# 经济高效的虚拟化和云安全

## 更安全的整合，更低廉的成本

虚拟化和云计算可以帮助您的组织在数据中心的硬件成本、运营支出及能源需求方面实现大幅节约，同时还可提高服务质量和业务灵活性。然而，很多组织却未意识到，在虚拟环境中使用现有的物理服务器安全解决方案会限制他们充分利用虚拟化和云技术的能力。更糟糕的是，这样会使他们以多种尚不可预见的方式暴露，从而造成严重的安全漏洞，甚至在执行并发安全操作时会出现性能下降。为此，趋势科技提供了专门的虚拟化安全解决方案，旨在帮助您充分、安全地利用虚拟化环境。

## 虚拟化和云旅程中的安全障碍

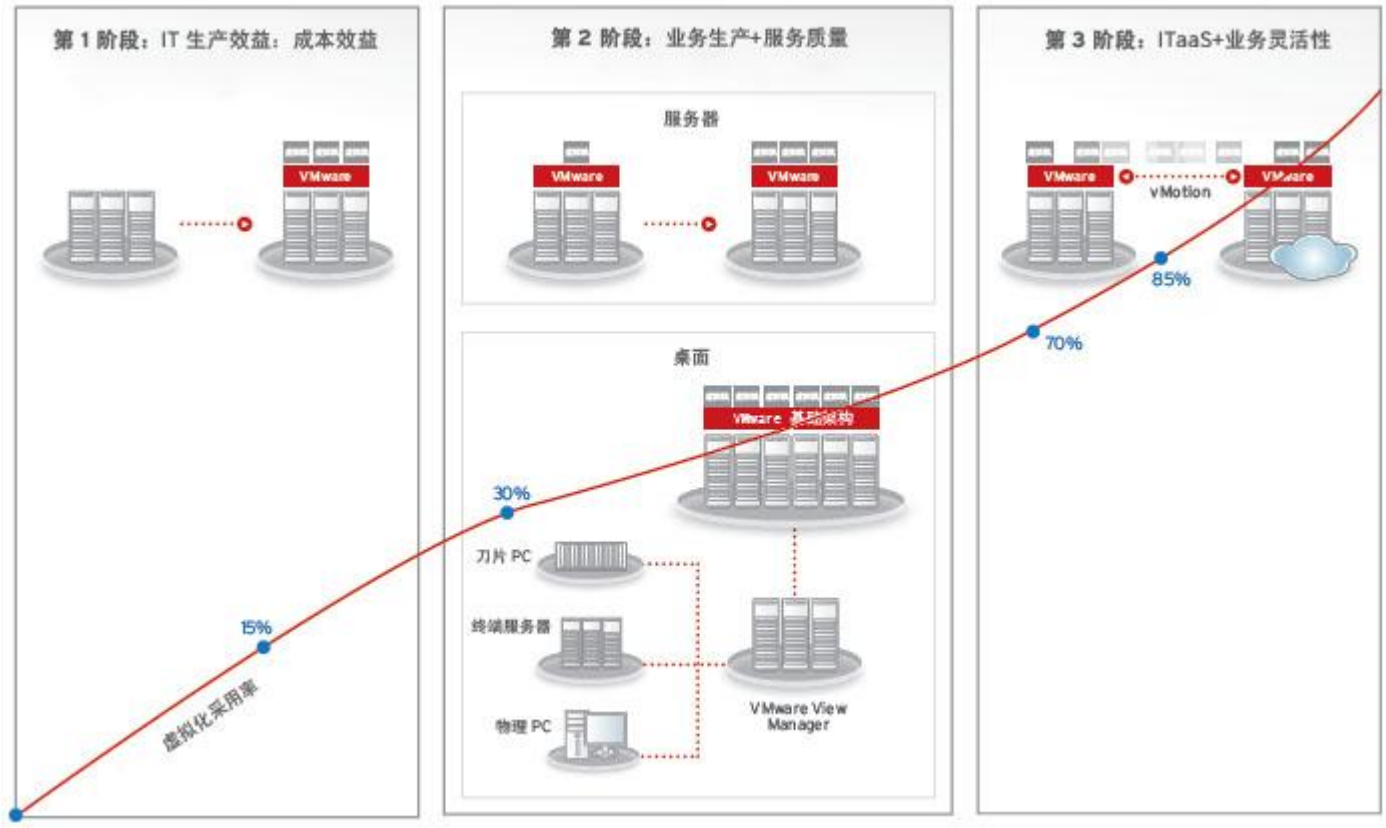
客户典型的虚拟化旅程可分为 3 个阶段：

**第 1 阶段：虚拟化 IT 系统** — Web 服务器、文件和打印服务器等

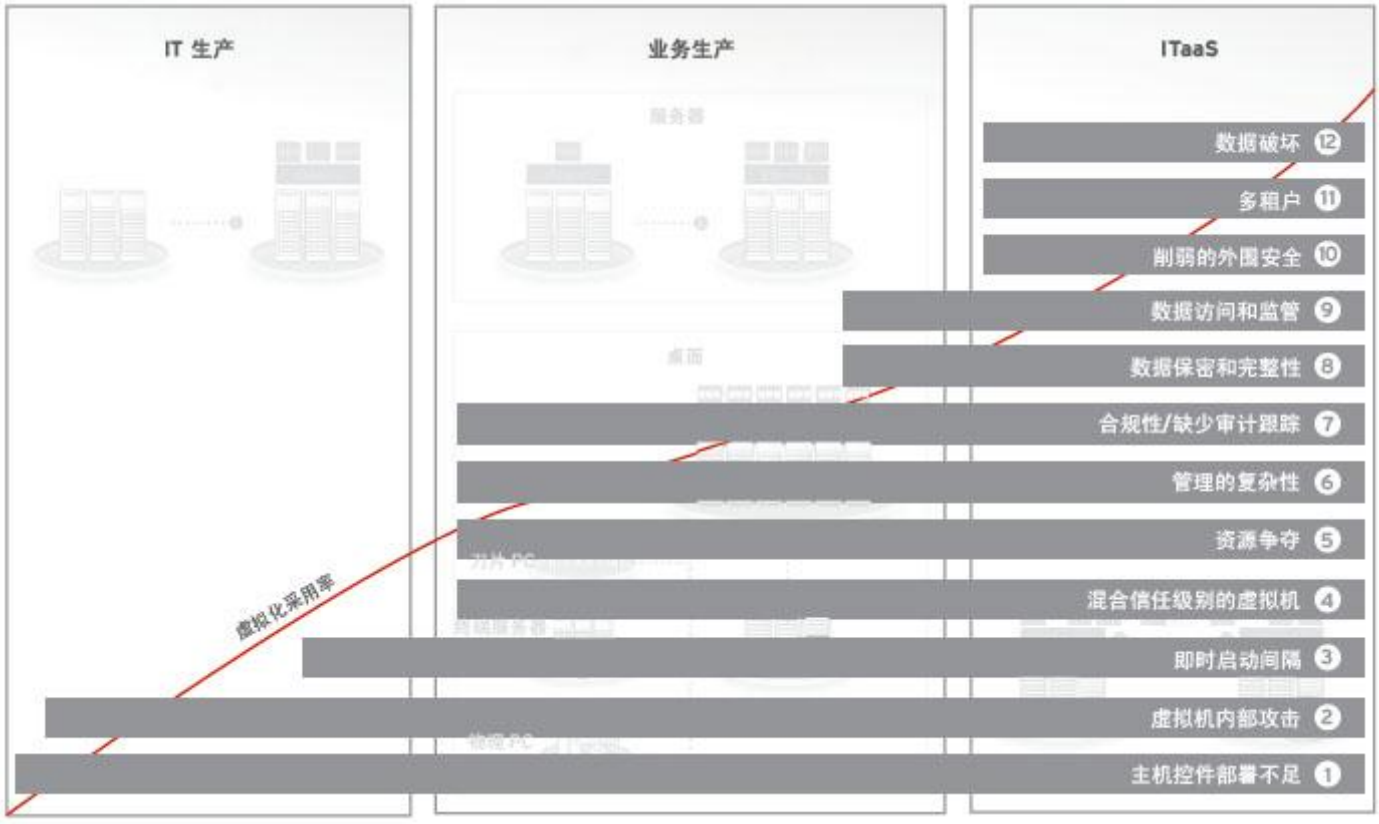
**第 2 阶段：虚拟化 LOB 系统** — 关键业务服务器和 1 级应用程序以及桌面

**第 3 阶段：采用私有云或公共云**

成本和效率优势可以加快您的虚拟化进程。但是，利用从物理服务器环境转变而来的传统安全解决方案可能会成为您虚拟化进程中的一大障碍，这些解决方案多数都出现在 X86 虚拟化之前，不能在此环境中运行。网络盲点、即时启动间隔、混合信任级别的工作负荷以及防病毒风暴等问题是此环境所特有的全新挑战，需要一种专门针对此环境的新型安全解决方案加以应对。



| **虚拟化之旅：**旅程中的安全障碍 | |
|---|---|
| 安全挑战 | 详细信息 |
| 基于主机的控件部署不足 | 文件完整性监控、主机 IDS/IPS 和防恶意软件往往因成本、复杂性或性能因素而部署不足 |
| 虚拟机内部攻击 | 传统网络安全设备无法检测或抑制恶意的虚拟机内部通信 |
| 即时启动间隔 | 持续确保“即时启动”虚拟机的安全并不断对其进行更新，这几乎是无法实现的。处于休眠状态的虚拟机最终可能会严重偏离基准，以致于仅仅启动它们就可能引入大量安全漏洞 |
| 混合信任级别的虚拟机 | 不同信任级别的工作负荷可能会整合到单台物理服务器上，而没有进行充分的分离 |
| 资源争夺 | 占用大量资源的操作（防病毒风暴和特征码文件更新）可能在很短的时间内导致系统不堪重负 |
| 管理的复杂性 | 虚拟化已导致虚拟机比物理机以更快的速度增长（虚拟机蔓延），从而增加了为每个虚拟机配置安全客户端时的复杂性，而且还要不断为每个虚拟机重新配置、修复和生成特征码 |
| 合规性/缺少审计跟踪 | 整合率越高，实现合规性（特别是关键业务/1 级应用程序合规性）的压力就越大。而且，虚拟化加大了维护审计跟踪以及了解由谁做了哪些更改的难度 |
| 数据保密和完整性 | 云环境中未加密的信息可能面临着各种风险，包括遭窃、未授权泄露以及恶意操作 |
| 数据访问和监管 | 云中的 Restful 认证* 可能遭受到暴力攻击和劫持，这些攻击会造成对数据进行未授权访问。职责分离中出现的问题可能会造成未授权的供应商访问数据（* 表达性状态转移） |
| 削弱的外围安全 | 安全机制在云服务提供商的掌控之下，外围安全机制大大削弱了 |
| 多租户 | 在云环境中，除了您的虚拟机，还有其他不熟悉的、潜在的恶意虚拟机，您对这些虚拟机的安全状况并不了解 |
| 数据破坏 | 有些云提供商在将存储提供给另一个租户循环利用之前不会覆盖存储；在存储被覆盖的情况下，如果系统出现崩溃或意外终止，那么数据可能会易于遭到攻击 |



## 增强的虚拟化安全

趋势科技拥有最广泛最深入的安全解决方案套件，专门用于保护虚拟环境的安全。趋势科技服务器深度安全防护系统提供了先进的安全软件来保护虚拟、物理和云服务器以及虚拟桌面上的操作系统、应用程序和数据可帮助您防止虚拟化数据中心出现数据泄露和业务中断，同时实现合规性。该解决方案还可实现更高的整合率、最大程度地提高性能以及提高运营灵活性。通过该解决方案，您的 IT 基础架构可获得全面、集成的保护，其中包括：


## 解决方案组件

趋势科技服务器深度安全防护系统包含以下解决方案组件：

- **趋势科技服务器深度安全防护系统客户端：**部署在虚拟机或物理服务器上为其提供保护的小型软件组件
- **趋势科技服务器深度安全防护系统网关：**一个打包的安全虚拟机，可保护 VMware vSphere 服务器上的其他所有虚拟机，并具有用于实现无客户端保护的功能
- **趋势科技服务器深度安全防护系统管理中心：**一种功能强大且可自定义的集中式控制台，用于管理客户端或网关
- **安全中心：**可以自动或按需为管理中心提供安全更新的门户
- **云安全智能防护网络：**新一代云客户端基础架构，用于为网关提供实时的恶意软件防护

趋势科技服务器深度安全防护系统网关和客户端

## 无与伦比的虚拟化安全

趋势科技服务器深度安全防护系统在保护虚拟服务器和桌面环境的安全方面远远优于市面上的其他任何产品。

1. **全面的安全防护。**趋势科技服务器深度安全防护系统由一个包含多个高级保护模块的集成安全解决方案组成，这些模块包括防火墙、入侵检测和防护、Web 应用程序防护、文件完整性监控、日志检查和防恶意软件。

2. **新一代体系结构。**趋势科技服务器深度安全防护系统与虚拟机监控程序 API 集成，可为 VMware vSphere 环境提供无客户端安全防护。趋势科技服务器深度安全防护系统网关与 VMware 携手趋势科技开发的全新 vShield Endpoint API 相集成，提供了业界第一个专用于保护 vSphere 平台的防恶意软件解决方案，且无需在虚拟机中使用客户端。此外，此网关还使用 VMsafe API 从虚拟机外部为所有虚拟机提供防火墙、IDS/IPS 和 Web 应用程序防护。

3. **终极灵活性。**趋势科技服务器深度安全防护系统网关可与任何客户虚拟机客户端一起使用，以最大程度地增加安全覆盖范围和可扩展性。客户端可用于高风险虚拟机以提供附加保护（例如完整性监控和日志检查），也可用于占用资源较多的虚拟机以最大程度地提高系统性能。如果删除了虚拟客户机客户端，则网关将自动介入为虚拟机提供保护。

4. **与 VMware 产品紧密集成。**趋势科技服务器深度安全防护系统还与 VMware vCenter 集成，因此它始终会盘点网络中的虚拟机，并可以在新虚拟机在网络中激活后自动保护它们。这种密切协作还可以使组织和运营信息从 vCenter 和 ESX 节点导入趋势科技服务器深度安全防护系统管理中心，将具体的安全措施应用于企业的 VMware 基础架构。

5. **即时防护。**趋势科技服务器深度安全防护系统还集成了趋势科技云安全智能防护网络，这是一种新一代的云客户端基础架构，将成熟的云技术和趋势科技实验室研究人员的专业技术结合起来，以实时为每个系统提供威胁相关信息。不再需要将生命期不断缩短的大型特征码文件不断下载到网络中的每个虚拟机。

6. **面向未来。**趋势科技服务器深度安全防护系统不仅仅可以从云中提供安全保护，还能为云提供安全保护，因此不管企业何时迁移至云环境，均可获得永久的安全保护。

### 功能和优势

- **防护技术集成套件：**组合多个模块以在服务器上实现全面的、经济高效的安全保护
- **虚拟机内部攻击防御：**检测并防御针对敏感数据的攻击（包括来自同一服务器上其他虚拟机的攻击），从而立即警告试图发起攻击的人
- **即时防护：**确保虚拟机（既包括新出现的虚拟机，也包括最近激活的虚拟机）在启动的一霎能够自动获得保护，而无需执行管理操作
- **防干扰：**将防恶意软件与正在扫描的虚拟机隔离，以抵御试图通过卸载、抑制或欺诈性地修复防病毒安全逃过检测的恶意软件
- **支持动态环境：**通过在每个虚拟机周围创建一个安全的容器来保护混合工作负荷虚拟机环境和多租户云环境
- **性能改进：**通过转交占用资源较多的操作（例如全系统扫描和特征码更新）来防止出现防病毒风暴和性能下降
- **简化管理：**无需管理员在每个虚拟机中配置客户端，也无需不断为每个客户端重新配置、修复和生成特征码，从而简化了管理

### 受保护的平台

- VMware vSphere
- Citrix XenServer
- Microsoft Hyper-V

### 相关产品

- 虚拟机核心保护
- 防毒墙网络版
- InterScan™ Web 安全网关
- InterScan™ 邮件安全网关

TREND MICRO™ 趋势科技