

Trend Micro™

# Core Protection for Virtual Machines

Speziell für den Schutz von VMware-Umgebungen entwickelt

Die Servervirtualisierung erhöht zwar die Effizienz des Rechenzentrums, stellt die Sicherheit der IT-Umgebung aber gleichzeitig vor eine besondere Herausforderung. Herkömmliche, aus der physischen Welt übernommene Sicherheitsmaßnahmen können virtuelle Umgebungen nicht ausreichend schützen. Diese Umgebungen sind besonders anfällig, wenn virtuelle Maschinen inaktiv oder offline sind, da sie sich nicht mit einem Virensuch-Agent oder Signatur-Updates schützen können. Darüber hinaus können ressourcenintensive Sicherheitsvorgänge, wie z. B. vollständige, zeitgesteuerte Systemüberprüfungen, die Leistung des Hosts deutlich reduzieren und die Sicherheit außer Kraft setzen, besonders dann, wenn sie gleichzeitig auf mehreren virtuellen Maschinen gestartet werden. Um sämtliche Kosten- und Produktivitätsvorteile der Virtualisierung nutzen können, brauchen Unternehmen eine Content-Security-Lösung, die speziell für die heutigen, hoch virtualisierten Rechenzentren entwickelt wurde.

**Trend Micro™ Core Protection for Virtual Machines** gibt Unternehmen die Möglichkeit, den wirtschaftlichen Nutzen der Virtualisierung voll auszuschöpfen, ohne die Sicherheit des Rechenzentrums zu beeinträchtigen. Diese Sicherheitslösung auf Virtualisierungsebene wurde speziell für VMware ESX/ESXi-Umgebungen entwickelt. Zum Schutz aktiver als auch inaktiver, virtueller Maschinen nutzt sie die VMsafe-APIs von VMware. Der mehrschichtige Schutz kombiniert dedizierte Suche mit einem Echtzeit-Agent auf jeder virtuellen Maschine.

## DIE WICHTIGSTEN FUNKTIONEN

### Optimiert für die Virtualisierung

- Schließt Sicherheitslücken, die nur in virtuellen Umgebungen vorkommen
- Schützt sowohl aktive als auch inaktive, virtuelle Maschinen mit einer Sicherheitsarchitektur auf Virtualisierungsebene
- Verbessert das Leistungsprofil virtueller Server durch das Ausführen ressourcenintensiver Vorgänge, wie z. B. die vollständige Systemüberprüfung, durch eine separate virtuelle Maschine
- Schützt vor VM-Wildwuchs durch Sicherstellung, dass neue virtuelle Maschinen automatisch für die Sicherheitssuche konfiguriert werden

### Herausragender Malware-Schutz

- Gewährleistet die Sicherheit inaktiver virtueller Maschinen und die Installation aktueller Pattern-Dateien, sobald die Maschinen aktiviert werden
- Schützt vor Malware, die versucht der Entdeckung durch Deinstallieren, Sperren oder betrügerisches Patchen des Virenschutzes zu entgehen
- Bietet eine zusätzliche Schutzschicht, indem der Such-Agent auf der einen virtuellen Maschine, der Suchvorgang selbst aber auf einer anderen Maschine ausgeführt wird

### Vereinfachte Verwaltung

- Lässt sich eng in die VMware-Verwaltungsinfrastruktur integrieren und reduziert dadurch die Komplexität der Sicherheitsverwaltung in virtuellen Umgebungen
- Synchronisiert sich permanent mit der VMware vCenter Management-Konsole und bleibt dadurch immer auf dem neuesten Stand
- Konfiguriert automatisch neue virtuelle Maschinen für die Sicherheitsüberprüfung, um VM-Wildwuchs besser unter Kontrolle zu halten
- Verwaltet Suchläufe und Pattern-Updates für inaktive virtuelle Maschinen, ohne dass diese dafür aktiviert werden müssen
- Optimiert leistungsintensive vollständige Suchvorgänge ohne Neukonfiguration

### Einfache Installation

- Lässt sich nahtlos in die Trend Micro OfficeScan Installationen integrieren
- Ermöglicht die zentrale Verwaltung über die OfficeScan Konsole, die auch zur Verwaltung der Desktops und physischen Server eingesetzt wird
- Bietet die Flexibilität, OfficeScan lokal auf jeder virtuellen Maschine und Core Protection for Virtual Machines für remote durchgeführte, vollständige Systemüberprüfungen zu verwenden

## SICHERHEITSSOFTWARE FÜR VIRTUELLE UMGEBUNGEN

### Geschützte Punkte

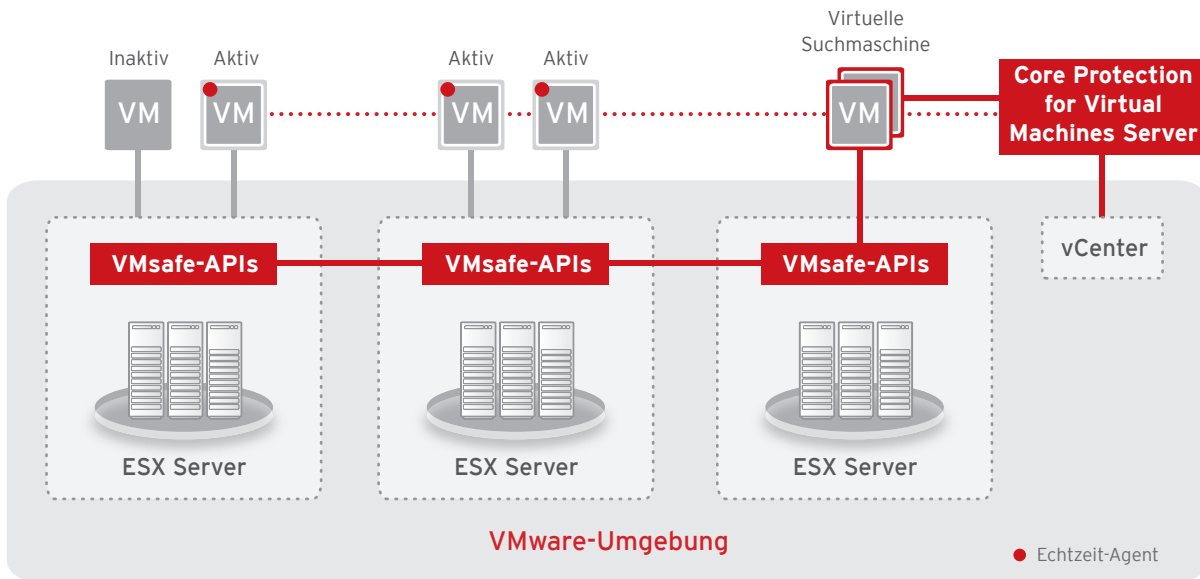
- Virtuelle Maschinen

### Bedrohungsschutz

- Internet-Bedrohungen
- Viren und Würmer
- Trojaner

## ENTSCHEIDENDE VORTEILE

- Schützt sowohl aktive als auch inaktive, virtuelle Maschinen
- Optimiert die Leistung bei maximaler Verfügbarkeit ohne Gefährdung der Sicherheit
- Immunisiert den Such-Agent gegen zerstörerische Malware-Aktivitäten
- Reduziert den Verwaltungsaufwand für virtuelle Umgebungen
- Integriert sich nahtlos in OfficeScan Installationen



Trend Micro Core Protection for Virtual Machines schützt virtuelle Umgebungen vor Bedrohungen der nächsten Generation, die auf Sicherheitslücken speziell in virtuellen Umgebungen abzielen.

SYSTEMVORAUSSETZUNGEN	
<b>Server</b>	
Betriebssystem	Microsoft™ Windows™ Server 2003 oder 2003 R2 Enterprise Edition (32 Bit) mit Service Pack 1 oder 2
Hardware	800 MHz Prozessor, 512 MB RAM, 1 GB Festplattenspeicher, Network Interface Card (NIC)
Webserver	Microsoft Internet Information Server (IIS) auf Windows Server 2003: Version 6.0
Webkonsole	300 MHz Prozessor, 128 MB RAM, 30 MB Festplattenspeicher, Microsoft Internet Explorer™ 6.0 oder Microsoft Internet Explorer™ 7.0
<b>Such-Agent</b>	
Betriebssystem	Microsoft Windows XP Professional Edition (32 Bit), Microsoft Windows Server 2003 oder 2003 R2 Enterprise Edition (32 Bit)
Hardware	300 MHz Prozessor, 256 MB RAM (512 MB für Update-Agents), 200 MB Festplattenspeicher (700 MB für Update-Agents), Network Interface Card (NIC)
<b>Echtzeit-Agent</b>	
Betriebssystem	Microsoft Windows 2000 Server, Windows XP Professional (32 Bit), Windows Server 2003 (oder 2003 R2) (32 Bit), Microsoft Windows Server 2003 (oder 2003 R2) (64 Bit), Windows Server 2008, Windows Vista Enterprise (32 Bit), Windows Vista Business (64 Bit)
Virtuelle Maschine	1 Prozessor, 128 MB RAM, 200 MB Festplattenspeicher, Network Interface Card (NIC) VMware
<b>Unterstützte Plattformen</b>	
VMware	VMware VI3 (ESX 3.5, ESXi, vCenter 2.5), vSphere 4.0

**Hinweis:** Für die Ausführung von Core Protection for Mirtual Machines ist VMware vCenter erforderlich.

**ERGÄNZENDE PRODUKTE**

**Serversicherheit**

- Deep Security
- ServerProtect

**Endpunktsicherheit**

- OfficeScan Client/Server Edition

**Produkte zur Internet-Sicherheit**

- InterScan™ Web Security Virtual Appliance

**Produkte zur Messaging-Sicherheit**

- InterScan™ Messaging Security Virtual Appliance



© 2009 by Trend Micro Incorporated. Alle Rechte vorbehalten.  
 Trend Micro, das Trend Micro T-Ball-Logo und TrendLabs sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen- und/oder Produktnamen sind Marken oder eingetragene Marken ihrer jeweiligen Eigentümer. Die Informationen in diesem Dokument können sich ohne vorherige Ankündigung ändern.  
 [DS01CPVM\_090622DE]  
[www.trendmicro.com](http://www.trendmicro.com)