Agentenlose Sicherheit

VMware vShield Endpoint und Trend Micro Deep Security

VMware und Trend Micro haben sich als Partner zusammengeschlossen, um die erste agentenlose Sicherheitslösung für VMware-virtualisierte Rechenzentren, Desktops und Clould-Umgebungen bereitzustellen.

Probleme mit herkömmlichen Antiviren-Lösungen

Virtualisierte Rechenzentren und Desktops sollten mit denselben starken und zuverlässigen Sicherheitstechnologien geschützt werden wie physische Computer. Allerdings können herkömmliche agentenbasierte Lösungen, die nicht speziell für die Virtualisierung konstruiert sind, zu erheblichen betrieblichen Sicherheitsproblemen führen. Agentenlose Sicherheitslösungen von VMware und Trend Micro bieten einen besseren Schutz für virtuelle Maschinen als ein Schutz, der für physische Computer konzipiert ist. Folgende Problempunkte werden gelöst:

- **Ressourcenbelastung:** Selbst im Ruhezustand belegen herkömmliche Sicherheitsagenten, z. B. Antiviren-Agenten, auf jeder virtuellen Maschine (VM) erheblichen Arbeitsspeicher, insbesondere dann, wenn mehrere Sicherheitsagenten auf jeder Maschine installiert sind, um einen umfassenden Schutz zu gewährleisten. Dies verringert die Konsolidierungsraten und erhöht Investitions- (CAPEX) und Betriebskosten (OPEX).
- **Antiviren-Stürme:** Werden Virensuchen oder geplante Sicherheitsupdates durch herkömmliche Antiviren-Lösungen gleichzeitig auf allen virtuellen Maschinen eines einzigen physischen Hosts gestartet, hat das einen sogenannten „Antiviren-Sturm“ zur Folge. Dieser kann innerhalb kürzester Zeit eine extreme Belastung des Systems verursachen und die Gesamtleistung reduzieren. Ähnliche „Stürme“ können auch bei anderen Arten von Sicherheitsprüfungen und -Updates auftreten.
- **Sofortlücken:** Werden VMs in schnellem Wechsel aktiviert und deaktiviert, ist es schwierig, für diese virtuellen Maschinen konsistent Schutz bereitzustellen und diesen auf dem aktuellen Stand zu halten. Inaktive VMs können im Laufe der Zeit so weit vom Basisschutz abweichen, dass allein das Aktivieren dieser Maschinen zu schwerwiegenden Sicherheitslücken führen kann.
- **Betriebsaufwand:** Administratoren müssen Sicherheitsagenten in neuen VMs bereitstellen, diese Agenten kontinuierlich neu konfigurieren, wenn die VMs verschoben werden oder den Status ändern, und regelmäßig Pattern-Updates für diese Agents durchführen. Dies kann äußerst zeitaufwändig sein und dennoch Sicherheitslücken offen lassen.

Die Lösung im Überblick

VMware und Trend Micro haben sich als Partner zusammengeschlossen, um agentenlosen Schutz für virtualisierte Rechenzentren und Desktop-VMs bereitzustellen. Die Lösung umfasst zwei sich gegenseitig bedingende Produkte:

- **VMware vShield Endpoint™** ist eine einzigartige Lösung, die den Schutz beim Einsatz in VMware vSphere™ und VMware View™ Umgebungen optimiert. Sie ermöglicht das Auslagern von Sicherheitsprozessen auf dedizierte, sicherheitsoptimierte virtuelle Maschinen, die von VMware Partnern bereitgestellt werden.
- **Trend Micro™ Deep Security** bietet eine sicherheitsoptimierte virtuelle Maschine, die VMware vShield Endpoint und andere VMware APIs nutzt, um agentenlosen Virenschutz, Integritätsüberwachung, Erkennung und Abwehr von Eindringlingen, eine Firewall, virtuelles Patching und Schutz von Webanwendungen für virtuelle VMware Maschinen bereitzustellen.

Vorteile

Diese gemeinsame Lösung bietet virtualisierten Rechenzentren und Desktops umfassenden Schutz vor aktuellen Bedrohungen sowie:

- **Höhere Konsolidierungsraten** durch Auslagerung von Sicherheitsprüfungen einzelner VMs auf eine einzige virtuelle Sicherheitsappliance auf jedem vSphere Host.
- **Höhere Leistung** durch Vermeidung von Antiviren-Stürmen und Ressourcenkonflikten durch mehrere Sicherheitsagenten.
- **Einfachere Verwaltung**, weil Agenten und deren Konfiguration und Aktualisierung dann überflüssig sind.
- **Höhere Sicherheit** durch manipulationssicheren Sofortschutz für neue VMs, koordiniert von der dedizierten Sicherheitsappliance.

Agentenlose Sicherheit für VMware kombiniert

VMware vShield Endpoint + Trend Micro Deep Security

VMware vShield Endpoint

VMware vShield Endpoint ist eine einzigartige Lösung, die den Schutz von Hosts und Endpunkten beim Einsatz in VMware vSphere™ und VMware View™ Umgebungen optimiert.

vShield Endpoint verbessert die Leistung, indem wesentliche Funktionen auf eine dedizierte Sicherheitsappliance ausgelagert werden und somit der Sicherheitsagent keine Belastung mehr für die virtuellen Maschinen darstellt. Diese fortschrittliche Architektur entlastet die Systemressourcen, verbessert die Leistungsfähigkeit und verhindert „Sicherheitsstürme" (Überlastung der Ressourcen bei Suchläufen und Signatur-Updates).

vShield Endpoint erhöht die Sicherheit durch eine manipulationssichere virtuelle Appliance (bereitgestellt von Trend Micro), die robuste und sichere Funktionen für die Hypervisor-Selbstprüfung in vSphere verwendet und so verhindert, dass die Schutzfunktionen beeinträchtig werden. Nachweisliche Richtlinieneinhaltung und die Erfüllung der Prüfanforderungen werden durch ausführliche Aktivitätsprotokolle des Sicherheitsservice ermöglicht.

Administratoren können VMware vShield Endpoint zentral über die vShield Manager-Konsole verwalten, die nahtlos in den VMware vCenter™ Server integriert werden kann, um die einheitliche Sicherheitsverwaltung für virtuelle Rechenzentren zu erleichtern.

Trend Micro Deep Security

Trend Micro Deep Security bietet eine umfassende Server-Sicherheitsplattform zur Vereinfachung von Sicherheitsabläufen. Gleichzeitig sorgt die Lösung für eine schnellere Rendite bei Virtualisierungs- und Cloud-Computing-Projekten. Die Plattform kann mit hervorragend aufeinander abgestimmten Modulen erweitert werden, um Server-, Anwendungs- und Datensicherheit für physische, virtuelle und cloudbasierte Server sowie virtuelle Desktops sicherzustellen. Deep Security bietet eine Vielzahl an agentenlosen Sicherheitskomponenten für virtuelle Maschinen von VMware. Dazu zählen Virenschutz, Integritätsüberwachung, Erkennung und Abwehr von Eindringlingen, Schutz von Webanwendungen, Anwendungssteuerung sowie eine bidirektionale Stateful-Firewall.

Diese Sicherheitsoptionen können in dieselbe virtuelle Appliance integriert werden, um den Schutz virtueller Maschinen von VMware zu erhöhen. Agentenbasierte Sicherheit steht für diese Sicherheitsoptionen ebenso zur Verfügung wie eine Protokollprüfung. Unternehmen können damit die agentenlosen und agentenbasierten Installationskonfigurationen kombinieren, die ihre physischen, virtuellen und cloudbasierten Server sowie ihre virtuellen Desktops am besten unterstützen.

Trend Micro ist ein führender Sicherheitspartner von VMware

TREND MICRO DEEP SECURITY

- Die erste kooperative VMware Sicherheitslösung wurde speziell entwickelt zur:
  - Nutzung von VMsafe APIs
  - Nutzung von vShield Endpoint APIs
  - Bereitstellung agentenlosen Malware-Schutzes (verfügbar seit 2010)
  - Bereitstellung verschiedener agentenloser Sicherheitsoptionen
- Bereits im ersten Jahr nutzten über 1000 Kunden agentenlosen Malware-Schutz
- Die Desktop-Konsolidierungsraten sind bis zu dreimal höher als bei traditionellen, branchenführenden Anti-Malware-Lösungen für physische Desktops.
- Für virtuelle Maschinen von VMware sind jetzt mehrere agentenlose Sicherheitsmodule verfügbar – alle in einer Sicherheitsplattform.

Komponenten der Sicherheitslösung

Der agentenlose Schutz von Trend Micro für VMware besteht aus folgenden Komponenten:

- VMware vShield Endpoint
- Trend Micro Deep Security (virtuelle Appliance)

Zudem erfordert der agentenlose Schutz für VMware folgende VMware Plattformen:

- VMware ESX/ESXi (mind. eine)
- VMware vCenter
- VMware View (nur für virtuelle Desktops erforderlich)
- VMware vShield Manager

Funktionsweise

1. **VMware vShield Endpoint** ermöglicht eine agentenlose Selbstprüfung der VM sowie die Überwachung von aktuellen, neuen und reaktivierten VMs, um stets aktuellen Schutz zu gewährleisten.
2. **Trend Micro Deep Security** arbeitet mit einer dedizierten, sicherheitsoptimierten virtuellen Appliance, die die VMware vShield APIs nutzt, um VMs vor netzwerk- und dateibasierten Bedrohungen zu schützen.
3. VMware vShield Endpoint sorgt dafür, dass Trend Micro Deep Security mit den Gast-VMs kommunizieren kann, um Sicherheit, wie Virenschutz, Integritätsüberwachung, Erkennung und Abwehr von Eindringlingen, Schutz von Webanwendungen, Anwendungssteuerung und eine Firewall, zu implementieren.
4. Dieser Sicherheitsansatz sorgt für den Schutz der Netzwerk- und Dateisysteme virtueller Server und Desktops, ohne dabei Sicherheitsagenten des Gastsystems zu installieren.

TREND MICRO™ | vmware®