

Trend Micro™

Deep Security 7.5

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 bei der Verbindung mit Partnern, Mitarbeitern, Lieferanten und Kunden. Diese gezielten Bedrohungen sind größer und raffinierter als je zuvor, und die Einhaltung von Datenschutzrichtlinien wird von Tag zu 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 Deep Security bietet fortschrittliche Sicherheit für physische, virtuelle und webbasierte Server sowie für virtuelle Desktops. Ob als Software, virtuelle Appliance oder hybrider Ansatz: Diese Lösung minimiert den Aufwand, rationalisiert die Verwaltung und bietet starke, agentenlose Sicherheit für virtuelle Maschinen. Außerdem erfüllt Deep Security durch mehrere Schutzmodule in einer konsolidierten Lösung eine Vielzahl von Anforderungen an die Richtlinieneinhaltung, wie z. B. die sieben wichtigsten PCI-Standards.

ARCHITEKTUR

NEU! Deep Security Virtual Appliance: Setzt beim agentenlosen Malware-Schutz, bei IDS/IPS, beim Webanwendungsschutz, bei der Anwendungssteuerung und beim Firewall-Schutz Sicherheitsrichtlinien transparent auf virtuellen VMware vSphere Maschinen durch – zur Integritätsüberwachung und Protokollüberprüfung auf Wunsch auch in Koordination mit dem Deep Security Agent.

Deep Security Agent: Diese kleine Software-Komponente, die auf dem geschützten Server oder der virtuellen Maschine installiert wird, setzt die Sicherheitsrichtlinie des Datenzentrums bei IDS/IPS, beim Schutz für Webanwendungen, bei der Anwendungssteuerung, bei der Firewall sowie bei der 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.

Smart Protection Network: Deep Security integriert sich in diese Cloud-Client-Infrastruktur der nächsten Generation, um vor neu auftretenden Bedrohungen in Echtzeit zu schützen, indem es Bedrohungs- und Reputationsdaten von Websites, E-Mail-Quellen und Dateien permanent auswertet und miteinander in Beziehung setzt.

INSTALLATION UND INTEGRATION

Schnelle Verteilung unter Einbindung bestehender IT- und Sicherheitsinvestitionen

- Die Integration in vShield Endpoint, VMSafe™ APIs und VMware vCenter ermöglicht die schnelle Installation auf ESX Servern als virtuelle Appliance, um virtuelle vSphere Maschinen sofort und transparent zu schützen.
- Detaillierte Sicherheitsereignisse auf Server-Ebene werden über mehrere Integrationsoptionen an ein SIEM-System, wie beispielsweise ArcSight™, Intellitactics, NetIQ, RSA Envision, Q1Labs, Loglogic, und andere Systeme weitergeleitet.
- Integration von Verzeichnissen auf Enterprise-Ebene, einschließlich Microsoft Active Directory.
- Die Agent-Software kann einfach über Standardsoftware-Verteilungsmechanismen, wie Microsoft® SMS, Novell 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 sieben 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 stärkere Konsolidierung virtueller Maschinen
- Vereinfacht die Verwaltung virtueller Server- und Desktop-Umgebungen durch die Bereitstellung von Anti-Malware und anderen Sicherheitsmechanismen in einer agentenlosen Konfiguration
- Vereinfacht die Administration durch serverweite automatische Verwaltung von Sicherheitsereignissen
- Bietet Schutz vor Angriffen auf Schwachstellen und setzt dabei vor allem auf die Programmierung sicheren Codes und die kosteneffiziente Implementierung ungeplanter Patches
- Vermeidet Kosten für die Verteilung mehrerer Software-Clients durch einen zentral verwalteten Mehrzweck-Software-Agent oder eine virtuelle Appliance

DEEP SECURITY MODULE

NEU! Agentenloser Malware-Schutz für VMware Umgebungen

- Integriert neue VMware vShield Endpoint APIs zum Schutz virtueller VMWare-Maschinen vor Viren, Spyware, Trojanern und anderer Malware ohne Belastung des Gastsystems
- Optimiert Sicherheitsaktionen zur Vermeidung von Sicherheitsbeeinträchtigungen bei System-Vollsuchen und Pattern-Updates
- Schützt die Sicherheitslösung vor Manipulation durch raffinierte Angriffe, indem sie die Malware von der Anti-Malware isoliert

Deep Packet Inspection

- Untersucht den gesamten eingehenden und ausgehenden Verkehr auf Protokollabweichungen, Richtlinienverletzungen oder Inhalte, die auf einen Angriff hindeuten
- Wird im Erkennungs- oder im Abwehrmodus betrieben, um Schwachstellen in Betriebssystemen und Enterprise-Anwendungen zu schützen
- Benachrichtigt automatisch über den Angreifer sowie den Zeitpunkt und das Ziel des Angriffs

Erkennung 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

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

Bidirektionale Stateful-Firewall

- Verringert die Angriffsfläche physischer, webbasierter und virtueller Server durch hochpräzise Filter, netzwerkspezifische Richtlinien und Location Awareness für alle IP-basierten Protokolle und für alle Frame-Typen
- Bietet zentrale Verwaltung von Firewall-Richtlinien für Server, einschließlich Vorlagen für alle gängigen Servertypen
- Verhindert Denial-of-Service- und Ausspäh-Angriffe

Integritätsüberwachung

- Überwacht wichtige System- und Anwendungsdateien, wie z. B. Verzeichnisse, Registrierungsschlüssel und -werte, um bösartige und unerwartete Änderungen zu entdecken
- Entdeckt neu erstellte Dateien sowie Änderungen an bestehenden Dateisystemen und berichtet darüber in Echtzeit
- Ermöglicht bedarfsgesteuerte, geplante oder Echtzeitsuche; überprüft Dateieigenschaften (PCI 10.5.5) und überwacht bestimmte Verzeichnisse

Protokollprüfung

- Sammelt und untersucht Betriebssystem- und Anwendungsprotokolle auf verdächtiges Verhalten, Sicherheitsereignisse und administrative Ereignisse in Ihrem gesamten Datenzentrum
- Unterstützt die Regeleinhaltung (PCI DSS 10.6), um die Erkennung wichtiger Sicherheitsereignisse zu optimieren, die sich in mehrfachen Protokolleinträgen verbergen
- Leitet Ereignisse zum Abgleich, zur Berichterstattung und zur Archivierung an ein SIEM-System oder einen zentralen Protokollserver weiter

GESCHÜTZTE PLATTFORMEN

Microsoft® Windows®

- 2000 (32 Bit)
- XP (32 und 64 Bit)
- XP Embedded
- Windows 7 (32 und 64 Bit)
- Windows Vista (32 und 64 Bit)
- Windows Server 2003 (32 und 64 Bit)
- Windows Server 2008 (32 und 64 Bit)
- Windows Server 2008 R2 (64 Bit)

Solaris™

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

Linux

- Red Hat® Enterprise 4.0, 5.0 (32 und 64 Bit)
- SUSE® Enterprise 10, 11 (32 und 64 Bit)

UNIX®*

- AIX 5.3, 6.1
- HP-UX® 10, 11i v2/v3

* Ausschließlich Integritätsüberwachung und Protokollprüfung verfügbar

VIRTUALISIERUNG

- **Virtuelle Appliance:** VMware vSphere 4.1
- **VMware®:** VMware ESX 4.1 Server (Gast-Betriebssystem)
- **Citrix®:** XenServer
- **Microsoft®:** HyperV
- **Sun:** Solaris 10 Datencontainer

STRATEGISCHE ZERTIFIZIERUNGEN UND PARTNERSCHAFTEN

- Common Criteria EAL 3+ (EAL 4 in Vorbereitung)
- 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
- Red Hat Ready-zertifiziert

Anforderungen an das Datenzentrum	Deep Packet Inspection			Firewall	Integritätsüberwachung	Protokollprüfung	NEU! Anti-Malware
	IDS/IPS	Schutz von Webanwendungen	Anwendungssteuerung				
Serverschutz	●			●	●	○	●
Sicherheit für Webanwendungen	●	●			○	●	
Virtualisierungssicherheit	●	○		●	●	○	●
Erkennung verdächtigen Verhaltens	○		●	●	●	●	
Sicherheit für webbasierten Datenaustausch	●	○		●	●	●	●
Berichte zur Einhaltung von Richtlinien	○	●	○	○	●	●	
Agentenbasiert	●	●	●	●	●	●	
Virtuelle Appliance	●	●	●	●			●

● Unerlässlich ○ Von Vorteil



© 2010 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- bzw. Produktnamen sind Marken oder eingetragene Marken ihrer jeweiligen Eigentümer. Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern. [DSO3DeepSecurity7.5_100721DE]

www.trendmicro.com