

Trend Micro™

## Deep Security 6

Server- und Anwendungsschutz für dynamische Datenzentren

Webpräsenz und Online-Aktivitäten sowie das Speichern und Austauschen von Daten spielen im 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: aufeinander abgestimmte, integrierte Produkte, Services und Lösungen, die vertrauliche Informationen kostengünstig schützen und das Risiko minimieren. Trend Micro hat die Lösung für die Sicherheitsanforderungen Ihres Datenzentrums.

Deep Security ist eine umfassende Software zum Schutz von Servern und Anwendungen, mit der sich sowohl physische als auch virtuelle Server – und webbasierte Umgebungen – selbst verteidigen können. Die Lösung erfüllt außerdem die sechs wichtigsten Anforderungen für die PCI-Richtlinieneinhaltung, einschließlich der Voraussetzungen für eine Firewall auf Webanwendungsebene, IDS/IPS, Integritätsüberwachung von Dateien und Netzwerksegmentierung sowie viele andere zentrale Eigenschaften.

### ARCHITEKTUR

- **Deep Security Agent.** Diese kleine Software-Komponente, die auf den geschützten Server oder die virtuelle Maschine verteilt 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.
- **Security Center.** Unser dediziertes Team aus Sicherheitsexperten hilft Ihnen dabei, den neuesten Bedrohungen immer einen Schritt voraus zu sein, indem es innerhalb kürzester Zeit Sicherheitsupdates zur Abwehr neu entdeckter Schwachstellen entwickelt und bereitstellt. Ein Kundenportal für den Zugriff auf Sicherheitsupdates, die dem Deep Security Manager zur Verteilung bereitgestellt werden.

### VERTEILUNG UND INTEGRATION

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

- Durch die Integration in VMware vCenter und ESX Server können Unternehmens- und Betriebsdaten von vCenter- und ESX-Knoten in den Deep Security Manager importiert und detaillierte Sicherheitskomponenten auf die VMware-Infrastruktur eines Unternehmens angewendet werden.
- Ausführliche Angaben zu Sicherheitsereignissen 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 unbekanntes Schwachstellen in Anwendungen und Betriebssystemen
- 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-Standards 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

- Ermöglicht Unternehmen, die Kostenreduzierung durch Virtualisierung oder webbasierte Datenverarbeitung effektiv zu nutzen
- Bietet Schutz vor Schwachstellen, um Prioritäten bei der Programmierung sicherer Codes zu setzen und ungeplante Patches kostengünstig zu implementieren
- Schützt umfassend durch zentral verwalteten Software-Agent und vermeidet Kosten für die Verteilung mehrerer Software-Clients

## 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
- Schirmt gegen Angriffe auf Anwendungsebene, SQL-Injection und Cross-Site-Scripting ab
- Liefert wertvolle Informationen über den Angreifer mit Datum/Uhrzeit und Ziel des Angriffs
- Benachrichtigt Administratoren bei einem Vorfall automatisch

### Entdeckung und Abwehr von Eindringlingen

- Verhindert den unbegrenzten Zugriff auf bereits veröffentlichte Schwachstellen und schützt dadurch vor bekannten und Zero-Day-Angriffen
- Schützt neu entdeckte Schwachstellen innerhalb weniger Stunden automatisch und kann ohne Neustart in Minuten auf Tausende von Servern verteilt werden
- Bietet direkten Schutz von Schwachstellen 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 unbekannter 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
- Schützt nach Bedarf oder Zeitplan, überprüft Dateieigenschaften (PCI 10.5.5) und überwacht bestimmte Verzeichnisse
- Bietet flexible und praktische Überwachungsfunktionen durch Ein- und Ausschlüsse und liefert prüffähige Berichte

### Schutz von Webanwendungen

- Unterstützt die Einhaltung von Richtlinien (PCI 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 besseren 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 physischer, webbasierter oder virtueller Server
- Bietet zentrale Verwaltung von Firewall-Richtlinien für Server, einschließlich Vorlagen für alle gängigen Server-Typen
- Verfügt über hochpräzise Filter (IP- und MAC-Adressen, Ports), spezifische Richtlinien für Netzwerkschnittstellen und Location Awareness
- Verhindert Denial-of-Service-Angriffe und entdeckt Reconnaissance-Angriffe
- Unterstützt alle IP-basierten Protokolle (TCP, UDP, ICMP usw.) und alle Frame-Typen (IP, ARP usw.)

### Protokollüberprüfung

- Sammelt Betriebssystem- und Anwendungsprotokolle und durchsucht sie nach Sicherheitsereignissen
- Optimiert die Erkennung wichtiger, sicherheitsrelevanter Ereignisse, 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 in 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

\* Nur 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 Schutz von Microsoft Anwendungen
- Zertifizierte Partnerschaft mit Microsoft
- Novell
- Partnerschaft mit Oracle
- Partnerschaft mit HP Business
- Auch als Red Hat Ready zertifiziert

DEEP SECURITY MODULE						
Anforderungen an das Datenzentrum	Deep Packet Inspection			Firewall	Integritätsüberwachung	Protokollüberprüfung
	IDS/IPS	Schutz von Webanwendungen	Anwendungssteuerung			
Serverschutz	●			●	●	○
Sicherheit von Webanwendungen	●	●			○	●
Virtualisierungssicherheit	●	○		●	●	
Entdecken verdächtigen Verhaltens	○		●	●	●	●
Sicherheit beim webbasierten Datenaustausch	●	○		●	●	●
Berichte zur Einhaltung von Richtlinien	○	●	○	○	●	●

● Notwendig ○ Von Vorteil



©2009 by Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das 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. [DS01DeepSecurity6\_090811DE]

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