Trend Micro™

DEEP SECURITY 9.5

Umfassende Sicherheitsplattform für physische, virtuelle und cloudbasierte Server

Virtualisierung und Cloud-Computing haben die heutigen Rechenzentren verändert. Dennoch verlassen sich viele Unternehmen bei ihrer Umstellung von herkömmlichen physischen Umgebungen auf moderne Rechenzentren mit Virtualisierung und Cloud-Nutzung noch immer auf veraltete Sicherheitssoftware. Veraltete Sicherheitssoftware führt in vielen Fällen zu einem erhöhten Betriebsaufwand in virtuellen Umgebungen und gleichzeitig zu einer geringeren Systemleistung und VM-Dichte. Außerdem verbleiben Sicherheitslücken, die eventuell dazu verleiten, geschäftskritische Arbeitsvolumina nicht in flexible und kostengünstige Cloud-Umgebungen zu verlagern. Letztendlich beeinträchtigt die Verwendung veralteter Sicherheitssoftware in modernen Rechenzentren somit die Rendite von Virtualisierung und Cloud-Computing.

Schutz vor Datenverlust und Unterbrechungen im Geschäftsablauf

Trend Micro™ Deep Security™ – verfügbar als Software oder Software as a Service (SaaS) – schützt Ihr Rechenzentrum und Ihre Cloud-Umgebung vor Datenverlusten und Unterbrechungen im Geschäftsablauf. Deep Security trägt zur Compliance bei, indem es Sicherheitslücken in virtuellen und cloudbasierten Umgebungen auf effiziente und wirtschaftliche Weise schließt, sowie kritische Komponenten auf Veränderungen überwacht..

Multifunktionale Sicherheit mit Verwaltung über ein zentrales Dashboard

Deep Security verfügt über integrierte Funktionen wie Malware-Schutz, Web Reputation, Firewall, Abwehr von Eindringlingen, Integritätsüberwachung und Logüberprüfung. So wird der Schutz von Servern, Anwendungen und Daten in physischen, virtuellen und cloudbasierten Umgebungen sichergestellt. Deep Security kann als zentraler Agent für viele verschiedene Funktionen in allen Umgebungen eingesetzt werden und vereinfacht dank eines einzigen Management-Dashboards für all diese Funktionen die Verwaltung sicherheitsrelevanter Vorgänge.

Nahtlose Integration zur Anwendung von Richtlinien in cloudbasierten Umgebungen

Deep Security kann nahtlos in Cloud-Plattformen wie Amazon Web Services (AWS), Microsoft Azure oder VMware vCloud Hybrid Service integriert werden. Dies ermöglicht es Ihnen, die Sicherheitsrichtlinien Ihres Rechenzentrums auch auf cloudbasierte Umgebungen anzuwenden. Dank der zahlreichen Funktionen von Deep Security, die für viele verschiedene Umgebungen optimiert wurden, können Unternehmen und Service-Provider ihren Anwendern eine individuelle und gleichzeitig sichere mandantenfähige Cloud-Umgebung zur Verfügung stellen.

Die wichtigsten Unternehmensanforderungen

Sicherheit für virtuelle Desktops
Konstante Leistung und gleichbleibende Konsolidierungsraten dank umfassender agentenloser Sicherheit, die den Schutz für VDI-Umgebungen maximiert.

Virtuelles Patching
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.

Compliance
Weist Compliance mit einer Reihe von Anforderungen nach, unter anderem PCI DSS 3.0, HIPAA, FISMA/NIST, NERC und SAS 70.

SCHNELLERE RENDITE BEI CLOUD-COMPUTING UND VIRTUALISIERUNG DURCH OPTIMALE SICHERHEIT FÜR DAS MODERNE RECHENZENTRUM

Virtualisierungssicherheit

Deep Security schützt virtuelle Desktops und Server vor Zero-Day-Malware und netzwerkbasierten Angriffen und reduziert gleichzeitig die Beeinträchtigungen der Betriebsabläufe, die durch Ressourcenengpässe und Notfall-Patching entstehen können.

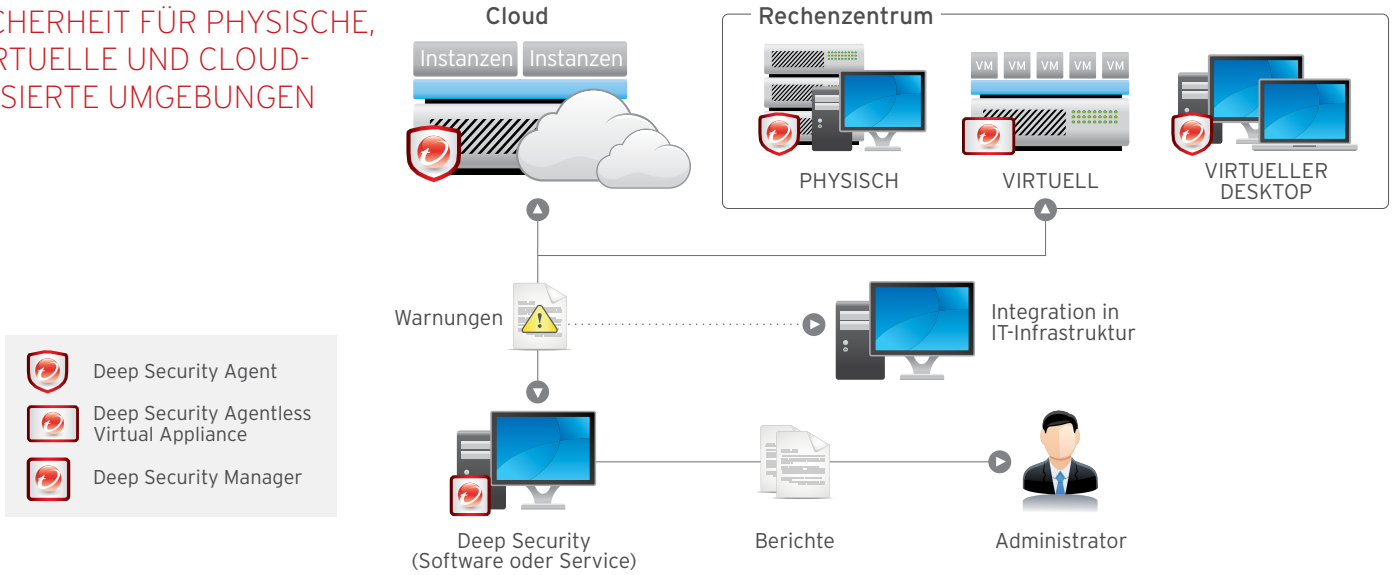
Cloud-Sicherheit

Mit Deep Security stellen Service-Provider und moderne Rechenzentren eine sichere, mandantenfähige Cloud-Umgebung mit auf cloudbasierte Arbeitsvolumina erweiterbaren Sicherheitsrichtlinien zur Verfügung. Diese Umgebung kann dank übergreifender Richtlinien zentral verwaltet werden.

Integrierte Serversicherheit

Deep Security konsolidiert alle Serversicherheitsfunktionen in einer umfassenden, integrierten und flexiblen Plattform, die den Schutz von physischen, virtuellen und cloudbasierten Servern optimiert.

SICHERHEIT FÜR PHYSISCHE, VIRTUELLE UND CLOUD-BASIERTE UMGEBUNGEN



ENTSCHEIDENDE VORTEILE

Schnellere Rendite bei Virtualisierung und Cloud-Computing

- Erzielt durch die höhere VM-Dichte eine effizientere Ressourcenauslastung und Verwaltung als herkömmliche, agentenbasierte Anti-Malware-Lösungen
- Ist als zentraler und leicht verwaltbarer Sicherheitsagent für viele verschiedene Funktionen und dank seiner tiefgreifenden Abwehrstrategien äußerst flexibel
- Bietet durch Deduplizierung von Suchvorgängen auf Hypervisor-Ebene ein unerreichtes Leistungsniveau
- Kann in Cloud-Plattformen wie AWS, Microsoft Azure oder VMware vCloud Hybrid Service integriert werden, wodurch Unternehmen die Verwaltung ihrer physischen, virtuellen und cloudbasierten Server anhandübergreifender Sicherheitsrichtlinien ermöglicht wird
- Service-Provider können ihren Kunden eine sichere öffentliche Cloud zur Verfügung stellen, die durch ihre mandantenfähige Architektur von der anderer Mandanten getrennt ist
- Bietet automatische Skalierung, Utility-Computing und Self-Service zur Unterstützung agiler Unternehmen mit softwarebasiertem Rechenzentrum
- Nutzt die enge Integration von Deep Security mit VMware zur automatischen Erkennung neuer VMs und zur Anwendung kontextbasierter Richtlinien für konsistente Sicherheit, sowohl im Rechenzentrum als auch in der Cloud
- Kann in VMware NSX™ integriert werden. Deep Security nutzt die Vorteile der Mikrosegmentierung im softwarebasierten Rechenzentrum dank Sicherheitsrichtlinien und -funktionen, die VMs überall automatisch nachverfolgen

Verhinderung von Datenverlusten 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
- Zeigt bei der Erkennung verdächtiger oder bösartiger Aktivitäten Warnmeldungen an und löst proaktive Abhilfemaßnahmen aus
- Prüft anhand von Web-Reputation-Bedrohungsdaten aus der globalen Domain-Reputationsdatenbank von Trend Micro die Integrität von Websites und schützt Anwender so vor infizierten Seiten
- Erkennt und sperrt Botnetze und gezielte Angriffe durch Command-and-Control-Kommunikation (C&C) mithilfe der gesammelten Bedrohungsdaten aus der globalen Domain-Reputationsdatenbank von Trend Micro

Maximale Senkung der Betriebskosten

- Vermeidet Kosten für die Verteilung mehrerer Softwareclients durch einen zentral verwalteten Mehrzweck-Software-Agent oder eine virtuelle Appliance
- Reduziert die Komplexität dank nahtloser Integration in Management-Konsolen von Trend Micro und VMware sowie Unternehmensverzeichnisse
- Bietet Abschirmung von Schwachstellen und ermöglicht so die Programmierung sicherer Codes und die kosteneffiziente Implementierung ungeplanter Patches
- Reduziert die Verwaltungskosten durch die Automatisierung repetitiver und ressourcenintensiver Sicherheitsmaßnahmen, minimiert falsche Sicherheitswarnungen und ermöglicht wirksame Reaktionen auf Sicherheitsvorfälle
- Reduziert mithilfe der Festlegung von vertrauenswürdigen Ereignissen und cloudbasierten Whitelists für Ereignisse den Aufwand der Dateiintegritätsüberwachung erheblich
- Erkennt Schwachstellen und verdächtige Software anhand der Empfehlungssuche, mit der Veränderungen erkannt werden und entsprechender Schutz von Schwachstellen bereitgestellt werden kann
- Sorgt dank des ressourcensparenden, dynamischeren und intelligenten Agents, der die Verteilung durch optimale Ressourcenzuweisung in Rechenzentrum und Cloud vereinfacht, für effizientere Betriebsabläufe
- Passt die Sicherheit an Ihre individuellen Richtlinien an, wodurch weniger Ressourcen für spezifische Sicherheitskontrollen erforderlich sind
- Vereinfacht die Administration durch eine zentrale Verwaltung für alle Trend Micro Sicherheitsprodukte. Dank der zentralen Berichterstellung für mehrere Sicherheitsfunktionen wird der bisherige Aufwand für die Erstellung von Berichten für einzelne Produkte deutlich reduziert.

Kosteneffiziente Richtlinieneinhaltung

- Erfüllt die wichtigsten Anforderungen für PCI DSS 3.0 sowie HIPAA, HITECH, NIST und SAS 70 mit einer integrierten und kosteneffizienten Lösung
- Erstellt Audit-Berichte, in denen abgewehrte Angriffe sowie der Status der Richtlinien-Compliance dokumentiert werden
- Verringert die Vorbereitungszeit und den erforderlichen Aufwand für die Unterstützung von Audits
- Unterstützt interne Initiativen zur Compliance, um die Sichtbarkeit von internen Netzwerkaktivitäten zu verbessern
- Nutzt eine bewährte, nach Common Criteria EAL 4+ zertifizierte Technologie

DEEP SECURITY PLATTFORMMODULE

Anti-Malware mit Web-Reputation-Technologie

- Nutzt VMware APIs zum Schutz virtueller Maschinen von VMware vor Viren, Spyware, Trojanern und anderer Malware ohne Belastung des Gastsystems
- Stellt einen Anti-Malware-Agent bereit, der den Schutz auf physische, virtuelle und cloudbasierte Server ausdehnt, einschließlich AWS-, Microsoft- und VMware-Umgebungen
- Bringt jetzt noch mehr Leistung durch Caching und Deduplizierung auf VMware-ESX-Ebene
- Optimiert Sicherheitsmaßnahmen zur Vermeidung von Antiviren-Stürmen, die häufig bei vollständigen Systemprüfungen und Pattern-Updates von herkömmlichen Sicherheitsfunktionen auftreten
- Schützt vor raffinierten Angriffen in virtuellen Umgebungen, indem Malware von kritischen Betriebssystem- und Sicherheitskomponenten isoliert wird
- Nutzt die globalen Bedrohungsinformationen des Trend Micro™ Smart Protection Network™, um Web-Reputation-Funktionen bereitzustellen, die für einen besseren Schutz von Servern und virtuellen Desktops sorgen

Abwehr von Eindringlingen

- Untersucht den gesamten eingehenden und ausgehenden Verkehr auf Protokollabweichungen, Richtlinienverletzungen oder Inhalte, die auf einen Angriff hindeuten
- Schützt automatisch vor bekannten, aber noch ungepatchten Schwachstellen durch virtuelles Patchen (Abschirmen) dieser Schwachstellen vor einer unbegrenzten Anzahl von Angriffen und kann ohne Neustart in Minutenschnelle auf Tausende von Servern verteilt werden
- Unterstützt die Compliance (PCI DSS, Abschnitt 6.6) zum Schutz von Webanwendungen und Daten
- Schützt vor SQL-Injection, Cross-Site-Scripting und anderen Schwachstellen in Webanwendungen
- Bietet direkten Schutz von Schwachstellen für alle wichtigen Betriebssysteme und über 100 Anwendungen, einschließlich Datenbank-, Web-, E-Mail- und FTP-Server
- Sorgt für mehr Transparenz und Kontrolle bei Anwendungen, die auf das Netzwerk zugreifen

Bidirektionale hostbasierte 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-Angriffe und erkennt Ausspäh-Angriffe
- Protokolliert Angriffe auf die Firewall auf dem Host und ermöglicht damit Compliance- und Audit-Berichte, die vor allem für öffentliche Cloud-Umgebungen besonders wichtig sind

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
- Nutzt die Intel TPM/TXT-Technologie zur Hypervisor-Integritätsüberwachung aller unberechtigten Änderungen und weitet so die Sicherheit und Compliance auch auf den Hypervisor aus
- Reduziert den Administrationsaufwand durch die Kennzeichnung von vertrauenswürdigen Ereignissen, wodurch Aktionen für ähnliche Ereignisse im gesamten Rechenzentrum automatisch repliziert werden
- Vereinfacht die Verwaltung durch eine weitgehende Reduzierung der bekannten vertrauenswürdigen Ereignisse mithilfe von automatisierten, cloudbasierten Whitelists des Trend Micro™ Certified Safe Software Service

Logüberprüfung

- Sammelt und untersucht Betriebssystem- und Anwendungslogs in mehr als 100 Dateiformaten auf verdächtiges Verhalten, Sicherheitsereignisse und administrative Ereignisse in Ihrem gesamten Rechenzentrum
- Unterstützt die Compliance (PCI DSS, Abschnitt 10.6) zur besseren Erkennung wichtiger Sicherheitsereignisse, die sich in mehrfachen Protokolleinträgen verbergen
- Leitet Ereignisse zum Abgleich, zur Berichterstattung und zur Archivierung an ein SIEM-System oder einen zentralen Protokollserver weiter

> „Mit Deep Security konnten wir auch eine andere Antiviren-Lösung auf unseren Servern ausmustern... Diese benötigte sehr viel Speicherplatz und hat aufgrund der Suchläufe eine hohe CPU-Last verursacht. Seit Deep Security haben wir diese Probleme nicht mehr."

Blaine Isbelle
Systemadministrator
Information Services Technology
Universität von Kalifornien in Berkeley

Installation und Integration

Schnelle Verteilung unter Einbindung bestehender IT- und Sicherheitsinvestitionen

- Die Integration in VMware vCenter ermöglicht die schnelle Installation auf ESX-Servern als virtuelle Appliance, um virtuelle vSphere-Maschinen sofort und transparent zu schützen.
- Detaillierte Sicherheitsereignisse auf Serverebene werden über mehrere Integrationsoptionen an ein SIEM-System weitergeleitet, wie beispielsweise ArcSight, Intellitactics, NetIQ, RSA Envision, Q1Labs oder Loglogic.
- Integration von Unternehmensverzeichnissen, einschließlich Microsoft Active Directory
- Die Agent-Software kann einfach über Standardsoftware-Verteilungsmechanismen verteilt werden, wie beispielsweise Chef, Puppet, AWS OpsWorks, Microsoft System Center Configuration Manager (SCCM), Novell ZENworks und Symantec Deployment Solution.

Zertifizierung für CSP

Trend Ready für Cloud-Service-Provider ist ein weltweites Testprogramm, mit dem Cloud-Service-Provider (CSP) die Kompatibilität Instances ihrer Services mit den branchenführenden Cloud-Sicherheitslösungen von Trend Micro nachweisen können.

PLATTFORMARCHITEKTUR

Deep Security Virtual Appliance. Setzt mit agentenlosem Malware-Schutz, Web Reputation, Abwehr von Eindringlingen, Integritätsüberwachung und Firewall-Schutz Sicherheitsrichtlinien transparent auf virtuellen VMware vSphere Maschinen durch – zur Logüberprüfung und umfassenden Abwehr auf Wunsch auch in Koordination mit dem Deep Security Agent.

Deep Security Agent. Setzt die Sicherheitsrichtlinie des Rechenzentrums beim Malware-Schutz, bei der Abwehr von Eindringlingen, bei der Firewall, bei der Integritätsüberwachung sowie bei der Logüberprüfung anhand einer kleinen Softwarekomponente durch, die auf dem geschützten Server bzw. der geschützten virtuellen Maschine installiert wird. (Diese kann mithilfe branchenführender Anwendungsverwaltungs-Tools wie Chef, Puppet oder AWS OpsWorks automatisch installiert werden.)

Deep Security Manager. Die leistungsstarke und zentrale Management-Konsole sorgt für rollenbasierte Administration und Richtlinienvererbung auf mehreren Ebenen, was eine gezielte Kontrolle ermöglicht. Funktionen zur Automatisierung bestimmter Aufgaben wie die Empfehlungssuche und die Ereigniskennzeichnung vereinfachen darüber hinaus die erforderliche Sicherheitsadministration. Und dank der mandantenfähigen Architektur ist eine Trennung der individuellen Richtlinien einzelner Mandanten sowie das Delegieren von sicherheitsrelevanten Verwaltungsaufgaben an die Administratoren der Mandanten möglich.

Globale Bedrohungsinformationen. Deep Security lässt sich in das Trend Micro Smart Protection Network integrieren, um vor neu auftretenden Bedrohungen in Echtzeit zu schützen. Dazu wertet es globale Bedrohungs- und Reputationsdaten von Websites, E-Mail-Quellen und Dateien permanent aus und setzt sie miteinander in Beziehung.

PLATTFORMARCHITEKTUR
Microsoft® Windows®
• Windows XP, Vista, 7, 8, 8.1 (32 und 64 Bit) • Windows Server 2003 (32 und 64 Bit) • Windows Server 2008, 2008 R2, 2012, 2012 R2 (64 Bit) • XP Embedded
Linux
• Red Hat® Enterprise 5, 6 (32 und 64 Bit)[1] • SUSE® Enterprise 10, 11 (32 und 64 Bit)[1] • CentOS 5, 6 (32 und 64 Bit)[1] • Amazon Linux[1] • Ubuntu 10, 12, 14.04 (64 Bit)[1] • Oracle Linux 5, 6 (32 und 64 Bit)[1] • CloudLinux 5, 6 (32 und 64 Bit)[1]
Oracle Solaris™
• Betriebssystem: 9, 10, 11 (64-Bit-Version SPARC), 10, 11 (64-Bit-Version x86)[2] • Oracle Exadata Database Machine, Oracle Exalogic Elastic Cloud und SPARC SuperCluster über die unterstützten Solaris Betriebssysteme
UNIX
• AIX 5.3, 6.1 auf IBM Power Systems[3] • HP-UX 11i v3 (11.31)[3]
VIRTUELL
• VMware®: 5.1/5.5/vCloud Networking und Security 5.1, View 4.5/5.0/5.1, ESX 5.5 • Citrix®: XenServer[4] • Microsoft®: HyperV[4]

[1] Unterstützung von Malware-Schutz nur für Suchläufe nach Bedarf
[2] Malware-Schutz nicht verfügbar
[3] Malware-Schutz nicht verfügbar, Firewall und Abwehr von Eindringlingen nur unter AIX
[4] Schutz ausschließlich über Deep Security Agent

Wichtige Zertifizierungen und Partnerschaften

- Bevorzugter Technologiepartner von Amazon
- Red Hat Ready-zertifiziert
- Validiert für Cisco UCS
- Common Criteria EAL 4+
- Validiert für EMC VSPEX
- Partnerschaft mit HP Business
- Programm für den Anwendungsschutz von Microsoft
- Zertifizierte Partnerschaft mit Microsoft
- Validiert für NetApp FlexPod
- Partnerschaft mit Oracle
- Tests zur PCI-Tauglichkeit für Host-basierte Systeme (HIPS) von NSS Labs
- Validiert für VCE Vblock
- Virtualisierung mit VMware

amazon web services | Partner Network
ADVANCED TECHNOLOGY PARTNER

vmware®

Microsoft Azure

TREND MICRO | TREND READY CLOUD SERVICE PROVIDER

SAP® Certified
Integration with SAP NetWeaver®

TREND MICRO™

Securing Your Journey to the Cloud