AsiaInfo | 亚信安全

亚信安全™
漏洞保护

针对终端的高级漏洞防护

如今企业终端面临比以往任何时候都更为复杂的攻击，特别是当终端在外网不再受多重安全保护的时候。另外，装有嵌入式操作系统的销售点设备和网络设备难于更新和修复。为了保护您的业务免受违规或有针对性的攻击，所有类型的终端都需要复合的保护方法，以保护数据和应用程序免受黑客攻击，Web威胁以及日益增加的远程漏洞威胁。

亚信安全™漏洞保护通过虚拟补丁来增强客户端的反病毒和反恶意软件的安全性，从而提供了更及时，更强大的终端防护。漏洞保护通过高性能的引擎，使用基于主机的入侵防护过滤器以及零日攻击监控来监控流量，以发现新的特定漏洞。因此，您可以检测网络协议偏差，类似攻击或违反安全策略的可疑内容。漏洞保护通过快速且易于部署的过滤器来防止这些漏洞被利用，这些过滤器能够在补丁部署之前即提供全面的保护。与其他亚信安全终端产品配合使用时，漏洞保护为处于任意位置的终端提供业界最广泛的保护。

软件

保护端点
- 终端

威胁防护
- 漏洞利用
- 分布式拒绝服务攻击
- 非法网络流量
- 网络威胁

关键优势
- 消除由于补丁缺失导致的风险暴露
- 延长了Windows XP等传统和支持终端操作系统的使用寿命
- 减少恢复的停机时间，增加对零日攻击的保护
- 允许根据自己的规划和时间表进行修复
- 通过提高数据安全合规性降低潜在的法律风险
- 增强远程和移动企业终端的防火墙保护

主要特征

防御高级威胁
- 在部署补丁之前阻止已知和未知的漏洞攻击
- 自动评估并为您的特定环境推荐所需的虚拟补丁
- 根据终端的位置动态调整安全配置
- 将终端对网络吞吐量，性能或工作效率的影响降到最小
- 通过多重保护，对终端屏蔽无用的网络流量
- 保护持有敏感数据的系统，关乎监管和公司政策合规

从关键业务流量中移除不良数据
- 通过控制过滤器来告警/阻止特定流量，例如即时消息和流媒体
- 使用深度包检测来识别可能会损害应用层的内容
- 过滤禁止的网络流量并通过状态检查确保允许的流量

提供更及时的保护
- 在部署补丁之前并且通常在补丁可用之前提供保护
- 保护操作系统和常见应用程序免受已知和未知攻击
- 检测使用支持的协议通过非标准端口隐藏的恶意流量
- 使用面向漏洞的网络检查来阻止可能会损害风险组件的流量
- 防止网络后门渗入公司网络
- 使用入侵防护签名阻止所有已知漏洞
- 使用自定义过滤器来保护自定义和传统应用程序

部署和管理现有的基础设施
- 通过轻量级代理体系结构保留终端性能
- 使用现有的终端安全解决方案轻松便捷地部署
- 使用管理控制台，通过简化的仪表板和基于用户的可见性，增加了便利性
- 按照Microsoft安全公告号，CVE编号或其他重要信息组织漏洞评估
- 提供与常用SIEM工具的日志集成
- 使用现有的officeScan插件管理器和管理控制中心简化部署和管理
- 减少立即修复和重启的需要，导致系统不必要的停机

漏洞保护可以立即停止物理和虚拟桌面以及笔记本电脑上的零日威胁，而不论其是否在线。漏洞保护通过主机级别入侵防护系统（HIPS）过滤器，行为学，统计学，启发式和协议执行技术，可在补丁可用或可部署之前防御漏洞。

这可以保护您的关键平台免受已知和未知威胁的侵害，其中包括Windows XP等传统操作系统和Windows 10等新系统。为支持分层的安全方法，漏洞保护与亚信安全完整用户保护解决方案集成，可提供多种相互关联的威胁和信息保护层。

漏洞保护可通过多个服务器的选项进行扩展，从而确保即使是最大型的组织也能进行终端部署。作为内部部署的软件应用程序，漏洞保护与其他亚信安全威胁防护解决方案相集成，以增强终端的整体威胁和恶意软件防护。

需要以下两个组件：

- 服务管理端安装在受支持的Windows平台上，并通过浏览器进行管理
- 客户端安装在受支持的Windows平台上

完整的用户保护

漏洞保护是亚信安全智能防护套件的一部分。

这些互连的多重安全套件可以保护用户及其数据，而不论设备所处位置。因此，您可以在多个层面获得最广泛的威胁防护功能：包括终端，应用程序和网关。 此外，您可以使用灵活的本地，云和混合部署模式，随着您的业务扩展您的保护内容。您只需简单地进行更改，而不需要增加新的许可。而且，您可以从管理控制台管理多个用户，从而为您提供完整的可视性。

适用于可靠性评估的系统安全需求

漏洞保护服务器系统需求
内存：4 GB（建议8 GB）
磁盘空间：1.5 GB（建议5 GB）
操作系统 • Microsoft Windows 2012 R2（64位） • Microsoft Windows 2012（64位） • Windows Server 2008 R2（64位） • Windows Server 2008（32位和64位）
浏览器 • Firefox 12+ • Internet explorer 9.x & 10.x • chrome 20+ 注意：必须在所有浏览器上启用Cookie

漏洞保护客户端系统需求
内存：128MB
磁盘空间： 500 MB
操作系统 • Windows 10（32位和64位） • Windows 8.1（32位和64位） • Windows Server 2012 R 2 （64位） • Windows 8 （32位和64位） • Windows Server 2012 （64位） • Windows 7 （32位和64位） • Windows Server 2008 R 2（64位） • Windows Server 2008 （32位和64位） • Windows Vista （32位和64位） • 使用” Windows Server 2003 SNP” 修复的Windows Server 2003 SP1（32位和64位） • Windows Server 2003 SP2 （32位和64位） • Windows Server 2003 R 2 SP2 （32位和64位） • Windows XP（32位和64位）

AsiaInfo | 亚信安全

云与大数据安全领导者