effort to satisfy independent auditors regarding the level of risk management applied to protecting corporate IT and especially financial IT systems.

Top Layer Networks Attack Mitigator™ IPS 5500 Intrusion Prevention System (IPS) Solutions provide public companies with the ability to comply with the implicit IT security mandates of Sarbanes-Oxley. In addition, Top Layer Network's SecureCommand+™ Central Management System (CMS) provides the reporting and logging capabilities for organizations to prove that security polices are being correctly followed. It also gives administrators the tools to respond to security threats and incidents in a consistent, compliant, and approved manner.

Finally, in addition to enabling compliance with SOX regulation, Top Layer Network's IPS provides a fast to deploy, very low maintenance security protection

solution that reduces the workload placed on IT security. The IPS 5500 improves security operations effectiveness and enhances the company's ability to proactively mitigate high-risk threats before they become successful exploits.

Business Challenges

To optimize the benefits of increased IT security spending, organizations have come to the conclusion that SOX compliance should be fully incorporated as part of strategic and tactical business reengineering and technology planning. In fact, for public financial and healthcare concerns, SOX is yet another step in the road covered by previous US legislation that affects these industries – the Gramm-Leach-Bliley Act (GLBA) for financial services, and the Health Insurance Portability and Accountability Act (HIPAA) for healthcare. Industry experience with these earlier pieces of legislation shows that initial efforts to comply have led to higher standards and tighter regulation as years go by. The strategic opportunity for IT in public companies is therefore to think beyond the immediate compliance deadline and look to establish controls that allow them to more easily comply with tighter regulations over time. In addition, building a defensible position against a class-action shareholder suit is one of the unfortunate situations that IT organizations need to plan for as they move forward in implementing their compliance activities. As the financial scandals in the early part of the decade showed, having an auditor sign off is no guarantee that lawsuits can be avoided, and Sarbanes-Oxley makes it clear that CEOs and CFOs are personally liable for any material misrepresentations.

In addition to meeting compliance objectives, business organizations have the fundamental goal of gaining and maintaining customers' trust through the Internet. Users must have confidence in the overall reliability and confidentiality of private information in order to participate with a particular vendor. Customers, partners, and stakeholders are increasingly demanding a higher degree of accountability for security.

Therefore, countering cyber-threats represents is a central strategic issue for regulatory compliance, business development, revenue increase, and, where applicable, maintaining shareholder value.

Intrusion Prevention System (IPS) solutions have rapidly become a requirement for Financial IT administrators tasked with security and availability concerns. Implementing the proper IPS solution is considered a "best-practice" in the eyes of Financial IT administrators.

To meet the Sarbanes-Oxley's general IT security requirements, organizations will need to proactively address security concerns such as:

- Undesired Access to financial and confidential records
- Malicious content that may alter, damage, or contribute to theft of sensitive information
- Rate-based attacks that can reduce or impede the availability of critical resources and information

- Proper monitoring, logging and reporting of security events for immediate response and auditing purposes

To comply with Sarbanes-Oxley and continue to be successful, business organizations must deploy the right IPS Solution as a fundamental component of their IT security strategy.

Understanding the Problem – Sensitive Data and Remote Exploits

Enterprise IT infrastructure provides a conduit for various online transactions and information to be executed across the Internet. Due to the potential sensitivity of the information, especially financial records, network and server infrastructures require a more formidable and customized level of protection above and beyond what network firewalls or IDS' can provide. Firewalls are designed to allow traffic flow through to its destination with minimal scrutiny. Even next generation firewalls attempt to address the problem with poorly performing software patches and upgrades. IDS solutions detect attacks based on known attack signatures, but are not architected for inline operation or proactive blocking of attacks. Even worse, an IDS that has been re-badged as an IPS can leave users helpless in the face of new web-specific attacks or attacks that attempt to slip through during peak usage. Certain established IPS vendors even contrast themselves against IDS vendors in a weak attempt to confuse the customer regarding the fact they are just an IDS-based IPS. By way of example, Code Red and Nimda are worms that took advantage of Microsoft web server vulnerabilities and inadequacies in firewalls and IDS solutions with devastating effect.

To ensure the success of financial portals, most businesses focus on securing the integrity of the data and the integrity of the transaction while in transit. However, if resources are not properly secured, then confidential data can be accessed or stolen at the source.

It is generally well known in system security and software development circles that large, complex programs contain bugs that cause security holes. Unfortunately, server operating systems and web applications are large, complex programs that contain security holes. Many of these vulnerabilities can be remotely exploited, resulting in a compromised web server, illegal data access and potentially severe legal and financial ramifications due to stolen or lost data. Businesses quickly become exposed and must scramble to prove compliance through having taken every precaution in protecting against such threats.

Finally, all organizations worry about the confidentiality of the data transmitted across the Internet. The TCP/IP protocol was not designed with security in mind; hence it is vulnerable to network eavesdropping. When confidential transactions and account data are transmitted from the server to the browser, or when the end-user sends private information to the server, someone may be listening in and have access to private records.

The critical areas of concern can be addressed by IPS technology. Left unprotected these vulnerabilities allow unauthorized remote users to:

- Steal confidential documents not intended for their eyes.
- Execute commands on the server host machine, allowing them to modify the system.
- Gain information about the specific server or database that will allow them to break into the system and alter, damage or steal private information, such as financial records.

Understanding the Problem – Maintaining Availability of IT Infrastructure

Any traditional network and server infrastructure that uses standard operating systems are susceptible to malicious content such as viruses, Trojans, and worms. However, a growing segment of targeted attacks involves rate-based attacks, such as network and application resource denial of service (DoS) attacks.

The huge financial loss that can be associated with network and server resource consumption causes great concern for financial IT organizations. Any networked system that shares some network infrastructure with the Internet has the potential for being compromised.

SOX requires that business organizations in the United States ensure the security and confidentiality of financial records and related information. Many institutions are increasingly receiving anonymous notifications from often well-organized groups that request payments to be made in order to avoid the launching of DoS attacks. Such blackmail requests are made with the understanding that the target cannot afford the losses associated with any possibility of revealing gaps in an organization's ability to offer proper protection of sensitive data and critical information and therefore failing to be compliant with Sarbanes-Oxley.

The most common DoS or DDoS (Distributed Denial of Service) attacks perpetrated by organized crime organizations, such as mentioned above, will target a device's network bandwidth or connectivity. Another form of attack, an application resource DDoS attack, is executed by flooding the target(s) with so many legitimately formatted requests that it becomes unavailable for normal use. Extortionists can launch DDoS attacks by taking advantage of either external or even internal computers, which can simultaneously launch hundreds of thousands of requests at the target.

Attackers know that connectivity DDoS attacks are very hard to stop because of the large number of randomly distributed attacking sources, which renders conventional protection mechanisms useless. Application resource attacks are equally devastating, as the requests are legitimate in format, but overwhelming in volume.

Only a security solution that can handle high-volumes of rate-based attacks as well as content-based attacks is required to prevent network downtime and prevent unauthorized access to confidential data.

Understanding the Problem – Monitoring, Auditing and Reporting

Organizations are investing significant time, money and resources in developing compliance programs to address the growing number of regulations that impact business and government. SOX requires management to explicitly take

responsibility for establishing and maintaining policies and programs that articulate and demonstrate compliance. When incorporating IT security technology for the reasons outline above, administrators and executives need to provide the following:

- Proof and documentation of adherence to security policies
- Verification when security policies are being violated and by whom.
- Generation of timely reports to accurately highlight and assess security threats and compliance exposure in real-time and forensically
- Monitoring of policies across multiple security devices

Without a proper management and reporting solution that can address these challenges, organizations run the risk of missed policy violations, inaccurate assessment, and an inability to prove that policies are being monitored and enforced. The impact to the business can be dramatic, including lost business, brand damage, fines and penalties, and loss in shareholder value.

How The Attack Mitigator IPS 5500 Ensures Confidentiality and Integrity of Critical Information

The Attack Mitigator IPS 5500 provides the strongest levels of protection for business-specific files, data center information, and network access against threats such as:

- **Content-Based Attacks** (including worms, Trojans, viruses and exploits of critical vulnerabilities)
- **Rate-Based Attacks** (such DoS and DDoS attacks)
- **Undesired Access of Sensitive Resources and Data** (with advanced stateful firewall features to protect against unauthorized user access and insider abuse)

The Attack Mitigator IPS 5500 is a purpose-built hardware platform, employing multiple high-performance ASICs and highly programmable FPGA. The system is optimized to be inline and keep sensitive data and mission critical financial systems safe from malicious activities.

The IPS 5500 provides the best protection mechanisms for:

- Compliance with SOX and SEC regulations in securing confidential information and systems while guaranteeing availability.
- Securing critical assets from both rate-based resource consumption attacks and penetration of server and application resources and databases.

The IPS 5500 can be installed and provide immediate protection using the preconfigured protection mechanisms that are preloaded with the device. Top Layer's Non-Stop Protection approach to IPS focuses on Protection, Performance, Management and Reliability.

Protection is a key element of any solution designed to maximize confidentiality and mission critical resource availability. The Attack Mitigator addresses protection in the following way:

- **Uncompromised Protection** – The latest hybrid attacks and advanced hacker evasion techniques necessitate a highly integrated multi-method approach to accurately detect and block cyber attacks. The Attack Mitigator inspects 100% of the packets and integrates many protection mechanisms, including its Deep Packet Inspection and Stateful Analysis Engines to understand application behavior and usage.
- **High Detection Accuracy** – Unlike signature-based IPS solutions, that are notorious for generating false positives, the Attack Mitigator’s proprietary Advanced Protocol Validation Modules eliminate false positives.
- **Protection Against Zero-Day and Unknown Exploits** – The Attack Mitigator’s proprietary Advanced Protocol Validation Modules provide leading edge protection against server attacks. These Advanced Protocol Validation Modules work by inspecting every packet and determining whether the stream of packets that makes up a transaction violates Permitted Protocol Usage.
- **Best In Class DDoS Protection** – Attacks against servers where there are no vulnerabilities are more prevalent than ever before. DDoS attacks now account for the greatest financial losses to businesses worldwide, and no IPS would be complete without comprehensive protection from these attacks. The Attack Mitigator, using patented DDoS protection mechanisms, and offers the most comprehensive protection from all types of DoS and DDoS attacks.
- **Continuously Stateful** – The Attack Mitigator maintains the most context (state) of any IPS device, by an order of magnitude. This is crucial for protection against slow, but debilitating attacks, ensuring high attack detection accuracy, and avoiding hacker evasion techniques.
- **Advanced Stateful Firewall Filters** – Many attackers gain undesired access via compromised or non-performing firewalls. The Attack Mitigator has tightly integrated advanced stateful firewall filters with all of its IPS protection mechanisms enabling it to deliver superior performance.

Performance is critical for an in-line IPS. Don’t be fooled by IPS vendors that claim they can stop an attack or claim to have signature updates. In practice, their ability to stop attacks under load must be drawn into question. It is much easier for an IPS vendor to be vague and claim their ability to stop a single attack in a clean environment versus in real usage scenarios. The key performance aspects for an in-line IPS are latency, throughput, DDoS rejection rates, operation under load, and scalability. The Attack Mitigator delivers industry-leading performance across all the key attributes and in many cases, operates at 3 – 5 times the performance levels offered by competitive products.

- **Lowest Latency Of Any IPS Device** – The Attack Mitigator is the first IPS to seamlessly integrate multiple protection mechanisms on a distributed ASIC platform. The results, latency measurements below 50 microseconds when all server protection mechanisms are enabled.
- **Scaleable Performance and Capacity** – The Attack Mitigator ProtectionCluster™ provides the highest level of performance by using unique load sharing

mechanisms. The ProtectionCluster™ provides a scalable solution and since it shares state across multiple units, it provides better protection to financial servers through more insight into conversations and transactions.

- **Outstanding Throughput** - It is very difficult for any administrator to be able to characterize all of the traffic on their network with a high degree of accuracy. What is the average bandwidth? What are the peaks? Is the traffic mainly one protocol or a mix? What is the average packet size and level of new connections established every second? The Attack Mitigator has been designed to eliminate these concerns by being able to operate in the most demanding networks with throughput of 8.8 Gbps with the ProtectionCluster™, which also provides better reliability.
- **Industry Leading DDoS Rejection Rates** – Today, DDoS attacks can be launched simultaneously from computer armies of 35,000 compromised machines, delivering seemingly harmless legitimate traffic at devastating multi-gigabit rates. Most firewalls advertise DDoS protection, but are rendered ineffective at 100Mbit/sec or less attacks. Today, attackers can easily target servers to prevent legitimate transactions or users from accessing the data and applications they need. Only the most advanced DDoS capabilities, designed in hardware, can stop these attacks while allowing legitimate business traffic to continue to flow to the intended destination. Top Layer has been at the leading edge of stopping high volume DDoS attacks for many years. The Attack Mitigator incorporates this technology in all of its IPS products and allows customers to combine traditional IPS protection features with full DDoS protection.
- **Performance When Under Attack** – This is the one performance metric purposely missing from most vendors datasheets. As a result of the tight integration of the protection mechanisms with the hardware architecture, datasheet performance for the Attack Mitigator is precisely that, even when under attack.

How The IPS 5500 and SecureCommand™ Ensure Proper Monitoring, Accounting, and Reporting of Security Events

The **IPS 5500** working in conjunction with **SecureCommand+** Central Management System (CMS) provides public companies with the ability to comply with the implicit IT security mandates that SOX compliance requires. By harnessing the information provided by one or more IPS 5500s deployed throughout the enterprise, the reporting and robust logging capabilities of the SecureCommand+ allow organizations to prove that security polices are being correctly followed – even providing an integral framework to empower administrators to respond to security threats and incidents in a consistent, compliant, approved manner. In other words, the combination of SecureCommand+ and the IPS 5500 enables IT Security organizations to deploy the best protection and also benefit from real-time and forensic security information as part of an overall SOX compliance solution.

Finally, in addition to enabling compliance with Sarbanes-Oxley regulation, SecureCommand+ provides a fast to deploy, very low maintenance security management framework to reduce the workload placed on IT security, improve security operations effectiveness, and enhance the company's ability to proactively mitigate high-risk threats before they become successful exploits. SOX

security compliance becomes significantly easier to manage and control with SecureCommand+ providing real-time monitoring, management and reporting of one or more IPS 5500s.

Return on Investment

Most of our customers who use the Attack Mitigator to protect their critical financial IT infrastructure tell us that the payback from their IPS investment is immediate. Customers typically provide the following reasons on how the Attack Mitigator provides rapid ROI:

- Protection from undesired access to confidential data minimizes financial liability and legal issues
- Eliminating server down time
- Avoid hurried patching of compromised servers that may cause follow on problems because of a lack of time to properly test patches
- Blocking attacks allows for increased bandwidth availability
- Increase network performance by eliminating unwanted and malicious traffic
- Reduce operating expenses incurred by maintaining and running older, ineffective security solutions
- Allowing legitimate transactions to continue to flow even in the face of the most brute force DoS and DDoS attacks
- Cost-effective solution for monitoring, logging and reporting across the entire enterprise where IPS 5500s are deployed

Many customers tell us that even one of these reasons can result in a 100% payback in a very short time. When combined, the business case for deploying the Attack Mitigator to protect mission critical financial IT infrastructures is compelling and no other IPS solution can claim this level of ROI.

Conclusions

Today Enterprises face a significant paradox based on the requirement to further enable fast and efficient access to account information and processing of financial transactions, while also providing additional mechanisms for ensuring confidentiality and uptime of IT infrastructure. Top Layer Networks has the best IPS solution for offering protection from undesired access, malicious content and rate-based attacks that target mission critical financial servers and networks. Top Layer also provides IT administrators the utmost peace of mind with fast response and continual updates to protect against new vulnerabilities and potential risks.

The Attack Mitigator IPS 5500 is a high-performance, scalable and reliable Solution that has been designed from the ground up to offer the best protection mechanisms and performance for detecting and eliminating cyber threats that target mission critical Financial systems and confidential information.

Top Layer, in collaboration with OpenService, has developed the SecureCommand+ Central Management System. This technology accepts unique security state information, as well as traditional inputs such as event and syslog data, from any number of Top Layer's Attack Mitigator IPS 5500s. The extra

intelligence provided with specialized IPS 5500 data inputs combined powerful risk-based correlation and analysis, gives IT administrators much more focused information to counter dynamic threats, quickly provision their IPS 5500s to defend against further attack and provide proper reports and audit trails for regulatory compliance.

To find out more on how the IPS 5500 and/or SecureCommand+ can offer a faster path to regulatory compliance call our sales hotline at 508-870-1300.

Further Reading

Public Company Accounting Oversight Board, Auditing Standard No. 2

<http://www.pcaobus.org/rules/Release-20040308-1.pdf>

ISACA/ITGI IT Control Objectives for Sarbanes-Oxley

http://www.isaca.org/Template.cfm?Section=About_Isaca&Template=/ContentManagement/ContentDisplay.cfm&ContentID=12406

An Overview of Sarbanes-Oxley for the Information Security Professional

Gregg Stults

http://www.giac.org/practical/GSEC/Gregg_Stults_GSEC.pdf

The Role of IT Security in Sarbanes-Oxley Compliance

Mary Fleming

<http://www.sans.org/rr/papers/31/1376.pdf>

Top Layer Networks, 2400 Computer Drive, Westboro, MA 01581

Phone: 508-870-1300, Fax: 508-870-9797, www.TopLayer.com