平台架构

亚信安全™ 服务器深度安全防护系统 Deep Security 虚拟设备 以透明的方式在 VMware vSphere 虚拟机上实施安全策略以提供无代理的防恶意软件、Web 信誉、入侵阻止、完整性监控和防火墙保护，如果需要还可以与亚信安全服务器深度安全防护系统客户端配合使用以进行日志检查和深度防御。

亚信安全™ 服务器深度安全防护系统 Deep Security 客户端 通过部署在受保护的服务器或虚拟机上的小型软件组件（可采用诸如 Chef、Puppet 和 AWS OpsWorks 等领先的操作管理工具自动部署）来实施数据中心的安全策略（防恶意软件、入侵防御、防火墙、完整性监控和日志检查）。

亚信安全™ 服务器深度安全防护系统 Deep Security 管理中心 强大的集中式管理控制台：基于角色的管理和多级别策略继承功能可进行精细控制。建议扫描和事件标记等任务自动化功能可简化日常安全管理。多租户架构使各个租户策略相互独立，并可将安全管理功能委派给租户管理员。

全球威胁情报 亚信安全™ 服务器深度安全防护系统 Deep Security 与亚信安全云安全智能防护网络集成，通过持续评估并关联网站、电子邮件资源和文件的全球性威胁和信誉情报，提供实时防护以免遭新出现威胁的危害。

平台架构

Microsoft®Windows®

- Windows XP,Vista,7,8,8.1（32位/64位）
- Windows Server 2003（32位/64位）
- Windows Server 2008,2008 R2,2012,2012 R2（64位）
- XP Embedded

Linux

- Red Hat® Enterprise 5,6（32位/64位）[1]
- SUSE® Enterprise 10,11（32位/64位）[1]
- CentOS 5,6（32位/64位）[1]
- Amazon Linux[1]
- Ubuntu 10,12,14.04（64位）[1]
- Oracle Linux 5,6（32位/64位）[1]
- Cloud Linux 5,6（32位/64位）[1]

Oracle Solaris™

- 操作系统：9,10,11（64位SPARC）,10,11（64位x86）[2]
- 通过支持Solaris操作系统的Oracle Exadata Database Machine,Oracle Exalogic Elastic Cloud和SPARC Super Cluster

UNIX

- AIX 5.3,6.1，位于IBM Power Systems上[3]
- HP-UX 11i v3 (11.31)[3]

虚拟

- VMware®：5.1/5.5/v Cloud Networking and Security 5.1,View 4.5/5.0/5.1,ESX 5.5
- Citrix®：Xen Server[4]
- Microsoft®：Hyper V[4]

重要认证和联盟

- Amazon 先进技术合作伙伴
- Red Hat Ready 认证
- 经过Cisco UCS 验证
- Common Criteria EAL 4+
- HP 业务合作伙伴
- Microsoft 应用程序保护方案
- Microsoft 认证合作伙伴
- Oracle 合作伙伴
- PCI Suitability Testing for HIPS(NSS Labs)
- 经过 VCE Vblock 验证
- VMware 虚拟化

vmware

Microsoft Azure

AsiaInfo 亚信安全

北京：86-10-5825 6889
上海：86-21-6384 8899
广州：86-20-8755 3895
南京：86-25-5851 2888
天津：86-22-6621 1165
成都：86-28-6687 6200
杭州：86-571-8190 3773

欲知更多网络安全及相关产品信息，
请拨打免费咨询电话：800-820-8876
或登录亚信安全官网：www.asiainfo-sec.com

亚信安全™

服务器深度安全防护系统 Deep Security

适用于物理、虚拟和云服务器的全方位安全平台

虚拟化和云计算使当今的数据中心改换了面貌。许多组织纷纷从传统的物理环境迁移至虚拟化和云环境的现代数据中心，但这些组织仍然使用传统的安全解决方案。传统的安全解决方案会增加虚拟环境中操作复杂性，同时降低了主机性能和虚拟机（VM）密度，造成安全空白，从而影响将关键业务应用转移至灵活的、低成本的云环境的信心。最终，在现代数据中心中使用传统的安全解决方案，会阻碍虚拟化和云计算的投资收益率（ROI）。

防止数据泄露和业务中断

亚信安全™ 服务器深度安全防护系统 Deep Security（可用作软件或软件即服务）旨在保护您的数据中心和云中应用免遭数据泄露和业务中断。通过跨虚拟环境和云环境经济高效地填补保护空白，同时实现合规性。

从单个控制台进行多功能安全托管

亚信安全™ 服务器深度安全防护系统 Deep Security 以集成模块为特色，这些模块包括防恶意软件、Web信誉、防火墙、入侵阻止、完整性监控和日志检查，可跨物理、虚拟和云环境确保服务器、应用程序和数据的安全。亚信安全服务器深度安全防护系统可跨所有环境作为单个多功能客户端部署，并通过适用于所有功能的单个管理控制台来简化安全操作。

无缝集成实现跨云环境扩展策略

亚信安全™ 服务器深度安全防护系统 Deep Security 与云平台（包括 Amazon Web Services (AWS)、Microsoft Azure 和 VMware vCloud Hybrid Service）无缝集成，让您能够将数据中心安全策略扩展到基于云的工作负荷。借助跨不同环境和优化后的广泛功能，亚信安全服务器深度安全防护系统有助于企业和服务提供商为其用户提供差异化的、多租户云安全环境。

重要业务问题

虚拟桌面安全

利用专门构建的、全面的无代理安全解决方案来保持虚拟桌面的性能和整合率，最大限度地增强对 VDI 环境的防护功能

虚拟补丁

在漏洞被利用之前将其屏蔽，从而消除紧急修补、频繁安装补丁和代价不菲的系统停机等不愉快的操作体验

合规性

达到并且证实符合一系列合规性要求，其中包括 PCI DSS 3.0、HIPAA、HITECH、FISMA/NIST、NERC、SAS 70 等等

提高新业务实施效率

集成NSX，可实现防护层之间的流自动化，安全策略部署更简便，且部署中无需要再重启 ESX 服务器，使得任意新增的ESX服务器都能到自动获得防护

多种虚拟化平台支持无代理安全技术

包括VMware vSphere, Citrix Xen, Miscrosoft Hyper-V, Huawei Fusion， China Cloud

通过实现现代数据中心的安全性，提升云和虚拟化的投资收益

虚拟化安全性

亚信安全™ 服务器深度安全防护系统 Deep Security 使虚拟桌面和服务器免受零日攻击、恶意程序和基于网络攻击的侵害，同时最大限度地降低资源利用率低和紧急修补导致的运营影响。

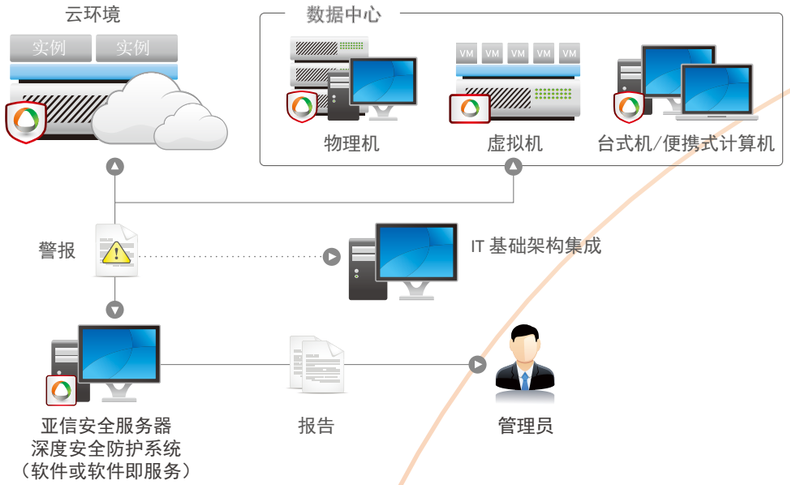
云安全

服务提供商、拥有现代数据中心的用户利用亚信安全服务器深度安全防护系统，可提供安全的多租户云环境，所利用的安全策略可扩展到云中应用，并通过统一的上下文感知策略集中管理。

集成的服务器安全

亚信安全™ 服务器深度安全防护系统 Deep Security 将所有服务器安全功能整合到一个全面、灵活的集成式平台上，该平台可以跨物理、虚拟和云服务器提供最佳防护。

跨物理、虚拟和云环境控制安全性



亚信安全Deep Security客户端

亚信安全Deep Security虚拟设备

亚信安全Deep Security管理中心

关键优势

提升虚拟化和云的投资收益

- 与有代理的传统防恶意软件解决方案相比，可实现更高效的资源利用率和管理、更高的虚拟机密度
- 作为单个易于管理的多功能安全代理，可增加灵活性和深度防御功能
- 通过虚拟机监控程序级别的重复数据不扫描功能，提供无与伦比的性能
- 与云平台（包括 AWS、Microsoft Azure 和 VMware vCloud Hybrid Service）集成，使组织可以通过统一的上下文感知安全策略来管理物理、虚拟和云服务器
- 通过多租户架构，使服务提供商可以通过独立于其他租户的方式向客户提供安全的公有云
- 提供自动扩展、实用程序计算和自助服务，以支持组织灵活运行软件定义的数据中心
- 利用亚信安全服务器深度安全防护系统与 VMware 的紧密集成，自动检测新虚拟机，并应用基于上下文的策略实现跨数据中心和云始终如一的安全性
- 与VMware NSX™ 集成。亚信安全服务器深度安全防护系统可在软件定义的数据中心扩展微分段的优势，无论虚拟机在什么地方，这些虚拟机均可以自动使用安全策略和防护功能

防止数据泄露和业务中断

- 在几乎不影响性能的情况下实时检测并处理虚拟服务器中的恶意软件
- 阻止试图通过卸载或中断安全程序避开检测的恶意软件
- 屏蔽 Web、企业应用程序和操作系统中的已知和未知漏洞
- 在检测到可疑或恶意活动后，发送警报并触发主动式预防措施
- 利用亚信安全的全球域信誉数据库 Web 信誉威胁情报，跟踪网站的可信度，并防止用户访问受感染的站点
- 使用亚信安全的全球域信誉数据库统一威胁情报，识别和阻止僵尸网络及目标攻击命令和控制（C&C）通信

最大程度降低运营成本

- 通过集中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而产生的成本
- 通过与亚信安全、VMware和企业目录的管理控制台紧密集成，降低了复杂性
- 提供了漏洞屏蔽功能，以便进行安全编码并以符合成本效益的方式实施非预定修补
- 通过自动执行重复和耗费资源的安全任务、减少误判安全警报的数量和启用安全事件响应工作流，降低了管理成本
- 通过基于云的事件白名单和可信事件，显著降低了管理文件完整性监控的复杂程度
- 通过建议扫描来检测系统和应用漏洞，从而部署策略防止漏洞被利用
- 利用更轻松、更加动态的智能代理来简化部署，最大限度地跨数据中心和云分配资源，从而确保提高运营效率
- 将安全性与您的策略需求相匹配，从而减少特定安全控件所需的专用资源
- 通过跨亚信安全安全产品进行集中式管理来简化管理。集中式报告多个安全控件可降低针对各个产品创建报告所带来的挑战

以符合成本效益的方式实现合规性

- 通过一个符合成本效益的集成解决方案满足 PCI DSS 3.0、HIPAA、HITECH、NIST 和 SAS 70 对应的主要合规性要求
- 提供审计报告，这些报告记录了阻止的攻击和合规性策略状态
- 减少了满足审计要求所需的准备时间和精力
- 支持内部合规性举措，提高了内部网络活动的可见性
- 利用获得 Common Criteria EAL 4+ 认证的成熟技术

亚信安全服务器深度安全防护系统平台模块

防恶意软件及 Web 信誉

- 集成 VMware vShield Endpoint API，无需占用任何客户虚拟机资源即可保护 VMware 虚拟机，防止其受病毒、间谍软件、木马和其他恶意软件的侵害
- 提供一个防恶意软件客户端，可将防护范围扩展到虚拟、物理和云服务器，包括 AWS、Microsoft 和 VMware 环境
- 可以通过缓存 VMware ESX 级别的数据和删除数据来提高性能
- 优化安全操作，避免全系统扫描和特征码更新时传统安全功能中出现常见的防病毒风暴
- 通过隔离恶意软件与关键操作系统和安全组件来防止虚拟环境中的复杂攻击。
- 与亚信安全™ 云安全智能防护网络™ 全球威胁情报集成，以提高 Web 信誉功能，从而更好地保护服务器和虚拟桌面

入侵阻止

- 检查所有输入和输出通信，不给任何违背协议、违反策略和可能导致攻击的内容以可乘之机
- 自动对已知的未经修补的漏洞进行虚拟补丁（屏蔽），防止其被无限制利用，只需几分钟即可将防护推送至数千台服务器，且无需重启系统
- 协助合规性（PCI DSS 第 6.6 部分）保护 Web 应用程序及其处理的数据
- 防止 SQL 注入、跨站点脚本攻击和其他 Web 应用程序漏洞
- 为所有主要的操作系统和超过 100 款应用程序（包括数据库、Web 服务器、电子邮件服务器和 FTP 服务器）提供立即可用的漏洞防护
- 可以更好地查看和控制访问网络的应用程序

基于主机的双向防火墙

- 通过精细过滤、针对网络的策略以及适用于所有基于 IP 的协议和帧类型的位置感知功能，缩小了物理、云和虚拟服务器的受攻击范围
- 集中管理服务器防火墙策略，包括适用于常规服务器类型的模板
- 防止拒绝服务攻击并检测侦察扫描
- 提供主机上防火墙事件日志记录，实现针对公共云部署尤为重要的合规性和审计报告

完整性监控

- 监控关键的操作系统和应用程序文件（如目录、注册表项和值），以便实时检测并报告恶意更改和意外更改
- 采用 Intel TPM/TXT 技术执行虚拟机监控程序完整性监控，监控对虚拟机监控程序是否进行了任何未经授权的更改，从而将安全性和合规性扩展到虚拟机监控程序层
- 通过可信事件标记功能（自动采取相同的处理措施处理整个数据中心内的类似事件）降低管理开销
- 通过亚信安全™ 认证安全软件服务提供的基于云的自动化白名单功能，极大地减少了已知良好事件的数量，使管理得以简化

日志检查

- 收集超过 100 种日志文件格式的操作系统和应用程序日志并进行分析，以确认数据中心内是否存在可疑行为、安全事件和管理事件
- 协助合规性（PCI DSS 10.6 部分）优化对隐藏在多个日志条目中的重要安全事件的识别
- 将事件转发至安全管理平台 (SOC) 系统或集中式日志服务器进行关联、报告和存档

部署和集成

快速部署：利用现有 IT 和安全投资

- 独家！集成NSX布署安全策略
- 创新！与vCenter Operation manager集成显示安全信息
- 通过与 vShield Endpoint 和 VMsafe™ API 及 VMware vCenter 集成，可以作为虚拟设备快速部署在 ESX 服务器上，部署之后可以立即以透明方式保护 vSphere 虚拟机
- 通过多个集成选项向 SOC 系统（包括 ArcSight、Intellitactics、NetIQ、RSA Envision、Q1Labs、Loglogic 和其他系统）提供详细的服务器级安全事件
- 与企业目录（包括 Microsoft Active Directory）的目录集成
- 可以通过 Chef、Puppet、AWS Opsworks、Microsoft System Center Configuration Manager (SCCM)、Novell ZENworks 等标准软件发布机制轻松部署客户端软件

CSP 认证

Cloud Service Providers 是一种专门针对云服务提供商 (CSP) 而设计的全球性测试程序，用于验证与亚信安全所提供的业界领先云安全解决方案的互操作性