Virmon 智能网络安全防御系统白皮书

01）VIRMON 网络安全防御系统介绍：

网络安全智能防御系统，全面的网络安全解决方案。Virmon 智能网络安全防御具有独创的创新技术，作者在该领域有多篇论文发表。
网站网址为 www.virmon.net(virmon.cn). Virmon 网络安全系统分为几个版本如下：
a)面向互联网用户的试用版本，智能个人防火墙系统。
b)面向付费用户的智能网络安全防御单机系统。(virmon Nsds)
c)面向服务器带多个节点的智能网络防御系统。
d)服务器等版本包括控制台，流量告警、取证审计。进程级别流量智能控制等。
Virmon 智能网络安全防御特色主要包括以下方面：
a)稳定的基于进程的网络通信数据包监控。
b)智能网络防御规则自动识别和生成，具有学习模式等。
c)网络智能流量监控，对系统运行的通信进程数据包流量做统计和监控。对进程流量做一个阀值，超过此阀值做报警和拦截等。
d)在网络协议底层网络层、传输层对网络通信做监控、过滤和拦截。有自己的状态连接链表对网络数据快速过滤。
e)网络通信内容检测，对非法、恶意通信的检测并自动生成规则报警。
f)完善的审计和报表等。
未来发展方向，对下一代网络协议 IPv6/IPv4 做全面控制和防御。IP 协议族等作基于网络元组的控制。发展为高效率的有状态防火墙。在分布式智能化方向发展。对有价值的网络数据和内容，做并行内容处理和检测，采用分布式数据内容检测和统一的规则策略分发等。规模节点的服务器集群、客户端群做统一控制和部署。在网络空间做网络态势分析，对分布式拒绝服务攻击(DDOS)、病毒、下载恶意程序、恶意通信流量等做检测和防御。对规模网络达到有效的控制和检测。

02)关于本网络安全系统涉及到算法

本算法主要是精确字符串匹配算法，今后将用于网络安全内容检测等方面。
本算法比已知的最快算法要更快。现在购买单机版附赠算法源码。

03) virmon 智能网络安全系统满足什么需要或解决什么问题？

对单位的主机网络流量做智能控制，防止入侵攻击、对入侵做全面检测。对网络安全全面控制。对金融或信息营业系统、企业营收系统等每一笔业务。只要 通过网络平台，就可以记录每一笔交易和检测内容。对基于互联网的业务等能深入做内容检测，利用作者验证的最新算法做内容分析和检测等。对数据封包的进程和每个封包大小都详细记录的软件现在还没有。
高级安全威胁 APT 困扰企业和事业单位安全，很难分析出威胁通信。本系统目标分析协议状态机，对 APT 攻击做防御。DDOS 类型的攻击，从进程流量可以设置上限或报警线，到一定流量后就报警或通知管理控制端。对网络拥堵等早做分流等操作。

04）virmon 智能网络安全系统未来发展

未来发展规划，在系统的网络协议多个层次全面控制网络安全。从链路层、网络层到传输层和应用层，对网络作防守和检测。构建网络协议的多层防御机制，在面向高速互联网络做到更安全和更为高速。做成世界级的网络安全防御系统。对云计算网络提供可信安全防御和监测系统。