

By John Vecchi

# SECURING VIRTUALIZED ENVIRONMENTS WITH McAfee INTRUSHIELD

Virtualization technology can offer significant advantages in enterprise data centers, but can also carry its own specific security risks. McAfee® IntruShield® network security and intrusion prevention system appliances are designed to provide comprehensive defenses against a wide array of external and internal threats in virtualized environments.

**V**irtualization technology has become a key tool in enterprise data centers. By enabling administrators to run multiple virtual machines (VMs) on a single physical server, it can offer tremendous advantages for both data centers and the overall enterprise, including simplified management, efficient utilization of hardware resources, and the flexibility to support specialized requirements for testing, support, and specialty applications.

As the use of virtualization technology increases, so does the need for comprehensive security strategies to help protect virtualized environments. Tools such as McAfee IntruShield network security and intrusion prevention system (IPS) appliances can help enterprises secure both the data center as a whole and virtualized environments in particular against a wide array of external and internal threats.

## UNDERSTANDING SECURITY IN VIRTUALIZED ENVIRONMENTS

Along with the significant advantages of virtualized environments come multiple security risks and challenges. All too often, however, security has been an afterthought for early adopters of virtualization technology. Best practices recommend implementing a formal security and information protection strategy that addresses the specific needs of virtualized environments.

Virtualized and non-virtualized environments share many of the same security challenges, but some are specific to virtualization (see Figure 1). Traditional computing platform threat vectors—including malware, worms, spyware, Trojan horses, and other attacks targeting software vulnerabilities—are still a concern, and the risk of propagating infections increases even further when enterprises do not take measures to help ensure the integrity of VMs. Setting up more than half a dozen VMs on a single physical server is like setting up a new data center, and as with any data center, its assets need protection.

One of the greatest vulnerabilities in a virtualized environment is the hypervisor, the platform that enables VMs with different operating systems to run on the physical system. It offers a single point of attack and can be vulnerable to *hyperjacking* attacks designed to take control of all VMs under its management. In addition, virtualized environments are typically more transient than non-virtualized environments. For example, servers may be programmed to go online and offline at unscheduled times for various reasons, such as load balancing. Those servers are potentially vulnerable to denial-of-service (DoS) attacks or other attacks (since they may have been offline during the latest patch update) that can cripple entire virtualized server farms.

### Related Categories:

McAfee

Security

Virtualization

Visit [DELL.COM/PowerSolutions](http://DELL.COM/PowerSolutions) for the complete category index.

## PROTECTING VIRTUALIZED ENVIRONMENTS WITH MCAFEE INTRUSHIELD

To help lock down a virtualized environment, it is critical to have a comprehensive approach to security—on the server, on the desktop, and on the network. McAfee offers security and compliance solutions for both virtualized and non-virtualized environments that are scalable, centrally managed, and comprehensive, spanning all three data center elements.

McAfee IntruShield network security platforms are IPS appliances designed for the first line of defense in virtualized environments—the network layer. These multidimensional, multi-vector appliances offer integrated protection through an easy-to-use, application-specific integrated circuit (ASIC)-based platform designed to provide broad physical and virtual asset protection, maximized business availability, and reduced security costs.

The IntruShield architecture integrates patented signature, behavioral anomaly, and DoS detection on a single virtualized appliance (see Figure 2). Its built-in IPS technology is designed to provide proactive, highly accurate protection against a wide range of network threats and attacks, including zero-day attacks, cyber attacks, and malware; spyware, phishing, and other unwanted programs; DoS, distributed DoS (DDoS), and SYN flood attacks; encrypted attacks, worms, Trojan horses, and evasions; instant messaging and peer-to-peer applications; voice over IP (VoIP) threats and vulnerabilities; and

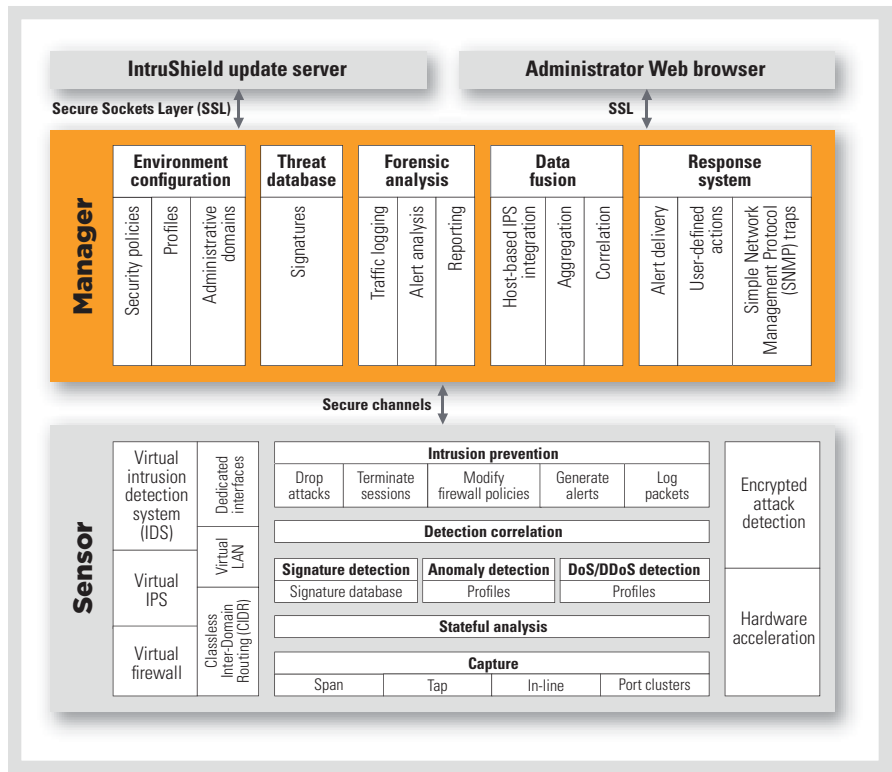


Figure 2. McAfee IntruShield architecture

threats and vulnerabilities specific to VMware® virtualized environments.

The IntruShield network security platform also consolidates additional security features in a single integrated console, including a virtual IPS, a virtual internal firewall, built-in physical and virtual host quarantine, and protocol-based dynamic rate limiting. And, to further increase detection and prevention accuracy, the IntruShield architecture employs a combination of threshold-based and patented self-learning, profile-based detection techniques.

For more information on how IntruShield security features can help defend against a variety of attacks, see the “McAfee IntruShield combats external and internal threats” sidebar in this article.

### DEPLOYING MULTIFACETED ENTERPRISE SECURITY

Comprehensive network security for virtualized environments requires implementing multiple components while maintaining network performance and flexibility. These components include protection for virtualized and non-virtualized resources and dynamic network devices, proactive protection for un-patched VMs, isolation of infected hosts, management of and limits on traffic and bandwidth, discovery of active hosts, and simple deployment and use.

The high-performance McAfee IntruShield network security platform treats virtualized environments holistically as part of the network infrastructure, just like other physical devices. It is designed to protect these environments

Vulnerabilities common to virtualized and non-virtualized environments	Vulnerabilities specific to virtualized environments
<ul style="list-style-type: none"> <li>Unsecured accounts, such as those with no password or no password expiration</li> <li>Unnecessary services</li> <li>Backdoors such as those created by malware, worms, spyware, Trojan horses, and other attacks</li> <li>Mis-configured Network BIOS shares or FTP servers</li> <li>Un-patched software allowing attacks such as buffer overruns and SQL injection</li> </ul>	<ul style="list-style-type: none"> <li>Offline, noncompliant, or under-protected VMs</li> <li>Vulnerabilities in the virtualization platform or hypervisor</li> <li>Propagation and activation of infected virtualized images</li> <li>Hyperjacking, in which a single attack can provide simultaneous access to multiple VMs and hypervisor rootkits</li> </ul>

Figure 1. Potential security vulnerabilities in both virtualized and non-virtualized environments

## McAfee IntruShield Combats External and Internal Threats

McAfee IntruShield is designed to provide comprehensive protection against multiple types of attacks on network security in virtualized environments, including both external and internal threats.

For example, a rogue access point or laptop, when given network access, could allow hackers to access a virtual machine (VM) on the network, launch attacks, steal sensitive data, or gain other unauthorized access. McAfee IntruShield and McAfee Network Access Control solutions work together to help prevent the rogue access point and hackers from penetrating the VM. IntruShield uses “black-hole” filtering to block the attacker’s traffic before it reaches the intended recipients, log the packets for later analysis, and alert administrators that intruders are attempting to breach the system.

In terms of internal threats, IntruShield could also help prevent a disgruntled employee from breaking into virtualized servers to steal credit card records, intending to sell the data or embarrass the company. IntruShield separates the network into virtual local networks and enforces firewall functionality using access control lists, which restrict internal user traffic to authorized subnets or to individual IP addresses. If an employee attempts to maliciously subvert network security measures, IntruShield can block the attacks before they reach sensitive systems. Once it has detected the attacks, IntruShield can automatically quarantine the malicious system and quickly alert administrators.

by addressing four primary aspects of security risk management (SRM): management, containment, threat prevention, and compliance and control (see Figure 3).

### Management

IntruShield was designed to support the dynamic, flexible nature of virtualized environments in which administrators can launch, move, and remove virtual systems without physically reconfiguring or rearranging hardware. The IntruShield built-in virtual IPS capability—which supports up to 1,000 virtual systems on a single appliance—integrates seamlessly with virtualized environments, enabling administrators to make network changes without physically unplugging and plugging in LAN cables. IntruShield also helps protect network segments as new VMs are brought online on different physical platforms, and can proactively apply and manage VM patches the same way it does physical devices. While administrators create, test, and install patches, IntruShield helps protect vulnerable VMs with an in-line IPS.

The IntruShield virtual IPS functionality also allows administrators to easily create custom IPS and firewall security policies

for virtualized environments. By adjusting different parameters, they can match security policies to specific VMs. In addition, close integration with McAfee ePolicy Orchestrator® software provides administrators with comprehensive system visibility for intelligent, centralized management and priority-based decision making.

### Containment

When IntruShield detects that VMs or physical servers have become infected, violated security policies, or could propagate threats to other network devices, it can quickly quarantine those systems to help prevent further damage. IntruShield

isolates quarantined systems from the rest of the network infrastructure and notifies administrators so that they can resolve the problem, restore the systems, and bring them back online as quickly as possible.

### Threat prevention

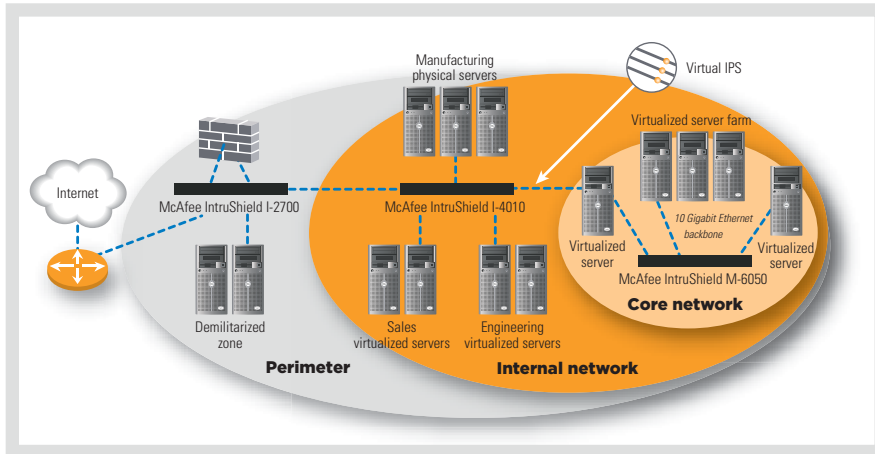
By helping block unwanted traffic at the network source—before it enters the virtualized environment—IntruShield can effectively secure both VMs and physical servers from attacks. When strategically placed in-line at different points on the network, it helps safeguard the entire virtualized data center (see Figure 4).

IntruShield is preconfigured with a recommended policy designed to provide accurate, proactive blocking for hundreds of attacks. It can also boost threat protection for virtualized environments by providing multiple vulnerability-based signatures for specific protection against potential exploits in the VMware virtualization platform. McAfee Avert® Labs continually adds to these signature sets as new vulnerabilities or threats arise to help comprehensively protect virtualized environments from the latest known and unknown exploits. And the IntruShield behavioral anomaly learning engine—which scans and remembers typical VM behaviors—helps detect unusual behavior so that IntruShield can quickly alert administrators to potential security problems.

The dynamic nature of virtualized environments, which allows administrators to quickly deploy new VMs, is one of their key advantages, but it also brings potential risk.

Security aspect	Advantages
Management	<ul style="list-style-type: none"> <li>Increased flexibility with minimal physical network changes</li> <li>Customized security policies to meet specific VM requirements</li> </ul>
Containment	<ul style="list-style-type: none"> <li>Containment of infected VMs</li> <li>Blocking of outbound malicious traffic</li> </ul>
Threat prevention	<ul style="list-style-type: none"> <li>Comprehensive security for virtualized and non-virtualized environments</li> <li>Integration with McAfee Foundstone, ePolicy Orchestrator, and Remediation Manager software for simplified threat detection and remediation</li> <li>Default blocking and vulnerability protection for VMware virtualization platforms</li> </ul>
Compliance and control	<ul style="list-style-type: none"> <li>Pervasive security for active and inactive hosts</li> <li>Compliance and governance rule sets, including network isolation</li> </ul>

Figure 3. Key aspects of McAfee IntruShield security for virtualized environments



**Figure 4.** Strategic placement of McAfee IntruShield appliances to help safeguard the entire virtualized data center

New VMs could be vulnerable to certain attacks that administrators may not be aware of. IntruShield integration with the McAfee Foundstone® vulnerability management solution enables administrators to launch real-time scans of both VMs and physical servers to help determine the potential level of vulnerability, after which the system vulnerability status is updated in the Foundstone risk database.

If a system was offline the last time a vulnerability scan took place, however, the Foundstone database may be out-of-date. In this case, if the system begins to propagate infected or malicious traffic once it is back online, IntruShield can detect this traffic, initiate a block and/or quarantine, and alert administrators to the problem. Administrators can then quickly launch a real-time Foundstone scan on the system. After the scan is completed and potential vulnerabilities have been discovered and presented in the IntruShield console, the system profile is updated in the Foundstone database. Administrators can then apply the appropriate patches to help fix the vulnerability. The closed-loop process provided by McAfee SRM integration also enables them to automatically initiate help-desk remediation tickets through McAfee ePolicy Orchestrator and McAfee Remediation Manager. In the meantime, IntruShield visibility and proactive network protection capabilities help reduce the urgency of needing to deploy system patches immediately.

### Compliance and control

IntruShield provides comprehensive network and system security visibility and control. Administrators can discover and see all active hosts on the network regardless of uncontrolled usage. For example, if an enterprise has a common operating environment deployed as its standard policy, administrators can monitor new VMs to help ensure that they comply with that policy, detect and protect traffic coming from the noncompliant VM, and contain and quarantine the noncompliant VM to help protect the rest of the systems on the network.

IntruShield also includes *rate limiting*, a key security and efficiency control that helps prevent low-priority VM network traffic from saturating host resources. Rate limiting helps ensure that each VM residing on a particular host has sufficient resources to continue operating at a high performance level. Granular, dynamic rate-limiting capabilities allow administrators to easily manage bandwidth by application, protocol type, or port allocation.

Also helpful to compliance and control is the IntruShield virtual internal firewall. This firewall extends the virtual IPS architecture to the internal firewall, enabling administrators to internally deploy Layer 3 and Layer 4 access control lists (ACLs) in a granular, virtual way. As such, this feature enables them to easily enforce different virtual firewall policies for a range

of IP addresses on a port, right down to individual hosts. By applying ACL rules that restrict access to certain resources from specific parts of the corporate network, administrators can also use IntruShield to enforce a generic security policy for internal compliance.

To help truly secure virtualized environments, network isolation is a necessity. The ability to isolate a virtualized environment from the network or other systems is a primary purpose of a network IPS such as IntruShield. In fact, network isolation is a key component to many compliance rule sets as well, such as payment card industry regulations. And as an in-line security device, IntruShield can help organizations meet a host of governance policies.

### CREATING SECURE VIRTUALIZED ENVIRONMENTS

As organizations embrace the advances of virtualization, implementing security strategies for this technology becomes increasingly important. McAfee IntruShield network security and IPS appliances can provide comprehensive protection to help both defend the data center as a whole and meet the specific security challenges of virtualized environments. 

**John Vecchi** is the director of product marketing for network security solutions at McAfee, responsible for product marketing activities for the McAfee portfolio of network security solutions, including the award-winning IntruShield network IPS product line. He has a B.A. in International Business from the University of St. Thomas.

**MORE**

**ONLINE**

[DELL.COM/PowerSolutions](http://DELL.COM/PowerSolutions)

---

**QUICK LINK**

**McAfee IntruShield:**  
[www.mcafee.com/intrushield](http://www.mcafee.com/intrushield)