



VMware vShield

Die Grundlage für zuverlässige Cloud-Infrastrukturen

BROSCHÜRE

Auf einen Blick

Für Unternehmen und Organisationen, die die Vorteile des Cloud Computing ohne Kompromisse im Hinblick auf Sicherheit, Kontrolle und Compliance nutzen möchten, bieten die Lösungen der VMware vShield™-Produktreihe umfassenden Schutz für virtuelle Rechenzentren und Cloud-Umgebungen. Mit vShield können Organisationen die Anwendungs- und Datensicherheit erhöhen. Das Programm schützt vor unbefugtem Eindringen ins Netzwerk, steigert die Leistung von Antiviren- und Anti-Malware-Programmen für Endpunkte erheblich, verbessert die Erkennung und Kontrolle sensibler Daten und beschleunigt die unternehmensweite IT-Compliance.

Sicherheitsbedenken bei Cloud-Umgebungen

Zahlreiche Organisationen erwägen, mittels Cloud Computing die Agilität zu steigern und die Kosten zu senken. Aktuelle Umfragen zum Thema Cloud Computing zufolge zögern jedoch viele Kunden aufgrund von Bedenken bezüglich Sicherheit, Kontrolle und Compliance mit dem Umstieg auf Cloud-Umgebungen. Daher suchen Unternehmen nach Lösungen für diese Probleme, damit sie von den Vorteilen des Cloud Computing profitieren können, ohne Abstriche bei Sicherheit, Kontrolle oder Compliance machen zu müssen.

Cloud-Sicherheit: Bedenken

- **Anwendungs- und Datensicherheit:** Aktuelle Cloud-Lösungen bieten Unternehmen nicht die modernen Tools, die sie benötigen, um Anwendungen zu schützen und/oder Datenverlust zu vermeiden.
- **Transparenz und Kontrolle:** Aktuelle Cloud-Lösungen bieten Sicherheitsadministratoren nicht die nötige Transparenz, um Sicherheitsrichtlinien während des gesamten Lebenszyklus zu kontrollieren, von der Definition über die Implementierung und Einhaltung bis hin zum Auditing.
- **Compliance-Management:** Die meisten Unternehmen verfügen bereits über Tools, Technologien und Prozesse zur Compliance-Sicherstellung und benötigen Cloud-Lösungen, die ein effizientes Compliance-Verfahren unterstützen.

Sicherheit für die Cloud mit VMware vShield

Virtualisierung ist nicht nur bei der Übertragung von Legacy-Anwendungen in die neue Cloud-Infrastruktur unverzichtbar, sondern spielt auch bei der Sicherheit von Cloud-Umgebungen eine wichtige Rolle. Der internationale Marktführer VMware® entwickelt und vertreibt bereits seit mehr als einem Jahrzehnt sichere und zuverlässige Virtualisierungslösungen. Mit den neuen Sicherheitslösungen der VMware vShield-Produktreihe für virtuelle Rechenzentren und Cloud-Umgebungen können Kunden sich ganz ohne Risiko für die Vorteile des Cloud Computing entscheiden. Nur mit VMware kann im Unternehmen

ein Cloud-Modell umgesetzt werden, das Lösungen für die individuellen geschäftlichen Herausforderungen bietet. Auf diese Weise kann die für Sie wichtigste Cloud – Ihre Cloud – sicher bereitgestellt werden.

Die wichtigsten Vorteile

Über die Grenzen der physischen Sicherheit hinaus

vShield bietet adaptive Sicherheit, die auch bei Migrationen zwischen Host stets auf den virtuellen Maschinen erhalten bleibt. Somit stellt die Unterstützung virtueller Maschinen in dynamischen Cloud-Umgebungen für Unternehmen kein Sicherheitsrisiko dar. Darüber hinaus lässt sich mit diesem Ansatz sicherstellen, dass Anwendungen in Cloud-Umgebungen effizient ausgeführt werden können, wobei die jeweilige Vertraulichkeitsstufe und Netzwerksegmentierung für Anwender und sensible Daten stets beibehalten werden.

Verbessertes und vereinfachtes Sicherheitsmanagement in einem Framework

vShield ermöglicht über ein einziges, umfassendes Framework die Absicherung virtueller Rechenzentren und Cloud-Umgebungen auf allen Ebenen – Hosts, Netzwerke, Anwendungen, Daten und Endpunkte. Es sorgt dafür, dass für alle in VMware-basierten Clouds bereitgestellten Anwendungen die erforderlichen Segmentierungen und Vertraulichkeitszonen eingehalten werden. In Kombination mit den Selbstprüfungsfunktionen der VMware vSphere®-Plattform bietet vShield sämtliche Funktionen zum Schutz von Hosts und virtuellen Maschinen. Zusammen mit bewährten Lösungen von VMware-Partnern sorgen diese Funktionen dafür, dass Anwendungen und Daten in VMware-basierten Clouds optimal geschützt sind.

Verringerung der Komplexität und Vermeidung von Antiviren-„Stürmen“

vShield nimmt der Virtualisierungssicherheit einiges an Komplexität. Organisationen können ihre Sicherheitsinfrastrukturen konsolidieren und müssen nicht mehr mit einer stetig steigenden Zahl von Softwareagenten, Sicherheitsrichtlinien, dedizierten Sicherheits-Appliances und „Air Gap“-Lösungen jonglieren. Darüber hinaus lassen sich mit vShield Antiviren-„Stürme“ im Zusammenhang mit Endpunkt-Sicherheitsagenten vermeiden, da keine Antiviren-Software auf einzelnen virtuellen Maschinen installiert werden muss.

Anwendungsschutz und Beschleunigung der IT-Compliance

vShield schützt Anwendungen im virtuellen Rechenzentrum vor Angriffen aus dem Netzwerk. Organisationen erhalten Einblick in und die Kontrolle über die Netzwerkkommunikation zwischen virtuellen Maschinen. Die Richtliniendurchsetzung erfolgt äußerst flexibel, da sie auf logischen Konstrukten wie VMware vCenter™-Containern und vShield-Sicherheitsgruppen und nicht nur auf physischen Konstrukten wie IP-Adressen beruht. vShield sucht

innerhalb der virtuellen Ressourcen nach sensiblen Daten wie Kreditkartennummern. Richtlinienverstöße werden gemeldet, sodass IT-Organisationen schnell einschätzen können, ob die jeweils geltenden regionalen Bestimmungen eingehalten werden.

Nutzung vorhandener Sicherheitslösungen

vShield ist zur nahtlosen Integration in vorhandene IT-Sicherheitsmaßnahmen im Unternehmen konzipiert. Hierzu dienen die so genannten REST-APIs (REST = Representational State Transfer), die eine individuelle Integration von vShield-Funktionen in Sicherheitslösungen anderer Anbieter ermöglichen. Darüber hinaus umfasst vShield eine Endpunktsicherheits-API, die eine Integration in vorhandene Antiviren- und Anti-Malware-Lösungen ermöglicht, und im Hinblick auf Sicherheitsinformationen, Ereignisverwaltung, Schutz vor unerwünschten Datenlecks, Änderungs- und Konfigurationsmanagement sowie Auditing mit allgemeinen Sicherheitslösungen vernetzbar ist.

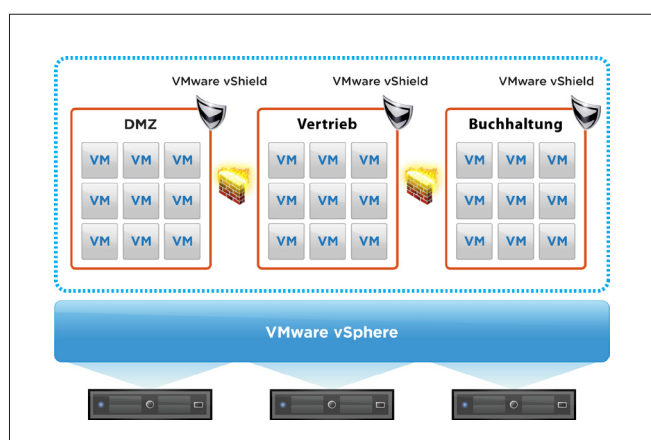
VMware vShield im Einsatz

Sicherheit für geschäftskritische Anwendungen

Mithilfe von vShield-Lösungen können Kunden problemlos Anwendungen unterschiedlicher Vertraulichkeitsstufen („Zonen“) im selben virtuellen Rechenzentrum ausführen (z.B. Produktion und Entwicklung, Finanzen und Vertrieb, klassifizierte und nicht klassifizierte Anwendungen usw.). Die Firewall auf Hypervisor-Ebene in vShield stellt sicher, dass für alle bereitgestellten Anwendungen die erforderlichen Segmentierungen und Vertraulichkeitszonen eingehalten werden.

Sichere Bereitstellung virtueller Desktops

Durch die Integration in VMware View™ ermöglicht vShield einen effizienteren Schutz von virtuellen Endpunkten und Anwendungen vor Viren und Malware. Dies wird erreicht, indem die Antiviren- und Anti-Malware-Funktionen von einzelnen virtuellen Maschinen auf eine sichere virtuelle Appliance



Mit VMware vShield können Organisationen geschäftsrelevante Sicherheitsgruppen erstellen und kritische Anwendungen vor Angriffen über das Netzwerk schützen.

ausgelagert werden, die den Host und alle darauf befindlichen virtuellen Maschinen schützt. Diese Herangehensweise optimiert das Sicherheitsmanagement und bietet zusätzlichen Schutz vor Antiviren-„Stürmen“, Performance-Engpässen und Botnet-Angriffen.

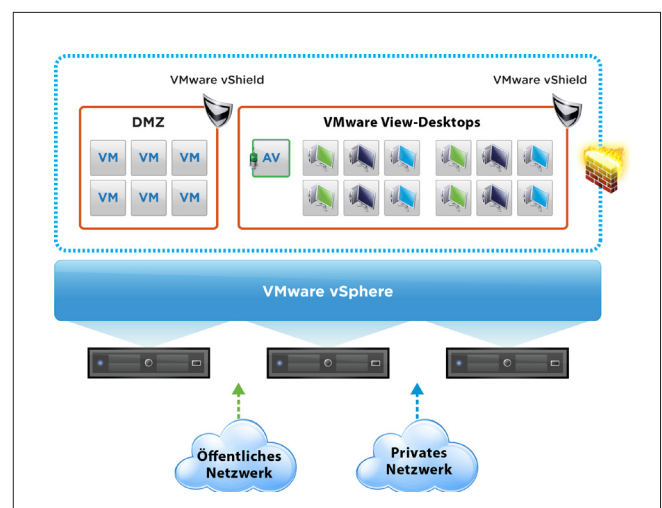
Darüber hinaus vereinfacht vShield die Einrichtung logischer Sicherheitsgrenzen um virtuelle Desktop-Infrastrukturen durch vollständige Netzwerkisolation und eine Reihe von Netzwerk-Gateway-Diensten, wie Firewalls, virtuellen privaten Netzwerken (VPNs) und dem DHCP-Protokoll.

Erkennung sensibler Daten zur Senkung des Risikos der Nichteinhaltung von Bestimmungen

Organisationen können mit vShield App with Data Security verlässlich sensible Daten in unstrukturierten Dateien erkennen. Mit mehr als 80 vordefinierten Vorlagen für landes- und branchenspezifische Bestimmungen können sensible Daten schnell ermittelt und angezeigt werden. Darüber hinaus wird durch die Verlagerung der Erkennungsfunktionen auf eine virtuelle Appliance die Performance gesteigert.

Sicherheit für mandantenfähige Umgebungen

Mit vShield-Lösungen können Unternehmen und Cloud-Serviceanbieter ganz unkompliziert IT-Umgebungen für mehrere Mandanten ausführen und Netzwerkressourcen sicher gemeinsam nutzen. Hierzu werden logische Sicherheitszonen erstellt, die eine vollständige Netzwerkisolation für virtuelle Rechenzentren ermöglichen. Außerdem bietet vShield detaillierte Kontrolle und Transparenz des Netzwerk-Gateway-Datenverkehrs sowie VPN-Dienste zum Schutz der Vertraulichkeit und Integrität der Kommunikation zwischen virtuellen Rechenzentren.



vShield optimiert den Antiviren- und Anti-Malware-Schutz in virtualisierten Umgebungen durch eine von VMware-Partnern bereitgestellte sichere virtuelle Appliance.

vShield-Lösungen

vShield Edge

Bei vShield Edge handelt es sich um eine Netzwerk-Gateway-Lösung, die den Rand des virtuellen Rechenzentrums mit DHCP, Netzwerkadressenübersetzung (NAT), Firewalls, Lastausgleich, Site-to-Site-VPN, Portgruppenisolierung und anderen Funktionen schützt und Unternehmen dabei unterstützt, eine korrekte Segmentierung zwischen den unterschiedlichen Organisationseinheiten aufrechtzuerhalten.

vShield App with Data Security

vShield App with Data Security schützt Anwendungen und Daten im virtuellen Rechenzentrum vor Angriffen über das Netzwerk. So können Organisationen geschäftsrelevante Richtlinien erstellen und verwalten, die an dynamische Cloud-Umgebungen anpassbar sind. Darüber hinaus bietet diese Lösung detaillierten Einblick in die Netzwerkkommunikation zwischen virtuellen Maschinen sowie eine genaue Richtlinieneinhaltung durch Sicherheitsgruppen. Die Erkennung unverschlüsselter sensibler Daten (wie beispielsweise Kreditkartennummern), die unter Umständen in Dateien auf virtuellen Maschinen gespeichert sind, wird ebenfalls unterstützt. Administratoren können Rechenzentren, Cluster und Ressourcenpools nach sensiblen Daten durchsuchen und tragen auf diese Weise dazu bei, dass die behördlichen Auflagen eingehalten werden. Mit REST-APIs können infizierte Dateien isoliert werden.

vShield Endpoint

vShield Endpoint erhöht die Sicherheit von virtuellen Maschinen und verbessert den Schutz von Endpunkten in erheblichem Umfang. Bei vShield Endpoint werden Antiviren- und Anti-Malware-Agenten-Verarbeitung auf eine dedizierte sichere virtuelle Appliance von VMware-Partnern ausgelagert. Die Lösung dient der Nutzung vorhandener Investitionen und ermöglicht Organisationen die Verwaltung von Antiviren- und Anti-Malware-Richtlinien für virtualisierte Umgebungen über dieselben Verwaltungsschnittstellen, die auch für die Sicherung von physischen Umgebungen verwendet werden.

vShield Bundle

vShield Bundle umfasst die folgenden Produkte der vShield-Produktreihe: vShield Edge, vShield App with Data Security, vShield Endpoint und vShield Manager.

vShield Manager

vShield Manager ist in allen vShield-Produkten enthalten und bietet einen zentralen Kontrollpunkt für die Bereiche Management, Bereitstellung, Reporting, Protokollierung und Integration von Sicherheitsservices von Drittanbietern. In Kombination mit vCenter Server kann vShield Manager außerdem zur rollenbasierten Zugriffskontrolle und zur Aufteilung der Zuständigkeiten im Rahmen eines einheitlichen Frameworks zur Verwaltung der Virtualisierungssicherheit genutzt werden.

vShield Zones

Das in vSphere enthaltene vShield Zones bietet in virtuellen Rechenzentren einen grundlegenden Schutz vor Bedrohungen aus dem Netzwerk. Neben Anwendungs-Firewalls kommt eine Richtlinienverwaltung auf der Grundlage von durch den Administrator festgelegten Zonen zum Einsatz. Hierbei wird auf grundlegende Datenverkehrsinformationen wie Quell-IP-Adresse, Zielport usw. zugegriffen.

Unterstützte Versionen

Weitere Informationen zu unterstützten Versionen von vSphere-, ESX- und VMware View-Umgebungen finden Sie unter www.vmware.com/de/products.

Kaufoptionen

vShield Edge, vShield App with Data Security, vShield Endpoint und vShield Bundle (in dem drei vShield-Produkte zusammengefasst sind) können separat voneinander erworben werden. vShield Manager ist im Lieferumfang sämtlicher vShield-Produkte enthalten. vShield Zones ist als integrierte Funktion von vSphere verfügbar.

Support und Services

VMware bietet Support und Wartung (Support and Subscription, SnS) der Stufen „Basic“ und „Production“ für alle VMware vShield-Kunden. Support für Antiviren- und Anti-Malware-Programme von Drittanbietern, die vShield Endpoint nutzen, ist beim jeweiligen Lösungsanbieter erhältlich.

Weitere Informationen

Wenn Sie ein VMware-Produkt erwerben 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 Angaben zu den Systemanforderungen finden Sie in der Dokumentation zu VMware vShield.

