VMware vShield App

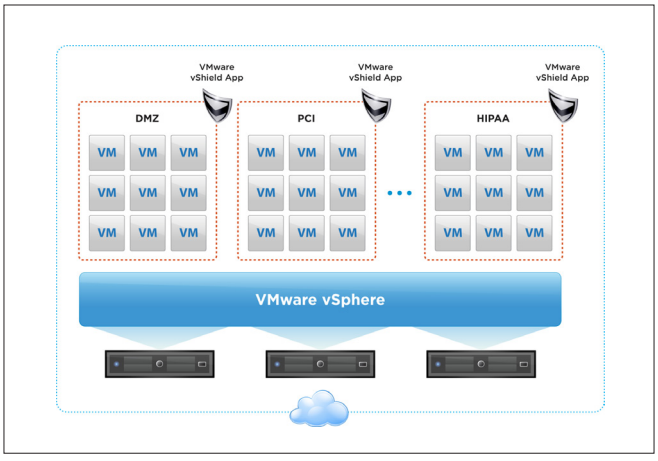
Anwendungsschutz bei netzwerkbasierten Angriffen

AUF EINEN BLICK

VMware vShield App, Teil der VMware vShield-Produktreihe von Sicherheitsprodukten für virtualisierte Umgebungen, schützt Anwendungen im virtuellen Rechenzentrum vor netzwerkbasierten Bedrohungen. vShield App ermöglicht Unternehmen einen detaillierten Einblick in die Netzwerkkommunikation zwischen virtuellen Maschinen und ermöglicht die Einhaltung detaillierter Richtlinien über Sicherheitsgruppen. Mit der Lösung wird außerdem die Zahl an Hardware und Richtlinien eingedämmt, die mit herkömmlichen Maßnahmen einhergehen. Dies führt zu einer kostengünstigen Lösung, mit der die Kunden die Sicherheitseinschränkungen ihrer physischen Umgebung überwinden können.

VORTEILE

- Verbessern Sie den Einblick in und die Kontrolle über die Netzwerkkommunikation zwischen virtuellen Maschinen.
- Eliminieren Sie den Bedarf an dedizierter Hardware und VLANs, um Sicherheitsgruppen voneinander zu trennen.
- Optimieren Sie die Auslastung von Hardware-ressourcen bei Wahrung höchster Sicherheit.
- Vereinfachen Sie die Compliance durch eine umfassende Protokollierung aller Netzwerkakti-vitäten virtueller Maschinen.



VMware vShield App ermöglicht die Einhaltung detaillierter Richtlinien über Sicherheitsgruppen.

Was ist VMware vShield App?

Bei VMware vShield App handelt es sich um eine Hypervisor-basierte, anwendungsorientierte Firewall-Lösung für virtuelle Rechenzentren. vShield App wird direkt in VMware vSphere™ integriert und sorgt dort für den Schutz vor internen netzwerkbasierten Bedrohungen und für die Reduzierung des Risikos von Richtlinienverletzungen innerhalb der firmeninternen Sicherheitsebenen. Hierfür kommen anwendungsorientierte Firewalls mit Deep Packet Inspection und Verbindungskontrolle auf Basis der Quell- und Ziel-IP-Adressen zum Einsatz.

vShield trägt zu einer Vereinfachung der Richtlinienkontrolle bei, indem es eine schnelle Erstellung geschäftsrelevanter Sicherheitsgruppen ermöglicht. Durch das Monitoring des Datenflusses wird der Netzwerkdatenverkehr der virtuellen Maschinen analysiert und Richtlinien für Sicherheitsgruppen werden dynamisch eingehalten. Administratoren können vShield App zentral über die in der Lösung enthaltene vShield Manager-Konsole verwalten. Durch die nahtlose Integration der Konsole in VMware vCenter™ Server wird das einheitliche Sicherheitsmanagement von virtuellen Rechenzentren erleichtert.

Wie funktioniert VMware vShield App?

vShield App kann auf jedem vSphere-Host installiert werden und kontrolliert und überwacht den gesamten Netzwerkdatenverkehr des Hosts. Das gilt auch für solche Pakete, die niemals über eine physische Netzwerkkarte transportiert werden. vShield App kann Richtlinien anhand von durch den Administrator definierten, geschäftsrelevanten Sicherheitsgruppen erstellen und einhalten, ohne dabei auf physische Grenzen oder statische Annahmen über Anwendungsbereitstellungen zurückgreifen zu müssen.

vShield App bietet eine zentrale Schnittstelle, über die vCenter Server für die konsequente Anwendung der Richtlinien auf mehreren vSphere-Hosts im virtuellen Rechenzentrum genutzt werden kann.

Wie wird VMware vShield App eingesetzt?

- **Beseitigung von Schwachstellen** – vShield App hilft Administratoren bei der Definition und Durchsetzung detaillierter Richtlinien für den gesamten Datenverkehr, der über einen virtuellen Netzwerkadapter geleitet wird. Dabei wird die Einsicht in den internen Datenverkehr im virtuellen Rechenzentrum verbessert und Umwege über die physischen Firewalls werden beseitigt.
- **Effektiver Schutz auch bei Änderungen** – Mit vShield App können Sie sicherzustellen, dass Änderungen der Netzwerktopologie keine Auswirkungen auf die Anwendungssicherheit haben. Erzielt wird dies durch kontinuierlichen Firewall-Schutz für virtuelle Maschinen, der auch bei der Migration von Host zu Host erhalten bleibt.
- **Effiziente Verwaltung dynamischer Richtinien** – vShield App hilft bei der Vereinfachung von Richtliniendefinitionen und bietet Administratoren einen umfassenden Kontext für die Definition und Neudefinition von internen Firewall-Richtlinien bei sich ändernden Geschäftsanforderungen.
- **Reduzierung der Gefahren durch Botnets** – vShield App unterstützt Sicherheitsadministratoren beim Schutz vor Botnets und anderen Angriffen, indem die Vergabe von Ports an vertrauenswürdige Anwendungen dynamisch erfolgt.
- **Kontrollierter Zugriff auf gemeinsam genutzte Ressourcen** – Mit vShield App können Sicherheitsadministratoren den Zugriff auf gemeinsam genutzte Dienste auf vSphere-Hosts wie Storage und Backup anhand der IP-Adresse einschränken.
- **Schnellere IT-Compliance** – vShield App verbessert die Einsicht in und die Kontrolle über die Sicherheit der Netzwerke virtueller Maschinen. Hierfür stehen Protokollierungs- und Audit-Tools bereit, die Großunternehmen für den Nachweis der Einhaltung interner Richtlinien und externer behördlicher Auflagen benötigen.

Hauptmerkmale

Firewall auf Hypervisor-Ebene

- Kontrolle des ein-/ausgehenden Datenverkehrs auf Ebene des virtuellen Netzwerkadapters durch Hypervisor-Überprüfung; Unterstützung von mehrfach vernetzten virtuellen Maschinen
- Möglichkeit der Durchsetzung auf Basis von Netzwerk, Anwendungsport, Protokollart (TCP, UDP), Anwendungstyp
- Dynamischer Schutz bei der Migration virtueller Maschinen
- IP-basierte Firewall mit Statuserhalt und Gateway auf Anwendungsebene für eine große Bandbreite an Protokollen, darunter Oracle, Sun Remote Procedure Call (RPC), Microsoft RPC, LDAP und SMTP (vollständige Liste der unterstützten Protokolle siehe Administratorhandbuch zu VMware vShield App)

Monitoring des Datenflusses

- Möglichkeit der Beobachtung von Netzwerkaktivitäten zwischen virtuellen Maschinen als Unterstützung bei der Definition und Neudefinition von Firewall-Richtlinien, bei der Erkennung von Botnets und bei der Sicherung von Geschäftsprozessen durch eine detaillierte Berichterstellung über den Anwendungsdatenverkehr (Anwendung, Sitzungen, Bytes)

Sicherheitsgruppen

- Vom Administrator festgelegte, geschäftsrelevante Gruppierungen von virtuellen Maschinen auf Basis der virtuellen Netzwerkadapter

Richtlinienverwaltung

- Verwaltung aller Funktionen über vShield Manager; Zugriff auf viele Funktionen auch über die vCenter Server-Schnittstelle
- Richtliniendurchsetzung bei Sicherheitsgruppen, vCenter-Gruppierungen und 5-Tupel-TCP (Quell-IP, Ziel-IP, Quellport, Zielport, Protokoll)
- Programmierbare Schnittstelle für Management und Einhaltung von Richtlinien über REST-APIs
- Unterstützung der Integration in die Management-Tools von Unternehmen für die Sicherheit

Protokollierung und Prüfung

- Grundlage ist das branchenübliche Syslog-Format
- Zugriff über REST-APIs und vShield Manager
- Durch den Administrator festgelegte Aktivierung und Deaktivierung der Protokollierung für Firewalls auf Regelebene

Weitere Informationen

Wenn Sie ein VMware-Produkt kaufen möchten oder weitere Informationen benötigen, setzen Sie sich unter der folgenden Telefonnummer direkt mit VMware in Verbindung: 0800 100 6711. Sie können auch unsere Website unter www.vmware.com/de/products besuchen oder online nach einem autorisierten Händler suchen. Ausführliche Produktspezifikationen und Systemanforderungen finden Sie im Administratorhandbuch zu VMware vShield App.

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Zweigniederlassung Deutschland: Freisinger Str. 3, 85716 Unterschleißheim/Lohhof Telefon: +49 89 370 617 000 Fax: +49 89 370 617 333 www.vmware.com/de
Copyright © 2010 VMware, Inc. Alle Rechte vorbehalten. Dieses Produkt ist durch US-amerikanisches und internationales Copyright und Gesetze zum Schutz des geistigen Eigentums geschützt. VMware-Produkte sind durch eines oder mehrere Patente geschützt, die auf der folgenden Webseite aufgeführt sind: http://www.vmware.com/go/patents-de. VMware ist eine eingetragene Marke oder Marke der VMware, Inc. in den USA und/oder anderen Ländern. Alle anderen in diesem Dokument erwähnten Bezeichnungen und Namen sind unter Umständen markenrechtlich geschützt.
Artikelnr.: VMW_10Q3_DS_PROD_VSHIELD_APP_A4_DE_R6