

TREND MICRO

KOSTENEFFIZIENTE VIRTUALISIERUNGSSICHERHEIT

Durch Virtualisierung können Sie bedeutende Einsparungen beim Betrieb Ihrer Datenzentren erzielen. Senken Sie die Hardware-Kosten und den Energiebedarf Ihres Unternehmens, und profitieren Sie von größerer Flexibilität beim Einsatz systemkritischer Software. Einige Unternehmen haben die Konsolidierung bereits umgesetzt und für jeden physischen Server in ihrer IT-Infrastruktur zehn oder mehr virtuelle Maschinen (VM) verteilt. Auch Ihr Unternehmen kann mit dieser Technologie vergleichbare Erfolge erzielen.

Die größte Herausforderung, vor der Ihr IT-Personal bei der Virtualisierung stehen könnte, ist die Umsetzung von Sicherheitsmechanismen, mit denen Sie Ihre Investitionen in die Virtualisierung in vollem Umfang ausschöpfen können. Dazu gehört, dass Sie virtuelle Maschinen mit unterschiedlichen Sicherheitsebenen auf demselben physischen Server ausführen können, um permanenten Schutz zu gewährleisten. Gleichzeitig können Mechanismen wie vMotion inaktive oder nicht verbundene virtuelle Maschinen schützen, damit Sie Ihre Virtualisierungsumgebung erweitern und die Vorteile des Cloud-Computings nutzen können. Trend Micro bietet Lösungen, mit denen Sie Ihre Virtualisierungsumgebung uneingeschränkt und sicher verwenden können.

Erweiterte Virtualisierungssicherheit

Trend Micro™ Virtualization Security Lösungen liefern erweiterte Sicherheitssoftware zum Schutz Ihrer Betriebssysteme, Anwendungen und Daten auf virtuellen und webbasierten Servern. Dadurch können Richtlinien auch bei höheren Server-Konsolidierungsraten eingehalten sowie Leistung und betriebliche Flexibilität maximiert werden.

Durch die Verteilung von Trend Micro Software auf Ihre physischen Server und virtuellen Maschinen erhält Ihre IT-Infrastruktur umfassenden, integrierten Schutz, bestehend aus folgenden Komponenten:

- Firewall
- Erkennung und Abwehr von Eindringlingen (IDS/IPS)
- Schutz von Webanwendungen
- Anwendungssteuerung
- Integritätsüberwachung
- Protokollprüfung
- Schutz vor Malware

Die Lösung gewährleistet die Einhaltung behördlicher und brancheninterner Richtlinien und Bestimmungen, wie z. B. PCI Data Security Standard, HIPAA, Gesetze über die Meldung von Sicherheitsverletzungen und unternehmensweite Sicherheitsrichtlinien.

Komponenten der Sicherheitslösung

Die kombinierte Lösung besteht aus den beiden Produkten Trend Micro™ Deep Security and Trend Micro™ Core Protection for Virtual Machines, die den Angriff auf vertrauliche Daten, Anwendungen und Ressourcen verhindern.

Deep Security bietet Server- und Anwendungsschutz, mit dem sich virtuelle Maschinen selbst verteidigen können. Core Protection for Virtual Machines ist eine Anti-Malware-Lösung auf Virtualisierungsebene. Zum Schutz aktiver und inaktiver virtueller Maschinen nutzt sie die VMsafe™-APIs von VMware.

- **Deep Security Manager:** Ein leistungsstarkes, zentrales Verwaltungssystem, mit dem Administratoren Sicherheitsprofile erstellen und auf Server anwenden können. Mit einer zentralen Konsole zur Überwachung von Alarmen und vorbeugenden Maßnahmen als Reaktion auf Bedrohungen kann die Lösung so konfiguriert werden, dass Sicherheitsupdates automatisch oder bei Bedarf auf die Server verteilt werden. Die Berichtsfunktion gewährleistet außerdem hervorragende Transparenz und Regeleinhaltung.
- **Deep Security Agent:** Diese kleine Software-Komponente wird auf geschützte, virtuelle Maschinen verteilt. Sie setzt Ihre Sicherheitsrichtlinien durch und ermöglicht Integritätsüberwachung und Protokollprüfung. Sie verteidigt virtuelle Maschinen, indem sie den gesamten eingehenden und ausgehenden Verkehr auf Protokollabweichungen, Richtlinienverletzungen und Inhalte, die auf einen Angriff hindeuten, überwacht. Bei Bedarf greift sie ein und neutralisiert die Bedrohung, indem sie bösartigen Datenverkehr sperrt.
- **Security Center:** Ein dediziertes Team aus Sicherheitsexperten, das Ihrem Unternehmen dabei hilft, den neuesten Bedrohungen immer einen Schritt voraus zu sein. Dafür werden in kürzester Zeit Sicherheitsupdates entwickelt und bereitgestellt, die neu entdeckte Schwachstellen abwehren und Risiken minimieren. Außerdem verwaltet das Security Center das Kundenportal, auf dem diese Sicherheitsupdates und -informationen bereitgestellt werden. Sicherheitsupdates können automatisch oder bei Bedarf an den Deep Security Manager übertragen und innerhalb von Minuten auf Tausende von Servern verteilt werden.
- **Core Protection for Virtual Machines:** Bietet dedizierte Suche für virtuelle Maschinen durch einen Echtzeit-Agent innerhalb jeder virtuellen Maschine. Der Agent schützt vor Malware, die versucht, der Entdeckung durch Deinstallieren, Sperren oder betrügerisches Patchen des Virenschutzes zu entgehen.

TREND MICRO

KOSTENEFFIZIENTE VIRTUALISIERUNGSSICHERHEIT

Serverschutz für virtuelle Maschinen

Deep Security bietet eine Vielzahl von Funktionen und Vorteilen für Ihr Datenzentrum:

- Unterstützt verschiedene Betriebssysteme: Die Lösung bietet gezielten, Software-basierten Schutz für eine größtmögliche Vielfalt von Plattformen, wie Microsoft Windows, Solaris und Linux, auf denen systemkritische Anwendungen ausgeführt und vertrauliche Daten gespeichert werden. Dies gilt sowohl für physische Umgebungen als auch für virtuelle Plattformen, wie VMware, Citrix oder Microsoft.
- Virtuelle Patches: Deep Security stoppt Angriffe auf typische Schwachstellen in Betriebssystemen und webbasierten Enterprise-Anwendungen in Unternehmen. Dadurch können Patches effizienter und regelmäßiger bei minimaler Beeinträchtigung von Host- oder IT-Ressourcen verteilt werden.
- Erkennung und Abwehr von Angriffen: Entdeckt und verhindert Angriffe auf vertrauliche Daten und macht das IT-Personal sofort auf den Angriffsversuch aufmerksam.
- Koordinierte Reaktion auf Bedrohungen: Die Lösung koordiniert die Bedrohungsreaktion zwischen dem Deep Security Agent auf einer bedrohten virtuellen Maschine und einer Deep Security Virtual Appliance, die sich über VMsafe-APIs mit dem Hypervisor verbindet. Dadurch werden Effizienz und Wirksamkeit der Sicherheitslösung maximiert.
- Nahtlose Integration in VMware vCenter und ESX Server: Durch die enge Integration können Unternehmens- und Betriebsdaten von vCenter- und ESX-Knoten in den Deep Security Manager importiert, und detaillierte Sicherheit kann auf die VMware-Infrastruktur eines Unternehmens angewendet werden.
- Zentrale, webbasierte Verwaltung: Mit dieser umfassenden Lösung kann das IT-Personal auf einer vertrauten Benutzeroberfläche im Explorer-Stil Sicherheitsrichtlinien erstellen und verwalten sowie Bedrohungen entdecken und vorbeugende Maßnahmen dagegen ergreifen.
- Empfehlungen zum proaktiven Schutz: Gemäß den Richtlinien und verteilten Anwendungen empfiehlt die Lösung proaktiv angemessene Server-Schutzmaßnahmen, um schneller und einfacher auf Bedrohungen zu reagieren.
- Vorlagenbasierte Verteilung: Die Lösung kann in virtuelle Vorlagen integriert werden, um die Verteilung zu vereinfachen und den Sicherheitsstatus problemlos zu erhöhen.

- Automatische Verteilung: Die Lösung stellt sicher, dass standardmäßige Sicherheitskonfigurationen zur Reduzierung von Risiken konsistent und automatisch auf alle entsprechenden Systeme angewendet werden.
- Protokollierung: Bei einem Vorfall benachrichtigt die Lösung automatisch das IT-Personal und stellt detaillierte Protokolldaten über Angreifer, Angriffszeitpunkt und Angriffsziel bereit.
- Berichterstellung: Deep Security erstellt und veröffentlicht nach Zeitplan oder bei Bedarf eine große Vielzahl detaillierter Berichte, um Angriffsversuche zu dokumentieren und einen überprüfbareren Verlauf von Sicherheitskonfigurationen und -änderungen zu bieten.
- Automatische Updates: Die Lösung liefert regelmäßige Sicherheitsupdates, um neu entdeckte Schwachstellen vor Angriffen zu schützen.

Herausragender Malware-Schutz

Trend Micro™ Core Protection for Virtual Machines wurde speziell für VMware-ESX/ESXi-Umgebungen entwickelt und bietet folgende Vorteile:

- 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, da der Such-Agent auf einer anderen virtuellen Maschine als die Suche selbst ausgeführt wird.
- Synchronisiert sich permanent mit der Management-Konsole des VMware vCenters, um immer auf dem neuesten Stand zu bleiben und den Aufwand zur Verwaltung virtueller Umgebungen zu reduzieren.
- Konfiguriert automatisch neue virtuelle Maschinen für die Sicherheitsüberprüfung, um VM-Wildwuchs besser unter Kontrolle zu halten.
- Optimiert leistungsintensive vollständige Suchvorgänge ohne Neukonfiguration.
- Integriert sich nahtlos in Trend Micro OfficeScan™ Client-Server Suite Installationen.

Weitere Informationen erhalten Sie unter:

<http://de.trendmicro.com/de/solutions/enterprise/security-solutions/virtualization/>