IPS 入侵防御系统产品功能参数

系统内置专业的入侵防御特征库，覆盖勒索、挖矿、webshell、僵尸网络、木马后门、蠕虫、信息泄漏、权限绕过、未授权访问、文件上传、文件读取、文件下载、文件包含、SSRF、XXE、CSRF、反序列化、代码执行、命令执行、XSS 攻击、SQL 注入、DOS 等攻击类型，入侵防御特征数量在 15000 条以上；
支持 2 条以上防护链路；
支持 IPv4\IPv6 双栈流量；
系统支持网线模式部署和透明多口桥部署；
支持对挖矿行为进行防护，并可将产生的挖矿行为生成日志，可通过源地址和目的地地址和信誉等级进行查询，可展示挖矿日志的威胁类型、挖矿值及协议等；
系统支持 WEB 过滤，对 web 内容，传输文件名称、传输文件内容过滤，支持邮件过滤，对邮件标题、邮件正文、附件名称、附件内容过滤，阻断并支持邮件提醒；
支持代理环境部署，支持通过 Tcp-Options 和 X-Forwarded-For 提取源；
可通过各种统计分析自行选择呈现当前整体威胁状态：如威胁事件级别分布、入侵事件-攻击类别分布、攻击类别趋势、TOP 入侵事件目的 IP、入侵事件发生趋势等等，支持 TOP5、10 展示；
系统支持敏感信息防护，包含财务数据、机密文档、技术文档、简历、收购与并购、身份证号码、手机号码、银行卡/信用卡；
支持规则变更部署功能，包括但不限于防护模式和转发模式；
支持 SQL 注入和 XSS 攻击检测，检测点包括 URL、COOKIE、REFERENCE、FORM、USERAGENT 和 XFORWARD；
支持双向检测功能，根据双向流量检测攻击，输出检测结果包含正在利用、攻击成功，支持 HTTP 请求/响应缓存；
系统内置智能分析能力，具备阻断的活动专项分析和综合威胁告警分析，其中阻断的活动应包括阻断的威胁、阻断的文件和阻断的 IP 专项分析；
支持部署在 IPV6，VLAN，QINQ，MPLS，GRE，VXLAN，PPPOE 等常见协议封装的环境中，可检测和拦截攻击行为；
系统支持端口聚合包括手动端口聚合模式和 LACP 聚合模式；
支持 HTTP 协议自适应解码、URL 解码、UTF7 解码、base64 解码、XML 解码、Unicode 解码、十六进制转换、CHR 解码、UTF-7 解码，支持解析 7 层以上混合编解码能力，可实现对多层编码攻击的检测，支持格式文本解析 JSON 解析、html 解析、multipart 解析；
支持 DGA 域名检测，支持 DGA 本地、远程升级方式，通过启动 DGA 域名检测，可将 DGA 检测到的 DNS 安全事件进行告警。
系统支持生产报表，分析维度应支持系统健康,安全告警,业务系统风险,终端风险,处置响应维度等，并支持个性化，包含自定义单位名称、汇报部门,联系人,联系电话,邮箱地址,logo 等，支持定期生产日报表、周报表、月报表
支持生成符合金融行业要求的合规报表；