



# Virtualisierung der Sicherheit am E-Mail-Gateway

*Flexibler, kosteneffizienter  
Schutz am E-Mail-Gateway*

*August 2009*





# VIRTUALISIERUNG DER SICHERHEIT AM E-MAIL-GATEWAY

## I. KOSTEN UND KOMPLEXITÄT TREIBEN DEN AUSBAU VON VIRTUALISIERUNG VORAN

Virtualisierungsprojekte gewinnen zunehmend an Bedeutung, da Unternehmen angesichts von Konjunkturschwäche und steigender Energiekosten nach Möglichkeiten suchen, Kosten und Komplexität ihrer Betriebsabläufe zu senken. In vielen Unternehmen werden umweltfreundliche IT-Entwicklungen eingeführt, um die Auswirkungen gestiegener Kosten auf den Gesamtumsatz des Unternehmens zu reduzieren. Gleichzeitig erfordern immer komplexere IT-Infrastrukturen immer mehr Verwaltungsaufwand und Ressourcen, die ohnehin knapp sind. Virtualisierung bietet Unternehmen eine Möglichkeit, diese Anforderungen zu erfüllen.

### **STEIGENDE ENERGIEKOSTEN**

Datenzentren verbrauchen heute fast ein Prozent der weltweit erzeugten Energiemenge, und bis 2020 wird sich der Verbrauch voraussichtlich vervierfachen. Strom macht heute mindestens 25 % der IT-Kosten eines Großunternehmens aus (Revolutionizing Datacenter Efficiency, McKinsey & Company Uptime Institute Symposium), und da wichtige Unternehmensanwendungen jederzeit einsatzbereit sein müssen, wird sich dieser Prozentsatz wahrscheinlich noch erhöhen. Auch wenn der Stromverbrauch von Datenzentren auf dem jetzigen Stand bleibt, werden die Kosten drastisch zunehmen, da die Nachfrage weltweit explosionsartig steigt und sich als Reaktion darauf die Kraftstoffpreise für beispielsweise Kohle oder Erdgas erhöhen.

### **HARDWARE-MÜDIGKEIT**

Da die Infrastruktur in den vergangenen Jahren immer komplexer geworden ist, haben viele IT-Unternehmen auf jedes neue Problem mit einer neuen Lösung reagiert. Sie wurden durch die gewaltige Zunahme von Hardware-Appliances zur Lösung individueller Probleme geradezu überschwemmt. Verteilung und Verwaltung neuer Server oder dedizierter Hardware-Appliances für jede dieser Anwendungen führt zu einem weiteren Anstieg von Kosten und Komplexität bei der Wartung des Datenzentrums. Zusätzlich zum erhöhten Platzbedarf in den Server-Racks sind die unzähligen Server und Hardware-Appliances mit unterschiedlichen Benutzeroberflächen für IT-Unternehmen aufwändig zu verwalten.

### **KOMPLEXE SERVERUMGEBUNGEN**

Herkömmliche Serververteilungen erfordern in der Regel einen langwierigen Kreislauf aus Beschaffung, Installation, Konfiguration, Testen und Verteilung, der es einem Unternehmen erschwert, wichtige Anwendungen zu installieren. Gleichzeitig werden nur wenige Server vollständig genutzt, so dass die Gesamtbetriebskosten steigen. Virtuelle Maschinen sind effizienter und können einfacher als physische Server und herkömmliche Software verteilt und installiert werden.



# VIRTUALISIERUNG DER SICHERHEIT AM E-MAIL-GATEWAY

## II. VIRTUALISIERUNG AUF MEHR FUNKTIONEN DES DATENZENTRUMS AUSWEITEN

Deutlich geringere Anschaffungs- und Betriebskosten sind überzeugende Gründe, den Schritt in Richtung Virtualisierung zu wagen. Die Übernahme einer einfachen, virtualisierten Infrastruktur kann die jährlichen Serverkosten pro Benutzer im Vergleich zu physischen, statischen x86-Serverkonfigurationen um bis zu 35 % senken. Infrastrukturen mit mehr als 25 % Virtualisierung, Speichervirtualisierung und Tools zur Systemverwaltung ermöglichen Kosteneinsparungen von bis zu 52 % pro Benutzer und Jahr (IDC, Business Value of Virtualization: Realizing the Benefits of Integrated Solutions, Juli 2008).

Daher wird das Konzept der Virtualisierung ausgedehnt: Von Servern, die nur Unternehmens- und Webanwendungen hosten, auf andere Funktionen des Datenzentrums, wie z. B. Netzwerk-Gateway-Sicherheitslösungen.

### WAS SIND VIRTUELLE APPLIANCES?

Eine virtuelle Appliance besteht aus einem vorinstallierten, vorkonfigurierten Betriebssystem und einem Application Stack, die als Einheit gefertigt, verteilt und gewartet, aktualisiert und verwaltet wird. Als vorgefertigte Einheit vereinfacht sie Verteilung und Administration, da automatische Patches und Updates durch einen einzelnen Anbieter erfolgen. Weil virtuelle Appliances keine zusätzliche Energie, Kühlung oder Hardware benötigen, können sie zusätzliche Funktionalität bieten, die sich nicht – oder kaum – auf die Umwelt auswirkt. Unternehmen implementieren virtuelle Appliances wegen einer Vielzahl von Funktionen – von Business Intelligence und Dokumentenverwaltung bis hin zu Backups, Netzwerküberwachung, Anwendungsentwicklung und Sicherheit.

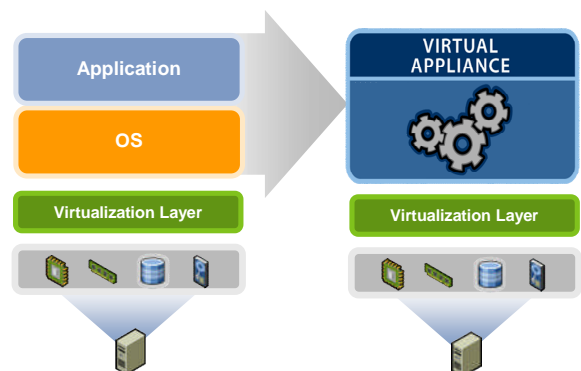


Abbildung 1: Eine virtuelle Appliance besteht aus einer Anwendung und einem Betriebssystem als einheitliche Lösung

### WARUM VIRTUELLE APPLIANCES ALS SICHERHEITSANWENDUNGEN AM E-MAIL-GATEWAY?

E-Mail-Sicherheit eignet sich besonders gut für die Kosteneinsparungen und Effizienzsteigerungen, die mit der Verteilung einer virtuellen Appliance verbunden sind. E-Mails sind aus dem Unternehmensalltag nicht mehr wegzudenken. Daher planen laut IDC 60 % der Unternehmen, ihre Ausgaben für E-Mail-Sicherheit auch in wirtschaftlich schwierigen Zeiten zu erhöhen. Ein Ende der Spam-Flut ist nicht in Sicht, so dass physische Server schnell überlastet und Verwaltungsressourcen strapaziert werden. Wegen extremer Schwankungen des Spam-Aufkommens lassen sich keine verlässlichen Aussagen über zukünftig erforderliche Serverkapazitäten treffen. Unternehmen sind vor die schwierige Wahl gestellt, entweder außerplanmäßig in zusätzliche Kapazitäten zu investieren, um die negativen Auswirkungen großer Spam-Mengen abzufangen, oder schwächere Leistung und unzufriedene Benutzer in Kauf zu nehmen.



## VIRTUALISIERUNG DER SICHERHEIT AM E-MAIL-GATEWAY

Viele Unternehmen planen den Einsatz virtueller Appliances, um ihre Sicherheitsziele am E-Mail-Gateway zu erreichen. Nach Schätzungen von Osterman Research werden bis zum Jahr 2010 bis zu 39 % der Antiviren- und Anti-Spam-Server virtualisiert sein (Why You Need to Consider Virtualization, September 2008). Außerdem planen laut IDC 34 % der Unternehmen, in den kommenden 12 Monaten virtuelle Sicherheitsappliances zur E-Mail-Sicherheit einzusetzen. Große Unternehmen (mit mindestens 10.000 Mitarbeitern) sind hierbei mit einem Anteil von 48 % deutlich in der Mehrzahl (IDC-Umfrage zu Messaging-Sicherheit: The Good, Bad, and Ugly, Februar 2009). Außerdem stellen virtuelle Sicherheitsappliances eines der am schnellsten wachsenden Segmente im Messaging-Sicherheitsmarkt dar: Mit einem Wachstum von 17 Millionen Dollar im Jahr 2008 auf 525 Millionen Dollar im Jahr 2013 entspricht dies einem durchschnittlichen jährlichen Zuwachs von 98 % (IDC Worldwide Messaging Security 2008 Vendor Shares and 2009-2013 Forecast).

### **VORTEILE BEIM VERTEILEN EINER VIRTUELLEN APPLIANCE UNTER VMWARE**

Virtuelle Appliances für die Messaging-Sicherheit in einer VMware-Umgebung bieten die gleichen Kostenvorteile am Gateway wie virtualisierte Lösungen für andere Funktionen des Datenzentrums, insbesondere niedrigere Kosten, geringerer CO<sub>2</sub>-Ausstoß, vereinfachte Verwaltung und leichte Verteilung. Zusätzliche Vorteile sind deutlich geringere Anschaffungs-, Wartungs- und Verwaltungskosten, woraus sich geringere Gesamtbetriebskosten als mit herkömmlicher E-Mail-Gateway-Sicherheit ergeben.

#### *Zeitersparnis durch vereinfachte Verteilung und Verwaltung*

Eine virtuelle Appliance spart Zeit beim Konfigurieren, Installieren, Patchen und Testen und senkt dadurch die allgemeinen Kosten für Administration und Verwaltung. Das Patchen der gesamten virtuellen Appliance (sowohl der Anwendung als auch des Betriebssystems) erfolgt automatisch durch einen einzelnen Anbieter, wodurch sich der Verwaltungsaufwand noch mehr verringert. VMware vCenter Server bietet Überwachung und Sicherheitsüberprüfung auf den virtuellen Appliances in der VMware-Umgebung und vereinfacht dadurch die Verwaltung.

#### *Stabile Betriebsabläufe durch Schutz am E-Mail-Gateway*

Da virtuelle Appliances für Messaging-Sicherheit die hohe Verfügbarkeit und Skalierbarkeit von VMware nutzen, können sie auch bei Strategien zur Stabilisierung von Betriebsabläufen eine wichtige Rolle spielen. VMware Data Recovery ermöglicht darüber hinaus schnelle und einfache Datensicherung und -wiederherstellung für virtuelle Maschinen.



## VIRTUALISIERUNG DER SICHERHEIT AM E-MAIL-GATEWAY

### *Hochverfügbarer Schutz am E-Mail-Gateway*

Virtuelle Appliances für die Messaging-Sicherheit eignen sich auch für umfangreiche Verteilungen in großen Unternehmen. Die Umgebungen von VMware Infrastructure und VMware vSphere bieten Belastbarkeit für alle Komponenten einer virtuellen Appliance, so dass Unternehmen die Zielsetzungen der Enterprise-IT, nämlich Zuverlässigkeit, Skalierbarkeit, Redundanz und Verfügbarkeit, erfüllen können. Außerdem nutzen virtuelle Messaging-Sicherheitsappliances VMware-Funktionen für verteilte Unternehmen, wie z. B.:

- **VMware VMotion:** Macht Schluss mit dem Ausfall von Anwendungen während geplanter Serverwartung, da virtuelle Maschinen und Appliances live auf allen Servern ohne Störung der Benutzer oder Verlust von Services migriert werden.
- **VMware Fault Tolerance:** Bietet permanente Verfügbarkeit ohne Datenverlust oder Ausfallzeiten für virtuelle Appliances und Anwendungen.
- **VMware High Availability:** Gewährleistet kosteneffizienten, automatischen Neustart aller Anwendungen innerhalb von Minuten nach Hardware- oder Betriebsystemausfall.

### **SKALIERBARKEIT FÜR CLUSTER-UMGEBUNGEN**

Außerdem ermöglichen VMware Infrastructure und VMware vSphere unbegrenzte Skalierbarkeit für den Schutz am E-Mail-Gateway in Cluster-Umgebungen. Administratoren von Datenzentren können mit geringerem Aufwand mehr Benutzer unterstützen und gleichzeitig hohe Leistung sicherstellen. Der VMware Distributed Resource Scheduler überwacht permanent den Einsatz aller verfügbaren Ressourcen und gleicht die Lasten von Server-Ressourcen dynamisch aus, um für die virtuellen Messaging-Sicherheitsappliances stets die richtigen Ressourcen bereitzustellen und den Schutz gemäß den unternehmerischen Prioritäten zu maximieren.

## III. VIRTUELLE APPLIANCES UND VAPPS FÜR DAS CLOUD-COMPUTING

Das vCloud-Projekt von VMware ermöglicht Cloud-Computing auf Enterprise-Ebene. Durch das bedarfsgerechte Bündeln von Computerressourcen zwischen virtuellen Datenzentren und Cloud-Service-Providern werden vorhandene und neue Anwendungen unterstützt. Ziel des vCloud-Projekts von VMware ist es, sowohl große als auch kleine Unternehmen beim sicheren Zugriff auf Rechenkapazität inner- und außerhalb ihrer Firewall zu unterstützen – wie, wann und so viel sie wollen, – um stabile Service-Qualität für jede Anwendung, ob intern oder als Service, zu gewährleisten.

Zusätzlich nutzt das vCloud-Projekt von VMware die große Palette von Anwendungen, die von Software-Anbietern unter VMware unterstützt werden, sowie das wachsende Ökosystem rund um VMware-bereite, virtuelle Appliances. Mit VMware-bereiten, virtuellen Appliances wird das Verteilen neuer Anwendungen, ob webbasiert oder lokal installiert, zum Kinderspiel. VMware-Partner wie Trend Micro setzen VMware-bereite, virtuelle Appliances ein, um Patchen, Verwalten und Migrieren webbasierter und lokal installierter Anwendungen zu vereinfachen.

Um einen nahtlosen Übergang auf Cloud-Strategien zu ermöglichen, hat VMware vApps eingeführt – die nächste Generation virtueller Appliances. Eine vApp ist eine vorgefertigte Software-Lösung, die aus mehreren virtuellen Maschinen besteht und als Einheit im Branchenstandard Open



## VIRTUALISIERUNG DER SICHERHEIT AM E-MAIL-GATEWAY

Virtualization Format (OVF) ausgeliefert und gewartet wird. In der Regel umfassen vApps alle Komponenten einer komplexen, mehrschichtigen Anwendung sowie die zugehörigen Betriebsrichtlinien und Service-Level. Am besten lassen sich vApps als selbstverwaltende und selbsterklärende Einheiten beschreiben, die alle Anwendungen unter allen Betriebssystemen unterstützen. Sie bieten Kunden einen Mechanismus, um ihre Anwendungen ohne Änderung des Service-Levels abwechselnd webbasiert oder lokal auszuführen. Das macht sie zu idealen Datentransportern für das Cloud-Computing. vApps können mit VMware vSphere 4.0 erstellt und verwaltet werden.

### IV. TREND MICRO MESSAGING SECURITY VIRTUAL APPLIANCE IST VMWARE-BEREIT

Trend Micro and VMware unterstützen Kunden beim Umbau ihres Datenzentrums mit Hilfe sicherer, flexibler Lösungen zur Optimierung ihrer Virtualisierungsprojekte. Die Trend Micro™ InterScan™ Messaging Security Virtual Appliance ist VMware-bereit und ergänzt virtualisierte Umgebungen nachweislich mit umfassendem Schutz am E-Mail-Gateway. VMware-bereite Lösungen gewährleisten grundlegende Kompatibilität und ein höheres Maß an Integration in VMware-Produkte. Das Logo „VMware Ready“ signalisiert Kunden, dass die Trend Micro Appliance VMware-spezifische Kriterien erfüllt und für das VMware-Betriebssystem Virtual Datacenter optimiert ist.

Die Trend Micro InterScan Messaging Security Virtual Appliance kann als eine dedizierte virtuelle Appliance auf branchenüblicher Bare-Metal-Hardware oder als eine VMware-bereite virtuelle Appliance in VMware ESX/Infrastructure-Umgebungen verteilt werden.

### V. UMFASSENDE VIRTUELLE SICHERHEIT AM E-MAIL-GATEWAY

#### **MEHRSCICHTIGE SPAM- UND PHISHING-ABWEHR SOWIE OPTIONALE VERSCHLÜSSELUNG**

Das Trend Micro Smart Protection Network™ verwendet eine Kombination aus webbasierten Reputation Services, um einen Großteil der bösartigen E-Mails abzuwehren, bevor sie das lokale Gateway erreichen. In die virtuelle Appliance integrierte Verteidigungsstrategien bieten umfassende E-Mail-Analyse mit Hilfe einer Vielzahl branchenführender Techniken, wie z. B. der zum Patent angemeldeten Bild-Spam-Erkennung zur Entdeckung bösartiger, eingebetteter URLs, sowie andere minutengenaue Mechanismen zur Abwehr neuer Spam-Techniken. Unternehmen können automatische, kundenspezifische Profiler und Reputation Services zur Abwehr von Spam und Viren einsetzen, indem sie eine Firewall zum Schutz vor dem Zugriff auf E-Mail-Verzeichnisse durch Directory-Harvest-Angriffe errichten. Außerdem verwendet InterScan Messaging Security Virtual Appliance Signaturen, Heuristiken und Reputation Services, um Phishing- und Spear-Phishing-Angriffe, die auf ein ganzes Unternehmen abzielen, abzuwehren.



## VIRTUALISIERUNG DER SICHERHEIT AM E-MAIL-GATEWAY

### **MEHRFACH AUSGEZEICHNETER SCHUTZ VOR VIREN UND SPYWARE**

Trend Micro stoppt Viren und Spyware, die in E-Mail-Anhängen versteckt sind. Unterstützt durch das Smart Protection Network™ liefert InterScan Messaging Security Virtual Appliance sofortigen Schutz, der wie eine virtuelle Nachbarschaftswache funktioniert. Die einzigartige Trend Micro Reputationsdatenbank speichert Bedrohungsdaten aus einem weltweiten Kundennetz, von Privatanwendern bis hin zu Großunternehmen. Mit jedem Angriff auf einen einzelnen Computer wird die Datenbank aktualisiert. Dadurch kann Trend Micro sein Wissen über Website-Reputation, Malware-Verhalten und Spam-Quellen verfeinern und nahezu Zero-Hour-Schutz bereitstellen.

### **FLEXIBLE CONTENT-FILTER**

Ein- und ausgehende E-Mails und Anhänge werden gemäß Anhangsmerkmalen, Wörterbüchern, Kennziffern und benutzerdefinierbaren Datenregeln nach unangemessenen Inhalten und Datenlecks durchsucht. InterScan Messaging Security Virtual Appliance bietet flexible Wiederherstellungsoptionen sowie unternehmensspezifische Haftungsausschlüsse, E-Mail-Quarantäne und Alarmmeldungen. Die Appliance ermöglicht die Erstellung von Richtlinien zur Einstufung von Absendern und Empfängern nach Unternehmen, Gruppen oder Einzelbenutzern und unterstützt Regeleinhaltung, Initiativen zur Unternehmensführung und den Schutz vor Datenverlust.

## **VI. KUNDEN WECHSELN ZUR VIRTUELLEN APPLIANCE VON TREND MICRO**

Trend Micro Kunden erweitern ihre Virtualisierungsstrategien, um auch den Schutz am E-Mail-Gateway mit Hilfe der Trend Micro InterScan Messaging Security Virtual Appliance zu virtualisieren.

### **OCHSNER HEALTH SYSTEM**

Ochsner Health System ist ein gemeinnütziges, von Universitäten unterstütztes System mit vielen Spezialbereichen zur Bereitstellung von Services des Gesundheitswesens im Südosten des amerikanischen Bundesstaates Louisiana. Um die Kosten des wachsenden Unternehmens unter Kontrolle zu halten, startete die IT-Abteilung mehrere Initiativen zur Kosteneinsparung, wie z. B. die Konsolidierung seiner E-Mail-Server. Die Hardware-basierte E-Mail-Gateway-Sicherheitslösung des Unternehmens konnte nicht effizient skaliert werden. Auf der Suche nach Alternativen war ein Kriterium der IT, dass die neue Lösung gut in die mit VMware virtualisierte Umgebung integrierbar sein musste. Ochsner entschied sich für die Trend Micro InterScan Messaging Security Virtual Appliance, da sie sowohl VMware-bereit war als auch Hochverfügbarkeits- und Wiederherstellungsfunktionen zur E-Mail-Kommunikation bereitstellte.

„Es war sehr wichtig, dass Trend Micro InterScan Messaging Security als VMware-bereit bestätigt war. Im Rahmen der Virtualisierungsprojekte unseres Unternehmens senkte das Verteilen einer virtuellen, statt wie zuvor einer Hardware-basierten, Appliance die Gesamtbetriebskosten und vereinfachte die Verwaltung.“

– Mark L. Smith, Netzwerkadministrator, Ochsner Health System



## VIRTUALISIERUNG DER SICHERHEIT AM E-MAIL-GATEWAY

### VII. VIRTUELLER SCHUTZ AM E-MAIL-GATEWAY IN VMWARE-UMGEBUNGEN

Gerade in wirtschaftlich schwierigen Zeiten gewinnen virtualisierte Lösungen für die Sicherheit am E-Mail-Gateway besondere Bedeutung. Trend Micro InterScan Messaging Security Virtual Appliance beschleunigt und vereinfacht die Bereitstellung von mehrfach ausgezeichnetem Schutz sowie die Nutzung von Faktoren wie Hochverfügbarkeit, Skalierbarkeit, Stabilisierung von Betriebsabläufen und Kosteneinsparung, die sich durch VMware-virtualisierte Umgebungen erzielen lassen.

Weitere Informationen finden Sie im VMware Virtual Appliance Marketplace unter <http://www.vmware.com/appliances>. Hier erfahren Sie mehr über virtuelle Appliances und können eine Testversion herunterladen. Trend Micro finden Sie im Internet unter [www.trendmicro.com](http://www.trendmicro.com).

#### **INFO ÜBER VMWARE**

VMware ist der weltweit führende Anbieter von Virtualisierungslösungen – vom Desktop über Datenzentren bis hin zum Internet – und bietet das Fundament für mehr Projekte der Daten-zentrumskonsolidierung und Virtualisierung als jedes andere Unternehmen. Zu seinen Kunden zählen über 130.000 Unternehmen jeder Größe und Branche, einschließlich aller Fortune-100-, 96 % der Fortune-1000 sowie mittelständische Unternehmen.

#### **INFO ÜBER TREND MICRO**

Trend Micro Incorporated, ein weltweit führender Anbieter von Lösungen im Bereich Internet Content Security für Unternehmen und Privatanwender, setzt seinen Schwerpunkt auf den sicheren Austausch digitaler Daten. Als Branchenpionier entwickelt Trend Micro integrierte Technologie zur Bedrohungsbewältigung, um Betriebsabläufe, Privatsphäre und geistiges Eigentum vor Malware, Spam, Datenverlust und den neuesten Internet-Bedrohungen zu schützen. Besuchen Sie TrendWatch unter [www.trendmicro.com/go/trendwatch](http://www.trendmicro.com/go/trendwatch), um mehr über die neuesten Bedrohungen zu erfahren. Für die flexiblen Trend Micro Lösungen, die in verschiedenen Formfaktoren erhältlich sind, bieten Bedrohungsexperten auf der ganzen Welt rund um die Uhr technischen Support. Viele dieser Lösungen werden durch das Trend Micro Smart Protection Network unterstützt, eine Content-Security-Infrastruktur der nächsten Generation mit webbasiertem Client zum Schutz der Kunden vor den Gefahren aus dem Internet. Die bewährten Sicherheitslösungen des transnationalen Unternehmens mit Hauptsitz in Tokyo werden über Unternehmenspartner weltweit vertrieben.

©2009 by Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das Trend Micro T-Ball-Logo und TrendLabs sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen- und/oder Produktnamen sind Marken oder eingetragene Marken ihrer jeweiligen Eigentümer. Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern. [WP01\_VMWARE\_0980730DE]