

船信入侵防御系统

船信入侵防御系统是中船信息公司推出的满足自主可控的国产化专业入侵防御产品。基于于飞腾、龙芯等国产处理器，搭载中标麒麟、银河麒麟等国产操作系统，采用自主研发的软件系统，稳定安全高效。凭借全面立体的高级威胁防护、云网协同的纵深防御体系、业务可视的自动化运维，为政府、金融、能源等行业用户提供运营安全保障。

产品特点 PRODUCT CHARACTERISTICS



自主可控

基于飞腾、龙芯等国产处理器，搭载中标麒麟、银河麒麟等国产操作系统，采用自主研发的软件系统，实现从硬件到软件的自主研发，生产、升级、维护的全程安全可控；

支持国家自主技术标准，涵盖可信计算标准，国家密码算法等，从底层技术标准上提升系统安全性；
满足三权分立相关要求，管理角色可划分为系统管理员、安全操作员、安全审计员，三类管理权限相互制约，持续保障信息安全。

全面检测

提供对系统、应用、恶意软件及客户端的精准检测，通过网络流量深度检测和解析技术，能够精准识别用户、应用、风险等多个维度信息，快速感知网络环境；

领先的病毒特征库，近万条入侵规则和千万级病毒特征库，有效检测和应对多种攻击。

智能防御

支持对僵尸网络攻击、DDoS 攻击、CC 攻击、跨站脚本攻击、暴利破解、漏洞利用、Web 攻击、垃圾邮件、钓鱼、木马病毒和恶意软件等一系列网络入侵威胁检测及防御。为用户提供 L2-L7 层的威胁防护，构建多维安全防护体系；

云网协同的纵深防御体系，与云端威胁情报、高级未知威胁 APT 防御（云沙箱 / 本地沙箱）实现智能化的协同联动。打破传统静态、被动、孤立的防护模式局限性，使安全有效性和防御实时性得大幅提升。

极简运维

集中管理，通过 HSM 实现统一的设备策略管理、设备健康状态监控、配置管理等。快速配置安全策略，定位安全故障，提升运维效率；

策略优化，基于用户的真实应用场景，预定义入侵防御策略。根据安全风险，自适应的进行安全防御策略调整，实现人工运维到智能运维，降低安全运营成本；

业务可视，为用户提供从网络到业务应用的可视化管理，

丰富的可视化流量和威胁趋势、日志、自定义报表等功能，快速掌握全面真实的网络状况，更好地做出防护措施。

硬件规格 HARDWARE SPECIFICATIONS

指标	船信 CX3201/CX3202
产品图片	
管理接口	1 个 Console 口、2 个 USB3.0 口、1 个 HA、1 个 MGT
网络接口	4 × GE (1 对 bypass)
扩展模块槽	1 个通用扩展槽
扩展模块选项	IOC-CX-8SFP-GC、IOC-CX-4SFP+-GC
存储	1T HDD
电源规格	标配 180W ATX 电源
外形尺寸 (W×D×H, mm)	1U (440x 400x43.6mm)

联系方式 CONTACT US

北京总部

地址：北京市海淀区中关村南大街乙 56 号方圆大厦

电话：010-6829 2500

传真：010-6829 2500

邮箱：client@csit.net.cn

网址：www.csit.net.cn

上海分公司

地址：上海市杨浦区河间路 1280 号中船工业大厦

电话：021-6543 1046

传真：021-5566 9801