VMware vShield Endpoint

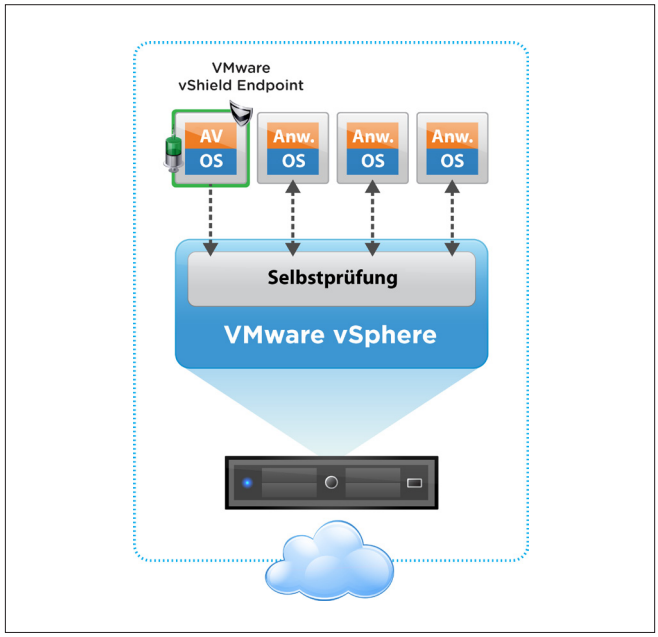
Verbesserte Endpunktsicherheit und -Performance für virtuelle Rechenzentren

AUF EINEN BLICK

VMware 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 Kunden die Verwaltung von Antiviren- und Anti-Malware-Richtlinien für virtualisierte Umgebungen über dieselben Verwaltungsschnittstellen, die auch für die Sicherung von physischen Umgebungen verwendet werden.

DIE WICHTIGSTEN VORTEILE

- Steigerung des Konsolidierungsverhältnisses und der Performance, weil auf den virtuellen Gastmaschinen keine Antiviren-Agenten ausgeführt werden müssen
- Optimierung der Antiviren- und Anti-Malware-Bereitstellung und -Überwachung in VMware-Umgebungen
- Verbesserung der Sicherheit durch Konsolidierung von Antiviren-Softwareagenten zur Begrenzung der Angriffsfläche
- Einhaltung von Compliance- und Audit-Anforderungen durch die Protokollierung von Antiviren- und Anti-Malware-Aktivitäten



Mit vShield Endpoint werden die Performance und das Konsolidierungsverhältnis von Antiviren- und Anti-Malware-Lösungen in virtualisierten Umgebungen verbessert.

Was ist vShield Endpoint?

vShield Endpoint revolutioniert die Art und Weise, in der virtuelle Gastmaschinen vor Viren und Malware geschützt werden. Mit der Lösung werden Antiviren-Programme und andere Tools für die Endpunktsicherheit in VMware vSphere®- und VMware View™-Umgebungen optimiert.

vShield Endpoint trägt zu einer Performance-Verbesserung bei, indem die Virenscanner-Aktivitäten von den einzelnen virtuellen Maschinen auf eine sichere virtuelle Appliance mit eigener Scanning-Engine und Speicherplatz für die Antiviren-Signaturen übertragen werden. Bei dieser Architektur wird für die Antiviren- und Anti-Malware-Funktionen auf den virtuellen Gastmaschinen kein Speicherplatz durch Softwareagenten belegt. Dadurch werden Systemressourcen freigegeben, die Performance gesteigert und das Risiko so genannter Antiviren-„Stürme“ (überlastete Ressourcen bei geplanten Scans und Signatur-Updates) ausgeschaltet. Da die sichere virtuelle Appliance im Gegensatz zu einer virtuellen Gastmaschine immer online ist, können Antiviren-Signaturen kontinuierlich aktualisiert werden. So sind die virtuellen Maschinen auf dem Host dauerhaft geschützt. Außerdem sind neue (bzw. zwischenzeitlich offline geschaltete) virtuelle Maschinen sofort mit den neuesten Antiviren-Signaturen geschützt, sobald sie online sind.

vShield Endpoint trägt mit einer manipulationssicheren virtuellen Appliance (die von VMware-Partnern bereitgestellt wird) zur Steigerung der Sicherheit bei. Die Appliance greift auf die robusten und sicheren Hypervisor-Selbstprüfungsfunktionen von vSphere zurück. Dadurch wird eine Gefährdung der Antiviren- und Anti-Malware-Dienste selbst vermieden.

vShield Endpoint bietet VMware-Partnern zudem Schnittstellen für die Implementierung von Scanning-Tools nicht nur für Dateien, sondern auch für Speicher und Prozesse. Organisationen können mehrere Sicherheitslösungen gleichzeitig einsetzen. So kann in einer sicheren virtuellen Appliance die Funktion zur Erkennung sensibler Daten aus VMware vShield App with Data Security und in einer anderen eine Antiviren-Lösung verwendet werden.

Organisationen können mittels detaillierter Aktivitätsprotokolle der Antiviren- bzw. Anti-Malware-Dienste Compliance nachweisen und eine Einhaltung der Audit-Anforderungen belegen.

Administratoren können vShield Endpoint 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 vShield Endpoint?

vShield Endpoint lässt sich direkt in vSphere integrieren und besteht aus drei Komponenten:

- Abgesicherte virtuelle Appliances (Bereitstellung durch VMware-Partner)
- Thin Agent für virtuelle Maschinen zur Verlagerung von Sicherheitsaufgaben (in VMware Tools enthalten)
- Das VMware Endpoint ESX®-Hypervisor-Modul, das die Kommunikation zwischen den ersten beiden Komponenten auf Hypervisor-Ebene ermöglicht

vShield Endpoint überwacht beispielsweise bei einer Antiviren-Lösung Ereignisse in Bezug auf Dateien in der virtuellen Maschine und benachrichtigt die Antiviren-Engine, die Scans durchführt und eine Maßnahme veranlasst. Die Dateien können sowohl beim Öffnen als auch nach einem bestimmten Zeitplan von der Antiviren-Engine auf der sicheren virtuellen Appliance geprüft werden.

Wenn eine Fehlerbehebung erforderlich ist, können Administratoren über die vorhandenen Antiviren- und Anti-Malware-Verwaltungstools angeben, welche Aktionen durchgeführt werden sollen. vShield Endpoint übernimmt das Management für alle Problemlösungen auf den betroffenen virtuellen Maschinen.

Wie wird vShield Endpoint eingesetzt?

Die vom VMware-Partner bereitgestellte Managementkonsole wird zur Konfiguration und Steuerung der auf der sicheren virtuellen Appliance gehosteten Partnersoftware verwendet. VMware-Partner können eine Benutzeroberfläche bereitstellen, über die das Management (einschließlich der Richtlinienverwaltung) genauso wie für Software durchgeführt wird, die auf einer dedizierten physischen Sicherheits-Appliance gehostet wird.

Der Arbeitsaufwand für Administratoren der virtuellen Infrastruktur reduziert sich enorm, da auf den virtuellen Maschinen keine Antiviren-Agenten verwaltet werden müssen. Stattdessen wird die sichere virtuelle Appliance über die Managementkonsole des Partners verwaltet. Auf diese Weise wird auch verhindert, dass häufige Updates für die einzelnen virtuellen Maschinen durchgeführt werden müssen. Zu Bereitstellungszwecken enthält VMware Tools den Thin Agent, und über das ESX-Modul wird die Hypervisor-Selbstprüfung aktiviert.

Die Administratoren der virtuellen Infrastruktur können die Bereitstellungen problemlos z.B. daraufhin überwachen, ob eine Antiviren-Lösung ordnungsgemäß funktioniert.

Hauptmerkmale

Antiviren- und Anti-Malware-Auslagerung

- vShield Endpoint trägt durch die über das vShield Endpoint ESX-Modul realisierte Auslagerung der Virenscan-Aktivitäten auf eine sichere virtuelle Appliance zu einer Steigerung der Performance bei.
- Aufgaben wie die Prüfung von Dateien, Speicher und Prozessen werden von den virtuellen Maschinen über einen Thin Client-Agenten und ein Partner-ESX-Modul auf eine sichere virtuelle Appliance ausgelagert.
- Mit vShield Endpoint EPSEC wird die Kommunikation zwischen virtuellen Maschinen und der sicheren virtuellen Appliance durch Selbstprüfung auf Hypervisor-Ebene verwaltet.
- Die Antiviren-Engine und die Signaturdateien werden nur auf der sicheren virtuellen Appliance aktualisiert, Richtlinien können jedoch auf alle virtuellen Maschinen eines vSphere-Hosts angewendet werden.

Fehlerbehebung

- In vShield Endpoint wird mittels Antiviren-Richtlinien festgelegt, ob eine problematische Datei gelöscht, isoliert oder anderweitig gehandhabt werden soll.
- Zur Fehlerbehebung bei Dateien innerhalb der virtuellen Maschine kommt der Thin Agent zum Einsatz.

Partner-Integrationen

- Über die EPSEC-API können VMware-Antiviren-Partner eine Selbstprüfung der Dateiaktivitäten im Hypervisor vornehmen und somit die eigene Lösung in vShield Endpoint integrieren. Über diese API werden zentrale Antiviren-Funktionen unterstützt.

vShield Manager, Richtlinienverwaltung und Automatisierung

- vShield Manager sorgt für die Bereitstellung und Konfiguration von vShield Endpoint mit vollem Funktionsumfang.
- REST-APIs (Representational State Transfer) ermöglichen die individuelle und automatisierte Integration von vShield Endpoint-Funktionen in Lösungen.
- Überwachungsberichte werden bereitgestellt.
- vShield Manager kann als vCenter-Plug-In genutzt werden.

Protokollierung und Prüfung

- Die Ereignisprotokollierung basiert auf dem branchenweit standardisierten Syslog-Format.

Unterstützte Versionen

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

Zugehörige Produkte

Die Sicherheitsprodukte der vShield-Reihe umfassen VMware vShield Edge zur Perimetersicherheit, vShield App with Data Security zum Schutz von Anwendungen vor Angriffen aus dem Netzwerk und zur Erkennung sensibler Daten, vShield Manager sowie vShield Bundle, in dem sämtliche Produkte zusammengefasst sind.

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 im Administratorhandbuch zu VMware vShield unter http://www.vmware.com/pdf/vshield_41_admin.pdf.

Zusätzliche Informationen zu vShield-Produkten finden Sie unter http://vmware.com/de/products.

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