**需求分析**

入侵攻击的检测及防御，是用户保障信息系统安全的核心需求之一，然而，有限的安全预算下如何防御日益更新的多样化攻击，对用户来说是个艰巨的挑战。入侵防御正是解决该问题的最佳解决方案：在线部署的入侵防御系统不但能发现攻击，而且能自动化、实时的执行防御策略，有效保障信息系统安全。由此可见，对于入侵攻击识别的准确性、及时性、全面性以及高效性，是优秀入侵防御产品必备条件。

**产品简介**

天清入侵防御系统（Intrusion Prevention System，以下简称“天清NGIPS”）是启明星辰自主研发的网络型入侵防御产品，围绕深层防御、精确阻断的核心理念，通过对网络流量的深层次分析，可及时准确发现各类入侵攻击行为，并执行实时精确阻断，主动而高效的保护用户网络安全。

天清入侵防御系统融合了启明星辰在攻防技术领域的先进技术及研究成果，使其在精确阻断方面达到国际领先水平，可以对漏洞攻击、蠕虫病毒、间谍软件、木马后门、溢出攻击、数据库攻击、高级威胁攻击、暴力破解等多种深层攻击行为进行防御，有效弥补网络层防护产品深层防御效果的不足。

**典型应用**

启明星辰入侵防御产品已广泛应用于政府、金融、能源、电信、军队等各行业领域，并积极拓展国际市场。根据CCID报告，启明星辰IDS/IPS产品已连续16年（至2017年）国内市场占有率第一；根据IDC报告，启明星辰IDS/IPS产品已连续3年（至2017年）排名市场第一；启明星辰在2016、2017连续2年成功入围Gartner IDPS魔力象限，成为少数入围Gartner魔力象限的国内厂商之一。

天清入侵防御系统V6.0典型应用如下：

  ● 透明部署于企业内联网、互联网网络边界：不改变原有网络拓扑，执行流量的深层次分析和攻击防御，保护子网终端及服务器的安全。

  ● 分布式部署统一管理：分布式部署于各个子网边界的入侵防御设备，可通过天清集中管理与数据分析中心软件统一管理起来，进行统一安全策略的配置、特征库升级、日志收集存储及集中监控。

  ● 与天阗APT联动，构建高级威胁防御方案  
     1.天清NGIPS对边界流量进行深层分析及防御，还原协议中包含的文件  
     2.天清NGIPS对文件执行恶意代码静态检测，同时将文件提交给天阗APT引擎  
     3.天清NGIPS从天阗APT引擎获取文件的准确检测结果及Callback特征  
     4.天清NGIPS针对Callback特征生成防护策略，执行自动防护

**用户价值**

天清入侵防御系统以其领先的攻击防御能力，在确保业务可用性的同时，可准确、及时、全面、高效的帮助用户抵御多样化的入侵攻击，尽可能的降低用户在攻击事件处理上的人力和资金投入，获得最佳的投资收益。