



WHITE PAPER

Intrusion Prevention

A Proactive Approach to Network Security



Where it all comes together.™



CONTENTS

+ Executive Summary	3
+ A False Sense of Security	3
+ Intrusion Detection: When All Else Fails	4
+ Intrusion Prevention: A New Paradigm	5
Current Intrusion-Prevention Technology	5
A Work in Progress	7
Moving Toward a Systematic Approach	7
+ Emerging Models of Intrusion Prevention	8
Internet Service Providers (In-the-Cloud IPS)	8
Managed Security Services (Outsourcing)	9
+ VeriSign® Managed Intrusion Prevention Service	10
+ The VeriSign Difference: Expertise, Intelligence, Trust	10
Seasoned Practitioners	10
Best-of-Breed Solutions	11
Unique Data and Infrastructure Intelligence	11
Stability and Trust	11
+ Conclusion	11
+ For More Information	12



Intrusion Prevention

A Proactive Approach to Network Security

+ Executive Summary

As the complexity and scope of network threats grow, forward-thinking companies are increasingly complementing traditional intrusion-detection systems (IDS) with intrusion-prevention systems (IPS). Unlike IDS devices, which merely identify potential threats, IPS technologies are designed to proactively block malicious traffic before it can do damage. To be most effective, intrusion prevention must encompass more than technology; it must evolve into a systematic approach that pervades every network and business process—whether internal or external.

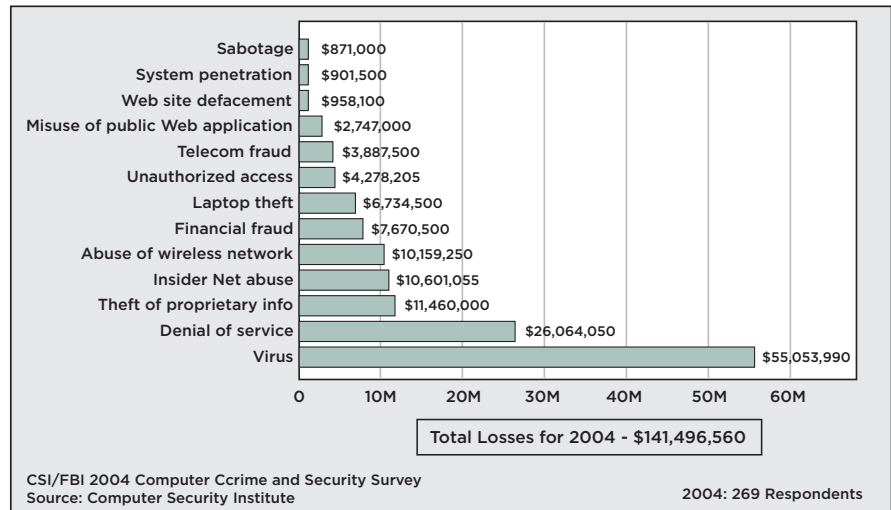
However, even the simplest IPS devices present challenges in network performance, policy setting, and overall complexity. As intrusion-prevention strategies mature, organizations will need considerable expertise and security intelligence to effectively architect, deploy, and maintain their IPS solutions. VeriSign® offers a suite of services that provide the security controls, deep expertise, and global intelligence needed to deploy and maintain a multitiered prevention strategy while freeing up personnel, technology, and financial resources for core business activities.

+ A False Sense of Security

Today's network attacks are not only more damaging but also more sophisticated. Hackers, phishers, and other cyber criminals are increasingly using multipronged exploits to detect and prey on network vulnerabilities. Even companies that have installed network-security systems are not immune. According to a study conducted by *CSO* magazine, the U.S. Secret Service, and the CERT Coordination Center at Carnegie Mellon University's Software Engineering Institute, e-crime cost organizations more than US\$666 million in 2003.

According to the 2004 CSI/FBI Computer Crime and Security Survey, published by the Crime Security Institute in conjunction with the Federal Bureau of Investigation, virus attacks accounted for the highest losses for respondents surveyed in 2004. Troublingly, 99 percent of those surveyed reported using antivirus software, 98 percent said they use firewalls, and 68 percent responded that they employ intrusion detection systems. Clearly, simply installing network-security technology does not guarantee protection. In many cases, it simply leads to a false sense of security.

Recognizing the need to address network security on multiple fronts, organizations are increasingly moving from passive and reactive network-security solutions that focus on intrusion detection to multilayer, proactive solutions that include both intrusion detection and intrusion prevention. As they embrace this new model, companies are also facing the fact that technology alone is not enough. Sound security policies and real-world expertise must also be applied.



Dollar Amount of Losses by Type

+ Intrusion Detection: When All Else Fails

Although most organizations set up protective technologies such as firewalls, antivirus software, and virtual private networks (VPNs), attacks still manage to penetrate their lines of defense. Even the best security is not foolproof. To counter weaknesses, many organizations install an IDS device.

Such devices, typically placed next to key entrances to the network, together act as a last-chance virtual safety net. They monitor network traffic, and, when other safety measures fail to stop suspicious traffic, they are designed to notify the organization of potential break-ins, malicious activity, or noncompliant traffic. IDS devices are passive; they cannot stop attacks.

Although passive analysis is useful, this process complicates identification of true threats, delays intervention, and bogs network administrators down. What may be merely suspicious in one environment may be valid in another, often causing inappropriately tuned sensors to elicit a high rate of false positives. If the system reports many such results, administrators may begin to ignore them or may become overwhelmed with responding. They may even mistakenly block legitimate traffic, bringing critical business operations to a standstill. On the other hand, if administrators tune systems to reduce false positives, the number of false negatives may increase, thereby increasing the risk that real threats will infiltrate the network.

In spite of their shortcomings, IDS devices are vital to any comprehensive network-security program—and will be, as long as human error, system bugs, and other security imperfections exist. In the long run, intrusion detection may take on a more diagnostic role, providing visibility into security events that do not necessarily present an immediate danger, inherently produce a high rate of false positives, or have a low priority (as in acceptable-use policies).

+ Intrusion Prevention: A New Paradigm

IPS devices have gained popularity as security professionals increasingly focus on stopping potential intrusions before they become a threat. An IPS can be thought of as a highly refined firewall, able to deny hostile traffic while allowing legitimate traffic to pass through. In contrast to IDS devices, IPS devices can actively intervene when they detect a potential attack or intrusion. Intervention may result in flagging of traffic for further manual assessment, session termination, or some other action.

In the CSI/FBI survey cited earlier, 45 percent of the respondents had already adopted IPS; these early adopters have focused primarily on stopping worms. Worm and virus outbreaks threaten corporate-network uptime, and success in stopping them can save a company significantly more than the cost of deploying an IPS appliance, which is also gaining popularity as a security checkpoint directly in front of mission-critical server farms.

Because IPS mechanisms are designed to analyze traffic in the context of other network activities and because they rely on a wide range of intelligence and data, leveraged across multiple detection methodologies, they detect intrusions more accurately than IDS devices. This capability reduces the number of false alarms and allows system administrators to focus on true threats.

Today's IPS devices are typically deployed in the same locations as firewalls and/or IDS devices: at points of ingress or directly on servers. More broadly speaking, these locations can be thought of as the two edges of the network: the outer perimeter (or even inside the Internet cloud) and down to the desktop level. Neither of these solutions is perfect, and many experts believe the technology won't reach full maturity until it is pushed into the actual network-switching fabric.

Current Intrusion-Prevention Technology

State-of-the-art network security involves a combination of technology, expertise, and policy. Although IPS technology is in its early stages, the following capabilities are critical to the effectiveness and success of a network-based IPS deployment:

- Performance
- Multimethod event detection
- Accuracy
- Up-to-the-second intelligence
- 24/7 monitoring

These capabilities are discussed below.

Performance

An IPS must not disrupt normal operations. When a network-based IPS is inserted inline, it must not introduce unacceptable or unpredictable latency into the network. Normal network traffic and host-based processes should operate identically, whether an IPS is running or not. Blocking actions must occur in real time or near real time, and latencies must be in the range of tens of milliseconds (not seconds). Network availability and reliability must remain high.

A network-based IPS must perform packet normalization, assembly, and inspection, and it must include the following capabilities:

Terminate malicious sessions: The IPS must drop malicious sessions, instead of simply resetting connections. To accomplish this procedure, network-based intrusion prevention must perform deep-packet inspection of all traffic and generally must use special-purpose hardware to achieve gigabit throughput.

Support blocking and packet inspection at wire speeds: Software-based approaches that run on general-purpose servers may be sufficient for small-enterprise use, and blade-based approaches may scale up to some large enterprises. However, for complex networks running at gigabit rates, application-specific integrated circuits (ASICs) and dedicated network-security processors are required to perform deep-packet inspection and support blocking at wire speeds.

Multimethod Event Detection

An IPS must employ multiple protocol-identification and analysis techniques to detect malicious actions. Detection capabilities must include not only simple signature-based matching of known attacks (such as that used by antivirus and IDS mechanisms) but also policy-, behavior-, and anomaly-based detection algorithms. These algorithms must operate at both application and network levels.

Accuracy

To block malicious traffic while allowing legitimate traffic to pass through, an IPS must be able to accurately distinguish between hostile events and normal events. This capability is as much a function of IPS technology as it is a result of proper configuration. As IPS mechanisms mature, they will likely be able to accurately identify and block higher percentages of attacks than today's first-generation IPS devices do. However, even the best technology will permit malicious traffic and block benign traffic if it is not tuned properly to the company's environment and device policies are not updated regularly. Creating and maintaining effective device policies is an intricate, time-consuming task. It requires an in-depth understanding of the company's unique business and security requirements and network topology, as well as extensive hands-on experience in planning and deploying security technology.

Up-to-the-Second Intelligence

Online threats are dynamic and constantly evolving. To proactively protect the network, an organization implementing an IPS must have the expertise, technology, and financial resources to actively monitor and research vulnerabilities, threats, and solutions. The organization (or its IPS provider) must also have split-second access to global intelligence regarding security events and patches, and it must be able to analyze and correlate data in such a way that it can anticipate, identify, and thwart new or undocumented threats. Finally, the organization should actively collaborate with industry consortiums, standards bodies, law enforcement agencies, and other organizations that share information about security threats and patterns.

24/7 Monitoring

As with IDS devices, security professionals must continuously monitor events generated from, and the health of, IPS devices. Because IPS technologies are deployed via inline devices, downtime can potentially result in either all traffic being blocked or malicious traffic being permitted into the company's environment. Effective monitoring requires more than around-the-clock security personnel watching network monitors for alerts; it also requires an intelligent infrastructure—active 24/7—that can analyze all traffic, correlate network events, and regularly evaluate the functioning of inline devices. In addition, to ensure availability and reliability of the monitoring infrastructure, all systems must be fully redundant.

A Work in Progress

Widespread use of IPS blocking is still immature, and it must be examined with care. An improperly configured IPS can lead to a false sense of security while doing nothing to protect the network, or, equally harmful, it can lead to a denial-of-service problem for the company. Other aspects of IPS also require improvement. The high-availability options for inline devices are not yet as robust on most platforms as enterprises demand. Support for complex and asymmetric routing scenarios is also weak. VeriSign's work with the leading IPS vendors makes us confident that by the second half of 2005 or in early 2006, most manufacturers will have addressed some or all of these issues. New releases will offer more robust high-availability options and monitoring controls, as well as refinements in operational blending of technologies used internally on these devices.

Moving Toward a Systematic Approach

A truly effective security strategy requires more than the purchase and deployment of IPS technology and other security devices. Strong network defense also requires sound security policies, proper deployment, and a pervasive, multilayered approach that builds in redundancies. The advantage of "defense in depth" is that an organization does not have to rely on a single control measure. (A Trojan may find a weakness in one control, for example, but in order to succeed in an exploit, it must discover multiple weaknesses.) A defense-in-depth approach also helps combat one of the primary sources of network attacks: infected or otherwise compromised home computers or laptops that connect to the corporate network.

The most effective defense-in-depth strategies combine an IPS with the following technologies and tactics to avoid a single point of network failure:

Email gateway: An in-the-cloud gateway can filter email before it reaches the organization. Besides preventing spam, viruses, or phishing exploits from ever reaching the organization, this approach reduces the network bandwidth, storage, and administration costs associated with quarantined mail and high volumes of spam.

Localized antivirus software: Email gateway filters and network antivirus solutions prevent viruses from entering the network via the Internet, VPNs, and other specified external ports; however, they do not prevent viruses from being introduced by machines that bypass network ports of entry (such as notebook computers that travel between a user's home and office.) To prevent this type of infiltration, organizations can install antivirus software directly on notebook computers and other portable devices that may skirt network-level screening.

Network firewalls: These programs are installed at gateways to external networks (such as extranets, the Internet, and VPNs) and regulate who or what can access the internal network.

Localized firewalls: These programs, like localized antivirus software, help reduce vulnerabilities introduced by notebook computers and other portable devices that can circumvent network-level firewalls.

Event logs: When properly monitored and analyzed, event logs help organizations identify patterns, evaluate events, correct vulnerabilities, and respond rapidly to threats.

Strong authentication: By combining something you have (such as a security token) with something you know (such as a password), strong authentication provides a more reliable method for verifying user identity than passwords do. State-of-the-art strong-authentication solutions provide a single platform for provisioning, managing, and using multiple authentication credentials, including smart cards, device-generated one-time passwords (OTPs), and digital certificates.

Integrity verification: Verifying the integrity of every machine every time it reconnects to the enterprise network ensures that the machine is free of viruses, spyware, Trojans, and other threats, and that it is running approved, properly configured security software.

+ Emerging Models of Intrusion Prevention

The adoption of IPS technologies and the move toward multilayered security strategies present a complex challenge for organizations. Creating and managing effective device policies requires extensive security expertise and time, especially as the number of devices proliferates across and beyond the network. In addition, companies need high-performance, high-availability infrastructures to support full-scale IPS solutions. Finally, companies must maintain 24/7 vigilance over security events and device health, and they must have split-second access to global security intelligence.

As IPS strategies mature, many organizations may seek assistance in deploying IPS technology—either by relying on their Internet service provider (ISP) to provide IPS services or by outsourcing IPS management to professionals whose core expertise is security.

Internet Service Providers (In-the-Cloud IPS)

Depending on their level of interaction with external networks, organizations with limited staff, technology, or financial resources may be able to rely on IPS mechanisms provided by their ISP; ISPs are quickly adopting intrusion prevention technology to combat phishing exploits, spam, worms, and other attacks.

When properly deployed and managed, in-the-cloud IPS offers the following advantages:

Better protection: Attacks are intercepted before they can reach the enterprise's site, and browsing environments are safer.

Significant network savings: Osterman Research reports that as of early 2004, spam represented between 55 and 75 percent of all enterprise email traffic. Ferris Research estimates that spam will cost U.S. businesses approximately US\$17 billion in 2005. By eliminating spam, phishing, and other unwanted email before it reaches the network, organizations not only strengthen security and improve worker productivity but also preserve valuable bandwidth.

Easier management: By contracting with their ISPs, companies create a single point of contact for connectivity and security services and receive a single service charge and bill. Besides streamlining management, this arrangement allows companies to negotiate better fees for communication and security services.

Rapid, low-cost deployment: Because the ISP provides existing infrastructure and technology for IPS, intrusion prevention can be deployed rapidly without incurring up-front capital costs.

Although in-the-cloud solutions provided by ISPs can prevent attacks on the local network (for example, by blocking viruses from replicating to other machines), their effectiveness diminishes as the organization's network grows to include business partners and extranets. A business partner, for example, may be able to access the network via a private line that bypasses the IPS, or an extranet might be set up as a VPN the IPS cannot see or evaluate because the VPN traffic is encrypted.

Before in-the-cloud IPS can gain a strong foothold among businesses, ISPs will have to address this issue. In addition, ISPs must prove that they can maintain high availability, high performance, and high reliability as their network grows and new services are added. Finally, to avoid blocking legitimate, business-critical traffic to an enterprise, ISPs will have to refine filtering mechanisms and parameter setting so they can address the unique requirements of each company.

Managed Security Services (Outsourcing)

As IPS devices and strategies increasingly permeate internal and external processes, management becomes more complex, and operational expertise and focus becomes more critical. Besides highly skilled, 24/7 management, an effective IPS requires an intelligent infrastructure that can analyze all traffic, correlate network events, and regularly evaluate the functioning of each device.

Recognizing the cost and complexity of meeting these requirements, many companies engage a managed-security-services provider (MSSP) to assess or manage key aspects of IPS security. By partnering with a qualified MSSP, companies can avoid many of the pitfalls associated with inadequate training, limited staffing, poor security intelligence, or insufficient infrastructure.

MSSPs offer the following advantages:

Staffing and skill set: Whereas existing security staff may lack the time, experience, or insight to tackle additional security projects, MSSPs can be more objective and more focused. They encounter a broad range of security issues and environments in their daily work, giving them experience that would be difficult to accumulate working within a single enterprise.

Trust: The involvement of an MSSP with a proven track record and global name recognition can help establish trust between the organization and external users who may not be acquainted with the enterprise and its security capabilities.

Intelligence: MSSPs tend to have faster, more global access to information about network vulnerabilities, impending attacks, and solutions.

Cost and time savings: Outsourcing key tasks to a third party is often less expensive than investing in in-house experts, technology, and 24/7 operation centers. Because security is their core business, MSSPs can justify heavy investment in highly qualified staff, ongoing training, and state-of-the-art technology. In addition, technology, methodology, and personnel are already in place, saving valuable time when first deploying an IPS solution.

+ VeriSign® Managed Intrusion Prevention Service

The VeriSign® Managed Intrusion Prevention Service, a component of the VeriSign suite of managed security services, allows companies to leverage VeriSign's substantial infrastructure capabilities and security expertise to create a highly effective IPS solution. Using the service, organizations can ensure that their IPS devices operate effectively to block unwanted traffic while intelligently allowing benign traffic to flow freely. VeriSign consultants work with each customer to develop and fine-tune intrusion prevention policies until they operate at peak efficiency. VeriSign also patches and upgrades all devices under management.

VeriSign Intelligent Infrastructure Services® are housed in highly available environments that provide 24/7 monitoring and management of security infrastructures for Global 2000 companies. Through TeraGuard™, the VeriSign information-management architecture, VeriSign analyzes and prioritizes all security events using a multitiered correlation process. This procedure allows VeriSign to quickly eliminate false positives and focus on the real threats and enables the company or its customers to take appropriate action.

Used with VeriSign's other security offerings, the Managed Intrusion Prevention Service provides a comprehensive, multilevel approach to network security that embraces state-of-the-art security controls, sound security policies, and superior security intelligence—all at a lower operational cost than could be achieved via an organization's internal resources.

+ The VeriSign Difference: Expertise, Intelligence, Trust

Although many vendors offer managed IPS solutions, few providers match VeriSign's expertise, intelligence-gathering capabilities, commitment to open standards, or role as trusted adviser. The VeriSign Managed Intrusion Prevention Service leverages exceptional knowledge, training, and experience; best-of-breed solutions; and VeriSign's history of stability and trust to deliver IPS solutions that not only are effective but also make the best use of existing in-house personnel, technology, and processes.

Seasoned Practitioners

The VeriSign consulting team includes one of the highest concentrations of credentialed experts in the industry. With an average of ten years' experience in enterprise information security and three or more industry certifications per consultant, VeriSign boasts expertise across the entire information-security and information-privacy spectrum. The VeriSign team has worked with companies of all sizes all over the world, from government agencies and Fortune 1000 companies to small start-ups and family-owned businesses. VeriSign customers include municipal, state, and federal agencies, financial institutions, health-care organizations, telecommunications carriers, and online retailers. The security team's expertise, dedication, and focus on customer service help ensure that each customer not only gets a real-world solution that meets its unique requirements but also receives prompt attention when security events or other issues arise.



Best-of-Breed Solutions

As a vendor-neutral provider of security services, VeriSign evaluates, certifies, and supports best-of-breed security products. It is a leading proponent of open standards-based technology for identity authentication and other security solutions, and it has led or participated in development of many best practices and common standards, including Open Authentication (OATH). By supporting off-the-shelf security devices and open standards-based technology, VeriSign can provide best-of-breed IPS solutions that leverage an enterprise's existing technology investments.

Unique Data and Infrastructure Intelligence

As a leading provider of critical Internet-infrastructure services, VeriSign has unique visibility into security patterns, trends, and threats on the Internet. VeriSign can extract and assimilate information not only from its managed security services but also from data sets connected with other services such as its global Domain Name System (DNS), payment, and antiphishing services. Leveraging this data and automated processes, VeriSign can be first off the mark in providing companies with visibility, aggregation, and correlation of worldwide Internet-related events. This capability is an important component for prevention of and response to attacks.

Stability and Trust

VeriSign is a leading provider of critical infrastructure services for the Internet and telecommunications networks. With more than 4,000 enterprise customers, it is the largest provider of trusted payment processing, and the company processes 30 percent of U.S. commerce transactions. It has maintained critical infrastructure such as the DNS with 100 percent availability for more than ten years.

+ Conclusion

IPS products are a rapidly maturing hybrid of technologies that need to be handled carefully. The VeriSign Managed Intrusion Prevention Service provides the expertise, infrastructure, and global intelligence needed to deploy and manage a cost-effective IPS solution that blocks malicious traffic while allowing legitimate traffic to pass freely. As IPS capability evolves to include not only technology but also multitiered strategies, VeriSign services will help organizations handle the increasing complexity while providing greater control over network security and freeing up valuable resources for core business activities.



+ For More Information

For more information about the VeriSign Managed Intrusion Prevention Service, please call 650-426-5310, email enterprise_security@verisign.com, or visit www.verisign.com.

+ About VeriSign

VeriSign Inc. (Nasdaq: VRSN) delivers intelligent infrastructure services that make the Internet and telecommunications networks more intelligent, reliable, and secure. Every day, VeriSign helps thousands of businesses and millions of consumers connect, communicate, and transact with confidence. Additional news and information about the company is available at www.verisign.com.

Visit us at www.Verisign.com for more information.

©2005 VeriSign Inc. All rights reserved. VeriSign, the VeriSign logo, "Where it all comes together," and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries. All other trademarks are the properties of their respective owners.

0019634 05/05