部署和整合

快速部署：利用现有 IT 投资和安全投资

- 客户端软件可以通过 Chef、Puppet、AWS OpsWorks、Microsoft System Center Configuration Manager (SCCM)、Novell ZENworks 部署解决方案等标准软件分发机制轻松部署
- 通过多种集成选项，可将详细的服务器级安全事件提供给 SIEM 系统，包括 HP ArcSight、Intellitactics、IBM QRadar、NetIQ、RSA Envision、Q1Labs、Loglogic 以及其他系统。
- 目录与企业目录集成，包括 Microsoft Active Directory

系统要求

Microsoft®Windows®

- Windows XP、Vista 7、8、8.1、10（32 位/64 位）
- Windows Server 2003（32 位/64 位）
- Windows Server 2008（32 位/64 位）、2008 R2、2012、2012 R2、2012 Server Core（64 位）、2016（64 位）2016 Server Core（64 位）
- XP Embedded（32 位/64 位）[1]

Linux[2]

- Red Hat® Enterprise 5、6、7（32 位/64 位）[3]
- SUSE® Enterprise 10、11、12（32 位/64 位）[3]
- CentOS 5、6、7（32 位/64 位）[5]
- Ubuntu 12、14、16（64 位，仅 LTS）[4、5]
- Oracle Linux 5、6、7（32 位/64 位）[4、5]
- CloudLinux 5、6、7（32 位/64 位）[2、4]
- Amazon Linux（32 位/64 位）[4、5]
- Debian 6、7（64 位）[2、4]

Oracle Solaris™[6、7]

- OS：10、11（64 位 SPARC）、10、11（64 位 x86）7、8
- 通过受支持的 Solaris 操作系统支持 Oracle Exadata Database Machine、Oracle Exalogic 、Elastic Cloud 和 SPARC Super Cluster

UNIX[6]

- 运行在 IBM Power System 上的 AIX 5.3、6.1、7.17、8
- HP-UX 11i v3 (11.31)7、9

云计算平台

- VMware® vSphere：5.5/6.0、View 4.5/5.0/5.1、ESX 5.5、6.2.X、6.5、NSX 6.2.X、6.3
- Citrix®：XenServer
- Microsoft®：HyperV
- 华为FusionSphere
- 华三 CAS
- 红山云
- 品高云
- 联通沃云
- 标准KVM平台

1由于可能会对 Windows XP Embedded 进行自定义，客户需要在自己的环境中验证操作的正确性，以确保运行亚信安全服务器深度安全防护系统客户端所需的服务和端口均已启用
2请参阅有关受支持内核的文档
3仅在 Red Hat 6（64 位）和 SUSE 11（64 位）客户端中支持 SAP 防护。要使 SAP 防护功能良好运行，必须在客户端启用防恶意软件模块
4仅对按需扫描提供防恶意软件支持
5有关受支持的版本，可查看最新的版本说明
6防恶意软件和 Web 信誉监控不可用
7通过 9.0 客户端受支持
8防恶意软件不可用
9仅日志审查和完整性监控
10 vCloud 网络和安全支持无客户端防恶意软件和完整性监控
11仅通过亚信安全服务器深度安全防护系统客户端提供防护

由 XGENTMSECURITY 提供支持

亚信安全服务器深度安全防护系统是亚信安全混合云安全解决方案的组成部分，该方案由 XGenTM提供支持。

主要认证和联盟

- Amazon 高级技术合作伙伴
- 经认证 Red Hat 就绪
- 经 Cisco UCS 验证
- 经 EMC VSPEX 验证
- 与 HP 建立业务合作伙伴关系
- Microsoft 应用程序防护计划
- Microsoft 认证合作伙伴
- 经 NetApp FlexPod 验证
- 与 Oracle 建立合作伙伴关系
- HIPS 的 PCI 适用性测试（NSS 实验室）
- SAP 认证（NW-VSI 2.0 和 HANA）
- 经 VCE Vblock 验证
- VMware 虚拟化

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™

为物理环境、虚拟环境、云环境及混合环境提供全面安全防护

虚拟化已让数据中心发生根本性变革，当前企业正将部分或全部工作负载转移至私有云和公有云。要想充分利用混合云计算的优势，就必须确保构建可保护所有服务器的安全系统，包括物理服务器、虚拟服务器或云服务器。

而且，这种安全系统不应妨碍主机性能和虚拟机 (VM) 密度，也不应影响虚拟化和云计算的投资回报率 (ROI)。亚信安全™服务器深度安全防护系统™是一款可提供全面安全防护的解决方案，专为虚拟环境和云环境而打造，因此不存在安全漏洞或性能影响。

防范数据泄露和业务中断

亚信安全服务器深度安全防护系统以软件、Amazon Web Services (AWS) 或 Microsoft®Azure™ 产品的形式推出，专门设计用于保护数据中心和云工作负载免受数据泄露和业务中断的影响。亚信安全服务器深度安全防护系统可以经济高效地避免混合云环境中的防护漏洞，帮助满足合规性要求。

在单个控制台中管理多个安全控制

亚信安全服务器深度安全防护系统集成了防恶意软件、Web 信誉、防火墙、入侵防御、完整性监控、应用程序控制和日志审查模块，可确保物理环境、虚拟环境和云环境中的服务器、应用程序以及数据安全无虞。亚信安全服务器深度安全防护系统可以作为一个单一的多功能客户端部署在所有环境中，通过一个管理控制台管理所有功能，让安全操作大为简化。您可以将亚信安全防毒墙控制管理中心用作控制台，也可以使用第三方系统，例如 VMware vRealize Operations、Splunk、HP ArcSight 或 IBM QRadar。

无缝集成可在云环境中扩展各策略使用范围。

亚信安全服务器深度安全防护系统可以与 AWS、Azure 和 VMware®工作负载等云平台无缝集成，将数据中心安全策略扩展至基于云的工作负载。亚信安全服务器深度安全防护系统包含一系列针对各种环境优化的功能，助力企业和服务提供商为其用户提供安全的差异化多租户云环境。

关键业务问题

- **虚拟桌面安全**
  借助专为最大限度地增强 VDI 环境防护而打造的全面安全功能，保持卓越的性能和整合率
- **虚拟修补**
  在漏洞被人利用之前，进行严密防护，消除紧急修补、频繁修补周期中的操作问题，避免出现代价高昂的系统停机
- **兼容性**
  证明符合一系列监管要求，包括 PCI DSS、HIPAA、NIST、SSAE 16 等

> “借助亚信安全服务器深度安全防护系统，我们无需在服务器上再使用另一种防病毒解决方案…如果使用的话，不仅会占用大量内存，还会因扫描而需要大量 CPU 处理时间。而使用亚信安全服务器深度安全防护系统则不会出现这些问题。”
>
> Blaine I sbelle
> 系统管理员
> 加州大学伯克利分校
> 信息服务技术部门

值得信赖的混合云安全

虚拟化安全

亚信安全服务器深度安全防护系统保护虚拟桌面和服务器免受勒索软件和网络攻击等零时差恶意软件的攻击，同时最大限度地降低资源效率低下和紧急修补造成的运营影响。

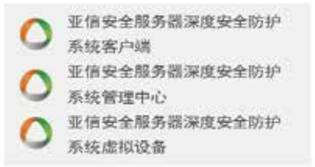
云安全

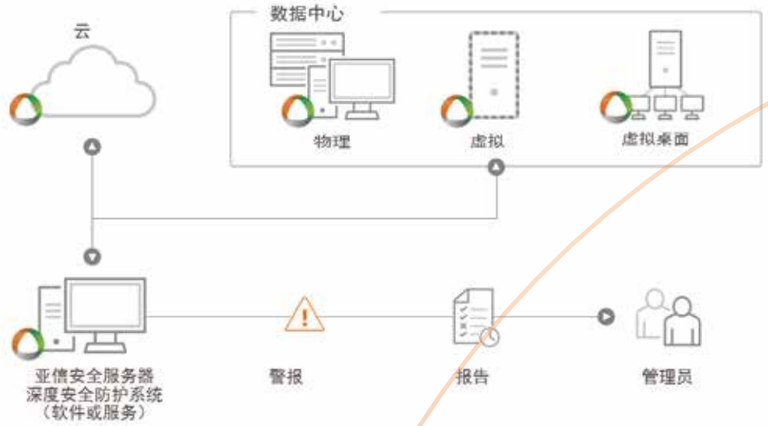
借助亚信安全服务器深度安全防护系统，服务提供商和现代化数据中心管理人员能够提供安全的多租户云环境，其安全策略可以扩展到云工作负载，并通过一致的上下文感知策略进行集中管理。

集成式服务器安全

亚信安全服务器深度安全防护系统将所有服务器安全功能整合到一个全面的集成式灵活平台中，该平台针对物理服务器、虚拟服务器和云服务器防护进行优化。

混合云安全





主要优势

行之有效、事半功倍

- 与传统的防恶意软件解决方案相比，VM 密度提高，可更高效地利用和管理资源
- 为一款易于管理的单一多功能安全客户端，灵活性提高并新增深度防御功能
- 通过虚拟机监控程序级别扫描重复数据删除功能，实现无与伦比的性能
- 与 AWS、Microsoft Azure 和 VMware vCloud Air 等云平台相集成，帮助企业通过一致的上下文感知安全策略管理物理服务器、虚拟服务器和云服务器
- 帮助服务提供商通过多租户架构为客户提供与其他租户隔离的安全公共云
- 提供自动扩展、实用计算和自助服务，让敏捷型企业可运行软件定义的数据中心
- 亚信安全服务器深度安全防护系统可以与 VMware 紧密集成，利用该功能能够自动检测新的虚拟机并应用基于上下文的策略，在数据中心和云端实现一致的安全性
- 与 VMware vSphere 6 和 NSXTM相集成。借助无论虚拟机位于何处均可自动应用的安全策略和功能，亚信安全服务器深度安全防护系统扩大了软件定义的数据中心中的微分隔优势

防止数据泄露和业务中断

- 防止未知应用程序在最关键的服务器上运行
- 实时检测和删除虚拟服务器中的恶意软件，同时尽可能减少对性能的影响
- 通过应用程序控制检测和阻止未经授权的软件
- 严密防护 Web 和企业应用程序以及操作系统中的已知和未知漏洞
- 通过沙盒分析提供先进的威胁检测和可疑对象修复
- 一旦检测到可疑或恶意活动，便发送警报并触发主动预防
- 借助亚信安全全球域名信誉数据库中的 Web 信誉威胁智能感知系统，可跟踪网站信誉并阻止用户访问受感染的站点
- 借助亚信安全全球域名信誉数据库中的统一威胁智能感知系统，可识别并阻止僵尸网络以及目标攻击命令和控制(C&C) 通信

最大限度地降低运营成本

- 借助集中管理的多用途软件客户端或虚拟设备，可消除部署多个软件客户端的成本
- 通过与亚信安全、VMware 以及 VMware vRealize Operations、Splunk、HP ArcSight 和 IBM QRadar 等企业目录中的管理控制台紧密集成，可降低复杂性
- 通过向主机应用预定义的策略保护所有环境中主机上的 Docker 容器，保护这些容器安全无虞
- 提供漏洞屏蔽，允许安全编码和经济高效地实施非预设的修补
- 通过自动执行重复和资源密集型安全任务、减少误报安全警报，并启用安全事件响应工作流，降低管理成本
- 通过基于云的事件白名单和可信事件，显著降低管理文件完整性监控的复杂性
- 通过漏洞扫描（建议设置）检测漏洞和软件，以检测变更并防范漏洞
- 客户端更加动态轻巧，大大简化了部署，可确保提高运营效率，从而最大限度地利用数据中心和云端的资源分配
- 安全性可满足您的策略需求，减少了专门用于特定安全控制的资源
- 通过跨亚信安全安全产品的集中管理简化管理。集中报告多个安全控制，更加易于为单个产品创建报告

实现经济高效的合规性

- 仅用一款经济高效的集成式解决方案即可满足 PCI DSS、HIPAA、SSAE 16 等的主要合规性要求
- 提供记录已防范攻击和合规政策状态的审计报告
- 减少完成审核所需的准备时间和精力
- 支持内部合规计划，能够提高内部网络活动的可见性

AsiaInfo | 亚信安全

亚信安全服务器深度安全防护系统功能

采用 Web 信誉的防恶意软件

- 与 VMware vShield Endpoint API 相集成可保护 VMware 虚拟机免受病毒、间谍软件、木马和其他恶意软件的攻击，无需占用客户虚拟机
- 提供了一款防恶意软件客户端，将防护扩展到物理服务器、虚拟服务器和云服务器，包括 AWS、Microsoft 和 VMware 环境通过 VMware ESX 级别缓存和重复数据删除，提高性能优化安全操作，避免全面系统扫描中常见的防病毒风暴和传统安全功能的模式更新
- 通过将恶意软件与关键操作系统和安全组件隔离开来，保护虚拟环境免于遭受复杂攻击
- 通过沙盒分析识别和分析可疑对象
- 与亚信安全TM云安全智能防护网络TM全球威胁智能感知系统相集成，享有多种加强对服务器和虚拟桌面防护的 Web 信誉功能

入侵防御

- 检查所有传入和传出流量的协议偏差、策略违规或表示攻击的内容
- 通过以虚拟方式修补（屏蔽）已知但未修补漏洞以避免遭受无限制的入侵，自动防护这些漏洞不遭受入侵，无需重新启动系统，即可将防护推送至数百台服务器
- 协助满足合规性要求（PCI DSS 6.6 节），防护 Web 应用程序及其处理的数据
- 抵御 SQL 注入、跨站点脚本以及其他 Web 应用程序漏洞
- 针对所有主要操作系统和 100 多个应用程序（包括数据库、Web、电子邮件和 FTP 服务器）提供现成的漏洞防护
- 加强对访问网络的应用程序的监视或控制

完整性监控

- 监控关键的操作系统和应用程序文件，例如目录、注册表项和值，以实时检测和报告恶意以及意外更改
- 利用 Intel TPM/TXT 技术执行虚拟机监控程序完整性监控，以发现对虚拟机监控程序的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
- 可信时间标记可自动复制整个数据中心中的类似事件操作，减少了管理开销
- 通过亚信安全TM安全软件认证服务的基于云的自动白名单大幅降低已知良好事件的数量，从而简化管理

日志审查

- 以超过 100 种日志文件格式收集和分析操作系统和应用程序日志，识别数据中心的可疑行为、安全事件和管理事件
- 协助满足合规性要求（PCI DSS 10.6 节），优化多个日志条目中重要安全事件的识别
- 将事件转发到 SIEM 系统或集中式日志记录服务器，以进行关联、报告及归档

双向主机防火墙

- 通过针对所有基于 IP 的协议和帧类型的细粒度过滤、每网络策略以及位置感知，减少物理服务器、云服务器和虚拟服务器的攻击面
- 集中管理服务器防火墙策略，包括常见服务器类型的模板
- 防止拒绝服务攻击并检测侦察扫描
- 在主机上提供防火墙事件记录，满足对公共云部署而言尤为重要的合规性和审计报告要求

应用程序控制

- 自动检测并阻止未经授权的软件
- 扫描计算机并确定计算机当前运行的应用程序
- 创建清单后锁定系统，防止新应用程序运行而不被列入白名单
- 集成到 DevOps 环境中，可对应用程序堆栈执行连续更改，同时利用 API 保持应用程序控制防护
- 帮助捕捉尚未签名的威胁，包括零时差威胁

体系结构

亚信安全服务器深度安全防护系统虚拟设备。在 VMware vSphere 虚拟机上透明地执行安全策略。对于 VMware NSX 环境而言，这可提供无客户端防恶意软件、Web 信誉、入侵防御、完整性监控以及防火墙防护。对于非 NSX 环境而言，可使用组合模式，其中虚拟设备用于无客户端防恶意软件和完整性监控，客户端用于入侵防御、应用程序控制、防火墙、Web 信誉以及日志审查。

亚信安全服务器深度安全防护系统客户端。通过部署在受保护的服务器或虚拟机上的小型软件组件（可以利用 Chef、Puppet 和 AWS OpsWorks 等领先运营管理工具自动部署），实施数据中心的安全策略（应用控制、防恶意软件、入侵防御、防火墙、完整性监控和日志审查）。

亚信安全服务器深度安全防护系统管理中心。功能强大的集中式管理控制台：基于角色的管理和多级策略继承，有助于执行精细控制。任务自动化功能（如“漏洞扫描（推荐设置）”和“事件标记”）可简化持续的安全管理。多租户体系架构支持个人租户策略隔离，并将安全管理委托给租户管理员。全球威胁智能感知系统。亚信安全服务器深度安全防护系统可以与云安全智能防护网络相集成，通过持续评估和关联网站、电子邮件来源及文件的全球威胁智能感知系统，提供实时防护，从而免受新兴威胁的攻击。

亚信安全服务器深度安全防护系统扫描程序是一种模块，该模块与 NetWeaver Virus Scan 接口系统集成后，可与 SAP 系统相集成，同时保护 SAP 系统。

SAP Partner