SecFox-EPS终端安全管理系统

当前企业和组织面临的挑战

随着网络技术的不断发展，用户的业务复杂度和使用者快速增长，网络的规模随之不断扩张，网络边界的含义也随之发生变化。面对这些变化的同时，企业用户也不断的受到了来自外部和内部的各种威胁，对于网络中的端点，尤其是终端，经常处于一种高风险的状态。于是，引发了一系列的问题：

- 如何有效地控制终端设备在内网中的随意接入、带出?
- 如何管理分布广泛的终端设备，保障它们正常运行?
- 如何方便地对终端使用行为进行监控?
- 如何发现终端设备的系统漏洞并自动分发补丁?
- 如何快速有效地定位网络中的病毒、蠕虫和黑客，及时准确地识别安全事件发生的源头?
- 如何统一管理内网中的移动存储介质?

SecFox-EPS：企业终端安全管理的守护者

SecFox-EPS（Endpoint Protection System）终端安全管理系统，是网御神州科技（北京）有限公司为用户终端安全保护量身定做的一套解决方案。SecFox-EPS具有丰富而完整的策略模版，能够根据不同用户的不同需要制定适合自己要求的策略，例如用户可以根据自己的需要启用流量监控策略、地址绑定策略、防火墙策略、软件分发策略、补丁更新策略、资产管理策略、移动存储策略、进程监控策略、接入控制策略、文件审计策略等等，代理将会把监控事件发送到总控中心。SecFox-EPS为用户提供了丰富的报表，使得管理人员能够从各种角度对企业和组织的终端安全状况进行分析，并支持报表模版，可以自动地、或者定期地产生报表（日报表、周报表、月报表）。

SecFox-EPS的主要功能包括：

- 终端接入管理
- 终端安全加固和运行监控
- 用户行为监控与审计
- 内网机密信息保护
- 终端代理自动维护与升级

符合等级保护要求的终端安全管理

现在的不安全问题基本上是由于PC机结构和操作系统的不安全引起。恶意攻击手段变化多端，原有应对措施都是采取封堵的办法，不能预测未来的攻击和入侵。如果在终端操作平台实施高等级防范，这些不安全因素将在源头即被控制，也就是从源头上控制安全隐患。事实上，所有入侵攻击都是从个人电脑终端上发起的，黑客利用被攻击系统的漏洞窃取超级用户权限之后，才大肆进行破坏活动。此外，即使是合法用户也应该纳入严格的访问控制，因为再坚固的堡垒也会从内部被攻破。

建立信息安全保障体系需要我们改变思维方式，从终端开始防范攻击。把不同信息系统分成不同的安全级别，然后严格按照安全级别所规定的要求，从事信息活动。等级保护不仅是对信息安全产品或系统的检测、评估以及定级，更重要的，它是围绕信息安全保障全过程的一项基础性的管理制度，是一项基础性和制度性的工作。

早在1994年，国务院147号令明确提出国家实行信息安全等级保护制度。1999年国家制定了国家标准《计算机信息系统安全保护等级划分准则（GB17859-1999）》。2003年中办国办27号文明确提出实施等级保护作为国家信息安全工作的重点工作之一，随后国家制定发布了一系列等级保护相关标准。2007年四部委43号文确定在全国范围内全面展开等级保护工作。

SecFox-EPS终端安全管理系统作为技术手段和管理工具，与其它安全产品一起，可以为信息系统安全等级保护的定级、实施和测评提供必要的安全防护。SecFox-EPS终端安全管理系统为满足《信息系统安全等级保护基本要求》技术要求部分的网络安全和主机安全要求提供了必要的技术手段，具体表现在：网络安全方面，提供了网络结构安全和边界完整性检查；主机安全方面，提供了身份鉴别、访问控制、安全审计、恶意代码防范、资源控制；另外，SecFox-EPS终端安全管理系统为满足《信息系统安全等级保护基本要求》管理要求部分的系统运维管理要求提供了灵活的管理工具，如：资产管理、介质管理、监控管理、系统安全管理、变更管理和安全事件处置。