辰信威胁防御安全网关TDSG

专业级恶意代码威胁综合防御产品，满足等级保护基本要求。

恶意代码威胁综合防御

全面综合防御文件体病毒和动态传播攻击特征的恶意代码威胁，拥有千万级威胁特征库且全量加载驱动，可覆盖恶意代码生命周期各项环节。

自主研发自主知识产权

辰信威胁防御安全网关TDSG，拥有完全自主知识产权。可满足新型网络环境安全需求、应对新形势下的恶意代码威胁的高性能边界安全产品。

可决策性风险分析

提供具有威胁评判依据的风险分析报告，精确呈现内部已存在的威胁和脆弱性事件，帮助用户对现有风险进行改善，快速获悉全网威胁态势。

灵活多样的部署应用

在部署模式上，支持串行阻断防御、并行威胁监听预警、串并混合三种部署方式，其灵活多样的部署应用，可满足用户不同安防需求，提升产品应用价值。

卓越性能和网络体验度

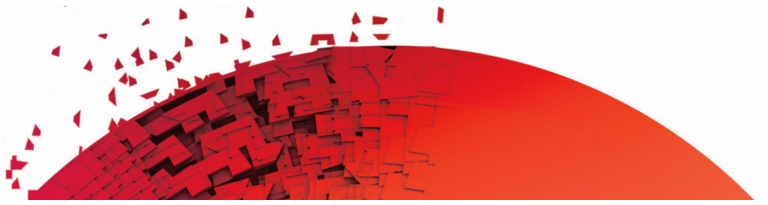
采用多种深度优化技术，打破传统网关性能瓶颈，不再出现丢包、页面卡顿等现象，从容应对苛刻的网络环境。

产品概述

在信息网络安全的诸多威胁中，恶意代码的危害无疑最大，众多数据交互途径都可能引入恶意代码，给组织带来安全风险。

辰信威胁防御安全网关TDSG，是针对近年来恶意代码威胁快速演变而设计的一款革新的网关级过滤设备，可全面高效防范恶意代码威胁的传播、动态式攻击，异常通讯。产品拥有卓越的性能和高可靠性，可有效保障业务的可持续性和稳定性。其灵活多样的应用场景会使用户体验到多重防御所带来的应用价值。

可适用多种复杂网路环境，即插即用的特性，无需用户变更现有网络架构，即可轻松实现防御。可适用于中小



功能特点

- **多链路防御**

支持多链路的串行防御、多接口的并行监测、及串并混合部署。透明接入，可融合各种复杂网络环境及各项业务应用区域。

- **静态病毒过滤**

病毒过滤业界协议支持最多，端口自适应防御，无需手动设定，具有多种病毒逃逸防御技术。

- **动态威胁防御**

以"僵木蠕"为特点的威胁通讯，通过静态分析、动态分析、和行为分析等，实现综合监控防御。

- **智能手机安全**

为BYOD时代智能终端的APP程序下载、应用通讯，隐私泄露，实现网络层威胁监控。

- **嗅探破解阻断**

为业务应用系统提供恶意嗅探和暴力破解行为监控防御，提升现有安全防御策略。

- **分布式集中管控**

支持分级分布式多节点设备集中管控，实现策略及威胁库统一应用。

- **风险分析报告**

有别于以"数量"为主的安全报告。以风险模型及数据挖掘综合而得，旨在精确定位已知威胁，预警潜在风险，提供可决策性依据。

型企业、大型机构、以及性能要求较为苛刻的高校和运营商。

在等级保护第三级基本要求中明确规定，“应在网络边界处对恶意代码进行检测和清除”，辰信威胁防御安全网关TDSG的部署应用，不仅实现对现有网络结构及业务应用的安全防御和结构补充，同时也完全满足等级保护基本要求和评测要求。

性能优势

“在业界，网关级防病毒产品始终面临着防御与高性能无法完美兼得的尴尬局面。辰信威胁防御安全网关TDSG克服多项技术难题，可给予用户最佳的安全体验。”

辰信威胁防御安全网关TDSG高性能优势的体现，主要源自产品设计架构、专有硬件、底层驱动、引擎及软件等多方环节的融合与深度优化，突破传统网关性能瓶颈壁垒，满足用户对高性能、高可靠性要求。

辰信威胁防御安全网关TDSG在零COPY和多核并行处理技术之上，应用专有“脉冲机制”，以保障在突发的恶意流量和超规模的恶意攻击场景下，保持引擎的高速匹配，确保网络在线体验度和安全防御。

辰信威胁防御安全网关TDSG具有多款型号，可应用于中小型企业、大型集团、及电信运营商等不同场景。