

Trend Micro™

Deep Security 8.0

Umfassende Sicherheitsplattform für physische, virtuelle und cloudbasierte Server

Virtualisierung und Cloud-Computing verändern die heutigen Rechenzentren. Während Unternehmen von rein physischen Umgebungen immer mehr auf einen Mix aus physischen, virtuellen und cloudbasierten Umgebungen umsteigen, reagieren viele von ihnen auf die aktuellen Bedrohungen immer noch mit einer Kombination aus veralteten Sicherheitslösungen. Dies kann jedoch die gewünschten Leistungsverbesserungen verhindern: Es entstehen unverhältnismäßig komplexe Abläufe, unerwünschte Sicherheitslücken, und letztendlich sind Unternehmen nicht in der Lage, umfassend in Virtualisierung und Cloud-Computing zu investieren.

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. Auf diese Weise können Sie Ihre Sicherheitslösung ganz auf Ihre Anforderungen zuschneiden – mit einer beliebigen Kombination aus Schutzanwendungen mit oder ohne Agent, einschließlich Malware-Schutz, Firewall, IDS/IPS, Schutz von Webanwendungen, Integritätsüberwachung und Protokollüberprüfung. Das Ergebnis: Eine umfassende, anpassbare und effiziente Server-Sicherheitsplattform, die geschäftskritische Unternehmensanwendungen und -daten vor Angriffen und Unterbrechungen des Betriebsablaufs schützt und dabei kein teures Notfall-Patching erfordert.

WICHTIGSTE FUNKTIONEN

Schnellere Rendite bei Virtualisierung, VDI und Cloud-Computing

- Bietet einen einfacheren und besser zu verwaltenden Schutz von VMs mit der ersten und einzigen agentenlosen Sicherheitsplattform für VMware-Umgebungen der Branche – einschließlich Malware-Schutz, Abwehr von Eindringlingen und Integritätsüberwachung
- **NEU!** Stellt eine agentenlose Integritätsüberwachung zur Verfügung, die eine bessere Sicherheit virtueller Server ohne Systembelastung garantiert
- Sorgt im Vergleich zu herkömmlichen Anti-Malware-Lösungen für eine 11-mal effizientere Ressourcenauslastung und unterstützt eine 3-mal höhere VM-Dichte
- Verbessert die Verwaltbarkeit der Sicherheitsfunktionen in VMware-Umgebungen, da die Notwendigkeit zum regelmäßigen Konfigurieren, Aktualisieren und Patchen von Agenten entfällt
- Sichert die virtuellen VMware View Desktops im lokalen Modus mit einem optionalen Agenten
- Koordiniert den Schutz virtueller Server, die zwischen Rechenzentrum und öffentlicher Cloud verschoben werden, dank virtueller Appliances und Agenten kontinuierlich und optimiert

Maximale Senkung der Betriebskosten

- Optimiert die Einsparungen von Virtualisierung und Cloud Computing durch stärkere Konsolidierung virtueller Maschinen
- Reduziert die Komplexität dank nahtloser Integration in Management-Konsolen von Trend Micro, VMware und Unternehmensverzeichnisse
- 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
- Reduziert die Verwaltungskosten durch die Automatisierung repetitiver und ressourcenintensiver Sicherheitsmaßnahmen, minimiert falsche Sicherheitsalarme und ermöglicht festgelegte Reaktionen auf Sicherheitsvorfälle
- **NEU!** Reduziert die Komplexität der Datei-Integritätsüberwachung mithilfe von cloudbasierten Whitelists für Ereignisse und der Festlegung von vertrauenswürdigen Ereignissen deutlich

Kosteneffiziente Richtlinieneinhaltung

- Erfüllt die wichtigsten Anforderungen für PCI DSS 2.0 sowie HIPAA, NIST und SAS 70 mit einer integrierten und kosteneffizienten Lösung
- Liefert detaillierte, prüffähige Berichte, die verhinderte Angriffe dokumentieren und den Status der Richtlinieneinhaltung anzeigen
- Verringert die Vorbereitungszeit und den erforderlichen Aufwand für die Unterstützung von Audits
- Unterstützt interne Initiativen zur Richtlinieneinhaltung, um die Sichtbarkeit von internen Netzwerkaktivitäten zu verbessern
- Nutzt eine bewährte, nach Common Criteria EAL 4+ zertifizierte Technologie

Verhindert Datendiebstahl und Unterbrechungen im Geschäftsablauf

- Erkennt und entfernt Malware auf virtuellen Servern in Echtzeit – bei minimaler Leistungsbeeinträchtigung
- Sperrt Malware, die versucht, der Entdeckung durch Deinstallieren oder anderes Außerkraftsetzen des Sicherheitsprogramms zu entgehen
- Schützt bekannte und unbekannte Schwachstellen in Web- und Unternehmensanwendungen und Betriebssystemen
- Erkennt verdächtige oder bösartige Aktivitäten und löst Warnmeldungen sowie proaktive und präventive Aktionen aus
- **NEU!** Nutzt die Web-Reputation-Funktionen einer der größten Domain-Reputationsdatenbanken der Welt, um die Integrität von Websites zu prüfen und Benutzer vor dem Zugriff auf infizierte Websites zu schützen
- **NEU!** Bietet Hypervisor-Integritätsüberwachung für VMware vSphere mit Intel TPM/TXT-Technologie

DEEP SECURITY PLATTFORMMODULE

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
- **NEU!** Stellt einen Anti-Malware-Agenten bereit, der den Schutz auf physische Server sowie im lokalen Modus auf virtuelle Desktops ausdehnt
- **NEU!** Lässt sich in das Trend Micro™ Smart Protection Network™ integrieren, so dass Web-Reputation-Funktionen für einen besseren Schutz von Servern und virtuellen Desktops genutzt werden können
- Optimiert Sicherheitsmaßnahmen zur Vermeidung von Antiviren-Stürmen, die häufig bei System-Vollsuchen und Pattern-Updates auftreten
- Schützt die Sicherheitslösung vor Manipulation durch raffinierte Angriffe in virtuellen Umgebungen, indem sie die Malware von der Anti-Malware isoliert

Integritätsüberwachung

- Überwacht wichtige System- und Anwendungsdateien, wie z. B. Verzeichnisse, Registrierungsschlüssel und -werte, um bösartige und unerwartete Änderungen in Echtzeit zu erkennen und zu melden
- **NEU!** Bietet eine agentenlose Integritätsüberwachung auf derselben virtuellen Appliance wie der agentenlose Malware-Schutz und die Abwehr von Eindringlingen, um eine höhere Sicherheit der virtuellen Server ohne Systembelastung zu erzielen
- **NEU!** Reduziert den Administrationsaufwand durch die Kennzeichnung von vertrauenswürdigen Ereignissen, wodurch Aktionen für ähnliche Ereignisse im gesamten Rechenzentrum automatisch repliziert werden
- **NEU!** Vereinfacht die Verwaltung durch eine starke Reduzierung der bekannten vertrauenswürdigen Ereignisse mithilfe von automatisierten, cloudbasierten Whitelists des Trend Micro Certified Safe Software Service
- **NEU!** Schützt den Hypervisor mithilfe der Hypervisor-Integritätsüberwachung mit Intel TPM/TXT-Technologie vor Angriffen

Erkennung und Abwehr von Eindringlingen

- Verhindert den unbegrenzten Zugriff auf bereits veröffentlichte Schwachstellen und schützt dadurch vor bekannten und Zero-Day-Angriffen
- Untersucht den gesamten eingehenden und ausgehenden Verkehr auf Protokollabweichungen, Richtlinienverletzungen oder Inhalte, die auf einen Angriff hindeuten
- Schützt neu entdeckte Schwachstellen innerhalb weniger Stunden automatisch und kann ohne Neustart in Minuten auf Tausende von Servern verteilt werden
- Lässt sich in agentenlose Anti-Malware und Integritätsüberwachung auf derselben virtuellen Appliance integrieren und bietet so einen erhöhten Schutz
- Bietet direkten Schutz von Schwachstellen für alle wichtigen Betriebssysteme und über 100 Anwendungen, einschließlich Datenbank-, Web-, E-Mail- und FTP-Server

Schützt Webanwendungen

- Unterstützt die Einhaltung von Richtlinien (PCI DSS 6.6) zum Schutz von Webanwendungen und Daten
- Schützt vor SQL-Injection, Cross-Site-Scripting und anderen Schwachstellen in Webanwendungen
- Schirmt Schwachstellen ab, bis der Code vollständig repariert ist
- Benachrichtigt automatisch über den Angreifer sowie den Zeitpunkt und das Ziel des Angriffs

Anwendungssteuerung

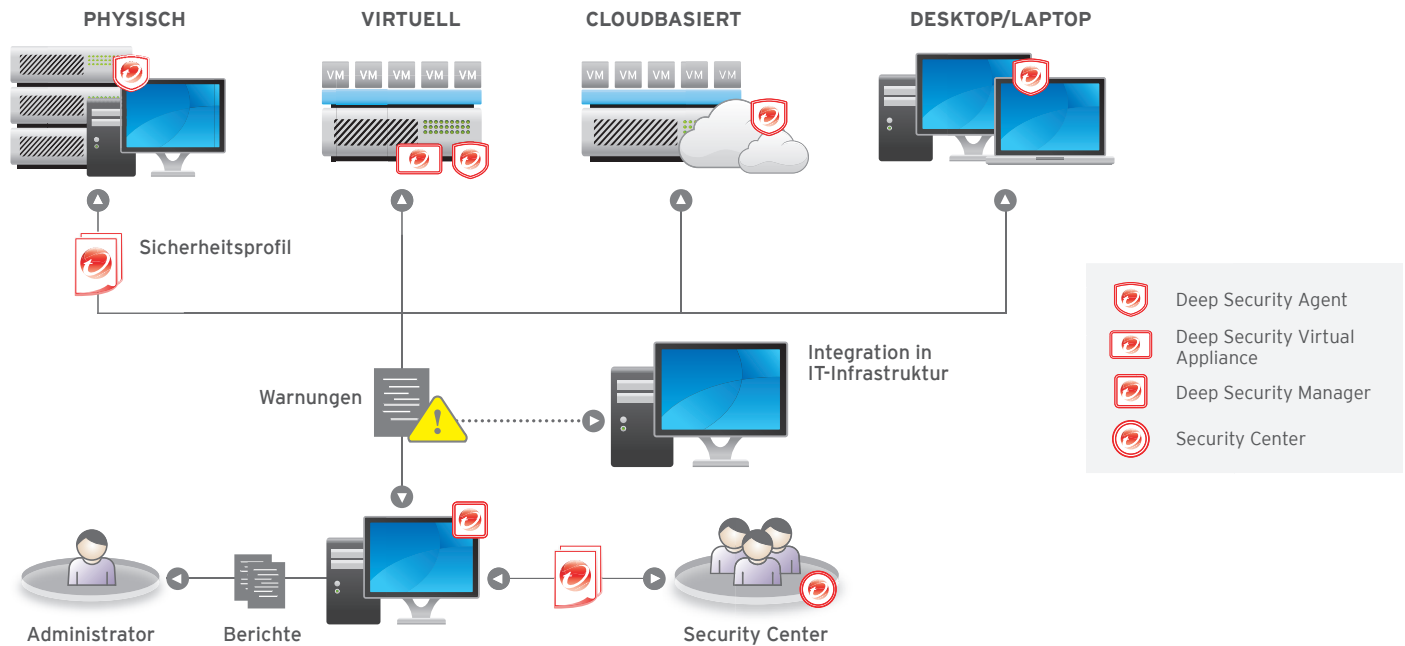
- Schafft mehr Sichtbarkeit und Kontrolle von Anwendungen, die auf das Netzwerk zugreifen
- Verwendet Regeln zur Anwendungssteuerung, um bösartige Software zu erkennen, die auf das Netzwerk zugreift
- Reduziert Sicherheitslücken auf Servern

Bidirektionale Stateful-Firewall

- Verringert die Angriffsfläche physischer, cloudbasierter und virtueller Server durch hochpräzise Filter, netzwerkspezifische Richtlinien und Location Awareness für alle IP-basierten Protokolle und für alle Frame-Typen
- Verwaltet Server-Firewall-Richtlinien zentral und enthält Vorlagen für alle gängigen Servertypen
- Verhindert Denial-of-Service- und Ausspäh-Angriffe

Protokollprüfung

- Sammelt und untersucht Betriebssystem- und Anwendungsprotokolle auf verdächtiges Verhalten, Sicherheitsereignisse und administrative Ereignisse in Ihrem gesamten Rechenzentrum
- 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



Deep Security erfüllt alle wichtigen Unternehmensanforderungen

Virtuelle Patches

Schirmt Schwachstellen ab, bevor sie ausgenutzt werden können, und beseitigt somit Probleme im Betriebsablauf, die durch Notfall-Patching, regelmäßige Patch-Zyklen und kostenintensive Systemausfälle verursacht werden.

Sicherheit für virtuelle Desktops und Server

Schützt virtuelle Desktops und Server vor Zero-Day-Malware und reduziert die Beeinträchtigungen der Betriebsabläufe, die durch Ressourcenengpässe und Notfall-Patching entstehen können.

Einhaltung von Richtlinien

Ermöglicht und belegt die Richtlinien-einhaltung für eine Reihe regulatorischer Bestimmungen, einschließlich PCI DSS 2.0, HIPAA, FISMA/NIST, NERC, SAS 70 und andere.

Integrierte Server-Sicherheit

Konsolidiert alle Server-Sicherheitsprodukte in einer umfassenden, integrierten und flexiblen Plattform, die den Schutz von physischen, virtuellen und cloudbasierten Servern optimiert

Datenschutz

Schützt und verwaltet den Zugriff auf kritische Daten in Ihrem Rechenzentrum und in privaten Cloud-Umgebungen sowie bei allen Datenbewegungen. Deep Security kombiniert fortschrittliche Technologien wie die Abwehr von Eindringlingen und die Integritätsüberwachung mit richtlinien-basierter Schlüsselverwaltungs-technologie, die durch die Integration in SecureCloud zur Verfügung steht.

ENTWICKELT FÜR VIRTUELLE VMWARE- UND CLOUD-UMGEBUNGEN

Deep Security wurde speziell für virtuelle Umgebungen konzipiert. Die agentenlose Architektur verhindert Antiviren-Stürme, minimiert die Komplexität der Sicherheitsabläufe und ermöglicht Unternehmen, die Dichte von VMs zu erhöhen und die Virtualisierung und Einführung von Cloud-Computing zu beschleunigen. Deep Security wurde in enger Zusammenarbeit mit VMware entwickelt und ist daher das erste Produkt in seiner Kategorie, das Unterstützung für VMware vSphere 5.0 und VMware vShield Endpoint 2.0 bietet. Deep Security ist außerdem vollständig abwärtskompatibel mit vSphere 4.1-Umgebungen. Der Deep Security 8.0 Manager unterstützt auch VMware-Umgebungen im gemischten Modus, die vSphere 5.0 und vSphere 4.1 unterstützen und durch die virtuellen Appliances von Deep Security 8.0 oder 7.5 geschützt werden.

PLATTFORMARCHITEKTUR

Deep Security Virtual Appliance. Setzt bei agentenloser Integritätsüberwachung, Malware-Schutz, IDS/IPS, Webanwendungsschutz, Anwendungssteuerung und Firewall-Schutz Sicherheitsrichtlinien transparent auf virtuellen VMware vSphere Maschinen durch – zur Protokollüberprüfung und umfassenden Abwehr 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 Rechenzentrums beim Malware-Schutz, bei IDS/IPS, beim Schutz für Webanwendungen, bei der Anwendungssteuerung, 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. Die 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, Novel Zenworks und Altiris, verteilt werden.

PLATTFORMARCHITEKTUR

Microsoft® Windows®

- 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 R2 (64 Bit)

Linux

- Red Hat® Enterprise 5, 6 (32 Bit und 64 Bit)¹
- SUSE® Enterprise 10, 11 (32 Bit und 64 Bit)¹

Solaris™

- Betriebssystem: 8, 9, 10 (64-Bit-Version SPARC), 10 (64-Bit-Version x86)¹

UNIX

- AIX 5.3, 6.1 auf IBM Power Systems²
- HP-UX 11i v3 (11.31)²

VIRTUELL

- VMware®: ESX/ESXi 3.x³, vSphere 4.0⁴, vSphere 4.1/5.0⁵, View 4.5/5.0⁵
- Citrix®: XenServer³
- Microsoft®: HyperV³

¹ Malware-Schutz nicht verfügbar

² Auf dieser Plattform sind nur die Integritätsüberwachung und Protokollprüfung verfügbar

³ Schutz ausschließlich über Deep Security Agent

⁴ Schutz über Deep Security Agent und Virtual Appliance für Firewall, IDS/IPS und Schutz von Webanwendungen, über Agent nur für andere Module

⁵ Schutz über Deep Security Agent nur für Protokollüberprüfung, über Agent und Virtual Appliance für alle anderen Module, separate Lizenz für vShield Endpoint erforderlich

Wichtige Zertifizierungen und Partnerschaften

- Common Criteria EAL 4+
- 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
- Partnerschaft mit Oracle
- Partnerschaft mit HP Business
- Red Hat Ready-zertifiziert



© 2011 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. [DS01_DeepSecurity8_110816DE]
www.trendmicro.com