



Trend Micro™

Core Protection for Virtual Machines

Designed specifically to secure VMware environments

While server virtualization increases efficiency in the data center, it also challenges the security of the IT environment. Traditional security imported from the physical world cannot fully protect virtual environments which are particularly vulnerable when virtual machines are dormant or offline as they are unable to protect themselves with a virus scan agent and signature updates. Also, resource-intensive security operations such as scheduled full system scans can significantly degrade the performance of the host and render the security ineffective, especially when initiated concurrently on multiple virtual machines. To fully realize the cost and productivity advantages of virtualization, enterprises need content security that is architected specifically to secure today's highly virtualized datacenter.

Trend Micro™ Core Protection for Virtual Machines enables enterprises to maximize the economic benefits of virtualization without compromising the security of their datacenter. Specifically designed for VMware ESX/ESXi environments, this virtualization-aware solution leverages the VMsafe APIs from VMware to secure both active and dormant virtual machines. Layered protection uses dedicated scanning virtual machines coordinated with real-time agents within each virtual machine.

KEY FEATURES

Optimized for Virtualization

- Closes security gaps unique to virtualized environments
- Protects both active and dormant virtual machines with a virtualization-aware security architecture
- Improves performance profile of virtual servers by running resource-intensive operations such as full-system scans from a separate scanning virtual machine
- Protects against the risk of VM sprawl by ensuring new virtual machines are automatically set up for security scanning

World-Class Malware Protection

- 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

Simplified Management

- Integrates tightly with the VMware management infrastructure, reducing the complexity of managing security within virtual environments
- Continuously synchronizes with the VMware vCenter management console to stay on top of virtual machine dynamics
- Automatically sets up new virtual machines for security scanning to better manage virtual machine sprawl
- Manages scanning and pattern updates for dormant virtual machines without requiring them to be activated
- Optimizes performance-intensive full-system scans without any reconfiguration

VIRTUALIZATION SECURITY SOFTWARE

Protection Points

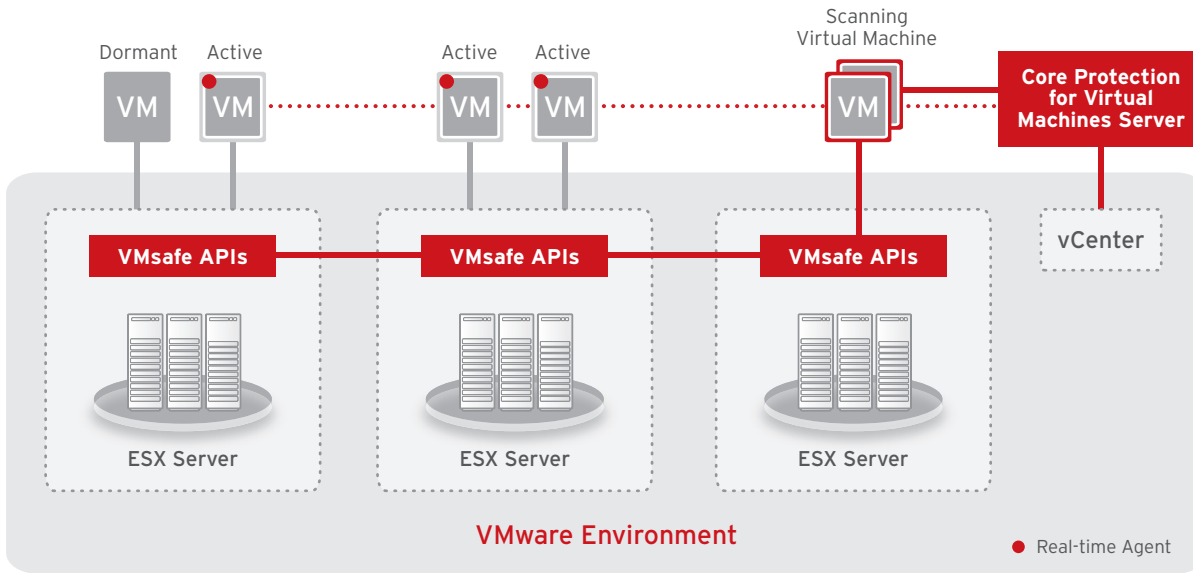
- Virtual Machines

Threat Protection

- Web Threats
- Viruses & Worms
- Trojans

KEY BENEFITS

- Secures virtual machines, whether active or dormant
- Optimizes performance for maximize uptime without compromising security
- Immunizes scan agent from disruptive malware activities
- Reduces the complexity of managing virtual environments



Trend Micro Core Protection for Virtual Machines secures virtual environments from next generation threats that target vulnerabilities specific to virtualization.

SYSTEM REQUIREMENTS	
Server	
Operating system	Microsoft™ Windows™ Server 2003 or 2003 R2 32-bit Enterprise Edition with Service Pack 1 or 2
Hardware	800MHz processor, 512MB RAM, 1GB disk space, Network Interface Card (NIC)
Web server	Microsoft Internet Information Server (IIS) on Windows Server 2003: version 6.0
Web console	300MHz processor, 128MB RAM, 30MB disk space, Microsoft Internet Explorer™ 6.0 or Microsoft Internet Explorer™ 7.0
Scanning Agent	
Operating system	Microsoft Windows XP Professional 32-bit Edition, Microsoft Windows Server 2003 or 2003 R2 32-bit Enterprise Edition
Hardware	300MHz processor, 256MB RAM (512MB for Update Agents), 200MB disk space (700MB for Update Agents), Network Interface Card (NIC)
Real-Time Agent	
Operating system	Microsoft Windows 2000 Server, Windows XP Professional 32-bit, Windows Server 2003 (or 2003 R2) 32-bit, Microsoft Windows Server 2003 (or 2003 R2) 64-bit, Windows Server 2008, Windows Vista Enterprise 32-bit, Windows Vista Business 64-bit
Virtual Machine Properties	1 CPU, 128MB RAM, 200MB disk space, Network Interface Card (NIC) VMware
Platform Support	
VMware	VMware VI3 (ESX 3.5, ESXi, vCenter 2.5), vSphere 4.0

Note: VMware vCenter is required in order for Core Protection for Virtual Machines to work.

COMPLEMENTARY PRODUCTS

Server Security

- Deep Security
- ServerProtect

Endpoint Security

- OfficeScan Client/Server Edition

Web Security Products

- InterScan™ Web Security Virtual Appliance

Messaging Security Products

- InterScan™ Messaging Security Virtual Appliance



©2009 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and TrendLabs are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [DS02CPVM_091016US]

www.trendmicro.com