永达电子

流量分析审计回溯系统

产品概述

流量分析审计回溯系统是一款实现事前预防、事中检测、事后取证的安全运维工具，面向政府、金融、运营商、军队、能源、医疗、企业等行业用户，在丰富场景中提供专业的全流量分析解决方案。

产品满足网络故障定位、异常威胁检测、全流量回溯分析、多点质量对比等需求，帮助用户提升网络流量可视化分析能力。

产品功能

01 - 全量存储，流量回溯

- 2-7 层协议解析：多维分析、深度检测、在线解码
- 多级下钻：支持3级以上信息钻取，支持9个以上业务关联元数据维度
- 元数据全量存储分析：支持流量元数据的全量存储、事后回溯、调查取证和在线分析
- 网络性能&质量监测：解析多项关键性能 KPI 指标，包括网络层、服务层、应用层等不同层级的网络性能指标，全面掌握网络性能动态

02 - 网络审计，还原行为

- 互联网/内网应用审计：内置6000+互联网预定义应用和自定义应用，提供深度的应用自定义与审计能力
- 上网行为审计：提供网络行为审计及留存能力
- 关联分析：审计结果自动关联原始数据，多维度展示关键信息，形成业务分析闭环
- 文件还原：支持 HTTP、FTP、邮件等不同协议的流量文件还原，为数据安全护航

03 - 可视化分析，汇总展示

应用可视 基于全局、应用、用户维度，对流量、质量、性能数据进行展示和钻取，例如流速、时延、抖动等数据

用户可视 根据用户的访问行为、流量行为进行画像

实现用户与组织架构的流量统计、行为画像及性能分析功能

报表展示 提供完善的预定义报表模板和灵活配置的自定义报表功能，通过邮件等形式，定期进行汇总展示

04 - 异常检测，防患未然

僵木蠕检测 具有高效检测引擎，实时更新热点事件特征，内置 400 万海量病毒库，结合威胁情报数据，全面检测流量中的已知与未知威胁

异常流量检测 对恶意攻击、非法外联、异常协议、DDoS 行为、弱密码扫描和暴力破解等威胁行为进行检测

智能告警 支持基于阈值及基线的流量告警策略，提供敏感域名、邮件关键字、组合特征值等告警方案

产品参数

性能指标

1.新建连接：**12万/秒**

2.并发连接：**100万**

3.吞吐量：**6.5G**

4.数据库入库速度：**10万/秒**

5.数据回溯速度：**5TB/秒**

* 备注：以上结果基于32 核 CPU、49G 内存的硬件环境。

硬件参数	
形态	2U机架安全设备
管理接口	1个10/100/1000BASE-T管理网口
业务接口	4个GE以太网接口，4个万兆光口(SFP+)
供电	支持220~240V AC，2个热插拔550W交流电源模块，支持1+1冗余
温度	5°C to 45°C
尺寸	650*440*89mm

* 规划中产品规格，具体当前可配置信息以详细产品手册为准。

产品亮点

分布式部署

- 集中化管理：本地数据采集存储，分布式统一管理监控
- 部署多台服务器时，提供控制台远程连接方案，实现远端数据分析管理

丰富元数据，一比一还原

- 可提取10余种网络协议的80+元数据
- 支持多种协议的原始文件还原

全包存储

- 秒级回溯：实时记录全网原始数据，高性能采集海量数据，整网流量稳定存储
- 确保原始数据可回溯、可分析、可佐证；秒级回溯异常情况，多维度挖掘数据价值

大容量，强存储

- 内置大容量存储空间，并可灵活扩展。可存储超过6个月时间的原始数据

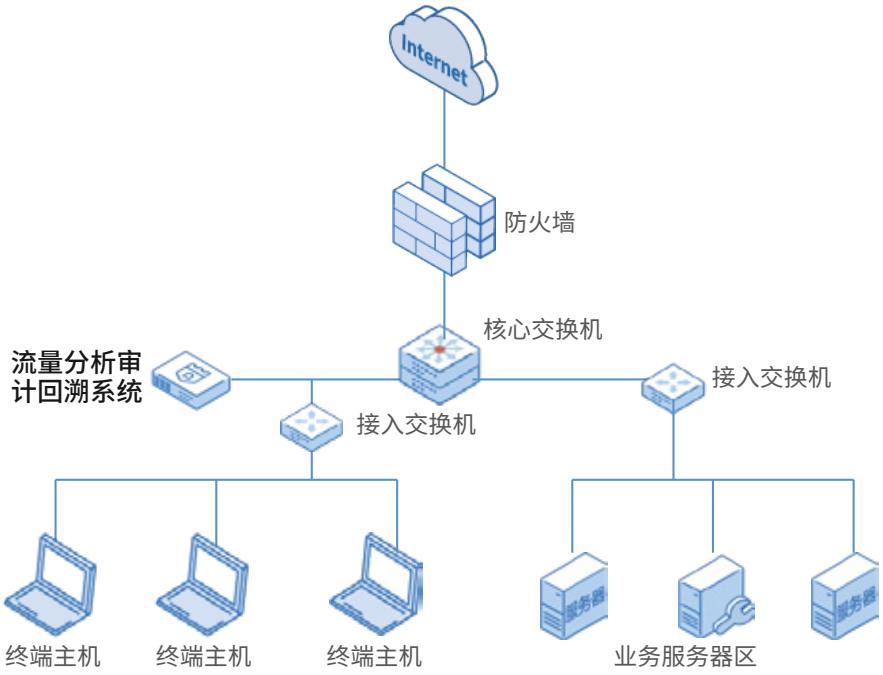
海量业务识别，精细质量监控

- 覆盖互联网常见应用和内网应用
- 为业务与应用分析，提供100+关键指标监控

快读写，高性能

- 最高可达40Gbps的实时处理能力
- 高性能实时处理，全量无损存储

设备部署



客户案例

国家部委

- 中共中央统一战线工作部
- 中华人民共和国工业和信息化部
- 中华人民共和国应急管理部
- 中华人民共和国科学技术部

地方政府

- 北京市东城区人民政府
- 成都市应急管理局
- 深圳市发展和改革委员会

国有企业单位

- 中国国家铁路集团有限公司
- 中国十八个铁路局集团有限公司
- 通号通信信息集团有限公司
- 北京经纬信息技术有限公司

本产品符合国家标准：

- GB-T 20945-2023《信息安全技术 网络安全审计产品技术规范》
- GB42250-2022《信息安全技术 网络安全专用产品安全技术要求》

深圳市永达电子信息股份有限公司
Shenzhen Y&D Electronics Information Co, Ltd.

★ 国家级高新技术企业　★ 国家信息安全服务二级资质企业
★ ITSS二级资质企业　★ 涉密信息系统集成甲级资质企业

地址：深圳市南山区科技北一路17号摩比天线大厦5楼
电话：0755-26727588　传真：0755-26727593
邮箱：sales@s-ec.com
官网：http://www.s-ec.com

售后热线 400-884-0006