IBM Security Virtual Server Protection for VMware

Ein höheres Maß an Kosteneffizienz, Compliance und Schutz mit optimierten Sicherheitsfunktionen für virtuelle Rechenzentren

Highlights

- Gewährleistet die dauerhafte Einhaltung von Sicherheitsrichtlinien, selbst wenn virtuelle Maschinen von einem ESX-Server auf einen anderen migriert werden
- Bietet Schutz vor Manipulationen und eine Firewall ohne hostbasierten Agenten
- Identifiziert Rootkit-Aktivitäten auf dem Gastbetriebssystem
- Verhindert die unkontrollierte Zunahme virtueller Server und verringert Risiken durch nicht autorisierte virtuelle Maschinen
- Überwacht und berichtet Aktivitäten in der virtuellen Infrastruktur im Hinblick auf Compliance-Anforderungen
- Trägt durch automatische Schutzfunktionen für virtuelle Infrastrukturen zu einer Reduzierung der Kosten und der Komplexität bei

Die Virtualisierung bietet IT-Unternehmen erhebliche Vorteile, allerdings wurden die vorhandenen Sicherheitslösungen nicht zur Verwendung in virtuellen Umgebungen optimiert. Traditionelle Sicherheitsprozesse und -technologien können zusätzliche Ebenen, wie z. B. Hypervisor, Management-Stack und virtuelle Netzwerke, nicht wirksam schützen. Demzufolge bieten virtualisierte Server möglicherweise ein geringeres Maß an Sicherheit als die physischen Server, die sie ersetzen. Die Unternehmen riskieren dadurch, Compliance-Anforderungen nicht einhalten zu können. Unternehmen müssen sich bei der Umsetzung von Virtualisierungslösungen über diese möglichen Risiken bewusst sein und die erforderlichen Sicherheitsmaßnahmen ergreifen. IBM Security Virtual Server Protection for VMware® ist eine integrierte Lösung zur Eingrenzung von Risiken, die speziell konzipiert wurde, damit Unternehmen bestmöglich von den Vorteilen der Servervirtualisierung profitieren und kritische virtualisierte Ressourcen gleichzeitig geschützt sind.

Firewall

IBM Security Virtual Server Protection for VMware beinhaltet eine Firewall-Technologie für die Unterteilung virtueller Netzwerke und verhindert nicht autorisierte Übertragungen zwischen vertrauenswürdigen Zonen.

Transparenter Schutz vor Manipulationen

Virtuelle Maschinen (VMs) können schnell konfiguriert und implementiert werden, sodass Unternehmen von einer höchst dynamischen Systemumgebung profitieren. Die marktführende IBM Technologie zum Schutz vor Manipulationen sorgt automatisch für den Schutz virtueller Maschinen, sobald diese online sind oder im Rechenzentrum verlagert werden.

Automatische Erkennung

Virtuelle Netzwerke können Mängel in puncto Transparenz nach sich ziehen, sodass traditionelle Tools und Prozesse zur Erkennung unwirksam werden. IBM Security Virtual Server Protection for VMware kann neue virtuelle Maschine automatisch erkennen. Dadurch steigen das Sicherheitsbewusstsein und die Transparenz in virtuellen Umgebungen.

VM-Rootkit-Erkennung

IBM Security Virtual Server Protection for VMware prüft auf transparente Weise die Installation von Rootkits in virtuellen Maschinen. Das Feature stellt eine Ergänzung zu traditionellen Anti-Mailware-Programmen dar, da es Rootkits identifiziert und gegen gängige Verfahren immun ist, die von Rootkits verwendet werden, um hostbasierte Agenten zu inaktivieren.

Analyse von Übertragungen zwischen virtuellen Maschinen

Netzwerkübertragungen zwischen VMs auf demselben physischen Server fahren die Maschine nicht herunter, was zu einem „Blind Spot“ führen könnte, eine besondere Herausforderung bei Übertragungen zwischen VMs mit unterschiedlichen Vertrauensebenen. Während traditionelle Host- und Netzwerksysteme zum Schutz vor Manipulationen keine Transparenz bei Übertragungen zwischen VMs bieten, überwacht IBM Security Virtual Server Protection for VMware Übertragungen zwischen virtuellen Servern, um Risiken zu beseitigen, bevor diese sich auf Ihre Systemumgebung auswirken.

Zugriffskontrolle auf virtuelle Netzwerke

VMs können schnell, aber nur mit einem geringen Maß an Transparenz, im Rechenzentrum installiert werden, sodass sich Sicherheitslücken ergeben können. IBM Security Virtual Server Protection for VMware bietet eine Zugriffskontrolle auf virtuelle Netzwerke, um Netzwerkzugriffe von einem virtuellen Server solange zu isolieren oder einzuschränken, bis die Sicherheit für diese virtuelle Maschine gewährleistet ist.

Prüfung virtueller Infrastrukturen

IBM Security Virtual Server Protection for VMware erstellt Berichte über Aktivitäten privilegierter Benutzer, wie z. B. über VMotion Events, Statusänderungen der virtuellen Maschine (Start, Stopp, Pause) und Anmeldeaktivitäten. Dadurch können sich die für Audits erforderlichen Vorbereitungen verkürzen.

IBM Virtual Patch-Technologie

Die IBM Virtual Patch-Technologie schirmt Schwachstellen in Betriebssystemen oder Anwendungen ab, damit sich Unternehmen auf vorhersehbare Zeiträume für die Installations-Zyklen von Patches verlassen können. Dies kann dazu beitragen, Unternehmen unabhängig von deren Patch-Strategie automatisch vor Sicherheitslücken auf virtuellen Servern zu schützen.

Das Potenzial unternehmensweiter Sicherheitskontrollen nutzen

Virtualisierungslösungen werden zwar immer häufiger eingesetzt, Unternehmen verlassen sich aber nach wie vor auf ein kombiniertes IT-Konzept, sodass physisch vorhandene Server und Netzwerkverbindungen auch weiterhin vorhanden sein werden und geschützt werden müssen. IBM möchte seine Kunden in Bezug auf die Sicherheit im Unternehmen von einem umfassenden Sicherheitskonzept überzeugen. IBM Security Virtual Server Protection for VMware gewährleistet den umfassenden Schutz der virtuellen Infrastruktur, ist aber gleichzeitig auch ein Element einer komplexeren unternehmensweiten Sicherheitsstrategie. Bei IBM Lösungen profitiert der Kunde von einer erstklassigen Sicherheitstechnologie, die zum Schutz aller Ebenen einer IT-Umgebung entwickelt wurde. Wenn die IT-Sicherheit für Netzwerke, Hosts, Endpunkte, Anwendungen und virtuelle Maschinen auf derselben zentralen Technologie basiert, ergibt sich für Unternehmen ein noch höheres Maß an Transparenz und Kontrolle durch eine effiziente und skalierbare Lösung.

Merkmale und Vorteile

Mit dieser Lösung werden dynamische Sicherheitsfunktionen umgesetzt, wo auch immer VMs installiert werden:

- Bietet Schutz vor Manipulationen und eine Firewall für umfassende Sicherheit ohne die Verwendung von Agenten
- Ermöglicht die Isolation von Workloads auf Netzwerkebene
- Erkennt automatisch virtuelle Maschinen, die von traditionellen Erkennungstools nicht gefunden werden
- Identifiziert Rootkit-Aktivitäten in virtuellen Maschinen auf transparente Weise
- Isoliert potenziell unsichere VMs, bis sichergestellt ist, dass sie kein Sicherheitsrisiko darstellen
- Überwacht Aktivitäten in virtuellen Infrastrukturen

Die Lösung trägt dazu bei, PCI DSS-basierte Audits (Payment Card Industry Data Security Standard) zu beschleunigen und zu vereinfachen sowie gesetzliche Bestimmungen durch Sicherheits- und Berichtsfunktionen speziell für virtuelle Infrastrukturen einzuhalten:

- Aufteilung virtueller Netzwerke in separate virtuelle Server, die dem PCI-Standard entsprechen
- Automatisierte Schutzfunktionen, um sicherzustellen, dass Sicherheitsmaßnahmen auch in äußerst dynamischen Umgebungen wirksam bleiben

Dies trägt im Vergleich zur Verwendung physischer Sicherheitslösungen in virtuellen Infrastrukturen mit automatischen Schutzfunktionen zu einer Reduzierung der Kosten und der Komplexität bei:

- Geringerer Aufwand für Systemadministratoren durch automatische Schutz-, Erkennungs- und Analysefunktionen
- Nutzung der IBM Virtual Patch-Technologie zum automatischen Schutz vor Sicherheitslücken auf virtuellen Servern, unabhängig von der Patch-Strategie

Höhere Effizienz mit dem IBM Security SiteProtector System

Das IBM Security SiteProtector System ist eine einfachere und kostengünstigere Möglichkeit zur Verwaltung von Sicherheitslösungen und zur einfacheren Einhaltung gesetzlicher Bestimmungen. Es zeichnet sich durch eine zentrale Verwaltung zur Kontrolle von Sicherheitsrichtlinien, Analysen, Benachrichtigungen und Berichten für Ihr Unternehmen aus und kann auch unter VMware ESX eingesetzt werden. Das IBM Security SiteProtector System bietet zentrale Funktionen für Konfiguration, Verwaltung, Analyse und Berichterstellung.

Größere virtuelle Sicherheit durch Forschungsergebnisse von IBM X-Force

Die erstklassigen IBM Sicherheitslösungen beruhen auf dem Know-how der Mitarbeiter des weltweit bekannten X-Force-Teams. Das umfangreiche Fachwissen dieser Mitarbeiter fließt in die IBM Sicherheitslösungen ein.

Unabhängig davon, ob es sich um eine physische 1U-Appliance oder eine Softwarekomponente auf einer virtuellen Maschine handelt – die IBM Lösungen basieren auf denselben sicherheitsspezifischen Inhalten, die von den Mitarbeitern des X-Force-Teams entwickelt wurden. Das X-Force-Team ist eine der weltweit am längsten bestehenden und bekanntesten kommerziellen Forschungsgruppen für Sicherheitslösungen. Diese führende Gruppe aus Sicherheitsexperten untersucht und beurteilt Schwachstellen und Sicherheitsprobleme, entwickelt Analysen und Gegenmaßnahmen, die in IBM Sicherheitsprodukte einfließen, und informiert die Öffentlichkeit über neue Sicherheitsrisiken im Internet. Das X-Force-Team liefert nicht nur aktuelle sicherheitsspezifische Inhalte für IBM Sicherheitsprodukte, sondern bietet auch den IBM X-Force Threat Analysis Service (XFTAS) an. Über diesen Service werden mithilfe detaillierter Analysen der weltweiten Rahmenbedingungen individuelle Informationen zu einer Vielzahl von Sicherheitsrisiken bereitgestellt, die sich auf das Netzwerk in Ihrem Unternehmen auswirken könnten.

Warum IBM?

IBM Security Virtual Server Protection for VMware wurde zum Schutz virtueller Rechenzentren als zentraler Komponente von Infrastrukturen entwickelt, ohne dabei die Systemeffizienz und -leistung zu verringern. Die Software bietet ein Höchstmaß an Schutz und bietet dem Kunden die Möglichkeit, Compliance-Standards einzuhalten, indem der Zugriff auf kritische Daten in virtuellen Maschinen eingeschränkt und der Benutzerzugriff überwacht wird. IBM kann auf ein umfassendes Angebotsportfolio mit Sicherheitslösungen verweisen, zu dem erstklassige Technologien für den Schutz der physischen Serverumgebung, Endpunkte, zentralen Netzwerkkomponenten, Anwendungen und vieles mehr gehören. Mit IBM Lösungen kann die Sicherheit virtueller Komponenten basierend auf der vorhandenen Technologie für die IT-Sicherheit zentral verwaltet werden. Der Kunde profitiert dadurch von einer größeren Effizienz und Skalierbarkeit. IBM bietet End-to-End-Sicherheitslösungen in virtualisierten Umgebungen, sodass Ihr Unternehmen schneller die Vorteile der Virtualisierungstechnologie realisieren kann.

Voraussetzungen	
Plattform	X86-Server mit VMware vSphere 4

Weitere Informationen

Wenn Sie mehr über IBM Security Virtual Server Protection for VMware erfahren möchten, wenden Sie sich bitte an den zuständigen IBM Vertriebsbeauftragten oder IBM Business Partner, oder besuchen Sie uns unter:

ibm.com/tivoli/security

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

WGD03008-DEDE-00