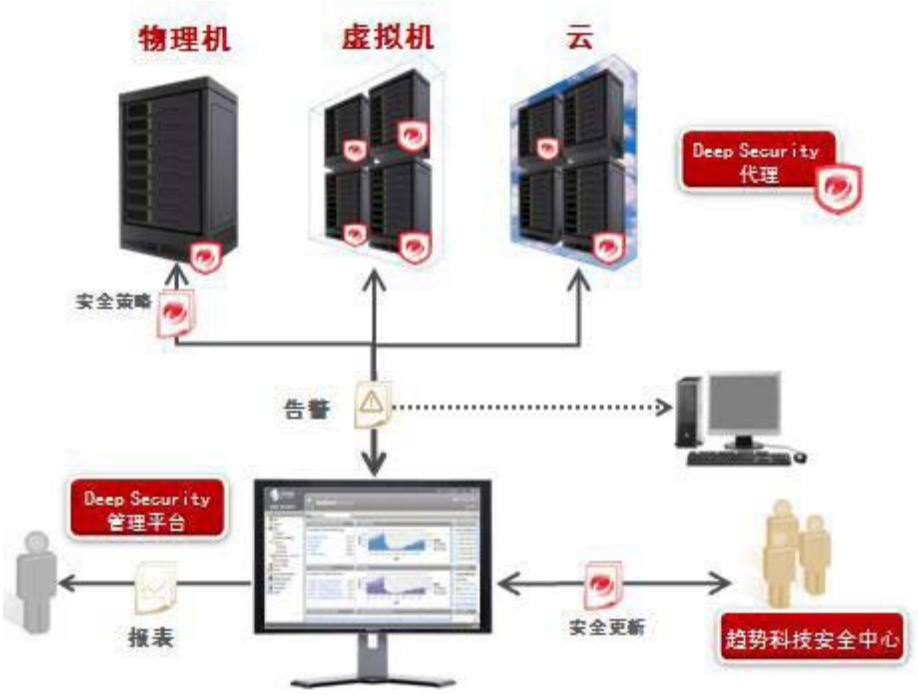
Trend Micro Deep Security 7 – 服务器深度安全防护系统

提供动态数据中心服务器及应用程序的保护



趋势科技提供有效率、简化、整合的产品和服务以及完整的解决方案。能在关注成本效益的条件下保护敏感的机密数据，并且将风险降至最低。趋势科技 Deep Security 是一套综合的服务器和应用程序保护软件，能使企业物理的、虚拟 的及云计算环境拥有自我防御能力。Deep Security 所采用的主动深度威胁保护技术，能实时自动追踪最新动态威胁，有效及优化配置安全策略，减低系统资源开销和安全管理成本。

无论是以软件、虚拟应用或是混合式的方式实施，Deep Security 可以减少系统开销、简化管理及加强虚拟机的透明性和安全性。除此之外，还遵循了广泛的规范性要求，包括六个主要的 PCI 规范要求，网络应用层防火墙、IDS/IPS、文件完整性监控及网络划分。 最新的主动性深度安全技术搭配完整的安全模块，广泛的操作平台、应用程序支持；趋势科技 Deep Security 是数据中心、服务器安全管理不可或缺的革命性单一统一管理系统。

架构

- **Deep Security Virtual Appliance (DSVA)** 在 VMware vSphere 虚拟机器上为 IDS/IPS、网络应用程序保护、应用程序控管及防火墙保护等透明化地加强安全策略--如果需要可以与 Deep Security Agent 协调合作提供完整性的监控及日志审计。
- **Deep Security Agent (DSA)** 部署于被保护的服务器或者虚拟机上的一个轻小的软件组件，能有效协助执行数据中心的安全政策(IDS/IPS、网络应用程序保护、应用程序控管、 防火墙、完整性监控及日志审计)。
- **Deep Security Manager (DSM)** 功能强大、集中式管理，是为了使管理员能够创建安全配置并将它们应用于服务器，监控 警报，对威胁采取预防措施，分发安全更新到各服务器，

生成报告。新的事件标注功能简化了大批量的事件管理。

- **Security Center** 我们的安全专家团队针对最新安全漏洞通过快速开发和提供安全更新来帮助您防御最新的威胁。客户门户网站让您可以访问能部署到 DSM 的安全更新。

部署及整合

整合既有的 IT 及安全投资进行快速部署

- 集成 VMware vCenter 的 VMware 和 ESX 服务器能够将组织与营运信息汇入 Deep Security Manager 中，这样详尽的安全就能被应用到企业的 VMware 基础结构上。
- 与 VMsafe ™ APIs 的集成使得它能在 ESX 服务器上作为一个虚拟应用快速部署，并立即开始透明化地保护 vSphere 虚拟机。
- 透过多种整合选项，提供详细的服务器级别的安全事件至 SIEM 系统，包括 ArcSight ™、Intellitactics、NetIQ、RSA Envision、Q1Labs、Loglogic 和其它系统。
- 能与企业级的目录作整合，包括 Microsoft Active Directory。
- 可配置的管理通讯方式，允许 Manager 或 Agent 发起通信请求，这样就能减少或消除一般情况下的中央管理系统所必须的对防火墙的修改。
- 可以透过标准的软件分发机制如 Microsoft ® SMS、Novel Zenworks 和 Altiris 轻松部署代理软件。

主要优势

最完整的安全软件

- 多层面安全防护
- 广泛的操作平台及服务应用支持
- 完整虚拟环境基础架构整合
- 灵活部署任何阶段 IT 环境

预防数据破坏及营运受阻

- 提供无论是实体、虚拟或云中的服务器防御
- 防堵在应用程序和操作系统上已知及未知的漏洞
- 防止网页应用程序遭受 SQL 注入及跨网站脚本攻击
- 阻挡针对企业系统的攻击
- 辨识可疑活动及行为，提供主动式和预防性的措施

协助企业遵循 PCI 及其它规范和准则

- 满足 6 大 PCI 数据安全准则及一系列广泛的其他法规要求
- 提供详细的可审计报告，包含已被阻止的攻击和策略遵循状态
- 减少支持审计所需要的准备时间和投入

实现经营成本的降低

- 透过服务器资源的合并，让虚拟化或云计算的节约更优化
- 透过安全事件自动管理机制，使管理更加简化
- 提供漏洞防护让安全编码优先化及和弱点修补成本有效化
- 通过一个中心管理的多用途软件代理或虚拟设备，消除了部署多个软件客户端所产生的成本

Deep Secrutiy 模块

深度包检查与过滤

- 检查所有进出的通信流中的对协议的违反，内含的攻击内容及策略违反
- 在侦测或预防模式下运作，以保护操作系统和企业应用程序漏洞
- 能够防御应用层攻击、SQL 注入及跨网站脚本攻击
- 提供有价值的信息，包含攻击来源、攻击时间及试图利用什么方式进行攻击
- 当攻击事件发生时，会自动通知管理员

入侵侦测和防御

- 防堵已知漏洞及零日攻击，避免无限制的攻击
- 每小时自动防堵发现到的最新漏洞，无须重新开机，即可在几分钟内就可将防御部署至成千上万的服务器上
- 提供包括数据库、网页、电子邮件和 FTP 服务器等 100 多个应用程序的漏洞保护
- 智能型防御规则提供零日保护，通过检测不寻常的内含恶意代码的协议数据，以确保不受未知的漏洞攻击

完整性监控

- 监视关键操作系统和应用程序文件，如目录、注册表项及数值，以侦测出恶意和未授权的更改
- 侦测现有文件系统中的修改及新文件的创建，并提供实时报告
- 可启动按需、计划或实时的侦测，检查文件属性 (PCI 10.5.5) ，监控特定目录
- 通过包含/排除和可审核报告，提供灵活且实用的监控

网页应用程序保护

- 协助遵循规范(PCI DSS 6.6)以保护网页应用程序和他们所处理的数据
- 防护SQL注入、跨网站脚本攻击和其它网页应用程序漏洞
- 在漏洞修补期间，提供完整的漏洞防护

应用程序控制

- 增加对应用程序访问网络的控管及可见度
- 使用应用程序控管规则，可侦测出恶意程序私下访问网络的行为

- 降低服务器漏洞

双向状态防火墙

- 减少的实体、云端及虚拟服务器被攻击的接口
- 集中管理服务器防火墙策略，包括常用的服务器模板
- 精细的过滤功能（IP与MAC地址、通讯端口），针对不同网络接口设计的策略和位置意识
- 防止DDos攻击和侦测扫描
- 包括所有基于IP的协议（TCP、 UDP、 ICMP 等）和所有帧类型（IP、ARP 等)

日志审计

- 收集和分析操作系统和应用程序日志中的安全事件
- 协助遵循规范(PCI DSS 10.6) 优化识别埋在多个日志项下的重要安全事件
- 将事件转至SIEM系统或中央日志服务器，做关联性分析、报告和归档
- 侦测可疑行为、收集数据中心的安全事件和管理操作，并使用OSSEC 语法来建立高级规则

能保护的平台

Microsoft Windows

- 2000 (32位)
- XP (32 /64位)
- XP Embedded
- Windows 7
- Windows Vista (32/64位)
- Windows Server 2003 (32/64位)
- Windows Server 2008 (32/64位)

Solaris

- OS：8,9,10 (64位SPARC, x86)

Linux

- Red Hat Enterprise 3.0 (32位), 4.0, 5.0 (32/64位)
- SUSE Enterprise 9, 10 (32位)

UNIX

- AIX 5.3
- HP-UX 10, 11i v2, 11i v3

虚拟化

- VMware：VMware ESX Server (guest OS)
- Citrix：XenServer Guest VM
- Microsoft：HyperV Guest VM
- Sun：Solaris 10 OS Partitions

主要认证及结盟

- Common Criteria EAL 3+
- PCI Suitability Testing for HIPS (NSS Labs)
- Virtualization by VMware
- Microsoft Application Protection Program
- Microsoft Certified Partnership
- Novell
- Oracle Partnership
- HP Business Partnership
- It is also certified Red Hat Ready