Trend Micro™

DEEP SECURITY™

Vollständige Sicherheit für physische, virtuelle, cloudbasierte und hybride Umgebungen

Die Virtualisierung hat Rechenzentren bereits entscheidend verändert und immer mehr Unternehmen verlagern ihre Workloads ganz oder teilweise in private und öffentliche Clouds. Damit Sie die Vorteile von hybridem Cloud-Computing nutzen können, muss Ihre Sicherheitslösung Schutz für all Ihre Server bieten – physische, virtuelle und cloudbasierte.

Die Sicherheitslösung sollte darüber hinaus weder die Systemleistung noch die VM-Dichte oder die Rendite (ROI) Ihrer Virtualisierungs- und Cloud-Computing-Investitionen mindern. Trend Micro™ Deep Security™ bietet umfassenden Schutz in einer Lösung, die speziell für virtualisierte und cloudbasierte Umgebungen entwickelt wurde, um Sicherheitslücken oder Leistungseinbußen zu verhindern.

Schutz vor Datenverlust und Unterbrechungen im Geschäftsablauf
Deep Security – verfügbar als Software, als Software as a Service (SaaS) oder als Angebot bei Amazon Web Services (AWS) oder Microsoft® Azure™ Marketplace – schützt Ihr Rechenzentrum und Ihre Cloud-Umgebung vor Datenverlusten und Unterbrechungen im Geschäftsablauf. Deep Security trägt zur Compliance bei, indem es Sicherheitslücken in hybriden Cloud-Umgebungen auf effiziente und wirtschaftliche Weise schließt.

Verwaltung mehrerer Sicherheitsfunktionen über ein zentrales Dashboard
Deep Security verfügt über integrierte Funktionen wie Malware-Schutz, Machine Learning-Prognosen, Web Reputation, Firewall, Intrusion Prevention, Integritätsüberwachung, Applikationskontrolle und Log-Überprüfung. So wird der Schutz von Servern, Anwendungen und Daten in physischen, virtuellen, Cloud- und Containerumgebungen sichergestellt. Deep Security kann als multifunktionaler Agent in allen Umgebungen eingesetzt werden und bietet ein einziges Dashboard für das Management aller Funktionen, wodurch die Verwaltung sicherheitsrelevanter Vorgänge vereinfacht wird. Als Dashboard können Sie Trend Micro Control Manager oder ein Drittanbietersystem wie VMware vRealize Operations, Splunk, HP ArcSight oder IBM QRadar verwenden.

Nahtlose Integration zur Anwendung von Richtlinien in cloudbasierten Umgebungen
Deep Security kann nahtlos in Cloud-Plattformen wie AWS, Azure und VMware® 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 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, HIPAA, NIST und SSAE 16.

> „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

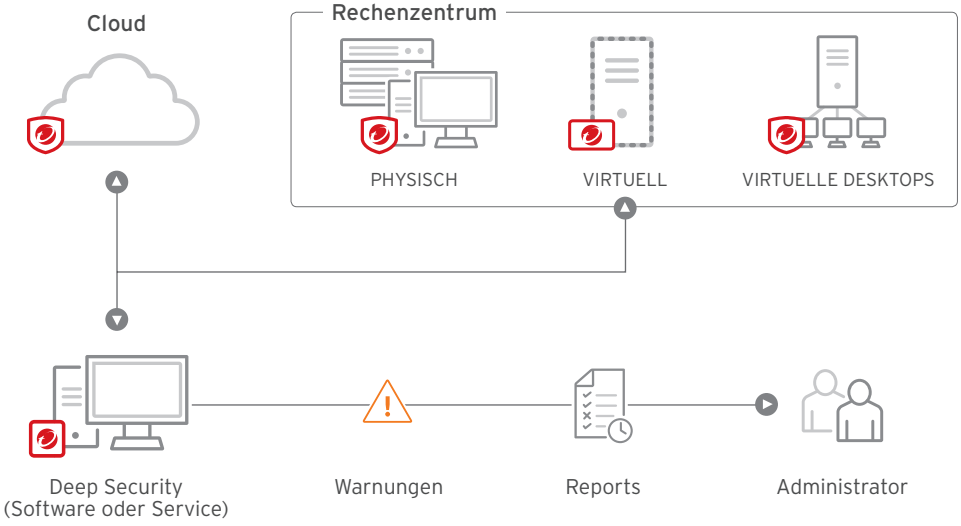
BEWÄHRTE HYBRID CLOUD SECURITY

Virtualisierungssicherheit
Deep Security schützt virtuelle Desktops und Server vor Zero-Day-Malware, einschließlich Ransomware, sowie netzwerkbasierten Angriffen. Gleichzeitig werden Beeinträchtigungen der Betriebsabläufe reduziert, die durch Ressourcenengpässe und Notfall-Patching entstehen können.

Cloud-Sicherheit
Mit Deep Security stellen Service-Provider und Leiter moderner Rechenzentren eine sichere, mandantenfähige Cloud-Umgebung mit Sicherheitsrichtlinien zur Verfügung, die auf Cloud-Workloads erweitert werden und zentral sowie konsistent verwaltet werden können.

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

HYBRID CLOUD SECURITY



ENTSCHEIDENDE VORTEILE

Hochwirksam und effizient

- Ermöglicht durch die höhere VM-Dichte eine effizientere Ressourcenauslastung und Verwaltung als herkömmliche Anti-Malware-Lösungen
- Fügt als multifunktionaler und einfach zu verwaltender Sicherheitsagent tiefgreifende Abwehrmechanismen hinzu und sorgt für mehr Flexibilität
- Bietet durch Deduplizierung von Suchvorgängen auf Hypervisor-Ebene ein unerreichtes Leistungsniveau
- Kann in Cloud-Plattformen wie AWS, Microsoft Azure oder Cloud integriert werden, wodurch Unternehmen die zentrale Verwaltung ihrer physischen, virtuellen und cloudbasierten Server anhand konsistenter und kontextsensitiver 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 die neuesten Versionen von VMware vSphere und NSX™ integriert werden. Deep Security nutzt die Vorteile der Mikrosegmentierung im softwarebasierten Rechenzentrum dank Sicherheitsrichtlinien und -funktionen, die VMs überall automatisch folgen, egal wohin diese wandern

Verhindert Datenverlust und Unterbrechungen im Geschäftsablauf

- Verhindert die Ausführung unbekannter Anwendungen auf Ihren geschäftskritischen Servern
- Erkennt und entfernt Malware auf virtuellen Servern in Echtzeit – bei minimaler Leistungsbeeinträchtigung
- Erkennt und sperrt unzulässige Software mittels Applikationskontrolle für mehrere Plattformen
- Schirmt bekannte und unbekannte Schwachstellen in Web- und Unternehmensanwendungen und Betriebssystemen ab
- Erkennt komplexe Bedrohungen und beseitigt verdächtige Objekte durch Sandbox-Analysen
- Zeigt bei der Erkennung verdächtiger oder bösartiger Aktivitäten Warnmeldungen an und löst proaktive Abhilfemaßnahmen aus
- Prüft anhand von Web-Reputation-Bedrohungsinformationen 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 Bedrohungsinformationen 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, VMware sowie Unternehmensverzeichnisse wie VMware vRealize Operations, Splunk, HP ArcSight und IBM QRadar
- Schützt Docker-Host und Container durch Anti-Malware-Scans und Intrusion Prevention
- Reduziert die Verwaltungskosten durch die Automatisierung repetitiver und ressourcenintensiver Sicherheitsmaßnahmen, minimiert falsche Sicherheitsalarme und ermöglicht festgelegte Reaktionen auf Sicherheitsvorfälle
- Reduziert erheblich die Komplexität der Verwaltung von Datei-Integritätsüberwachungen durch die Verwendung cloudbasierter Listen von bekannt vertrauenswürdigen Ereignissen
- Identifiziert Schwachstellen und verdächtige Software anhand der Empfehlungssuche, mit der Veränderungen erkannt werden und entsprechender Schutz von Schwachstellen bereitgestellt wird
- Sorgt für effizientere Betriebsabläufe dank eines noch ressourcensparenderen, dynamischereren und intelligenten Agents, der die Verteilung durch optimale Ressourcenzuweisung über das Rechenzentrum bis hin zur Cloud vereinfacht
- 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 Compliance

- Erfüllt die wichtigsten Compliance-Anforderungen für PCI DSS sowie HIPAA, SSAE 16 und andere mit einer integrierten und kosteneffizienten Lösung
- Erstellt Audit-Berichte, in denen verhinderte 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 zertifizierte Technologie

DEEP SECURITY FUNKTIONEN

Malware-Schutz mit Verhaltensüberwachung und Machine Learning-Prognose

- Nutzt VMware vShield Endpoint APIs zum Schutz virtueller Maschinen von VMware vor Viren, Spyware, Trojanern, Ransomware und anderer Malware
- Stellt einen Anti-Malware-Agent bereit, der den Schutz auf physische, virtuelle und cloudbasierte Server ausdehnt, einschließlich AWS-, Microsoft- und VMware-Umgebungen
- Bringt mehr Leistung durch agentenloses 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 komplexen Angriffen in virtuellen Umgebungen, indem Malware von kritischen Betriebssystem- und Sicherheitskomponenten isoliert wird
- Setzt fortschrittliche Machine Learning-Technologien ein, um Bedrohungsinformationen zu korrelieren und eine eingehende Dateianalyse durchzuführen, um unbekannte Sicherheitsrisiken zu erkennen
- Ermöglicht die Erkennung verdächtiger Aktivitäten oder nicht autorisierter Änderungen sowie schnelle Quarantäne und Wiederherstellung
- Identifiziert und untersucht verdächtige Objekte mithilfe von Sandbox-Analysen
- Lässt sich in die globalen Bedrohungsinformationen aus dem Trend Micro™ Smart Protection Network™ integrieren, so dass Web-Reputation-Funktionen für einen besseren Schutz von Servern und virtuellen Desktops genutzt werden können

Log-Überprüfung

- 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

Intrusion Prevention

- 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 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, wie Datenbank-, Web-, E-Mail- und FTP-Server
- Sorgt für mehr Transparenz und Kontrolle bei Anwendungen, die auf das Netzwerk zugreifen, einschließlich Regelsätzen, um das systemweite Ausführen unerwünschter Software zu blockieren

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- und Ausspäh-Angriffe
- Protokolliert Angriffe auf die Firewall des Hosts 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 sowie 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 Erkennung von Ereignissen mithilfe des automatisierten, cloudbasierten Whitelisten-Abgleichs von bekannt harmlosen Ereignissen durch den Trend Micro™ Certified Safe Software Service

Applikationskontrolle für mehrere Plattformen

- Erkennt und sperrt unzulässige Software auf Windows- und Linux-Servern automatisch
- Durchsucht Computer und ermittelt, welche Applikationen aktuell installiert sind
- Sperrt das System nach der Inventarisierung und verhindert damit die Ausführung neuer, nicht in den Whitelists verzeichneter Anwendungen
- Lässt sich in eine DevOps-Umgebung integrieren, um kontinuierliche Änderungen an Anwendungspaketen zu unterstützen und mithilfe von APIs Schutz durch Applikationskontrolle zu bieten

ARCHITEKTUR

Deep Security Virtual Appliance. Setzt Sicherheitsrichtlinien transparent auf virtuellen VMware vSphere Maschinen durch. VMware NSX-Umgebungen werden damit Sicherheitsfunktionen wie agentenloser Malware-Schutz, Web Reputation, Intrusion Prevention, Integritätsüberwachung und Firewall-Schutz bereitgestellt. Der kombinierte Modus (Combined Mode) kann verwendet werden, bei dem die virtuelle Appliance agentenlosen Malware-Schutz und Integritätsüberwachung bietet, während der Agent Intrusion Prevention, Applikationskontrolle, Firewall-Schutz, Web Reputation und Log-Überprüfung sicherstellt.

Deep Security Agent. Setzt die Sicherheitsrichtlinie des Rechenzentrums bei der Applikationskontrolle, beim Malware-Schutz, bei Intrusion Prevention, der Firewall, der Integritätsüberwachung sowie der Log-Überprüfung 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 sowie ereignisbasierte Aufgaben vereinfachen darüber hinaus die erforderliche Sicherheitsadministration. 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 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.

Der **Deep Security Scanner** kann über die NetWeaver Viren-Scan-Schnittstelle in SAP-Systeme integriert werden und schützt diese zuverlässig.

SAP Partner

Zertifizierung für CSP

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

INSTALLATION UND INTEGRATION

Schnelle Verteilung unter Einbindung bestehender IT- und Sicherheitsinvestitionen

- 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.
- Detaillierte Sicherheitsereignisse auf Serverebene werden über mehrere Integrationsoptionen an ein SIEM-System weitergeleitet, wie beispielsweise HP ArcSight, Intellitactics, IBM QRadar, NetIQ, RSA Envision, Q1Labs, Loglogic, Splunk oder Sumologic.
- Integration von Unternehmensverzeichnissen, einschließlich Microsoft Active Directory

Der Entwicklung von Deep Security 10 liegen flexible Praktiken für ständige Innovation und Entwicklung zugrunde. Wir freuen uns über die Einführung von **Feature Releases**, womit neue Funktionen direkt nach ihrer Bereitstellung bereits vor dem nächsten vollständigen Release bereitgestellt werden können. So können Sie sich ganz flexibel dafür entscheiden, neue Funktionen zu nutzen, sobald ein Produkt damit ausgestattet wird, und müssen nicht auf das nächste vollständige Release warten.

DEEP SECURITY RELEASE			
Security Tools und Funktionen	**10.0**	**10.1 Feature Release***	**10.2 Feature Release***
Applikationskontrolle	✓ Linux	✓ + Windows	✓
– Globale Blacklist			✓
– Windows Trusted Updates			✓
– Ereignissammlung			✓
Intrusion Prevention	✓	✓	✓
Malware Prevention	✓	✓	✓
– Verhaltensüberwachung	✓	✓	✓
– Machine Learning			✓
Web-Reputation	✓	✓	✓
Protokollinspektion	✓	✓	✓
Integritätsüberwachung	✓	✓	✓
Unterstützung von Docker-Containern	✓	✓	✓
Windows Server 2016	✓		✓
Unterstützung von SQL 2016 für Deep Security Manager			✓
PostgreSQL-Unterstützung		✓ (Einzelmandant)	✓ (Mehrmandanten- und Multi-AZ-Bereitstellungen)
Installation von Netzwerktreibern ohne Betriebsunterbrechung		✓	✓
Single Sign On mit SAML 2.0		✓	✓
Produkt-Newsfeed		✓	✓
TippingPoint und Deep Security (IPS) Regelzuordnung			✓

* Feature Releases werden nach dem nächsten größeren Release von Deep Security während der Verfügbarkeit sechs Monate lang unterstützt.

SYSTEMANFORDERUNGEN

Microsoft® Windows®

- Windows XP, Vista, 7, 8, 8.1, 10 (32 Bit/64 Bit)
- Windows Server 2003 (32 Bit/64 Bit)
- Windows Server 2008 (32 Bit/64 Bit), 2008 R2, 2012, 2012 R2, 2012 Server Core (64 Bit), 2016 (64 Bit), 2016 Server Core (64 Bit)
- XP Embedded (32 Bit/64 Bit)[1]

Linux[2]

- Red Hat® Enterprise 5, 6, 7 (32 Bit/64 Bit)[3]
- SUSE® Enterprise 10, 11, 12 (32 Bit/64 Bit)[3]
- CentOS 5, 6, 7 (32 Bit/64 Bit)[5]
- Ubuntu 12, 14, 16 (64 Bit, nur LTS)[4, 5]
- Oracle Linux 5, 6, 7 (32 Bit/64 Bit)[4, 5]
- CloudLinux 5, 6, 7 (32 Bit/64 Bit)[2, 4]
- Amazon Linux (32 Bit/64 Bit)[4, 5]
- Debian 6, 7 (64 Bit)[2, 4]

Oracle Solaris™ [6, 7]

- Betriebssystem: 10, 11 (64-Bit SPARC), 10, 11 (64-Bit x86)[7, 8]
- Oracle Exadata Database Machine, Oracle Exalogic Elastic Cloud und SPARC SuperCluster über die unterstützten Solaris Betriebssysteme

UNIX[6]

- AIX 5.3, 6.1, 7.1 auf IBM Power Systems[7, 8]
- HP-UX 11i v3 (11.31)[7, 9]

VIRTUELL

- VMware® vSphere: 5.5/6.0, View 4.5/5.0/5.1, ESX 5.5, 6.2.X, 6.5, NSX 6.2.X, 6.3
- Citrix®: XenServer[11]
- Microsoft®: HyperV[11]

[1] Aufgrund der diversen Anpassungsmöglichkeiten unter Windows XP Embedded bitten wir unsere Kunden, den ordnungsgemäßen Betrieb in ihrer eigenen Umgebung zu überprüfen, um sicherzustellen, dass die für die Ausführung des Deep Security Agenten erforderlichen Services und Ports aktiviert sind.
[2] Informationen zu unterstützten Kernels finden Sie in der Dokumentation.
[3] Unterstützung für SAP-Schutz ist nur bei Red Hat 6 (64 Bit) und SUSE 11 (64 Bit) und nur agentenseitig verfügbar. Das Malware-Schutzmodul muss agentenseitig aktiviert sein, damit der Schutz in SAP ordnungsgemäß funktioniert.
[4] Unterstützung von Malware-Schutz nur für On-Demand-Suchläufe
[5] Informationen zu unterstützten Versionen finden Sie in den neuesten Versionshinweisen.
[6] Malware-Schutz und Web-Reputation-Überwachung nicht verfügbar
[7] Support über 9.0 Agenten
[8] Malware-Schutz nicht verfügbar
[9] Nur Log-Überprüfung und Integritätsüberwachung
[10] vCloud Networking and Security ermöglicht agentenlosen Malware-Schutz und Integritätsüberwachung
[11] Schutz ausschließlich über Deep Security Agent

UNTERSTÜTZT DURCH XGEN™ SECURITY

Deep Security ist eine Komponente von Trend Micro Hybrid Cloud Security – unterstützt durch XGen™.

Wichtige Zertifizierungen und Partnerschaften

- Bevorzugter Technologiepartner von Amazon
- Red Hat Ready-zertifiziert
- Validiert für Cisco UCS
- Common Criteria EAL 2+
- 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
- Von SAP zertifiziert (NW-VSI 2.0 und HANA)
- Validiert für VCE Vblock
- Virtualisierung mit VMware

TREND MICRO™

Securing Your Journey to the Cloud