

Trend Micro™

# Deep Security 7

Server- und Anwendungsschutz für dynamische Datenzentren

Webpräsenz und Online-Aktivitäten sowie das Speichern und Austauschen von Daten spielen in Unternehmen eine immer größere Rolle. Deshalb steigt die Gefahr von Cyber-Angriffen, unabhängig davon, ob Anwendungen als Verbindung zu Partnern, Mitarbeitern, Lieferanten oder Kunden verwendet werden. Diese gezielten Bedrohungen sind größer und raffinierter als je zuvor, und die Einhaltung von Datenschutzrichtlinien wird mit jedem Tag schwieriger. Ihr Unternehmen braucht kompromisslose Sicherheit, mit der Sie Ihr Datenzentrum durch Virtualisierung und webbasierte Datenverarbeitung modernisieren können, ohne die Leistung zu reduzieren.

Trend Micro bietet aufeinander abgestimmte, integrierte Produkte, Services und Lösungen, die vertrauliche Informationen kosteneffizient schützen und das Risiko minimieren. Deep Security ist eine umfassende Software zum Schutz von Servern und Anwendungen, mit der sich physische, virtuelle und webbasierte Umgebungen verteidigen können. Ob als Software, virtuelle Appliance oder hybrider Ansatz implementiert: Diese Lösung minimiert den Aufwand, rationalisiert die Verwaltung und macht den Schutz virtueller Maschinen noch transparenter und leistungsfähiger. Außerdem erfüllt Deep Security eine Vielzahl von Anforderungen an die Richtlinieneinhaltung, wie z. B. die sechs wichtigsten PCI-Standards: eine Firewall auf Webanwendungsebene, IDS/IPS, die Integritätsüberwachung von Dateien und Netzwerksegmentierung.

## ARCHITEKTUR

- **Deep Security:** setzt Sicherheitsrichtlinien auf virtuellen Maschinen unter VMware vSphere transparent durch: für IDS/IPS, Webanwendungsschutz, Anwendungssteuerung und Firewall-Schutz. Falls gewünscht, erfolgt dies in Koordination mit dem Deep Security Agent zur Integritätsüberwachung und zur Protokollüberprüfung.
- **Deep Security Agent:** Diese kleine Software-Komponente, die auf dem geschützten Server oder der virtuellen Maschine installiert wird, setzt die Sicherheitsrichtlinie des Datenzentrums (IDS/IPS, Schutz für Webanwendungen, Anwendungssteuerung, Firewall, Integritätsüberwachung und Protokollüberprüfung) durch.
- **Deep Security Manager:** Mit dieser leistungsstarken, zentralen Verwaltung können Administratoren Sicherheitsprofile erstellen und diese auf Server anwenden, Warnmeldungen überwachen und vorbeugende Maßnahmen gegen Bedrohungen durchführen, Sicherheitsupdates auf Server verteilen und Berichte erstellen. Eine neue Funktion zur Kennzeichnung von Ereignissen erleichtert die Bewältigung von Massenergebnissen.
- **Security Center:** Unser dediziertes Team aus Sicherheitsexperten hilft Ihnen dabei, den neuesten Bedrohungen immer einen Schritt voraus zu sein, indem es Sicherheitsupdates zur Abwehr neu entdeckter Schwachstellen innerhalb kürzester Zeit entwickelt und bereitstellt. Ein Kundenportal ermöglicht Ihnen den Zugriff auf Sicherheitsupdates, die dem Deep Security Manager zur Verteilung bereitgestellt werden.

## INSTALLATION UND INTEGRATION

### Schnelle Verteilung unter Einbindung bestehender IT- und Sicherheitsinvestitionen

- Durch die Integration in VMware vCenter und ESX Server können Unternehmens- und Betriebsdaten in den Deep Security Manager importiert und detaillierte Sicherheit auf die VMware-Infrastruktur eines Unternehmens angewendet werden.
- Die Integration in VMsafe™ APIs ermöglicht die schnelle Installation auf ESX Servern als virtuelle Appliance, um virtuelle vSphere Maschinen sofort und transparent zu schützen.
- Detaillierte Berichte über Sicherheitsereignisse auf Serverebene werden über mehrere Integrationsoptionen an ein System für Sicherheitsinformationen und Ereignisverwaltung (SIEM), einschließlich ArcSight™, Intellitactics, NetIQ, RSA Envision, Q1Labs, Loglogic und anderer Systeme, weitergeleitet.
- Integration von Verzeichnissen auf Enterprise-Ebene, einschließlich Microsoft Active Directory.
- Konfigurierbare Verwaltungskommunikation minimiert Änderungen an der Firewall, die normalerweise bei zentral verwalteten Systemen notwendig sind, oder macht diese überflüssig, da der Manager oder der Agent die Kommunikation selbst auslöst.
- Die Agent-Software kann einfach über den Standardsoftware-Verteilungsmechanismus wie Microsoft® SMS, Novel Zenworks und Altiris verteilt werden.

## ENTSCHEIDENDE VORTEILE

### Verhindert Datendiebstahl und Unterbrechungen im Geschäftsablauf

- Errichtet eine Verteidigungslinie am physischen, virtuellen oder webbasierten Server
- Schützt bekannte und unbekannte Schwachstellen in Anwendungen und Betriebssystemen
- Schützt Webanwendungen vor SQL-Injection und Cross-Site-Scripting
- Stoppt Angriffe auf Unternehmenssysteme
- Erkennt verdächtige Aktivitäten und Verhaltensweisen, um vorbeugende Maßnahmen zu ergreifen

### Unterstützt die Einhaltung von PCI und anderen Vorschriften und Standards

- Erfüllt die sechs wichtigsten PCI-Datensicherheitsstandards und viele andere Anforderungen an die Richtlinieneinhaltung
- Liefert detaillierte, prüffähige Berichte, die verhinderte Angriffe dokumentieren und den Status der Regeleinhaltung anzeigen
- Verringert die Vorbereitungszeit und den erforderlichen Aufwand für die Unterstützung von Audits

### Senkt Betriebskosten

- Optimiert die Einsparungen von Virtualisierung und Cloud Computing durch die Konsolidierung von Serverressourcen
- Vereinfacht die Administration durch automatische Verwaltungsabläufe bei Sicherheitsereignissen
- Bietet Schutz vor Angriffen auf Schwachstellen, um Prioritäten bei der Programmierung sicheren Codes zu setzen und ungeplante Patches kosteneffizient zu implementieren
- Keine Kosten für die Installation mehrerer Software-Clients durch zentral verwaltete Mehrzweck-Software-Agents oder virtuelle Appliances

## DEEP SECURITY MODULE

### Deep Packet Inspection

- Untersucht den gesamten eingehenden und ausgehenden Verkehr auf Protokollabweichungen, Richtlinienverletzungen und Inhalte, die auf einen Angriff hindeuten
- Wird im Erkennungs- oder im Abwehrmodus betrieben, um Schwachstellen in Betriebssystemen und Enterprise-Anwendungen zu schützen
- Schützt vor Angriffen auf Anwendungsebene, SQL-Injection und Cross-Site-Scripting
- Gibt wertvolle Informationen über den Angreifer sowie Datum/Uhrzeit und Ziel des Angriffs
- Benachrichtigt Administratoren bei einem Vorfall automatisch

### Erkennung und Abwehr von Eindringlingen

- Schützt vor bekannten und Zero-Day-Angriffen, indem bereits veröffentlichte Sicherheitslücken vor einer unbegrenzten Anzahl von Angriffen abgeschirmt werden
- Schirmt neu erkannte Sicherheitslücken innerhalb weniger Stunden automatisch ab und kann ohne Neustart in Minuten auf Tausende von Servern verteilt werden
- Bietet direkten Schutz von Sicherheitslücken für über 100 Anwendungen, einschließlich Datenbank-, Web-, E-Mail- und FTP-Server
- Intelligente Regeln entdecken ungewöhnliche Protokolldaten mit böartigem Code und schützen so vor Zero-Day-Angriffen von unbekanntem Exploits, die eine noch nicht veröffentlichte Schwachstelle angreifen

### Integritätsüberwachung

- Überwacht wichtige System- und Anwendungsdateien, wie z. B. Verzeichnisse, Registrierungsschlüssel und -werte, um böartige und unerwartete Änderungen zu entdecken
- Entdeckt neu erstellte Dateien sowie Änderungen an vorhandenen Dateisystemen und berichtet dies in Echtzeit
- Ermöglicht Suchläufe nach Zeitplan, in Echtzeit und nach Bedarf, überprüft Dateieigenschaften (PCI 10.5.5) und überwacht bestimmte Verzeichnisse
- Liefert flexible und praktische Überwachung durch die Möglichkeit von Ein- und Ausschlüssen sowie durch prüffähige Berichte

### Schutz von Webanwendungen

- Unterstützt die Einhaltung von Richtlinien (PCI DSS 6.6), um Webanwendungen und die von ihnen verarbeiteten Daten zu schützen
- Schützt vor SQL-Injection, Cross-Site-Scripting und anderen Schwachstellen in Webanwendungen
- Schirmt Schwachstellen ab, bis der Code vollständig repariert ist

### Anwendungssteuerung

- Bietet verbesserten Überblick und Kontrolle über Anwendungen, die auf das Netzwerk zugreifen
- Verwendet Regeln zur Anwendungssteuerung, um böartige Software zu erkennen, die auf das Netzwerk zugreift
- Reduziert Sicherheitslücken auf Servern

### Bidirektionale Stateful-Firewall

- Verringert die Angriffsfläche von physischen, webbasierten und virtuellen Servern
- Verwaltet zentral Firewall-Richtlinien für Server, einschließlich Vorlagen für alle gängigen Serverarten
- Bietet hochpräzise Filter (IP- und MAC-Adressen, Ports), Entwicklung spezifischer Richtlinien für Netzwerkschnittstellen und Location Awareness
- Verhindert Denial-of-Service- und Ausspäh-Angriffe
- Unterstützt alle IP-basierten Protokolle (TCP, UDP, ICMP usw.) und alle Frame-Typen (IP, ARP usw.)

### Protokollüberprüfung

- Sammelt Betriebssystem- und Anwendungsprotokolle und analysiert sie in Bezug auf Sicherheitsereignisse
- Unterstützt die Regeleinrichtung (PCI DSS 10.6), um optimal wichtige, sicherheitsrelevante Ereignisse zu erkennen, die sich in mehrfachen Protokolleinträgen verbergen
- Leitet Ereignisse zum Abgleich, zur Berichterstattung und zum Archivieren an ein System für Sicherheitsinformationen und Ereignisverwaltung (SIEM) oder an zentrale Protokollserver weiter
- Entdeckt verdächtige Verhaltensweisen, sammelt Sicherheitsereignisse und administrative Aktionen in Ihrem Datenzentrum und erstellt erweiterte Regeln mittels OSSEC-Syntax

## GESCHÜTZTE PLATTFORMEN

### Microsoft® Windows®

- 2000 (32 Bit)
- XP (32 und 64 Bit)
- XP Embedded
- Windows 7
- Windows Vista (32 und 64 Bit)
- Windows Server 2003 (32 und 64 Bit)
- Windows Server 2008 (32 und 64 Bit)

### Solaris™

- Betriebssystem: 8, 9, 10 (64-Bit-SPARC, x86)

### Linux

- Red Hat® Enterprise 3.0 (32 Bit), 4.0, 5.0 (32 und 64 Bit)
- SUSE® Enterprise 9, 10 (32 Bit)

### UNIX® \*

- AIX 5.3
- HP-UX® 10, 11i v2, 11i v3

\* Ausschließlich Integritätsüberwachung und Protokollprüfung verfügbar

## VIRTUALISIERUNG

- VMware®: VMware ESX Server (Gast-Betriebssystem)
- Citrix®: XenServer (Gast-VM)
- Microsoft®: HyperV (Gast-VM)
- Sun: Solaris 10 Partitionen

## STRATEGISCHE ZERTIFIZIERUNGEN UND PARTNERSCHAFTEN

- Common Criteria EAL 3+
- Tests zur PCI-Tauglichkeit für Host-basierte Systeme (HIPS) von NSS Labs
- Virtualisierung mit VMware
- Programm für den Anwendungsschutz von Microsoft
- Zertifizierte Partnerschaft mit Microsoft
- Novell
- Partnerschaft mit Oracle
- Partnerschaft mit HP Business
- Zertifiziert außerdem von Red Hat Ready

DEEP SECURITY MODULE						
Voraussetzung für das Datenzentrum	Deep Packet Inspection			Firewall	Integritätsüberwachung	Protokollüberprüfung
	IDS/IPS	Schutz von Webanwendungen	Anwendungssteuerung			
Serverschutz	●			●	●	○
Web Application Security	●	●			○	●
Virtualisierungssicherheit	●	○		●	●	○
Erkennung verdächtigen Verhaltens	○		●	●	●	●
Sicherheit für webbasierten Datenaustausch	●	○		●	●	●
Berichte zur Einhaltung von Richtlinien	○	●	○	○	●	●

● Unerlässlich ○ Von Vorteil



© 2009 Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das Trend Micro T-Ball-Logo, OfficeScan und Trend Micro Control Manager sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen- und/oder Produktnamen sind Marken oder eingetragene Marken ihrer jeweiligen Eigentümer. Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern. [DS01DeepSecurity7\_091019DE]

[www.trendmicro.com](http://www.trendmicro.com)