Trend Micro

CLOUD AND DATA CENTER 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 und hybriden Umgebungen nicht außer Acht lassen. Denn bei Vernachlässigung nur eines einzelnen Sicherheitsaspekts kann es zu Sicherheitslücken kommen, die Internetbedrohungen Einlass gewähren und zu schwerwiegenden Datenverlusten führen können. Darüber hinaus müssen Sie unabhängig von Ihrer Computing-Umgebung über geeignete Sicherheitsmaßnahmen verfügen, um geltende Compliance- und Datenschutzvorgaben einzuhalten.

Trend Micro Cloud and Data Center Security Lösungen schützen Anwendungen und Daten, verhindern Unterbrechungen im Betriebsablauf und stellen gleichzeitig die Einhaltung von Compliance-Anforderungen sicher. Ganz gleich, ob Sie physische oder virtuelle Umgebungen, Cloud-Instanzen oder Webanwendungen schützen möchten – mit der Trend Micro™ Deep Security Plattform bietet Trend Micro Ihnen die fortschrittliche Serversicherheit, die Sie für derartige Umgebungen benötigen.

Gründe für Trend Micro Sicherheitslösungen für Clouds und Rechenzentren

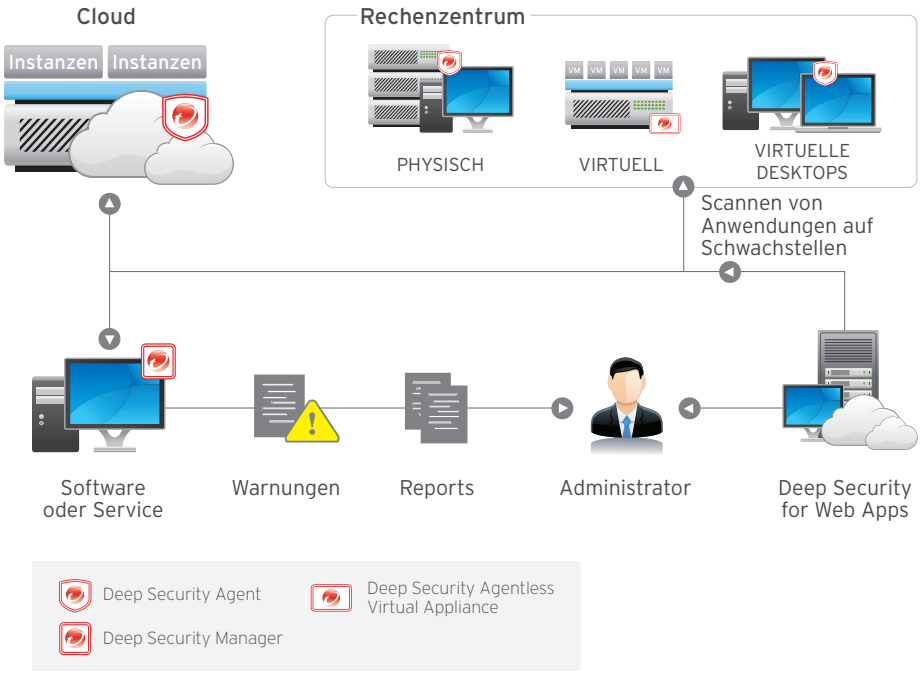
- Schützt physische, virtuelle und cloudbasierte Umgebungen mit einer umfassenden Lösung
- Bietet umfassende Sicherheitsfunktionen vom weltweiten Marktführer im Bereich Serversicherheit
- Spart Ressourcen ein und senkt Kosten durch automatische Richtlinienverwaltung und Lifecycle Management mit optimierter Sicherheit
- Verfügbar als Software oder Software as a Service (SaaS)-Option mit zentraler Verwaltung für hybride Umgebungen

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 drastisch zu reduzieren.

[1] IDC Worldwide Endpoint Security 2013-2017 Forecast and 2012 Vendor Shares, Abbildung 2, doc #242618, August 2013

DEEP SECURITY PLATTFORM

Beim Wechsel von physischen und virtuellen Umgebungen in die Cloud werden Verwaltungs- und Installationsprozesse durch eine zentrale, umfassende Sicherheitslösung erheblich vereinfacht und beschleunigt. Zentrale Verwaltung und Abschirmung von Schwachstellen sparen Zeit und Ressourcen. Darüber hinaus trägt unsere agentenlose Architektur durch Optimierung virtueller Server und Verbesserung der Leistung zu einer beschleunigten Rendite bei.



„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

TREND MICRO SICHERHEITSLÖSUNGEN FÜR CLOUDS UND RECHENZENTREN

BEWÄHRTE VIRTUALISIERUNGSSICHERHEIT

Optimierte Sicherheit für moderne Rechenzentren unterstützt Betreiber und Architekten von Rechenzentren dabei, Betriebskosten unter Kontrolle zu halten und gleichzeitig die Leistung durch eine Sicherheitslösung zu steigern, die für virtuelle Umgebungen optimiert wurde. Reduzieren Sie Risiken und Kosten und sparen Sie Zeit durch automatische Richtlinienverwaltung, agentenlosen Betrieb und eine zentrale Verwaltung.

FLEXIBLE CLOUD-SICHERHEIT

Sofortschutz für die Cloud unterstützt Cloud-Architekten darin, bei der Installation vertraulicher Anwendungen in der Cloud die Anforderungen einer gemeinsamen Sicherheitsverantwortung zu erfüllen. Nutzen Sie flexiblen Schutz für dynamische Arbeitsabläufe in Amazon Web Services (AWS), Microsoft Azure und VMware vCloud.

SICHERHEIT FÜR WEBANWENDUNGEN

Kontinuierlicher Schutz für Webanwendungen hilft IT-Verantwortlichen, vertrauliche Transaktionen und Daten in externen Webanwendungen ohne störende Fehlalarme zu schützen. Schwachstellensuchen für Plattformen und Anwendungen kombiniert mit Tests durch Sicherheitsexperten schützen Anwendungen vor raffinierten Angriffen.

„Ich habe Deep Security selbst installiert und für die Installation auf 100 virtuellen Maschinen weniger als einen Tag gebraucht. Über Nacht konnte ich beobachten, wie unsere Arbeitsspeicherauslastung um 27 % sank."

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

OPTIMALE SICHERHEIT FÜR DAS MODERNE RECHENZENTRUM

Die marktführende Sicherheit von Trend Micro schützt virtuelle Desktops und Server sowie cloudbasierte und hybride Architekturen vor Zero-Day-Malware und anderen Bedrohungen. Gleichzeitig reduziert sie Beeinträchtigungen von Betriebsabläufen, die durch Ressourcenengpässe 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 an, indem es die Installation und Deinstallation von VMs automatisch verfolgt.

Deep Security bietet die folgenden Funktionen:

- Malware-Schutz mit Web Reputation zum Schutz vor häufig verwendeten Infektionsquellen
- Überwachung von Datei- und Systemintegrität zu Compliance-Zwecken
- Erkennung und Abwehr von Eindringlingen zur Abschirmung von ungepatchten Schwachstellen
- Stateful-Firewall zur Bereitstellung einer anpassbaren Firewall für jeden einzelnen Server
- Logüberprüfung zur Erkennung wichtiger Sicherheitsereignisse und Erstellung entsprechender Berichte

Optimierung der Ressourcen im Rechenzentrum

Deep Security bietet einen besseren Sicherheitsansatz mit agentenlosem Schutz. Durch die Installation auf Hypervisor-Ebene muss nicht auf jeder VM ein separater Agent installiert und verwaltet werden. Einzelne Server und VMs werden dadurch nicht mit Signaturbibliotheken und Erkennungs-engines überladen, was die Bereiche Verwaltung, Netzwerk-auslastung, Suchlaufgeschwindigkeit, hostweite CPU- und Arbeitsspeicherauslastung, Input-/Output-Operationen pro Sekunde (IOPS) und Gesamtspeicher erheblich verbessert.

Zudem ermöglicht diese zentrale Architektur einen Such-Cache. Der Such-Cache verhindert doppelte Suchen auf ähnlichen VMs und kann so die Leistung ganz erheblich verbessern. Vollständige Suchen werden bis zu 20-mal und Echtzeitsuchen bis zu 5-mal schneller ausgeführt. Anmeldungen an VDI werden ebenfalls beschleunigt. Auch VDI-Sicherheit wird durch die agentenlose Architektur maximiert und stellt sicher, dass die Leistung virtueller Desktops und des zugrunde liegenden Hosts nicht durch die zusätzliche Systembelastung eines Sicherheits-agenten beeinträchtigt wird.

Um die Bereitstellung weiter zu vereinfachen, nutzen Trend Micro Lösungen außerdem die Vorteile neuester VMware Plattforminnovationen. Die enge Integration von Trend Micro Produkten in VMware ermöglicht den automatischen Schutz neuer virtueller Maschinen direkt nach deren Einrichtung sowie die automatische Bereitstellung geeigneter Sicherheits-richtlinien – und das alles ohne die Installation eines Agenten. Dies ist eine weitere wichtige Methode zur Vermeidung von Sicherheitslücken.

Der agentenlose Ansatz wird in der neuen NSX-Plattform von VMware weiter fortgesetzt, damit Unternehmen bei der Migration auf die neue Architektur die beschriebenen Leistungs-vorteile weiter nutzen können.

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. Stabile Bericht- 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 z. B. SIEM kann die Sicherheitsverwaltung ganz leicht in andere Rechenzentrumsabläufe eingegliedert werden. Alle Kontrollen werden über eine zentrale virtuelle Appliance verwaltet, sodass die manuelle Aktualisierung von Agenten – eine besonders schwierige Aufgabe bei schneller Skalierung – entfällt. Das Dashboard beinhaltet Daten aus Cloud-Umgebungen wie Amazon Web Services (AWS), Microsoft Azure und VMware vCloud, sodass Sie all Ihre Server unabhängig vom Standort problemlos über ein zentrales Tool verwalten können.

Kosteneffiziente Compliance

Die wichtigsten Anforderungen für PCI DSS 3.0 sowie HIPAA, NIST und SAS 70 werden durch folgende Elemente erfüllt:

- **Detaillierte, prüffähige Reports**, die abgeschirmte Schwach-stellen, erkannte Angriffe und den Status der Compliance anzeigen
- **Weniger Vorbereitungszeit und -Aufwand** um Audits durch zentrale Sicherheitskontrollen und konsolidierte Berichte zu unterstützen
- **Unterstützung interner Compliance-Initiativen**, um die Sichtbarkeit von internen Netzwerkaktivitäten zu verbessern
- **Bewährte Technologie**, die nach Common Criteria EAL 4+ zertifiziert ist
- **Datensicherheit** mit FIPS 140-2-validierter Verschlüsselung bietet maximalen Datenschutz und sichere Funktionen zur Datenvernichtung

SOFORTSCHUTZ FÜR DIE CLOUD

Der Wechsel in die Cloud vollzieht sich aufgrund damit verbundener Kosteneinsparungen, Agilität und anderer Vorteile zunehmend schneller. Bei der Migration Ihrer IT-Infrastruktur in die Cloud müssen Sie nach dem Modell der geteilten Verantwortung jedoch sicherstellen, dass Sie eine geeignete Sicherheitslösung implementieren, die interne und behördliche Compliance-Vorgaben erfüllt.

Der Sofortschutz für Cloud-Umgebungen von Trend Micro wurde für führende Cloud-Service-Provider (CSPs) einschließlich AWS, Microsoft Azure und VMware vCloud optimiert. Dank schneller und einfacher Integration in CSP-Architekturen ist unser Sofortschutz effizient und flexibel, sodass Sie die Agilitäts- und Kostenvorteile der Cloud vollständig nutzen können. Durch Kompatibilität mit führenden Tools zur Verteilung in der Cloud wie Chef, Puppet, RightScale, OpsWorks, Salt etc. lässt sich unsere Sicherheit direkt in Ihre bestehenden flexiblen Umgebungen integrieren.

Mit dem Trend Ready für Cloud-Service-Provider-Programm können Sie ganz sicher sein, dass Trend Micro Schutz mit Ihrem CSP kompatibel ist. Trend Micro zeichnet Cloud-Service-Provider mit dem Status „Trend Ready" aus, sobald die Installation, die Aktivierung sowie das reibungslose Funktionieren von Trend Micro Deep Security und SecureCloud innerhalb der Betriebsumgebungen des Cloud-Service-Providers erfolgreich überprüft wurden.

Verhindert Datenverlust und Unterbrechungen im Geschäftsablauf

Tausende Kunden schützen bereits Millionen Server mit dem Sofortschutz für Cloud-Umgebungen von Trend Micro und profitieren von folgenden umfassenden Sicherheitsfunktionen:

- Schwachstellenerkennung durch das Durchsuchen von Anwendungen
- Malware-Schutz mit Web Reputation zum Schutz vor häufig verwendeten Infektionsquellen
- Überwachung von Datei- und Systemintegrität zu Compliance-Zwecken
- IDS/IPS zur Abschirmung von ungepatchten Schwachstellen
- Stateful-Firewall, um für jeden Server eine anpassbare Firewall bereitzustellen
- Logüberprüfung zur Erkennung wichtiger Sicherheitsereignisse
- Verschlüsselung zum Schutz vertraulicher Daten bei der Übertragung und im Speicher

Reduziert Betriebskosten

Der Sofortschutz für Cloud-Umgebungen von Trend Micro stellt fortschrittliche Server-sicherheit für Cloud-Instanzen 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 Ressourcenkosten. Automatische Abschirmung von Schwachstellen verhindert Betriebsunterbrechungen durch Notfall-Patches.

AutoSync ermöglicht es außerdem, anpassbare Richtlinienvorlagen auf Basis von Instanz-metadaten durchzusetzen, damit alle Richtlinien automatisch auf die Server angewendet werden, für die sie vorgesehen sind.

Kosteneffiziente Compliance

Die wichtigsten Anforderungen für PCI DSS 3.0 sowie HIPAA, NIST und SAS 70 werden durch folgende Elemente erfüllt:

- **Detaillierte, prüffähige Reports**, die abgeschirmte Schwachstellen, erkannte Angriffe und den Status der Compliance anzeigen
- **Weniger Vorbereitungszeit und -Aufwand** um Audits durch zentrale Sicherheits-kontrollen und konsolidierte Berichte zu unterstützen
- **Unterstützung interner Initiativen zur Compliance**, um die Sichtbarkeit von internen Netzwerkaktivitäten zu verbessern
- **Bewährte Technologie**, die nach Common Criteria EAL 4+ zertifiziert ist
- **Datensicherheit** mit FIPS 140-2-validierter Verschlüsselung bietet maximalen Daten-schutz und sichere Funktionen zur Datenvernichtung
- **Umfassende Funktionen** ermöglichen es, die Anzahl unterschiedlicher Sicherheitslösungen zu verringern

> „Unternehmen sind mit ständig wachsenden und dynamischen Internetbedrohungen konfrontiert. Deep Security wehrt Bedrohungen ab und schützt 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

> „Wir schätzen sowohl die Möglichkeit zur separaten Implementierung von Malware-Schutz-funktionen auf jedem einzelnen Server als auch die umfassenden Sicherheitsfunktionen von Deep Security, wie z. B. die Erkennung und Abwehr von Eindringlingen oder das virtuelle Patching."

Shuichi Hiraki
Associate Manager
Infrastruktur, Informationssysteme
Astellas Pharma Inc.

KONTINUIERLICHER SCHUTZ FÜR WEBANWENDUNGEN

Internetbedrohungen konzentrieren sich zunehmend auf das gezielte Angreifen von Anwendungen und den unberechtigten Zugriff auf wertvolle Daten. Diese Anwendungen werden immer häufiger nicht nur im Rechenzentrum, sondern auch in der Cloud gespeichert, was den Sicherheitsaufwand weiter erhöht. Schwachstellen müssen erkannt und sofort abgeschirmt werden, damit Ihre Anwendungen und Daten umfassend geschützt sind. Wenn Sicherheitslücken erst durch die Auswirkungen eines erfolgreichen Angriffs erkannt werden, ist es bereits zu spät.

Erkennung und Abschirmung von Schwachstellen

Trend Micro Deep Security for Web Apps bietet intelligentes Durchsuchen von Anwendungen in der komplexen Bedrohungsumgebung von heute. Mit automatischen Scans und praktischen Tests durch Sicherheitsexperten schützt diese umfassende Lösung Webanwendungen kontinuierlich vor hochkomplexen Angriffen, ohne das Sicherheitsteam durch Fehlalarme zu belasten.

Unterstützung bei der PCI-Richtlinieneinhaltung durch integrierte Erkennung und Sicherheitsfunktionen

Mithilfe integrierter Schutzmaßnahmen wie IPS werden Schwachstellen direkt nach ihrer Erkennung vor potentiellen Angriffen abgeschirmt. Kontinuierliches Suchen und Abschirmen von Schwachstellen trägt zur PCI-Compliance bei.

Bei Erkennung von Schwachstellen in Anwendungen werden zudem native Web Application Firewall (WAF)-Regeln erstellt, um einen einfachen Import in eine bereits installierte WAF zu ermöglichen. Diese Regeln bieten Ihnen Schutz vor Angriffen auf Anwendungen, bevor Sie Code- und Konfigurationsfehler beheben können.

Unbegrenzte SSL-Zertifikate

Deep Security for Web Apps unterstützt Sie bei der Erfüllung von SSL-Anforderungen und überwindet Kostenhürden durch den Einsatz der erforderlichen SSL-Zertifikate zum Schutz von Onlinetransaktionen in Zusammenarbeit mit einem weltweit vertrauenswürdigen Sicherheitspartner. Sie können unbegrenzte SSL-Zertifikate einschließlich Extended Validation (EV)-Zertifikate kostengünstig verwenden.

Trend Micro Sicherheitslösungen für Clouds und Rechenzentren schützen Ihre Anwendungen und Daten, verhindern Unterbrechungen im Betriebsablauf und stellen gleichzeitig die Einhaltung von Richtlinien sicher. Ganz gleich, ob Sie physische oder virtuelle Umgebungen, Cloud-Instanzen oder Webanwendungen schützen möchten – mit der Trend Micro™ Deep Security Plattform bietet Trend Micro Ihnen die fortschrittliche Serversicherheit, die Sie für virtuelle, cloudbasierte oder physische Server benötigen.

Die Trend Micro Deep Security Plattform stellt einen besonders effizienten agentenlosen und agentenbasierten Schutz für physische, virtuelle und cloudbasierte Server bereit. Die Lösung greift auf der Hypervisor-Ebene und ermöglicht damit eine maximale Effizienz. Ihre virtuellen Server und virtuellen Desktopinfrastrukturen (VDI) werden durch agentenlose Sicherheit geschützt, ganz ohne den Aufwand von Endpunktinstallationen. Deep Security wurde für führende Virtualisierungslösungen und Cloud-Service-Provider-Architekturen wie **Amazon Web Services**, **Microsoft Azure** und **VMware vCloud** optimiert.

Weitere Informationen zu unseren Sicherheitslösungen für Clouds und Rechenzentren oder zu verfügbaren Testversionen erhalten Sie unter http://www.trendmicro.de/grossunternehmen/cloud-sicherheit-und-schutz-von-rechenzentren/index.html

> „Trend Micro Deep Security for Web Apps bietet uns einen besseren Überblick über unsere Schwachstellen und ermöglicht es uns, diese Probleme schneller anzugehen und unsere IT-Maßnahmen gezielter und effizienter zu gestalten."

Mark Dunkerley
Team-Leiter, Messaging- und Domain-Services
Adventist Health System Information Services

TREND MICRO™

Securing Your Journey to the Cloud