



McAfee Protection-in-Depth Strategy

Network Intrusion Prevention Systems Justification and ROI

Table of Contents

Are My Critical Data Safe?	3
<hr/>	
The Effects and Results of an Intrusion	3
<hr/>	
Why the Demand for IPS?	3
<hr/>	
What Will IPS Technology Provide?	4
<hr/>	
The Role of IT—Protecting the Revenue Stream	4
<hr/>	
What Is the Return on Investment?	4
<hr/>	
Real-Life Case Study—A Leading Computer Security Vendor	4
<hr/>	
Actual Return on Investment	5
<hr/>	
McAfee PrimeSupport	5
<hr/>	
Conclusion	5

Are My Critical Data Safe?

An organization's critical data have never been more at risk. Today's IT professionals face unending challenges in the area of proactive risk management:

- Today's attacks are more frequent, more lethal, and spread faster than ever
- Patching has become impossible to keep current, leaving critical systems and infrastructure dangerously exposed during vulnerability windows
- Regulatory requirements for protecting data privacy, integrity, and confidentiality are now in force
- Despite heavy investments, security gaps still exist

Adopting a layered, Protection-in-Depth™ approach is a pragmatic philosophy that combats enterprise security threats. Simply stated, the McAfee® Protection-in-Depth Strategy is one built upon the notion that leveraging multiple, complementary technologies will provide the maximum protection against targeted attacks and vulnerabilities.

The Protection-in-Depth architecture is proactive security in a very dynamic environment. This means realtime risk management and remediation—the ability to stop, block, and clean attacks—as well as Intrusion Prevention Systems (IPS) that can be implemented to manage all trusted systems.

By combining best-of-breed technologies, organizations will achieve a more comprehensive and robust security posture, meaning fewer successful attacks, more efficient use of scarce security resources, and lower operating costs than simply deploying one limited technology and hoping it will protect the organization.

If targeted attacks and malicious code writing remained static, it might be harder to rationalize redundant security technology. However, this is a dynamic, thriving, and furtive threat whose momentum and technology continue to grow. No security professional can ever predict all future vulnerabilities or the exploits that invariably will follow.

The Effects and Results of an Intrusion

Intrusions and targeted attacks may result in:

- Loss of data
- Loss of reputation
- Loss of time
- Loss of business availability

Any or all of the above will result in financial implications for your business (for example, see the case study on page 4).

A more detailed analysis of the financial implications of an intrusion exposes the reliance of modern businesses on data. Companies depend on information to maintain daily operations and to control their supply chain. What are the

implications, for example, of having a critical application that controls the supply chain go out of service for an hour just before the Christmas holiday?

Successful attacks inflicting network downtime may affect organizations in several areas, including:

- Negative impact to end users due to productivity losses resulting from the loss of access and availability to the external network
- Negative impact to IT as a result of the exorbitant time required to restore availability and uncover the extent of damage from an attack
- Negative public impact to the organization by failing to protect client-sensitive data, failing to meet regulatory compliance and protection requirements, and by creating a potentially damaging customer and market perception that internal networks and data may not be secure
- Negative impact on profitability due to the loss of business availability

An intrusion or compromise consists of multiple stages: reconnaissance, scanning, gaining access, maintaining access, and clearing tracks. Host and network intrusion prevention systems are both targeted at the same goal—protecting critical assets from very sophisticated threats. Integrating the best of each architecture provides a solution whose sum is greater than its parts.

In the recent report titled *Intrusion Prevention* by the Department of Trade and Industry (DTI), it was concluded that the time and resources spent on investigation and remediation are remarkably high for such attacks and intrusions. Such costs will be significantly reduced with an IPS, since an IPS solution will provide a proactive measure of protection.

Why the Demand for IPS?

The evolution of hybrid attacks utilizing multiple vectors to breach security infrastructure has highlighted the need for enterprises to defend themselves against a constantly shifting threat.

Organizations have suffered catastrophic damage to their business confidentiality, integrity, and availability as intrusions have become more virulent. In a matter of minutes, companies can suffer significant lost revenue as production lines go dark and order taking and fulfillment processes come to a halt due to attacks like Sasser, SQL Slammer, and Nimda.

Traditional firewall and anti-virus solutions are necessary to prevent the transfer of malicious code, but are not sufficient to address the new generation of threats and targeted attacks. Security solutions that proactively protect vital information assets in real time, without waiting for new signature creation and distribution, are needed.

What Will IPS Technology Provide?

An Intrusion Prevention System is a system that protects the following:

Confidentiality—Protecting the confidentiality of information stored in electronic format on a computer system and preventing any form of unauthorized viewing or copying. Threats involve the introduction of backdoor programs, keyboard-logging programs, and other programs designed to allow unauthorized personnel access to information.

Integrity—Protecting the integrity of the information stored in electronic format on a computer system and preventing any form of unauthorized alteration or modification. Threats involve backdoor programs, network worms, and other programs that are designed to alter or erase information.

Availability—Protecting the availability of a computing resource, network, system, or information stored in electronic format on such a system or network and preventing any use or access by unauthorized personnel. Threats include Denial of Service (DoS) attacks and backdoor programs that allow the use of resources by unauthorized personnel for unauthorized purposes.

Due to the dynamic nature of network intrusions and threats, deploying a combination of both network and host IPS technologies provides the greatest level of protection for critical data and critical applications. Network IPS solutions are deployed inline at the network perimeter, core, or remote office. They are designed to protect your critical infrastructure by blocking internal and external attacks on the wire and are considered the first line of defense. Host IPS solutions are deployed on servers, desktops, and laptops. They are designed to protect critical systems and applications by blocking attacks at the host and are considered the last line of defense.

The Role of IT—Protecting the Revenue Stream

The subsequent points highlight some of the key concerns and challenges that IT teams are confronted with on a daily basis. The following are based on a typical company operating in 2004:

- \$300 million click revenue
- 24/7 DAT delivery—failure means close of business
- 24/7 technical support
- Product delivery dates
- Reducing the cost of patching and avoiding cost of clean-up (IT cost only)

What is the cost if a mission-critical electronic point-of-sale (EPOS) system goes down in a store for even an hour? The revenue stream of the affected business will be at risk and the company will be reliant on the IT department to identify the threat and fix the problem.

What is the cost if the critical server controlling the online ordering and e-commerce systems is hacked, compromised, and taken offline?

Network security systems that protect infrastructure, processes, and data are critical to the success of any company. Any interruption to a process can bring down a critical service or application, resulting in loss of business availability and revenue.

What Is the Return on Investment?

The following questions can be used to determine the costs involved in managing a malicious attack or virus outbreak:

- What is the cost to an organization if its Internet presence is abused or unavailable?
- What is the estimated cost to an organization if it experiences a security breach?
- What is the estimated cost to the reputation of an organization if it experiences a security breach?
- What is the estimated monetary cost to your organization for implementing a business continuity plan or parts thereof?

For most any organization, the cost of the above will far outweigh the cost of purchasing, implementing, and managing the IPS. This argument has been proved in the case study that follows.

Real-Life Case Study—A Leading Computer Security Vendor

This global computer security powerhouse withstood more than 50 million attacks in 2003. For Ted Barlow, chief security officer, a top priority is to keep the attackers at bay while protecting not only the company's reputation as a computer security leader, but also its corporate applications and content. This includes things like customer relationships, supply chains, financials, and intellectual property—such as source code.

This security leader embarked on a Protection-in-Depth Strategy to block or prevent attacks before they reach the network, rather than passively detecting network attacks as they speed past the perimeter. This means realtime risk management and remediation; the ability to stop, block, and clean attacks; and scalable IPS that can be implemented to manage all trusted systems.

“IntruShield was much more accurate over many more different types of attacks than competing technologies.”

— Ted Barlow, Chief Security Officer

Actual Return on Investment for Network Intrusion Protection

The figures below are based on the above company's case study and highlight the calculations used to determine the actual ROI:

- IT Cost Avoidance**—The average cost of the Slammer virus in IT time alone amounted to \$240,000. In 2003 there were four similar outbreaks
 Annual cost = \$1 million
- Protected Revenue Stream**—E-Commerce is relatively small with an average of 16,000 orders per hour. The downtime amounted to \$60,000 an hour. Some companies were down for up to sixty hours, with an average of ten hours per major outbreak in 2003, where there were four similar outbreaks
 Annual cost = \$2.4 million
- Cost of Ownership**—Prior to using McAfee IntruShield®, there were six dedicated IDS analysts. By installing IntruShield Appliances this resource was reduced to two and four were redeployed to proactive roles
 Annual cost = \$400,000
- Leveraging Existing IT Investments**—The customer's current investment in firewall technology amounts to \$500,000. Without using IntruShield Appliances in front of these firewalls, the SoBig virus, generating 3 million inbound e-mails per hour over a five-day period, would have caused a loss of productivity amounting to \$19,021 in firewall downtime. In 2003, there were four similar outbreaks
 Annual cost = \$76,084

This being a very large deployment, a total of forty-three network IPS appliances (all in failover) were deployed with capital expenditures spread over a total of three years.

Total IPS Investment of \$600,000

Annual Cost of \$200,000

Annual Return on Investment

Cost of Investment	\$200,000
Savings	\$3,876,084
ROI	19.38:1

McAfee PrimeSupport

McAfee has pursued a strategy of providing best-of-breed technology for each type of security and performance management application—but the Protection-in-Depth Strategy is more than just deploying and implementing best-of-breed solutions today. Prevention is certainly our first priority, but inevitably, you will have to react to a problem.

The McAfee PrimeSupport® program is essential for making the most of your investment in McAfee System and Network Protection Solutions. McAfee's PrimeSupport team has all the right resources and is ready to deliver your needed service solution. PrimeSupport resources include: delivering authorization to access all available maintenance releases and product upgrades, access to a comprehensive suite of additional online self-support capabilities, live telephone support accessible 24/7/365, available assigned support account managers, and a range of software and hardware support solutions that can be tailored to meet your needs.

Conclusion

Combining best-of-breed network and host IPS technology results in the most comprehensive and robust defensive posture. Implementing and deploying proactive IPS technologies will result in fewer successful attacks, more efficient use of scarce security resources, and lower operating costs than simply deploying a single, limited technology and praying you avoid an attack.

Integrating the strengths of each of the architectures provides a solution whose sum is greater than its parts. By deploying the complementary and integrated Protection-in-Depth technologies of McAfee Network and Host IPS Solutions, organizations can achieve superior protection and a proven ROI, all at a reasonable cost.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com

McAfee® products denote years of experience and commitment to customer satisfaction. The McAfee PrimeSupport® team of responsive, highly skilled support technicians provides tailored solutions, delivering detailed technical assistance in managing the success of mission-critical projects—all with service levels to meet the needs of every customer organization. McAfee Research, a world leader in information systems and security research, continues to spearhead innovation in the development and refinement of all our technologies.

McAfee, Protection-in-Depth, IntruShield, and PrimeSupport are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. The color red in connection with security is distinctive of McAfee® brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners. © 2004 Networks Associates Technology, Inc. All Rights Reserved.

6-nps-ins-roi-001-1004