VMware vShield Endpoint

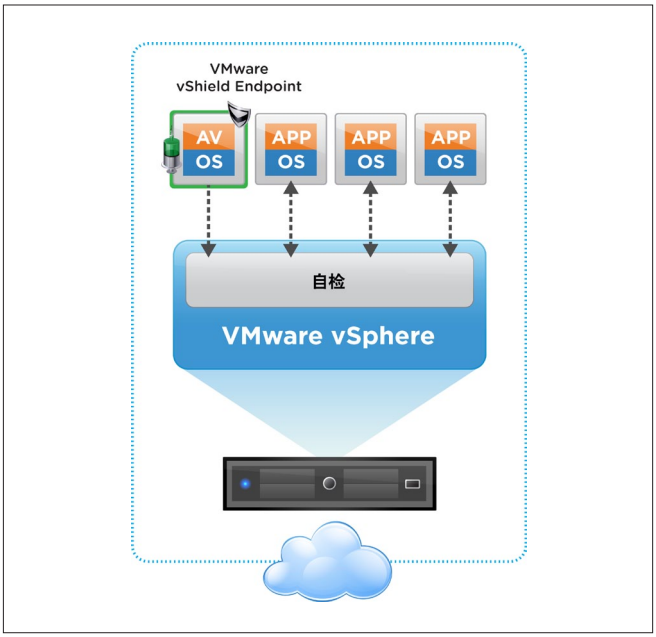
增强虚拟数据中心的端点安全并提高性能

概览

VMware vShield™ Endpoint 可增强虚拟机的安全性，同时将端点保护性能提高几个数量级。vShield Endpoint 可将防病毒和防恶意软件代理处理工作负载卸载到由 VMware 合作伙伴提供的专用安全虚拟设备上。此解决方案旨在充分利用现有投资，让客户在用于保护物理环境安全的同一个管理界面上管理虚拟化环境中的防病毒和防恶意软件策略。

主要优点

- 通过消除客户虚拟机上的防病毒代理，提高整合率以及性能。
- 简化 VMware 环境中的防病毒和防恶意软件部署和监控流程。
- 通过整合防病毒软件代理来减小受攻击面，从而提高安全性。
- 通过将防病毒和防恶意软件活动记入日志来满足遵从性和审核要求。



vShield Endpoint 可提高虚拟化环境中的防病毒和防恶意软件的性能和整合率。

什么是 vShield Endpoint？

vShield Endpoint 彻底革新了大家固有的如何保护客户虚拟机免受病毒和恶意软件攻击的观念。该解决方案优化了防病毒及其他端点安全保护，以便在 VMware vSphere® 和 VMware View™ 环境中使用。

vShield Endpoint 通过将病毒扫描活动从各个虚拟机卸载到安全虚拟设备来提高性能，该虚拟设备具有病毒扫描引擎以及存储的防病毒特征码。对于防病毒和防恶意软件功能，这种体系结构可以消除客户虚拟机中的软件代理，释放系统资源，提高性能，并消除防病毒“风暴”（在进行计划内扫描和特征码更新过程中出现的资源超负荷）的风险。安全虚拟设备与客户虚拟机不同，它不会离线，因此它能够持续更新防病毒特征码，从而为主机上的虚拟机提供无中断保护。同时，新虚拟机（或已经离线的现有虚拟机）在联机时将立即受到最新防病毒特征码的保护。

vShield Endpoint 借助经过安全强化且防篡改的安全虚拟设备（由 VMware 合作伙伴提供，并利用 vSphere 中强大而安全的虚拟化管理程序自检功能）增强了安全性，可减少防病毒和防恶意软件服务本身的漏洞。

vShield Endpoint 还为 VMware 合作伙伴提供接口来实现文件扫描，以及内存扫描和进程扫描。组织可以同时使用多个安全解决方案；例如，他们可以在一个安全虚拟设备中使用 VMware vShield App with Data Security 的敏感数据发现功能，同时在另一个安全虚拟设备中使用防病毒解决方案。

公司可以通过防病毒或防恶意软件服务提供的详细活动日志记录，证明遵从性并满足审核要求。

管理员可通过随附的 vShield Manager 控制台集中管理 vShield Endpoint，该控制台与 VMware vCenter™ Server 无缝集成，以便对虚拟数据中心进行统一的安全管理。

vShield Endpoint 的工作原理

vShield Endpoint 直接嵌入到 vSphere 中，由以下这三个组件组成：

- 经过加强的安全虚拟设备，由 VMware 合作伙伴提供
- 虚拟机精简代理，用于卸载安全事件（包含在 VMware Tools 中）
- VMware Endpoint ESX® 虚拟化管理程序模块，用于支持前两个组件在虚拟化管理程序层上的通信

例如，对于防病毒解决方案，vShield Endpoint 将监视虚拟机文件活动并通知防病毒引擎，然后再由引擎进行扫描并返回处置信息。该解决方案支持在访问时进行文件扫描，以及由安全虚拟设备中的防病毒引擎发起的按需（计划内）文件扫描。

当需要进行修复时，管理员可以使用他们现有的防病毒和防恶意软件管理工具指定要执行的操作，同时由 vShield Endpoint 管理受影响虚拟机中的修复操作。

vShield Endpoint 的用途

由 VMware 合作伙伴提供的管理控制台用于配置和控制在安全虚拟设备中托管的合作伙伴软件。VMware 合作伙伴可以提供一个用户界面，以便使该管理体验（包括策略管理）与管理专用物理安全设备上托管的软件完全相同。

可大幅减少虚拟基础架构管理员的工作量，因为不存在需要管理的虚拟机防病毒代理。相反，合作伙伴的管理控制台用于管理安全虚拟设备。此外，这种方法不需要管理每个虚拟机的频繁更新。在部署方面，VMware Tools 包含精简代理，并且 ESX 模块支持虚拟化管理程序自检。

虚拟基础架构管理员可以轻松监控部署，以确定防病毒解决方案是否正常运行等情况。

主要功能特性

卸载防病毒和防恶意软件负载

- vShield Endpoint 使用 vShield Endpoint ESX 模块将病毒扫描活动卸载到安全虚拟设备中，通过在该设备上执行防病毒扫描提高性能。
- 通过瘦客户端代理和合作伙伴 ESX 模块，将文件、内存和进程扫描等任务从虚拟机卸载到安全虚拟设备中。
- vShield Endpoint EPSEC 使用虚拟化管理程序层的自检功能来管理虚拟机与安全虚拟设备之间的通信。
- 防病毒引擎和特征码文件只在安全虚拟设备内更新，但可对 vSphere 主机上的所有虚拟机应用策略。

修复

- vShield Endpoint 实施防病毒策略，以指定应删除、隔离还是以其他方式处理恶意文件。
- 精简代理负责管理虚拟机内的文件修复活动。

合作伙伴集成

- EPSEC API 在虚拟化管理程序中提供对文件活动的自检，使 VMware 防病毒合作伙伴实现 vShield Endpoint 集成。基本的防病毒功能可通过此 API 提供支持。

vShield Manager，策略管理和自动化

- vShield Manager 提供全方位的 vShield Endpoint 部署和配置。
- 使用表述性状态转移 (REST) API 可以实现 vShield Endpoint 功能与各种解决方案的自定义自动集成。
- 提供监控报告。
- vShield Manager 可用作 vCenter 插件。

日志记录与审核

- 事件日志记录采用基于行业标准的 syslog 格式。

支持的版本

有关受支持的 vSphere、ESX 和 View 环境版本的信息，请访问 http://www.vmware.com/cn/products。

相关产品

vShield 安全产品系列还包括：提供边界安全的 VMware vShield Edge；用于保护应用程序免受网络攻击和发现敏感数据的 vShield App with Data Security；vShield Manager；以及包含所有产品的 vShield Bundle。

了解更多信息

要获取相关信息或购买 VMware 产品，请拨打 010-59934310 或 59934306、访问 http://www.vmware.com/cn/products 或在线搜索授权代理商。有关产品规格和系统要求的详细信息，请参见《VMware vShield 管理指南》：http://www.vmware.com/pdf/vshield_41_admin.pdf。

有关 vShield 产品的其他信息，请访问 http://www.vmware.com/cn/products。

VMware, Inc. 3401 Hillview Ave Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-475-5001 www.vmware.com
北京办公室 北京市海淀区科学院南路 2 号融科资讯中心 C 座 8 层 邮编：100190 电话：+86-10-5993-4310 或 5993-4306
上海办公室 上海市徐汇区淮海中路 1010 号嘉华中心 27 楼 2720-2721 室 邮编：200031 电话：+86-21-6103-1234
广州办公室 广州市天河北路 233 号中信广场 7401 室 邮编：510613 电话：+86-20-3877-1938 www.vmware.com/cn