解决方案简介

通过趋势科技产品优化虚拟桌面安全和性能

概览

VMware vShield 利用虚拟化所带来的独特安全优势（比如自检、变更感知以及利用现有投资的能力）提供优于物理解决方案的云安全保护。vShield 可使 VMware 云比其他任何环境都更安全，因为它可以：

1 **为云部署提供全面保护**

2 **降低实施和管理复杂性**

3 **提高基础架构性能**

4 **加快 IT 合规性的实现**

针对 VMware View 的趋势科技无客户端安全

虚拟化是云计算体系结构的基础。作为倍受客户信赖的虚拟化领导者，VMware 正在指引着通往云计算道路的方向。通过与趋势科技这样的业界领先者通力协作，VMware 正在帮助各种规模的企业向云计算转变，以进入一个最终可以同时解决 IT 成本、复杂性和安全这几大难题的 IT 新时代。

基于 VMware 产品构建的云 – 比其他任何环境都更安全

正如虚拟化是从旧式应用程序向新式云基础架构进行转变不可或缺的基础，它也是云环境中不可或缺的安全保障条件。VMware vShield 系列产品为新一代云安全奠定了基础。

针对增强的端点安全的新桌面模式

VMware View 5 可在客户的“IT 即服务”之旅中为其提供以用户为中心的计算。通过 VMware View，客户能够使操作系统和应用程序脱离物理桌面硬件，并在私有云中管理操作系统、应用程序和数据，从而交付 IT 即服务。

VMware View 5 可以简化 IT 管理，同时可在私有云中提高安全性及对最终用户计算的控制。通过细化的控制级别，IT 可以根据企业策略自定义用户体验、访问及个性化设置。VMware View 5 可以为日常工作中需要应用程序、统一通信和三维图形的用户提供具有最高保真度的体验。由于可跨多种设备平台访问，优化的性能可适应各种用户需求，VMware View 可提供一种全新的工作方式。现在，IT 可以提供弹性的云计算桌面服务，同时具有终极控制、灵活性和性能，当然最重要的还有安全性。

全面实现安全

趋势科技是虚拟化安全领域公认的领军企业，已携手 VMware 联合提供针对虚拟桌面环境进行优化的、具有虚拟化感知能力的安全解决方案。他们已针对虚拟桌面环境开发了一套完整的保护套件，以为各种虚拟桌面方案提供最强的安全保护。趋势科技 Deep Security 与 VMware vShield Endpoint 和 VMware View 结合使用，可以最大程度地保护您的虚拟桌面，同时最大程度地提高性能。

服务器和虚拟桌面保护

趋势科技 Deep Security

专为 VMware 设计的第一套且是唯一一套安全合作伙伴解决方案

- 第一次与 VMsafe API 集成
- 第一次与 vShield Endpoint API 集成
- 第一次提供无客户端防恶意软件

发布第一年就有超过 1000 个客户使用无客户端防恶意软件

虚拟桌面整合率比主要的传统物理桌面防恶意软件解决方案高 3 倍之多。

趋势科技 Deep Security 为物理、虚拟、云服务器以及虚拟桌面提供单一安全平台。趋势科技是第一个与 VMware vShield API 集成的安全供应商，以通过前沿的无客户端技术为您提供更好的保护、更低的管理复杂性以及更高的性能。VMware 和趋势科技解决方案旨在满足虚拟桌面环境的严苛要求，以最大程度地加强保护和安全，同时在性能不受影响的情况下提高 ROI。

使用虚拟桌面时，您的桌面是在数据中心内受保护的服务器上运行，因此可以帮助您保持所需的控制和安全。另外，通过虚拟端点，如果设备丢失或被盗，则敏感数据会存储在数据中心内并受到保护。但是，在虚拟桌面基础架构中使用专为物理桌面提供的安全解决方案可能会导致性能下降、虚拟机密度减小以及虚拟桌面 ROI 降低。因此，若要安全利用虚拟桌面，客户需要能够解决此 IT 环境特有的挑战的安全解决方案。通过使趋势科技无客户端防恶意软件在 VMware 环境中运行，您可以获得具有虚拟化感知能力的安全解决方案，以应对虚拟环境特有的威胁，同时最大程度地提高性能。

虚拟桌面环境特有的挑战

物理和虚拟桌面都需要防恶意软件的保护，但是虚拟桌面防恶意软件安全解决方案必须专为共享资源环境设计。如果部署了传统的物理安全解决方案，则则跨所有单个虚拟桌面实例的防恶意软件会造成主机性能下降，这与您要使用虚拟桌面提高效率的初衷相悖。虚拟桌面的易配置性可能会造成难以保证虚拟桌面安全及时更新。只有具有虚拟化感知能力的安全解决方案可以应对下面这些虚拟桌面安全挑战：

- 资源争夺：在虚拟桌面部署中，大量桌面共享主机的硬件资源，共享比例通常为 60:1 甚至更高。同步安全更新和全系统扫描可能会导致桌面性能显著下降：可用性受限或虚拟机整合率降低。
- 即时启动间隔：虚拟桌面可以快速配置、克隆、恢复至以前的实例、暂停和重新启动，所有这些操作都简单易行。漏洞或配置错误可能会在不知情的情况下传播，休眠的桌面映像可以通过过期安全重新激活。
- 合规性和数据隐私：虚拟桌面的易配置性和移动性，导致很难维护任意给定时间虚拟桌面安全状况的可审计记录。但是，很多法规要求对当前防恶意软件防护提供证明。

传统防恶意软件模型与无客户端防恶意软件对比

- 虚拟桌面密度更大
- 安全性更高
- 管理更容易
- 性能更高

VMware 和趋势科技

趋势科技虚拟和云安全

- 用于服务器和虚拟桌面安全的 Deep Security
- 用于数据保护的 SecureCloud

趋势科技 VMware Ready 安全虚拟设备

- Web 安全
- 邮件安全
- 电子邮件加密
- 数据丢失预防

趋势科技无客户端安全设备专为 VMware 虚拟桌面设计

趋势科技 Deep Security 与 VMware vShield Endpoint API 集成，以为您提供无客户端防恶意软件。这种无客户端安全可以优化虚拟化性能并降低管理复杂性，因此非常适用于您的 VMware View 虚拟桌面环境。强化安全的专用虚拟设备与 VMware Hypervisor API 集成，以访问每个客户虚拟桌面中的小型 VMware 驱动程序来协调交错更新和扫描。占用大量资源的操作（例如全系统扫描）通过单独的扫描安全虚拟设备执行。

该安全虚拟设备可以确保虚拟桌面在休眠时是安全的，而且在重新激活后可以使用最新的安全更新。此“实时”无客户端安全可以提供虚拟补丁修复，以防御零日威胁并降低紧急修复虚拟桌面的需要。有了专用的安全虚拟设备和无客户端防护，可以避免因安全客户端占用额外空间而影响虚拟机和底层主机。由于无需部署、配置或更新客户端，因此无客户端安全还可以降低管理复杂性。

专为虚拟桌面设计的安全帮您推动企业向前发展

- 提高虚拟桌面 ROI – 交错更新和扫描以及不在客户虚拟机上使用客户端，可以减轻底层主机上的资源负担，从而最大程度地提高性能，增加虚拟桌面整合率。
- 实时、防干扰安全 – 专用强化安全虚拟设备可在虚拟机的整个生命周期内为虚拟机提供最新防护，包括虚拟补丁修复。
- 增强可见性和控制力 – 趋势科技 Deep Security 与 VMware vShield Endpoint 和 VMware View 结合使用，深入剖析虚拟桌面安全并简化虚拟化环境合规性的实现。

虚拟桌面的强大功能可让您的组织发生转变。趋势科技携手 VMware 提供的安全解决方案可以优化虚拟桌面保护和性能，是您的理想之选。如果让用户可以随时随地在任何设备上访问其桌面、应用程序和数据，无疑会达到一种共赢的局面。

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA，电话 877-486-9273，传真 650-427-5001，www.vmware.com