

TREND MICRO

COST-EFFECTIVE VIRTUALIZATION SECURITY

Virtualization can help your organization achieve significant datacenter operations savings—you can reduce hardware costs and energy demands and achieve greater flexibility in deploying mission-critical software applications. Organizations have leveraged consolidation to attain deployment of 10 or more virtual machines (VMs) for each physical server in their IT infrastructure—your business can utilize this technology for similar results.

The greatest challenge your IT personnel might face in virtualization is applying security mechanisms that enable you to fully utilize your virtualization investment. This includes enabling you to host virtual machines with different security levels on the same physical server, providing continuous protection while using mechanisms such as vMotion, protecting virtual machines when dormant or offline, and enabling you to extend your virtualization environment to take advantage of cloud computing. Trend Micro offers solutions to ensure that you can fully and safely utilize your virtualization environment.

Enhanced Virtualization Security

Trend Micro™ Virtualization Security solutions deliver advanced security software to protect operating systems, applications and data on virtual and cloud servers to help ensure compliance, while allowing higher server consolidation rates, and maximizing performance and operational flexibility.

With Trend Micro software deployed on your physical servers and virtual machines, your IT infrastructure receives comprehensive, integrated protection, which includes:

- Firewall
- Intrusion detection and prevention (IDS/IPS)
- Web application protection
- Application control
- Integrity monitoring
- Log inspection
- Malware protection

The solution helps ensure compliance with industry regulations and standards such as the PCI Data Security Standard, HIPAA, breach notification laws, and corporate policies.

Solution Components

The combined Virtualization Security solution is comprised of two products, Trend Micro™ Deep Security and Trend Micro™ Core Protection for Virtual Machines that help stop attacks before they impact critical data, applications, and resources.

Deep Security provides server and application protection that enables virtual machines to become self-defending. Core Protection for Virtual Machines is virtualization-aware antimalware solution that leverages the VMware VMsafe™ APIs to secure both active and dormant virtual machines.

- **Deep Security Manager**—a powerful, centralized management system that enables administrators to create security profiles and apply them to servers. With a centralized console for monitoring alerts and preventive actions taken in response to threats, it can be configured to automate or distribute security updates to servers on demand. It also enables you to generate reports for superior visibility and compliance.
- **Deep Security Agent**—a small software component deployed on virtual machines being protected, to enforce your security policies and enable integrity monitoring and log inspection capabilities. It defends virtual machines by monitoring incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations. When necessary, it intervenes to neutralize the threat by blocking malicious traffic.
- **Security Center**—a dedicated team of security experts that helps keep your company ahead of the latest threats by rapidly developing and delivering security updates to address newly discovered vulnerabilities and minimize risk. It also manages the customer portal used to access these security updates and information. Security updates can be delivered to Deep Security Manager, automatically or on-demand, and deployed within minutes to thousands of servers.
- **Core Protection for Virtual Machines** provides dedicated scanning virtual machines coordinated with real-time agents within each virtual machine to protect against malware that attempt to escape detection by uninstalling, inhibiting, or fraudulently patching antivirus security



TREND MICRO

COST-EFFECTIVE VIRTUALIZATION SECURITY

Server Defense for Virtual Machines

Deep Security brings a wide range of features and benefits to your datacenter:

- **OS flexibility:** It provides targeted, software-based protection for the widest range of platforms used to run mission-critical applications and store sensitive data, including Microsoft Windows, Solaris, and Linux—whether they're running in physical environments or on a virtual platform such as VMware, Citrix, or Microsoft.
- **Virtual patching:** It helps stop attacks on software vulnerabilities commonly found in the operating systems and Web-based enterprise applications that organizations rely on. As a result, patches can be deployed more efficiently and regularly, with minimal impact on host or IT resources.
- **Attack detection and prevention:** Detects and prevents attacks targeting sensitive data, immediately alerting personnel of the attempt.
- **Coordinated security response:** The solution will coordinate the security response between the Deep Security Agent software on a threatened virtual machine and a Deep Security Virtual Appliance using VMsafe APIs that connect into the hypervisor, maximizing security efficiency and effectiveness.
- **Tight integration with VMware vCenter Server and ESX Server:** This close coordination enables organizational and operational information from vCenter and ESX nodes to be imported into Deep Security Manager, and detailed security to be applied to an enterprise's VMware infrastructure.
- **Centralized, Web-based management:** This streamlined approach enables IT personnel to create and manage security policies—and track threats and preventive actions taken in response to them—from a familiar, Explorer-style UI.
- **Proactive protection recommendations:** The solution proactively recommends appropriate protective measures for servers, based on policies and deployed applications, to more quickly and easily ensure that the correct steps are taken.
- **Template-based deployment:** The solution can be built into virtual templates to simplify deployment and easily increase security posture.

- **Automated deployment:** The solution ensures that standard security configurations are consistently and automatically applied to all appropriate systems, reducing risk.
- **Logging:** The solution automatically notifies IT personnel when an incident occurs, providing detailed log information on who attacked, when they attacked, and what they attempted to exploit.
- **Reporting:** The solution generates and issues a wide variety of detailed reports, on a scheduled or ad hoc basis, to document attempted attacks and provide an auditable history of security configurations and changes.
- **Automated updates:** The solution delivers regular security updates to protect newly discovered vulnerabilities from exploitation.

World-Class Malware Protection

Trend Micro™ Core Protection for Virtual Machines is specifically designed for VMware ESX/ESXi environments, and:

- Ensures that virtual machines are secure when dormant and ready to go with the latest pattern updates whenever activated.
- Protects against malware that attempt to escape detection by uninstalling, inhibiting, or fraudulently patching antivirus security.
- Provides an extra layer of immunity by running the scanning agent on a separate virtual machine than the machine being scanned.
- Continuously synchronizes with the VMware vCenter management console to stay on top of virtual machine dynamics and reduce the complexity of managing virtual environments.
- Automatically sets up new virtual machines for security scanning to better manage virtual machine sprawl.
- Optimizes performance-intensive full-system scans without any reconfiguration.
- Works seamlessly within Trend Micro OfficeScan™ Client-Server Suite deployments.

For more information please call **+1-877-21-TREND** or visit us at: www.trendmicro.com/virtualization