IBM Security Virtual Server Protection for VMware

Be more cost-effective, compliant and secure with optimized security for virtual data centers

Highlights

- Ensures that security policy remains persistent even as virtual machines migrate from one ESX server to another
- Provides intrusion prevention and firewall without the need for a host-based agent
- Identifies rootkit activity within the guest operating system
- Helps control virtual server sprawl and mitigates risk introduced by unauthorized virtual machines
- Monitors and reports on virtual infrastructure activity helping to address compliance requirements
- Helps reduce cost and complexity with automatic protection features for virtual infrastructure

Virtualization offers significant benefits to the IT organization, but existing security solutions are not optimized to work in the virtual environment. Traditional security processes and technologies cannot effectively protect the additional layers, including the hypervisor, management stack and virtual network. As a result, virtualized servers may be less secure than the physical servers they replace, leaving organizations at risk of not meeting compliance mandates. Organizations should approach virtualization with an awareness of these new potential risks and apply needed security controls. IBM Security Virtual Server Protection for VMware® is an integrated threat mitigation solution designed to allow organizations to fully exploit the benefits of server virtualization while protecting critical virtualized assets.

Firewall

IBM Security Virtual Server Protection for VMware provides firewall technology to allow for virtual network segmentation and prevent unauthorized communication between trust zones.

Transparent Intrusion Prevention

Virtual machines (VMs) can be rapidly configured and deployed, resulting in a highly dynamic environment. IBM's market-leading intrusion prevention technology automatically protects virtual machines as they come online or move across the data center.

Automatic discovery

Virtual networks can also introduce visibility gaps that render traditional discovery tools and processes ineffective. IBM Security Virtual Server Protection for VMware can perform automatic discovery of new virtual machines. This helps increase security awareness and visibility across the virtual environment.

VM rootkit detection

IBM Security Virtual Server Protection for VMware transparently inspects VMs to detect installation of rootkits. This feature complements traditional antimalware by identifying rootkits while being immune to common techniques used by rootkits to disable host-based agents.

Inter-VM Traffic Analysis

Network traffic between VMs within the same physical server does not exit the machine, which can create a blind spot that is of special concern between VMs of varying trust levels. While traditional host and network intrusion prevention systems do not have visibility into traffic between VMs, IBM Security Virtual Server Protection for VMware monitors traffic between virtual servers to stop threats before they impact your environment.

Virtual network access control

VMs can be quickly introduced into the data center with little oversight, and as a result, security exposures can be introduced. IBM Security Virtual Server Protection for VMware performs virtual network access control to quarantine or limit network access from a virtual server until the VM security posture has been confirmed.

Virtual infrastructure auditing

IBM Security Virtual Server Protection 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

IBM Virtual Patch® technology shields vulnerabilities in operating systems or applications while allowing organizations to engage in predictable patching cycles. This can help automatically protect organizations against vulnerabilities on virtual servers regardless of their 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 servers 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 Security Virtual Server Protection 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, organizations gain even greater security visibility and control from an efficient, scalable solution.

Features and Benefits

Enforces dynamic security wherever VMs are deployed:

- Provides agentless intrusion prevention and firewall for defense-in-depth security
- Enables network-level workload isolation
- Automatically discovers VMs not seen by traditional discovery tools
- Transparently identifies rootkit activity within the virtual machines
- Quarantines potentially unsafe VMs until their security posture can be validated
- Monitors virtual infrastructure activity

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:

- Offers virtual network segmentation to separate virtual servers that are within the PCI scope
- Automated protection ensures security controls remain in place even in the most dynamic environments

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 Security SiteProtector System

IBM Security 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 organization and is supported on VMware ESX. Designed for simplicity and flexibility, the SiteProtector System can provide centralized configuration, management, analysis and reporting.

Improving virtual security with IBM X-Force research

IBM 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 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 security products, and educates the public about emerging Internet threats. In addition to providing security content updates to IBM security products, the X-Force team also provides the IBM 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 Security Virtual Server Protection 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 Security Virtual Server Protection 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 comprehensive 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 Security Virtual Server Protection for VMware, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/tivoli/security

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

Produced in the United States of America
October 2010

WGD03008-USEN-00