Trend Micro™

DEEP SECURITY™ PACKAGES

Eine breite Palette an Optionen zum Schutz von physischen, virtuellen, Cloud-, Container- und hybriden Umgebungen

Die Virtualisierung hat Rechenzentren bereits entscheidend verändert und immer mehr Unternehmen verlagern ihre Workloads ganz oder teilweise in private und öffentliche Clouds sowie in Container. Wenn Sie die Vorteile von Virtualisierung und hybridem Cloud-Computing nutzen möchten, müssen Sie wirksamen Schutz ihrer gesamten Server in physischen, virtuellen, Cloud- sowie hybriden Umgebungen sicherstellen.

Mit Deep Security können Sie Ihre virtuelle, Cloud- und Containerumgebung sicher und ohne Leistungs- und Effizienzeinbuβen skalieren. Damit entfällt auch die betriebliche Problematik, verschiedene Sicherheitslösungen verwalten zu müssen, was zwangsläufig uneinheitliche Richtlinien und einen enormen Verwaltungsaufwand mit sich bringen würde.

Deep Security ist in vier verschiedenen Paketen erhältlich, die auf die Sicherheitsanforderungen jeder Organisation zugeschnitten sind.

MALWARE PREVENTION SECURITY PACKAGE

Beinhaltet Anti-Malware, Inhaltsfilterung, Verhaltensanalyse und vorausschauende, maschinelle Lernverfahren

Anti-Malware

- Bietet agentenlose und agentenbasierte Optionen zur Integration in VMware und andere virtuelle Umgebungen
- Sandbox-Analyse mit Erkennung komplexer Bedrohungen und Reaktion auf verdächtige Objekte

Inhaltsfilterung

- Stärkerer Schutz gegen Bedrohungen aus dem Internet für Server und virtuelle Desktops
- Integration in Web-Reputation-Funktionen von Trend Micro™ Smart Protection Network™ zum Schutz von Anwendern und Anwendungen durch Blockade des Zugriffs auf schädliche URLs

Verhaltensanalyse

- Sucht nach Verhaltensweisen, die auf Schädlichkeit hinweisen, beispielsweise Verschlüsselung von Dateien mit Ransomware, wodurch automatisch verschlüsselte Dokumente gesichert und schädliche Änderungen gestoppt werden
- Überprüfung des Arbeitsspeichers in Echtzeit, um verdächtige Prozesse zu erkennen und zu beenden

Predictive Machine Learning

- Setzt fortschrittliche Machine-Learning-Technologien ein, um Bedrohungsinformationen zu korrelieren und eine eingehende Dateianalyse durchzuführen. In Kombination mit einer Sicherheitslösung auf mehreren Ebenen können so neue, unbekannte Sicherheitsrisiken erkannt und Server besser vor weit verbreiteten Angriffen geschützt werden.
- Führt eine Verhaltensanalyse von unbekannten oder seltener vorkommenden Prozessen durch, um zu bestimmen, ob eine neue oder unbekannte Bedrohung versucht, das Netzwerk zu infizieren

NETWORK SECURITY PACKAGE

Beinhaltet Intrusion-Prevention (IPS)- und Firewall-Funktionen

Intrusion Prevention

Schirmt bekannte Schwachstellen vor Exploits ab, bis diese korrigiert werden können

- Sorgt für zeitnahen Schutz gegen bekannte und Zero-Day-Angriffe
- Nutzt Schwachstellenregeln zur Abschirmung einer bekannten Schwachstelle vor einer unbegrenzten Anzahl an Exploits
- Bietet sofortigen Schwachstellenschutz für mehr als 100 Anwendungen, darunter Datenbanken sowie Internet-, E-Mail- und File Transfer Protocoll (FTP)-Server.
- Liefert automatisch Regeln, die neu entdeckte Schwachstellen wie Shellshock und Heartbleed innerhalb von Stunden abschirmen und in Minutenschnelle ohne Systemneustart an Tausende von Servern übermittelt werden können
- Erhöht die Transparenz oder Kontrolle von Anwendungen, die auf das Netzwerk zugreifen
- Identifiziert schädliche Software, die auf das Netzwerk zugreift, und sorgt für eine geringere Angriffsfläche bei Servern

Firewall

Verringert die Angriffsfläche physischer und virtueller Server

- Zentralisiert mit einer bidirektionalen Stateful-Firewall die Verwaltung von Firewall-Richtlinien
- Unterstützt die Aufteilung virtueller Maschinen in Zonen und verhindert Denial-of-Service-Angriffe
- Bietet umfassenden Schutz für alle IP-basierten Protokolle und Frame-Typen sowie hochpräzise Filter für Ports, IP- und MAC-Adressen

Mit Deep Security profitieren Sie von erweitertem Bedrohungsschutz für Ihre hybriden Umgebungen. Die Hybrid Cloud Security Lösung von Trend Micro, powered by XGen™, bietet folgende Funktionen:

- Umfassende Sicherheitsfunktionen wie Anti-Malware mit Inhaltsfilterung, Verhaltensanalyse, Predictive Machine Learning, hostbasierte Firewall, Eindringungserkennung und -vorbeugung (IDS/IPS), Integritätsüberwachung, Anwendungskontrolle und Protokollinspektion
- Abschirmung von Schwachstellen durch virtuelles Patching, um Anwendungen und Server gegen Schwachstellen zu schützen
- Vertrauenswürdiger Schutz für Docker-Container in allen Umgebungen mit vordefinierten, auf den Host angewendeten Richtlinien zum Schutz der Container
- Flexible Bereitstellung mit Software oder As-a-Service-Angeboten – einfacher Servicebetrieb durch umfassende Mandantenfunktionalität inbegriffen
- Kostensenkung und geringere Komplexität dank enger Integration in VMware, AWS und Azure. Durch eine einzige Plattform für Management und Kontrolle der Sicherheit in physischen, virtuellen und Cloud-Umgebungen wird der Betriebsaufwand reduziert.
- Einfache Verwaltung dank enger Integration in Management-Konsolen von Trend Micro, VMware und Unternehmensverzeichnisse
- Einhaltung wichtiger behördlicher Auflagen im Zusammenhang mit PCI DSS, HIPAA, NIST, SSAE 16 und vielen weiteren Richtlinien

SYSTEM SECURITY PACKAGE

Umfasst Anwendungskontrolle, Integritätsüberwachung und Protokollinspektionsfunktionen

Integritätsüberwachung

Erkennt und meldet bösartige und unerwartete Änderungen an Dateien und System-Registry in Echtzeit

- Überwacht kritische Betriebssystem- und Anwendungsdateien wie Verzeichnisse, Registry-Schlüssel und Werte, um bösartige und unerwartete Änderungen in Echtzeit zu erkennen und zu melden
- Erhöht die Sicherheit virtueller Maschinen mittels agentenloser Konfiguration ohne zusätzliche Systembelastung
- Schützt den Hypervisor mit innovativer Hypervisor-Integritätsüberwachungstechnologie vor Exploits
- Reduziert den Administrationsaufwand durch die Kennzeichnung von vertrauenswürdigen Ereignissen, wodurch Aktionen für ähnliche Ereignisse im gesamten Rechenzentrum automatisch repliziert werden

Anwendungskontrolle

Erkennt und blockiert automatisch nicht autorisierte Software

- Durchsucht eine Maschine und bestimmt, welche Anwendungen derzeit darauf ausgeführt werden
- Riegelt das System ab, sobald der Bestand erstellt wurde, und verhindert so, dass neue Anwendungen ausgeführt werden, bevor sie freigeschaltet wurden
- Wird in eine DevOps-Umgebung integriert, um ständige Änderungen an Anwendungsstapeln zu unterstützen und gleichzeitig Anwendungskontrollschutz mithilfe von APIs zu bewahren
- Fügt eine zusätzliche Schutzebene für Bedrohungen hinzu, für die noch keine Signaturen verfügbar sind, einschließlich einiger Zero-Day-Bedrohungen

Protokollinspektion

Bietet Transparenz hinsichtlich wichtiger Sicherheitsereignisse, die in Protokolldateien gespeichert sind

- Optimiert die Identifizierung wichtiger Sicherheitsereignisse, die in mehreren Protokolleinträgen im Rechenzentrum gespeichert sind
- Leitet verdächtige Ereignisse an ein Sicherheitsinformations- und Ereignismanagement-System (SIEM) weiter oder an einen zentralen Protokollierungsserver zur Korrelation, Berichtserstellung und Archivierung
- Unterstützt und verbessert die bei OSSEC erhältliche Open-Source-Software

ENTERPRISE SECURITY PACKAGE

Das umfassendste Paket, das alle Funktionen von Deep Security enthält – einschließlich Anti-Malware, Inhaltsfilterung, Verhaltensanalyse, Predictive Machine Learning Intrusion Prevention (IPS), Firewall, Integritätsüberwachung, Anwendungskontrolle und Protokollinspektion

- Konsolidiert alle Serversicherheitsfunktionen in einer umfassenden, integrierten und flexiblen Plattform, die den Schutz von physischen, virtuellen und cloudbasierten Servern optimiert
- Beschleunigt Virtualisierungsinvestitionen
- Minimiert die Auswirkungen auf die Serversicherheit
- Deckt bei der Umstellung auf die Cloud die hybriden Sicherheitsanforderungen ab

Tausende Kunden weltweit schützen bereits Millionen Server mit Deep Security, einer Komponente der Hybrid Cloud Security Lösung von Trend Micro, powered by XGen™ Security. Sie stellt marktführende Sicherheitsfunktionen in Form verschiedenster Produktpakete für physische, virtuelle und cloudbasierte Server über eine zentrale, integrierte Plattform bereit.

Weitere Information finden Sie unter **www.trendmicro.com/deepsecurity**.

> Bevor wir zu Trend Micro kamen, mussten wir verschiedene Sicherheitslösungen zusammenfügen und hatten dabei keinen konsolidierten Überblick über die Sicherheit unserer gesamten Systeme. Dank Deep Security können wir jetzt ganz problemlos eine nachweislich sichere Lösung entwickeln und bereitstellen.
>
> **Gerry Miller**
> Gründer und Chief Technologist, Cloudticity

> Seit unserer Umstellung auf Deep Security haben wir jetzt eine integrierte Lösung. Wir verwalten nun einzelne Produkte über einzelne Fenster. Damit können wir die Sicherheitsstufen aller Server von einer zentralen Stelle aus verwalten.
>
> **Sener Sargın**
> Operations Support Manager, Ipragaz

POWERED BY XGEN™ SECURITY

Deep Security ist eine Komponente der Hybrid Cloud Security Lösung von Trend Micro, powered by XGen™.

TREND MICRO™

Securing Your Journey to the Cloud