Helps customers to be more cost-effective, compliant and secure by delivering integrated and optimized security for virtual data centers

IBM Virtual Server Security for VMware

Highlights

- ***Enforces dynamic security wherever virtual machines (VMs) are deployed***
- ***Provides multilayered intrusion prevention and firewall***
- ***Increases virtual server uptime and availability with virtual rootkit detection***
- ***Helps to accelerate and simplify your Payment Card Industry Data Security Standard (PCI DSS) audit, and achieve compliance with security and reporting functionality customized for the virtual infrastructure***
- ***Helps reduce cost and complexity over using physical security solutions in virtual infrastructures with automatic protection features***

Virtualization offers significant benefits to the IT organization, but many existing security solutions are not optimized to work in the virtual environment and may leave organizations at risk of not meeting compliance mandates. Instead of complementing the virtual infrastructure, some security agents drain resources and add management overhead.

IBM Virtual Server Security for VMware® offers integrated threat protection for VMware vSphere™ 4 that provides protection for every layer of the virtual infrastructure, including host, network, hypervisor, virtual machine (VM) and traffic between VMs. The solution leverages VMware VMsafe™ integration to offer protection that is scalable, isolated, centralized, visible and efficient.

Transparent intrusion prevention and firewall

IBM Virtual Server Security for VMware provides multilayered IPS and firewall technology to protect the virtual data center in a solution that is purpose-built to protect the virtual environment at the core of the infrastructure.

Automatic discovery

Virtual servers operate in a dynamic state which can render traditional security technology ineffective. With IBM Virtual Server Security for VMware, the security virtual machine can perform automatic discovery of all VMs. This helps increase security awareness and visibility across the virtual environment.

VM rootkit detection

Virtualization-based rootkits are particularly worrying because they can cause the hypervisor to become malware, and can conceal themselves from traditional security tools. IBM Virtual Server Security for VMware transparently inspects VMs to detect installation of rootkits.

Inter-VM Traffic Analysis

While traditional host and network intrusion prevention systems do not have visibility into traffic between VMs, IBM Virtual Server Security for VMware monitors traffic between virtual servers to stop threats before impact.

Virtual network access control

IBM Virtual Server Security for VMware performs virtual network access control to quarantine or limit network access from a virtual server until VM security posture has been confirmed.

Virtual infrastructure auditing

IBM Virtual Server Security for VMware reports on privileged user activity such as VMotion events, VM state changes (start, stop, pause) and login activity which can reduce the preparation time required to support audits.

IBM Virtual Patch technology

Automatically protects vulnerabilities on virtual servers regardless of patch strategy.

Harnessing the power of enterprise security control

While virtualization continues to expand, organizations are still taking a hybrid approach to IT, and physical server boxes and network connections will continue to exist and require protection. IBM encourages clients to take a defense-in-depth approach to enterprise security. The IBM Virtual Server Security for VMware solution provides defense-in-depth for the virtual infrastructure, but it is also one layer of a larger enterprise security strategy. With IBM, clients can benefit from world class security technology designed to protect every layer of the IT environment. With network, host, endpoint, application and virtual security all built on the same core technology, enterprises gain even greater security visibility and control from an efficient, scalable platform.

The IBM Proventia® Management SiteProtector™ system offers a simpler, cost-effective way to manage security solutions and ease regulatory compliance by providing a central management point to control security policy, analysis, alerting and reporting for your business and is supported on VMware ESX. Designed for simplicity and flexibility, the SiteProtector system can provide centralized configuration, management, analysis and reporting for the full IBM Internet Security Systems™ (ISS) Proventia product family, along with IBM Virtual Server Security for VMware.

Features and Benefits

Enforces dynamic security wherever VMs are deployed

- *Provides multilayered intrusion prevention and firewall to offer defense-in-depth, visible security*
- *Enforces automatic VM discovery in order to reduce VM sprawl*
- *Provides VM rootkit detection and virtual infrastructure auditing*
- *Offers inter-VM traffic analysis*

Helps to accelerate and simplify your PCI DSS audit, and achieve compliance with security and reporting functionality customized for the virtual infrastructure

- *Quarantines or limits network access until VM security posture can be validated*
- *Offers dashboard visibility into the virtual host OS and the virtual network to identify vulnerabilities*
- *Enables network-level workload isolation*

Helps reduce cost and complexity over using physical security solutions in virtual infrastructures with automatic protection features

- *Reduces system administrator workload with automatic protection, discovery and assessment features*
- *Leverages IBM Virtual Patch® technology to automatically protect vulnerabilities on virtual servers regardless of patch strategy*

Gaining efficiency with the IBM Proventia Management SiteProtector system

IBM Proventia Management SiteProtector system offers a simpler, cost-effective way to manage security solutions and ease regulatory compliance by providing a central management point to control security policy, analysis, alerting and reporting for your business and is supported on VMware ESX. Designed for simplicity and flexibility, the SiteProtector system can provide centralized configuration, management, analysis and reporting for the full IBM ISS Proventia product family, along with IBM Virtual Server Security for VMware.

Improving virtual security with IBM Internet Security Systems X-Force research

IBM ISS security excellence is driven by the world-renowned X-Force® team. The X-Force team's primary security intelligence is infused into IBM security solutions. Whether a physical 1U appliance or a piece of software installed on a virtual machine, IBM solutions are backed by the same security intelligence and threat content, developed by the X-Force team. The X-Force team is one of the of the oldest and best-known commercial security research groups in the world. This leading group of security experts researches and evaluates vulnerabilities and security issues, develops assessment and countermeasure technology for IBM Internet Security Systems products, and educates the public about emerging Internet threats. In addition to providing security content updates to IBM ISS products, the X-Force team also provides the IBM Internet Security Systems X-Force Threat Analysis Service (XFTAS). The XFTAS delivers customized information about a wide array of threats that could affect your network through detailed analysis of global threat conditions.

Why IBM?

IBM Virtual Server Security for VMware was purpose-built to protect the virtual data center at the core of the infrastructure—without decreasing system efficiency or performance. Along with superior protection, IBM Virtual Server Security for VMware helps clients meet regulatory compliance standards by limiting access to critical data housed on virtual machines and tracking user access. IBM offers a complete security portfolio—including leading protection technologies for the physical server environment, endpoints, the network core, applications and more. With IBM, virtual security can be managed centrally alongside existing IT security technology, so clients can realize greater efficiency and scalability. IBM brings comprehensive, end-to-end security to virtualization, enabling you to more quickly realize the benefits of virtualization technology.

Requirements

Platform	X86 servers with VMware vSphere 4

For more information

To learn more about IBM Virtual Server Security for VMware, please contact your IBM representative or IBM Business Partner, or visit the following Web site:

ibm.com/services/security

IBM Global Services
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
November 2009

SED03097-USEN-00