防毒墙网络版系统要求

推荐的最低服务器要求

防毒墙网络版服务器操作系统：
- Windows Server 2008 (SP2) 和 2008 R2 (SP2) (x64) 版本
- Windows Storage Server 2008 (x86/x64)、Storage Server 2008 R2 (SP1) (x64) 版本
- Windows HPC Server 2008 和 HPC Server 2008 R2 (x64)
- Windows MultiPoint Server 2010 (x64) 和 2012 (x64)
- Windows Server 2012 和 2012 R2 (x64) 版本
- Windows MultiPoint Server 2012 (x64) 版本
- Windows Storage Server 2012 (x64) 版本
- Windows Server 2016 (x64) 版本

防毒墙网络版服务器平台：
处理器：1.86 GHz Intel Core 2 Duo（2 个 CPU 内核）或更高
内存：最低 1 GB（建议 2 GB），其中至少有 500 MB 专门用于防毒墙网络版（在 Windows 2008 系列上）
- 最低 2 GB，其中至少有 500 MB 专门用于防毒墙网络版（在 Windows 2010/2011/2012/2016 系列上）

磁盘空间：最低 6.5 GB、最低 7 GB（采用远程安装）

防毒墙网络版边缘中继服务器平台：
处理器：2 GHz Intel Core 2 Duo（2 个 CPU 内核）或更高
内存：最低 4 GB
磁盘空间：最低 50 GB
操作系统：Windows Server 2012 R2
网卡：
1. 2 个网卡连接
   - 一个用于 Intranet 连接至防毒墙网络版服务器
   - 一个用于外部连接至外部部署的防毒墙网络版客户端

2. 1 个网卡配置，以针对 Intranet 和 Internet 连接使用不同的端口

数据库：
1. SQL Server 2008 R2 Express（或更高版本）
2. SQL Server 2008 R2（或更高版本）

推荐的最低客户端要求

客户端操作系统：
- Windows XP (SP3) (x86) 版本
- Windows XP (SP2) (x64)（专业版）
- Windows Vista (SP1/SP2) (x86/x64) 版本
- Windows 7（配备/未配备 SP1）(x86/x64) 版本
- Windows 8 和 8.1 (x86/x64) 版本
- Windows 10（32 位和 64 位）
- Windows 10 IoT Embedded
- Windows Server 2003 (SP2) 和 2003 R2 (x86/x64) 版本
- Windows Compute Cluster Server 2003（主动/被动）
- Windows Storage Server 2003 (SP2)、Storage Server 2003 R2 (SP2) (x86/x64) 版本
- Windows Server 2008 (SP2) (x86/x64) 和 2008 R2 (SP1) (x64) 版本
- Windows Storage Server 2008 (SP2) (x86/x64) 和 Storage Server 2008 R2 (x64) 版本
- Windows HPC Server 2008 和 HPC Server 2008 R2 (x86/x64) 版本
- Windows Server 2008/2008 R2 故障转移群集（主动/被动）
- Windows MultiPoint Server 2010 和 2011 (x64)
- Windows Server 2012 和 2012 R2 (x64) 版本
- Windows Storage Server 2012 和 2012 R2 (x64) 版本
- Windows MultiPoint Server 2012 (x64) 版本
- Windows Server 2012 故障转移群集 (x64)
- Windows Server 2016 (x64) 版本
- Windows XP Embedded Standard (SP1/SP2/SP3) (x86)
- Windows Embedded Standard 2009 (x86)
- Windows Embedded POSReady 2009 (x86)、Embedded POSReady 7 (x86/x64)
- Windows 7 Embedded (x86/x64) (SP1)
- Windows 8 和 8.1 Embedded (x86/x64) 版本

客户端平台：
处理器：300 MHz Intel Pentium 或等效版本（Windows XP、2003、7、8、8.1、10 系列）
- 最低 1.0 GHz（建议 2.0 GHz）Intel Pentium 或等效版本（Windows Vista、Windows Embedded POS、Windows 2008 (x86) 系列）
- 最低 1.4 GHz（建议 2.0 GHz）Intel Pentium 或等效版本（Windows 2008 (x64)、Windows 2016 系列）

内存：最低 256 MB（建议 512 MB），其中至少有 100 MB 专门用于防毒墙网络版（Windows XP、2003、Windows Embedded POSready 2009 系列）
- 最低 512 MB（建议 2.0 GB），其中至少有 100 MB 专门用于防毒墙网络版（Windows 2008、2010、2011、2012 系列）
- 最低 1.0 GB（建议 1.5 GB），其中至少有 100 MB 专门用于防毒墙网络版（Windows Vista 系列）
- 最低 1.0 GB（建议 2.0 GB），其中至少有 100 MB 专门用于防毒墙网络版（Windows 7 (x86)、8 (x86)、8.1 (x86)、Windows Embedded POSReady 7 系列）
- 最低 1.5 GB（建议 2.0 GB），其中至少有 100 MB 专门用于防毒墙网络版（Windows 7 (x64)、8 (x64)、8.1 (x64) 系列）

磁盘空间：最低 650 MB

> “利用像我们这样部署的企业网络，在整个国家/地区内通讯，能够在一个平台下确保移动设备和桌面设备的安全，从而可简化我们的网络安全性管理，并提高我们团队的工作效率。”
>
> Greg Bell，
> IT总监
> DCI Donor Services

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

AsiaInfo | 亚信安全

亚信安全™

防毒墙网络版™

曾经我们看待恶意威胁就是黑与白 — 阻止恶意的部分，而保留好的部分。而现在，辨别好坏是非常困难的，组织对待其终端安全越来越审慎，并更加清楚地认识到，基于特征码识别的传统技术在应对狡猾的勒索病毒和未知威胁时，其防护能力远远不足。新一代的防护技术可以有效的应对某些的威胁，但却无法应对其它威胁，而在一个终端加入多个防护工具会导致很多兼容性问题，无法协同工作。让情况更加复杂的是，您用户的终端可以访问外部的资源和设备越来越多，包括访问提供云服务的各种资源。您需要的的终端安全是可以提供各种维度的保护，以抵御各种类型的威胁，并来自有拥有丰富的恶意防护经验和业界优良口碑的供货商。

亚信安全防毒墙网络版（具有 XGen™ 终端安全性）将高精准机器学习融入现有的各种威胁防御技术组合中，从而进一步清除终端安全隐患。它可在您的整个环境中不断学习、调整和自动共享威胁情报。这种混合型的威胁防护是通过一种体系结构来提供的，该体系结构可更高效地利用终端资源，并最终在 CPU 和网络利用率方面超越竞争对手。

防毒墙网络版是我们的云安全智能防护套件的一个关键组件，该套件可在一个颇具吸引力的软件包中提供更多的网关和终端防护功能，比如应用程序控制、入侵防护（漏洞防护）、终端加密、数据丢失防护(DLP)等。其他亚信安全解决方案通过终端调查和取证来扩展您对高级攻击的防护。此外，Deep Discovery 网络沙盒可在本地检测到新的威胁时快速响应（实时签名更新）终端，从而缩短启动保护所需的时间，并降低恶意软件的传播。这种现代威胁安全技术借助集中可视化、管理和报告，让贵组织感觉非常易于使用。

保护点

- 物理终端
- 虚拟化终端（加载项）
- Windows 电脑和服务器
- Mac 计算机
- 销售点 (POS) 和 ATM 终端

威胁防护

- 高保真机器学习（执行前和运行时）
- 行为分析（针对脚本、注入、勒索软件、内存和浏览器攻击）
- 文件信誉
- 变体防护
- 信息普查检测
- Web 信誉
- 安全漏洞防御（主机防火墙、安全漏洞防护）
- 命令和控制 (C&C) 阻止
- 数据丢失防护 (DLP) 模块
- 设备控制
- 好文件检查
- 沙盒与入侵泄露检测集成

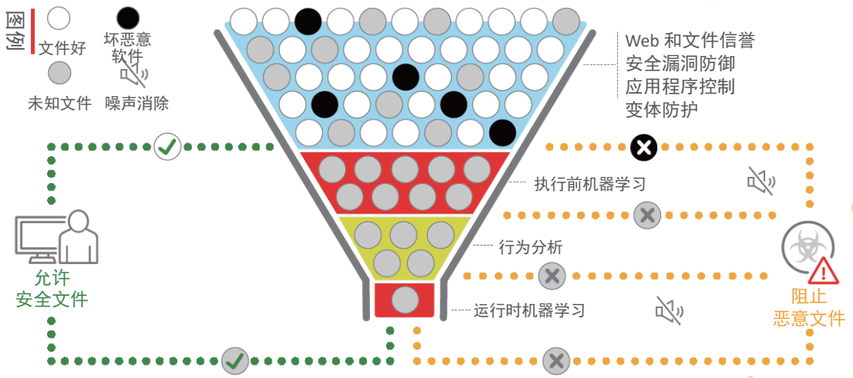
一切尽在掌握

- 高级恶意软件和勒索软件防护：保护终端（无论是否在企业网络中）免受恶意软件、特洛伊木马、蠕虫病毒、间谍软件和勒索软件的攻击，并进行调整以抵御新出现的未知变体的侵袭。
- 联动的威胁防御：防毒墙网络版在您的网络中及通过亚信安全的全局云威胁情报与其他安全产品本地集成，以便在检测到新威胁时向终端提供网络沙盒快速响应更新，从而缩短启动保护所需的时间，并降低恶意软件的传播。
- 集中可视化和控制：多个防毒墙网络版服务器在与亚信安全™防毒墙控制管理中心™一起部署时，可通过单个控制台进行管理，以提供全面的用户可见性。
- 移动安全集成：通过利用控制管理中心集成亚信安全™移动安全和防毒墙网络版，以跨所有终端集中进行安全管理和策略部署；移动安全包括移动设备威胁防护、移动应用程序管理、移动设备管理 (MDM) 和数据保护。

优势

最高的 XGen™ 终端安全性

将高保真机器学习与其他检测技术相融合，以针对勒索软件和高级攻击形成最广泛的防护。



- 使用最高效的技术逐步过滤出威胁，从而进行最大程度的检测，而不出现误报。
- 将无需使用特征码技术（包括高保真机器学习、行为分析、变体防护、统计检查、应用程序控制、安全漏洞防御和好文件检查）与其他技术（例如文件信誉、Web 信誉及命令和控制（C&C）阻止）相结合。
- 亚信安全是首家融合高保真机器学习的公司，高保真机器学习不仅可在执行前还可在运行时过程中对文件进行独特分析，以实现更加精确的检测。
- 在各个层级使用信息普查检测技术和白名单检查等噪声消除技术可减少误报。
- 和其他安全产品及时共享网络可疑活动和文件，以阻止后续攻击。
- 高级勒索软件防护功能可监控终端上的可疑文件加密活动、终止恶意活动，甚至在必要时恢复已丢失的文件。

影响最低

降低用户影响和管理成本。

- 轻型且优化的安全性在恰当的时间利用恰当的检测技术，来确保对设备和网络产生的影响最小。
- 利用终端状态的全面集中视图，可以快速了解安全风险。
- 贯穿安全保护层自动共享威胁情报有助于抵御整个组织中新出现的威胁。
- 利用边缘中继实现外部部署的合规性和防护，员工利用边缘中继可在企业网络之外工作，并在没有VPN的情况下仍连接至防毒墙网络版。
- 可定制的控制台契合不同的管理职责。
- 24x7 全天候支持意味着，如果出现问题，亚信安全可随时快速解决问题。

经验证的安全合作伙伴

亚信安全拥有持续创新的历史，可提供最高效且最有效的安全技术。我们始终向前看，开发出抵御未来不断变化的威胁所需要的技术。

- 拥有超过 25 年的安全创新历史。
- 为超过 1.55 亿个终端提供保护。
- 深受全球 50 强企业中 45 家企业的信赖。
- 自 2002 年以来在 Gartner 终端保护平台魔力象限中一直位居领导者地位，2017年在“前瞻性”象限中遥遥领先。

关键业务问题

- 越来越多的新的恶意软件和勒索软件被漏检
- 需要一个整体的解决方案来抵御PC终端、Mac 和 VDI 上的所有已知和未知威胁
- 终端安全解决方案之间相互不通信，无法协同，延长启动保护所需的时间，并增加管理负担
- 用户远程工作及通过云等以新的方式共享信息会带来风险
- 当高级威胁和数据保护无法集成时，IT 效率会下降

> “当时我的第一个目标是，消除以前的终端解决方案在我们的系统中所花费的沉重开销，”Jamieson 表示。
>
> “防毒墙网络版帮助我实现了这一目标…
> 当时我的第二个目标是，引入真正有效的安全性。由于我们替换了以往的解决方案，因此可以看到亚信安全确实已经阻止了感染发生。”
>
> Bruce Jamieson，
> A&W Food Services of Canada
> 网络系统经理

定制您的终端保护

利用可选的安全模块扩展您的现有亚信安全终端安全性，并利用补充性终端解决方案来扩大保护范围：

数据丢失防护（DLP）模块

保护您的敏感数据，以实现最大程度的可见性和控制。

- 确保网络内外私有数据的安全，包括在文件离开您的网络之前对文件进行加密
- 防止通过云存储、USB驱动器或已连接的移动设备、Bluetooth连接及其他介质发生数据泄漏
- 涵盖范围最广的设备、应用程序和文件类型
- 利用更高程度的可见性和实施助力实现合规性

Vulnerability Protection 选项

立即终止您的物理和虚拟台式机及笔记本电脑上的零日威胁（无论是否在网络中）。利用基于主机的入侵防御系统（HIPS），亚信安全™ Vulnerability Protection 可在修补程序可用或可部署之前，抵御已知和未知的漏洞。将保护扩展至关键平台，其中包括旧版操作系统（如 Windows XP）。

- 通过利用虚拟修补来防御漏洞，从而消除暴露于风险的可能性
- 减少恢复和紧急修补所需的停机时间
- 允许依据您自己的主张和时间表进行修补
- 借助基于CVE、MS-ID、严重性的报告识别安全漏洞

Endpoint Application Control 选项

通过阻止不需要和未知的应用程序在您的企业终端执行操作，从而增强对恶意软件和针对性攻击的防御。

- 防止用户或机器执行恶意软件
- 动态策略可降低管理影响，并有利于实现活动用户环境的灵活性
- 将系统仅锁定至贵组织希望使用的应用程序
- 使用来自数十亿文件的相关威胁数据来创建和维护经验证的良好应用程序的最新数据库

亚信安全安全 Mac 版模块

在您的网络上为 Apple Mac 客户端提供一个保护层，方法为：阻止它们访问恶意站点及分发恶意软件（即使恶意软件并不针对Mac OS X也是如此）。

- 减少暴露于基于 Web 的威胁的可能性，包括快速传播的针对 Mac 的恶意软件
- 遵守 Mac OS X 观感，以提供积极的用户体验
- 通过跨终端（包括 Mac）进行集中式管理，从而节省时间和精力

虚拟台式机基础架构 (VDI) 模块

允许您同时针对物理和虚拟桌面将终端安全性合并到一个解决方案中。

- 识别客户端是在物理终端上还是在虚拟终端上，并针对其特定环境优化保护和性能
- 序列化扫描、更新和白名单基本镜像和以前扫描的内容，以保留主机资源

亚信安全™ 防毒墙控制管理中心™ 选项

此集中安全管理控制台可确保来自亚信安全的多个互联安全层进行一致的安全管理、完全可视化和报告。它还可跨本地、云和混合部署模型扩展可视化和控制。集中管理与基于用户的可视化相结合，可改善保护效果、降低复杂性，并消除安全管理中冗余和重复的任务。控制管理中心还通过亚信安全™云安全智能防护网络™提供对可采取措施的威胁情报的访问权，亚信安全™云安全智能防护网络™利用全局威胁情报从云中交付实时安全，防止您受到威胁侵袭。