Complete Risk Management
Harnessing Vulnerability Management and Intrusion Prevention Systems
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Overview</td>
<td>3</td>
</tr>
<tr>
<td>The Changing Nature of the Threat</td>
<td>3</td>
</tr>
<tr>
<td>A Growing Need for a New Response</td>
<td>3</td>
</tr>
<tr>
<td>Incorporating Vulnerability Management</td>
<td>4</td>
</tr>
<tr>
<td>Elevating the Management Imperatives</td>
<td>5</td>
</tr>
<tr>
<td>Understanding Intrusion Prevention</td>
<td>5</td>
</tr>
<tr>
<td>Bridging the Technical/Management Gap</td>
<td>5</td>
</tr>
<tr>
<td>McAfee PrimeSupport</td>
<td>6</td>
</tr>
<tr>
<td>About the Sponsors</td>
<td>6</td>
</tr>
</tbody>
</table>
Executive Summary

This report provides an executive overview of evolving security threats to the enterprise, and explores how organizations are responding to the new nature of these threats in a strategic, integrated, and proactive manner. The security requirements raised by this strategic approach are prompting a growing number of executives to revisit the way they deploy their security resources to protect critical information assets. It is the conclusion of this report that organizations must integrate security risk management and intrusion prevention system (IPS) solutions. By combining the capabilities of these two security activities, organizations cannot only improve their security posture, but they can do so in a more cost-effective manner.

Overview

Research conducted by Q&A Research and reported in November 2004, found that about 75 percent of the 300 IT managers surveyed believe their networks are more secure than they were a year ago. However, 81 percent of these respondents, who represented companies with annual revenues exceeding $30 million, confirmed that the number of attacks is increasing. And about 20 percent of respondents said that hackers had been able to access their companies’ networks.

The statistics tell a familiar story. Bad guys continue to attempt to penetrate and damage IT assets of organizations large and small. Good guys continue to work tirelessly to anticipate and respond to threats as they manifest themselves. However, as we approach the mid-point of the decade, a few trends are converging to fundamentally change the nature of the threats organizations face. This is prompting a growing number of executives to change the way security solutions are selected to manage and mitigate risks posed by these threats.

The Changing Nature of the Threat

Like all things digital, the effectiveness, sophistication, and efficiency of malicious code progresses at an exponential rate. There are not only a greater number of attacks that enterprise networks must be aware of and respond to, there are also a growing variety of threats that are morphing to create hybrid strains of viruses, worms, phishes, and other malicious manifestations of hacker activity.

Viruses today may serve as platforms from which worms may be launched; worms may serve as a way to gather information to execute phishing scams. Indeed, it is increasingly difficult to maintain the nice and neat categories into which threats can be placed.

Also, these threats are getting technically more intelligent and autonomous. The malicious activities are increasingly automated to a point where a single hacker can now have many times the impact that he or she had as recently as eighteen months ago. (This impact has been further exacerbated by growing dependence on networked business processes within and between organizations and among consumers.)

“The major change in the nature of corporate threats is that up until approximately eighteen months or two years ago, vulnerabilities were exploited by a few individuals with varying levels of sophistication and determination—hackers—who were attempting to compromise individual systems or widespread network vulnerabilities. Now many more hackers are launching a whole squadron of automated attacks simultaneously on different parts of the organization.”

—Brian Kenyon, Foundstone®

Finally, the hacking community has grown—one might even say matured—beyond the early generation of hackers who were simply interested in disrupting business continuity for the sake of bragging rights or to demonstrate their programming prowess. The fastest growing segment of the hacking community is driven by a profit motive that has led to their treating their vocation as a zero-sum business activity in which their revenues come directly at the expense of their victims. One can think of this as the professional criminalization of segments of the hacking community.

The net result of these trends is that a growing percentage of the threats to which organizations are exposed are being executed in a more focused and strategic manner.

A Growing Need for a New Response

Much has been said and written in recent months about the need to develop a Protection-in-Depth™ approach to security. Not as much as one would think, however, has been done to actually implement an integrated and proactive corporate security strategy.

According to a recent Harris Interactive survey of FORTUNE 1000 companies, there is still a major gap between what
enterprises say they are doing about threats and what actually is being done to remediate the risk.

Most of the high-level executives surveyed gave their organizations a B average when describing their ability to respond to natural and man-made disasters. But such was not the assessment of managers responsible for day-to-day security matters. Only 58 percent said that they were better prepared now than before the blackout of 2003 that kept much of the Northeast off the grid for days. (That figure is actually down from 67 percent in 2003 who said they were better prepared for attacks in a post-9/11 environment).

Why would this be?

The answer has to do with the pitfalls associated with the most common approaches that organizations take to securing their enterprise operations. Most security operations have purchased and deployed a wide array of point solutions in response to specific threats that have manifested themselves.

While some efforts have been made to integrate these solutions, most remain largely disconnected from one another, representing a series of tactical investments and activities that are both time-consuming and labor-intensive to manage.

This helps to explain why a study released by IDC found that worldwide demand for information security professionals will grow at nearly 14 percent per year for the next several years. (This is about twice the rate of growth for general IT positions.)

Indeed, a majority of IT executives surveyed in a recent benchmark study conducted by Nemertes Research’s complained about the time it takes for their anti-virus software to detect and alert them to a new virus outbreak. Respondents indicated that finding methods that can shrink the time between awareness and response to potential threats are a top priority for the enterprise IT community.

A new, viable alternative is needed for responding to the next generation of enterprise system threats that is:

- Not tactical
- Not purely reactive
- Not manual/labor-intensive

The rising number and ever-increasing sophistication of enterprise network threats require organizations to establish and continually update network security policies, procedures, and technology solutions. What is called for is an integrated and proactive approach to managing the security threat lifecycle, which harnesses efforts to prevent incidents and seamlessly works with systems that dynamically manage and respond to system risks.

"On a high level, the first priority for organizations is to establish information technology governance. IT governance includes the policies and procedures covering all aspects of network and data use. Governance needs to address the quality of network service, with network security being instrumental to ensuring quality results."

—Peter Schavacker, McAfee, Inc.

With appropriate integrated and proactive security strategies, organizations can have a multi-level defense system that intelligently allocates scarce resources according to both the value and vulnerability level of assets. A good place to start is by integrating vulnerability management (VM) activities with IPS solutions.

Incorporating Vulnerability Management

In order to manage network security risk, an organization must be able to discover, inventory, and prioritize network assets. Additionally, organizations must gather and analyze threat intelligence and correlate it to network devices. Also needed is a system for tracking and reporting the manual or automated remediation executed to address identified risks.

VM enables a systematic analysis of how various elements of risk affect corporate digital assets. It allows organizations to identify, prioritize, and mitigate risk based on how important the asset-threat equations of specific network components are to the organization. In order to implement a VM strategy, it is necessary to understand the basic elements of risk. For the purposes of this report, risk is defined by the following equation:

Risk = Asset Value x Vulnerability x Threat

The terms vulnerability and threat are often used as synonyms for risk by non-technical managers and executives. This explains the tactical—or point-solution-based—approach to security adopted by large segments of industry.

Vulnerability refers to the current disposition of specific assets to specific threats. For instance, if a router is misconfigured, or is missing patches to a known virus or worm, then it is vulnerable to those threats.
Threats refer to the disposition of malicious code, events, or incidents. For instance, the identification of new viruses—or new versions/strains of viruses—will contribute to the number of threats an organization must be aware of and be prepared to mitigate. There are known and unknown threats.

In order to strategically manage risk, it is important to have a clear idea of:

- Which information assets are critical to company operations
- The extent to which critical assets are vulnerable to attack
- The nature of actual threats—active efforts—to access, corrupt, and/or otherwise disrupt digital assets

Understanding the interplay among these three variables provides the basis for making decisions about how to best mitigate and respond to risks companies face on a day-to-day basis. It represents a fundamental departure from the traditional standard operating procedures of most security organizations.

Elevating the Management Imperatives

VM elevates security from an arcane activity that responds to specific incidents, and provides a basis from which a more proactive strategy can be implemented to make certain that critical assets, applications, and processes receive security resources that are commensurate with their importance to the organization.

The most dramatic result from a successful VM implementation will be the restoration of normalcy to the information security war room. The ability to identify areas of weakness (or high risk) proactively, rather than reactively responding to a flurry of alarms, should eliminate the fire-drill atmosphere that can develop every time a minor event manifests itself.

A rational VM strategy allows organizations to establish reasonable risk tolerance levels and manage their response accordingly. It should allow organizations to establish a manageable policy based on the quality of assets that must be protected, allocating appropriate resources based on a solid understanding of the organization’s risk level.

“For instance, if the IPS solution is inline, offending packets can be dropped silently, causing the connection to fail. Whether or not the connection is inline, the session can also be summarily dropped by sending TCP Resets or ICMP Unreachable messages to the client, server, or both. Or, the offending IP address can be shunned—blocked—for a specific time period.”

—Mike Fratto, Network Computing Magazine

Understanding Intrusion Prevention

IPS activities are designed to sniff out and stop incoming intrusion attempts—including those made by viruses, network-attacking worms, etc.—that are known as well as those that are so-called zero-day threats, for which patches aren’t yet available.

IPS solutions represent a significant step beyond intrusion detection systems (IDS) and firewall technology. Whereas IDS solutions passively monitor traffic by sniffing packets off a switch port, an IPS resides inline like a firewall, intercepting and forwarding packets. It can thus block attacks in real time. It is also a step beyond firewall technology.

Firewalls have a largely static configuration: security administrators define acceptable traffic and use the features of the firewall to enforce those policies.

Most observers believe that effective intrusion prevention depends on solid integration with intrusion detection and other perimeter security tools (such as firewalls). While IPS technology is still relatively new, it is gaining currency among a growing number of security professionals as the best way to protect assets even before software vendors issue patches for known security holes. It is also seen as an intelligent way to prepare for—and defend—against denial-of-service (DoS) attacks.

A properly integrated IPS solution can play a major role in dealing with malicious traffic that gets past the corporate firewall.

Bridging the Technical/Management Gap

The real payoff to security professionals comes when VM and IPS initiatives are integrated and automated. In order to identify mission-critical devices, organizations need to prioritize applications and assets. They also need to identify all assets that are highly vulnerable.
Automated solutions are available to prioritize assets and to identify the extent and severity of vulnerabilities for network devices. Based on standard and customized rules, these solutions are able to prioritize assets by distinguishing between servers and desktop machines, between local and network-wide applications.

For example, the solution would rank a device running a bank of Web servers higher than a single-user, desktop device.

When working with IPS solutions, VM systems are able to dynamically react and respond to information about potential network threats and automatically update the capabilities of the IPS. The more remediation performed automatically by the IPS, then the less human/manual intervention is required. This allows scarce human and technical resources to be devoted to legitimate exception management activities.

Establishing linkages between VM systems that identify which systems must be protected first and best, combined with a IPS strategy that is calibrated to enforce dynamic policies in different parts of the network in different (but appropriate) ways, can significantly enhance the security posture of the enterprise while reducing the amount of human and technical resources that must be expended.

**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.

**About the Sponsors**

In the summer of 2004 IPS leader McAfee, Inc. acquired Foundstone, Inc., a pioneer in the development of security risk management solutions. In so doing, McAfee is making an integrated set of security offerings available to the broad information technology community that will enable managers to develop a comprehensive, integrated, and strategic approach to improving their security posture.

According to industry research firm IDC, the vulnerability assessment and management (VA&M) and intrusion detection market is expected to experience increasing growth over the next few years, reaching $1.6 billion by 2008. The most significant growth is expected during the next three years, a period over which analysts expect the proactive characteristics of IPS to play an increasingly important role in enterprise security investments.

In its April 2004 report, *Worldwide Security Software 2004–2008 Forecast*, IDC identified Foundstone as a leader who is advancing the concepts of risk management, policy compliance, and other trends. Foundstone was also noted as one of the fastest growing VA&M solution providers at 100-percent-plus growth per year.

Foundstone has developed an enterprise risk solution (ERS) that is designed to help FORTUNE 1000 companies discover, inventory, and prioritize global network assets. The suite of offerings included in ERS provide organizations implementing SRM strategies with an integrated set of technologies that identify vulnerabilities and threats to mission-critical assets, providing continuous and proactive protection and intelligent, measurable remediation.

Foundstone’s risk assessment and management solutions activate continuous protection of the right assets, from the right threats, with the right measures. The optimal balance of software, people, and processes are put in place to support rapid change while maintaining business and IT stability. Solutions are supported through open standards, best practices, and continuous improvement.

McAfee, meanwhile, continues to create computer security solutions that prevent intrusions on networks and protect computer systems from the next generation of blended attacks and threats.
In a recent IDC report on worldwide intrusion detection and prevention, the research analyst firm declared that “McAfee is the largest intrusion prevention appliance vendor” for 2003.

Gartner placed McAfee in the leader quadrant of its most recent Magic Quadrant for Intrusion Detection Systems, 2H03 published in April 2004. According to the report, McAfee was listed in the leaders quadrant in the IDS Magic Quadrant. The report stated that emerging technologies such as intrusion prevention systems are enhancing network security by enabling enterprises to block attacks to protect their networks and IT resources. Firewalls, vulnerability management, and IPS solutions counter threats posed by worms, increased hacking activity, and malicious enterprise insiders.

Infonetics Research recently again named McAfee IntruShield® the worldwide, inline, network intrusion prevention revenue market-share leader for the third consecutive quarter. According to data published in an Infonetics Research report titled Intrusion Detection and Prevention Products Quarterly Worldwide Market Share & Forecasts, IntruShield leads the market with the highest market share in the second quarter of 2004.

IntruShield also won the 2004 Frost & Sullivan Technology Leadership Award for IDS/IPS. The Frost & Sullivan award is bestowed each year upon the company demonstrating excellence in technology leadership within its industry. Frost & Sullivan evaluated and scored several companies and McAfee beat competitors based on the company’s ability to clearly demonstrate its excellence in technology development, from initial concepts and new product innovation to continuous refinement and improvement.

*NOTE: The Magic Quadrant is copyrighted April 13, 2004, by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period.

McAfee and Foundstone
The combination of Foundstone’s vulnerability management and McAfee’s intrusion prevention and Secure Content Management™ solutions together provide the most comprehensive portfolio of proactive risk management and mitigation solutions available to protect IT infrastructures. For more information about Foundstone products and services from McAfee, please visit us at www.foundstone.com or www.mcafee.com.

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, FoundStone, Protection-in-Depth, IntruShield, Secure Content Management, 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. © 2005 McAfee, Inc. All Rights Reserved.