Trend Micro

HYBRID CLOUD SECURITY

Virtuelle, cloudbasierte, physische und hybride Umgebungen einfach und wirksam schützen

EINFÜHRUNG

Wenn Sie die betrieblichen und wirtschaftlichen Vorteile von Virtualisierung und Cloud-Computing nutzen, dürfen Sie auch einen wirksamen Schutz Ihrer virtuellen Rechenzentren, Cloud-Installationen, hybriden Umgebungen und Container nicht außer Acht lassen. Denn bei Vernachlässigung auch nur eines einzelnen Sicherheitsaspekts kann es in Ihrer Verteidigungslinie zu Lücken kommen, die Bedrohungen Einlass gewähren und zu schwerwiegenden Datenverlusten führen können. Darüber hinaus müssen Sie unabhängig von Ihrer Computing-Umgebung über geeignete Sicherheitsmaßnahmen verfügen, um branchenspezifische und datensicherheitsrelevante Compliance-Anforderungen zu erfüllen.

Trend Micro Hybrid Cloud Security wird durch XGen™ unterstützt und schützt Anwendungen und Daten auf Ihrem Server, verhindert Unterbrechungen im Betriebsablauf und unterstützt Sie darin, schneller regulatorische Compliance zu erreichen. Ganz gleich, ob Sie Anwendungen auf Servern in physischen und virtuellen Umgebungen oder Cloud- und Container-Umgebungen schützen möchten – mit **Trend Micro™ Deep Security™** bietet Trend Micro Ihnen die fortschrittliche Serversicherheit, die Sie für hybride Cloud-Umgebungen benötigen.

Trend Micro ist der **führende Anbieter von Serversicherheit für physische, virtuelle und cloudbasierte Umgebungen**[1]. Wir bieten die umfassendsten Sicherheitsfunktionen kombiniert mit einer automatischen Verwaltung, um Risiken und Kosten deutlich zu reduzieren.

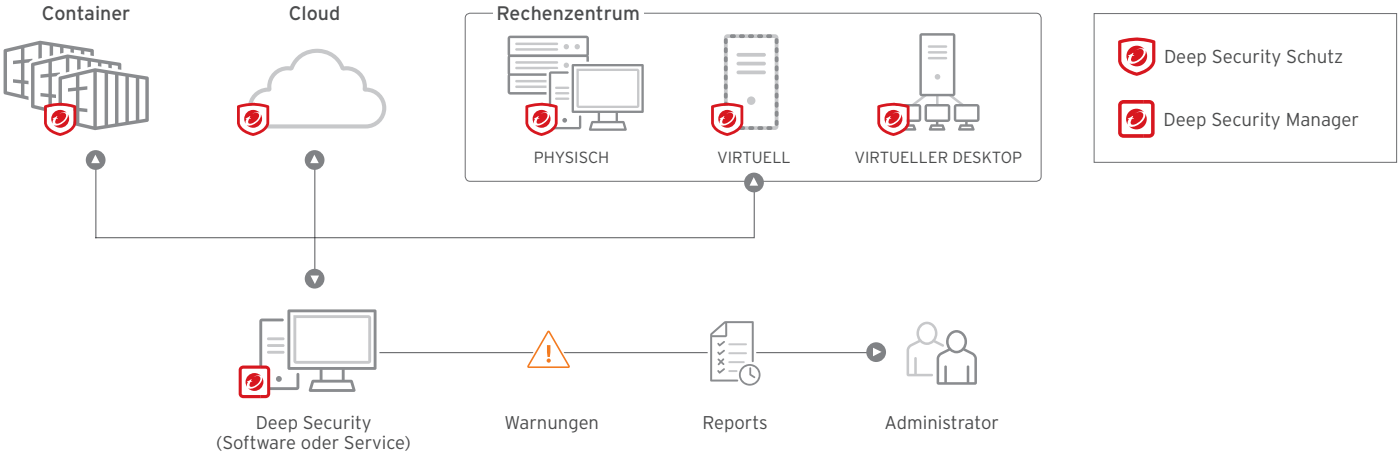
[1] IDC, Worldwide Endpoint Security Market Shares, 2015: Currency Volatility Headwind, #US41867116, November 2016

Gründe für Trend Micro Hybrid Cloud Security

- Schützt physische, virtuelle sowie cloud- und containerbasierte Umgebungen mit zentraler Transparenz und Kontrolle
- Bietet umfassende Sicherheitsfunktionen vom weltweiten Marktführer im Bereich Serversicherheit
- Reduziert die Anzahl der erforderlichen Sicherheitsprodukte, die Sie zum Schutz der hybriden Umgebung und zum Erfüllen der Compliance-Anforderungen benötigen
- Spart Ressourcen ein und senkt Kosten durch automatisierte Richtlinienverwaltung und umgebungsspezifisch optimierten Schutz
- Verfügbar als Software, als Software as a Service (SaaS) oder über die Marketplaces von AWS und Microsoft Azure
- Wird unterstützt durch XGen™ Security, eine generationsübergreifende Kombination aus Sicherheitskontrollen, die für führende Umgebungen optimiert sind

DEEP SECURITY

Deep Security kombiniert mehrere Sicherheitsmethoden in einem Produkt, das die Verteilung und Verwaltung der Sicherheit erheblich beschleunigt und erleichtert. Die Migration aus physischen in virtuelle Umgebungen und in die Cloud wird wesentlich vereinfacht. Die Lösung unterstützt darüber hinaus Microservices-Architekturen und bietet Schutz für Docker-Container. So können Sie Ihr dynamisches Rechenzentrum konsistent und zuverlässig schützen. Deep Security bietet eine zentrale Verwaltung, automatische Servererkennung und Abschirmung von Schwachstellen. Sie sparen damit Zeit und Ressourcen. Durch optimale Integration in Umgebungen wie VMware, AWS und Microsoft Azure wird die Leistung ohne Einbußen bei der Sicherheit maximiert.



TREND MICRO HYBRID CLOUD SECURITY

BEWÄHRTE VIRTUALISIERUNGSSICHERHEIT

Die Trend Micro Hybrid Cloud Security-Lösung, powered by XGen™, schützt Ihre virtuellen Umgebungen – einschließlich VMware Cloud™ on AWS – und macht sie transparenter. Zudem sorgt sie für eine geringere Komplexität und senkt das Risiko beim Verwalten der Sicherheit über mehrere Umgebungen hinweg. Deep Security wurde für das virtualisierte Rechenzentrum optimiert, damit Betriebs- und Sicherheitsteams die Sicherheit bei minimaler Beeinträchtigung der Leistung maximieren können. Profitieren Sie von reduzierten Risiken, weniger Betriebskosten und einer schnellen Reaktion auf Bedrohungen mit automatischer Richtlinienverwaltung, Hypervisor-basierter Sicherheit und zentraler Transparenz und Kontrolle.

AUTOMATISIERTER SCHUTZ FÜR DIE CLOUD

Deep Security schützt Ihre Cloud-Umgebung, indem es die Anforderungen einer gemeinsamen Sicherheitsverantwortung für Installationen in der Cloud erfüllt. Die Lösung bietet flexiblen Schutz für dynamische Workloads in Amazon Web Services (AWS), Microsoft® Azure™, Google Cloud und den Umgebungen anderer CSP. Für Unternehmen, die Microservices mit Containern nutzen, bietet Deep Security außerdem Schutz für Docker-Container, indem der Host-Schutz reibungslos bis auf den Container selbst ausgedehnt wird und ein sicheres und agiles DevOps-Modell ermöglicht.

> „Ich habe Deep Security selbst installiert und für die Installation auf 100 virtuellen Maschinen weniger als einen Tag gebraucht. Dabei ist unsere Arbeitsspeicherauslastung über Nacht um 27 % gesunken.“

Nick Casagrande
IT-Leiter
Southern Waste Systems LLC
Florida, USA

SICHERHEIT FÜR DAS MODERNE RECHENZENTRUM

Die marktführende Sicherheit von Trend Micro schützt virtuelle Desktops und Server, Cloud-Umgebungen, Docker-Container und hybride Architekturen vor Zero-Day-Malware, einschließlich Ransomware, sowie komplexen Bedrohungen. Gleichzeitig reduziert sie Beeinträchtigungen von Betriebsabläufen, die durch Sicherheitsvorgänge und Notfall-Patching entstehen können.

Automatische Bereitstellung umfassender Sicherheitsfunktionen im Rechenzentrum

Um die Virtualisierungsvorteile nutzen und effizient arbeiten zu können, muss im Rahmen des Bereitstellungsprozesses des Rechenzentrums eine speziell für virtuelle Umgebungen entwickelte Sicherheitslösung automatisiert werden. Trend Micro stellt nicht nur sicher, dass physische Server und virtuelle Maschinen (VMs) direkt nach ihrer Bereitstellung geschützt sind, sondern empfiehlt und verwendet auch nur die jeweils relevanten Richtlinien. Deep Security passt sich an dynamische Umgebungen mit virtuellen und cloudbasierten Szenarien an, indem es die Installation und Deinstallation von VMs automatisch verfolgt und den angemessenen Schutz bereitstellt.

Deep Security bietet die folgenden Funktionen:

- Malware-Schutz mit Web-Reputation-Technologie, Machine Learning-Prognosen und Sandbox-Analyse-Integrationsunterstützung zur Abwehr von Malware-Angriffen, einschließlich Ransomware und Angriffen wie WannaCry und Erebus
- Netzwerksicherheit, einschließlich Erkennung und Vermeidung von Eindringlingen (IDS/IPS) zur Abschirmung ungepatchter Schwachstellen sowie einer Stateful-Firewall zur Bereitstellung einer anpassbaren Firewall für jeden einzelnen Server
- Systemsicherheit, einschließlich Überwachung von Datei- und Systemintegrität zu Compliance-Zwecken, Applikationskontrolle für mehrere Plattformen zum Schutz von Servern und zur Vermeidung von Ransomware sowie Log-Überprüfung zur Erkennung wichtiger Sicherheitsereignisse und Erstellung entsprechender Berichte

Optimierung der Ressourcen im Rechenzentrum

Mit der Integration auf Hypervisor-Ebene über VMware NSX verfolgt Deep Security einen optimierten Ansatz für Virtualisierungssicherheit. Die Lösung wird automatisch und ohne Ausfallzeiten installiert. Es muss also kein separater Agent auf jeder virtuellen Maschine installiert und verwaltet werden. Einzelne Server und VMs werden dadurch nicht mit Signaturbibliotheken und Erkennungsengines überladen, was die Bereiche Verwaltung, Netzwerkauslastung, Suchlaufgeschwindigkeit, hostweite CPU- und Arbeitsspeicherauslastung, Input-/Output-Operationen pro Sekunde (IOPS) und Gesamtspeichernutzung erheblich verbessert.

Dieser zentralisierte Ansatz ermöglicht den Einsatz eines hocheffizienten Scan Caches, der doppelte Scanvorgänge auf ähnlichen VMs unnötig macht. Damit wird die Leistung erheblich verbessert. Vollständige Suchen werden bis zu 20-mal und Echtzeitsuchen bis zu 5-mal schneller ausgeführt. Anmeldungen an einer VDI werden ebenfalls beschleunigt.

Um die Provisionierung weiter zu vereinfachen, machen sich die Trend Micro Lösungen außerdem die Vorteile neuester VMware Plattforminnovationen wie NSX und VMware Cloud on AWS zunutze. Die Integration in VMware NSX ermöglicht den automatischen Schutz neuer virtueller Maschinen direkt nach deren Einrichtung sowie die automatische Bereitstellung geeigneter Sicherheitsrichtlinien und den Schutz vor Sicherheitslücken. Dank der einzigartigen Integration von Trend Micro Produkten in vRealize Operations Management haben Unternehmen über ein zentrales Dashboard Einblick in Rechenzentrumsabläufe und -sicherheit.

Effiziente Verwaltung der Sicherheitslösung auch beim Wechsel auf neue Umgebungen

Die Sicherheitsverwaltung über ein zentrales Dashboard ist einfach und ermöglicht eine kontinuierliche Überwachung mehrerer Kontrollen für physische, virtuelle und cloudbasierte Umgebungen. Zuverlässiges Reporting und Warnfunktionen unterstützen Sie dabei, sich auf wirklich wichtige Ereignisse zu konzentrieren, sodass Sie Probleme schnell erkennen und entsprechend reagieren können. Durch eine einfache Integration in andere Systeme wie Security Information and Event Management (SIEM) kann die Sicherheitsverwaltung ganz leicht in andere Rechenzentrumsabläufe eingegliedert werden. Dank der Integration in NSX wird die Sicherheit zentral verwaltet. Damit entfällt die manuelle Aktualisierung von Agenten – eine besonders schwierige Aufgabe bei schneller Skalierung. Das Dashboard beinhaltet unter anderem Daten aus Cloud-Umgebungen wie AWS, Microsoft Azure und Google Cloud, sodass Sie all Ihre Server unabhängig vom Standort problemlos über ein zentrales Tool verwalten können. Die Unterstützung von Microservices-Architekturen und Containern ermöglicht Ihnen eine sichere und dynamische Weiterentwicklung Ihres Rechenzentrums.

Optimiert für:

vmware®

amazon web services

Microsoft Azure

> „Deep Security war genau die richtige Wahl für unser Rechenzentrum und bietet hervorragenden Schutz für unsere virtualisierten Server und Desktops sowie unsere ständig im Wandel begriffene Umgebung. Ich bin begeistert!“

Orinzal Williams
Geschäftsführer
United Way of Atlanta
Georgia, USA

AUTOMATISIERTE SICHERHEIT FÜR DIE CLOUD

Der Wechsel in die Cloud vollzieht sich aufgrund damit verbundener Kosteneinsparungen sowie Agilitäts- und Effizienzsteigerungen mit wachsender Geschwindigkeit. Bei der Migration Ihrer IT-Infrastruktur in die Cloud müssen Sie nach dem Modell der geteilten Verantwortung jedoch sicherstellen, dass von Ihnen in die Cloud verschobene Workloads geschützt sind und Ihre Sicherheitslösung interne und behördliche Compliance-Vorgaben erfüllt.

Deep Security wurde für führende Cloud Service Provider (CSPs), darunter AWS, Microsoft Azure und Google Cloud, optimiert. Die Lösung vereinfacht den Einsatz führender Orchestrierungstools wie Chef, Puppet, SaltStack, Ansible und AWS Opworks durch die Bereitstellung von Installationsbeispielen und eine automatische Generierung von Richtlinienskripts, mit denen Sicherheit als Teil des Cloud-Betriebs verwaltet werden kann.

Verhindert Datenverlust und Unterbrechungen im Geschäftsablauf

Die branchenführenden Sicherheitsfunktionen von Trend Micro, mit denen bereits Tausende Kunden weltweit Millionen Server schützen, helfen Unternehmen:

- sich mithilfe bewährter Host-basierter Netzwerksicherheitskontrollen, z. B. Erkennung und Abwehr von Eindringlingen (IDS/IPS), vor Netzwerk- und Anwendungsbedrohungen zu schützen
- sich vor Sicherheitslücken zu schützen – die Lösungen schirmen unzureichend geschützte Anwendungen und Server umgehend mit einem virtuellen Patch ab, bis betroffene Workloads ersetzt werden können
- den Zugriff auf Server zu sperren, sodass mithilfe von Applikationskontrollen für Windows und Linux nur zulässige Prozesse ausgeführt werden können
- Workloads vor Malware wie Ransomware zu schützen und sicherzustellen, dass Server und Anwendungen sicher sind
- verdächtige Änderungen auf Servern zu identifizieren, darunter Änderungen an Registrierungseinstellungen, Systemordnern und Anwendungsdateien, die nicht geändert werden dürfen

Reduziert Betriebskosten

Trend Micro stellt fortschrittliche Serversicherheit für Cloud-Workloads bereit und verwaltet gleichzeitig den Schutz auf virtuellen und physischen Servern im Rechenzentrum.

Die integrierte Verwaltungskonsole bietet eine zentrale, aktuelle Übersicht über das Sicherheitsprofil Ihrer gesamten Cloud-Umgebung und spart durch eine effizientere Sicherheitsverwaltung Zeit und Ressourcen. Automatische Abschirmung von Schwachstellen verhindert Betriebsunterbrechungen durch Notfall-Patches.

Die enge Integration von Deep Security in AWS und Azure ermöglicht es Ihnen, Workloads zu erkennen und Sicherheit entsprechend zu verteilen. Dazu gehört auch, anpassbare Richtlinienvorlagen auf Basis von Instanz-Metadaten durchzusetzen, damit alle Richtlinien automatisch auf die Server angewendet werden, für die sie vorgesehen sind.

BESCHLEUNIGTE COMPLIANCE FÜR HYBRIDE CLOUDS

Compliance-Anforderungen im Zusammenhang mit wichtigen Richtlinien wie PCI DSS, HIPAA, NIST, SSAE-16 und GDPR gelten für das gesamte Rechenzentrum und die Cloud. Deep Security unterstützt Sie dabei durch folgende Leistungsmerkmale:

- **Detaillierte, Audit-fähige Reports**, die abgeschirmte Schwachstellen, erkannte Angriffe und den Status der Compliance anzeigen
- **Weniger Vorbereitungszeit und -aufwand**, zur Unterstützung von Audits durch zentrale Sicherheitskontrollen und konsolidierte Berichte
- **Unterstützung interner Compliance-Initiativen**, um die Transparenz interner Netzwerkaktivitäten zu verbessern
- **Bewährte Technologie**, die nach Common Criteria EAL2 zertifiziert ist

Weitere Informationen zu Funktionen von Hybrid Cloud Security oder zu verfügbaren Testversionen erhalten Sie unter
http://www.trendmicro.de/grossunternehmen/hybrid-cloud-security/index.html

Verfügbar unter: awsmarketplace Microsoft Azure

Trend Micro Hybrid Cloud Security wird unterstützt durch XGen™, unseren intelligenten, optimierten und vernetzten Sicherheitsansatz.

POWERED BY XGen™ SECURITY

> „Unternehmen sind mit ständig wachsenden und dynamischen Internetbedrohungen konfrontiert. Deep Security wehrt Bedrohungen ab und sichert damit das Onlineerlebnis unserer Kunden. Dies schützt sowohl unseren guten Ruf als auch den unserer Kunden."

Todd Redfoot
Chief Information Security Officer (CISO) bei Go Daddy

TREND MICRO™

Securing Your Journey to the Cloud