SinoTelecom 欣诺通信
www.sino-telecom.com


网络安全产品解决方案

数据链路采集 / 公共互联网安全治理系统 / 接入网数据采集

上海欣诺通信技术股份有限公司

Contents / 目录

COMPANY

PROFILE

公司介绍

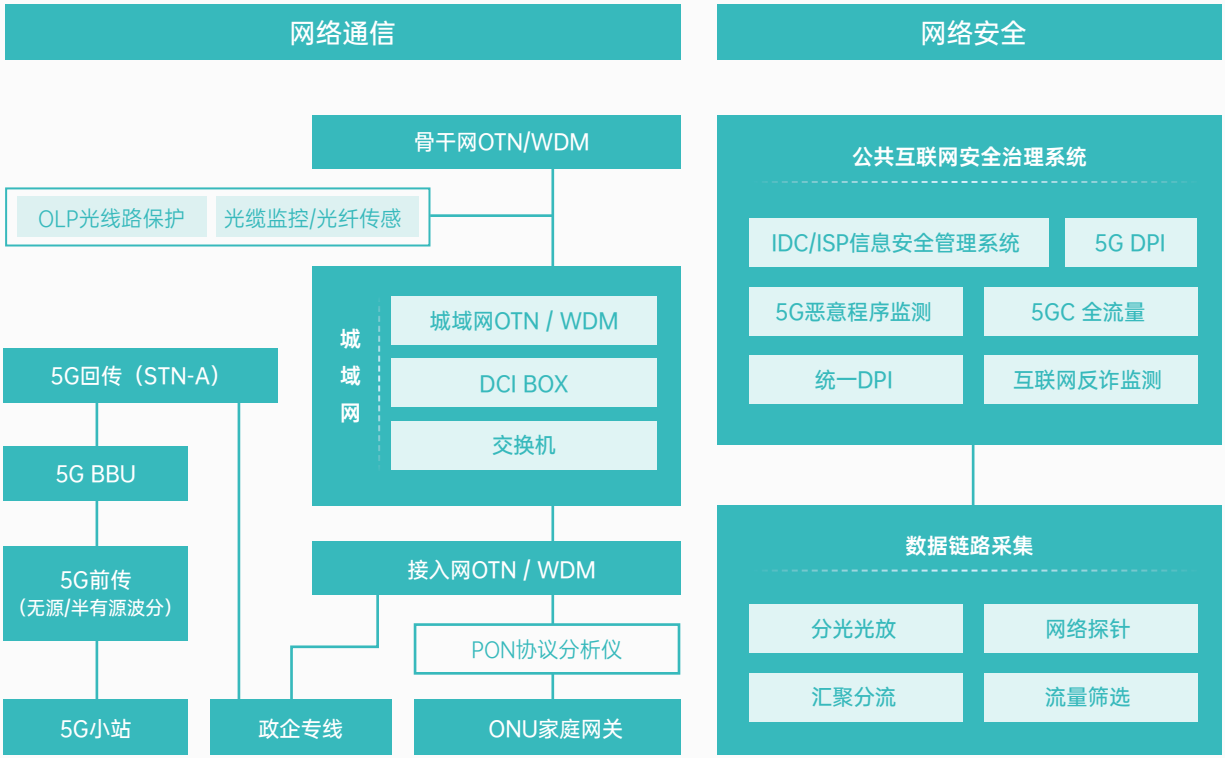
上海欣诺通信技术股份有限公司是一家专注于网络通信与信息安全技术融合发展的研发型高科技公司，坐落于风景秀丽的松江新城，系国家认定的高新技术企业、国家级"专精特新小巨人"企业、上海市科技小巨人企业和上海市战略性新兴企业。

欣诺的网络通信解决方案主要包括光网络和数据通信，产品包括100G+ OTN/WDM、DCI/新型城域波分、接入OTN以及STN-A、数据中心交换机、IPRAN等传输和数通产品；公司的网络安全解决方案主要包括数据链路采集和公共互联网安全治理系统，产品包括从分光/光放、汇聚分流到固网DPI、5G DPI、5G 恶意程序监测、5GC全流量等软、硬件安全产品。网络通信和网络安全作为公司发展的"双引擎"，在公司发展过程中相互支撑、协同发展，目前已形成了良好的齐头并进的发展态势。

"欣然一诺，全力以赴！"是全体欣诺人一直秉持的宗旨，我们致力于给客户提供更高性价比的解决方案，并配以更灵活的市场策略和更贴心的服务，为此我们在全国各省会城市都已建立销售和服务网点，以便更快速地响应客户需求。

随着新基建时代的到来，欣诺过去五年持续大规模研发投入形成的产品和技术储备特别适用于5G时代大带宽、低时延和高安全性的网络需求，我们特别珍惜这来之不易的战略机遇期，尽力给客户提供高性价比的解决方案以及完善的售后服务支撑和供货保障，力争成为国内通信和安全市场上的一支中坚力量。

欣诺通信产品/市场图谱



欣诺通信国内客户不仅有中国电信、中国移动、中国联通等传统电信运营商，还包括广电、电力、铁路、公安等专网客户群。海外客户更是遍及5大洲。

欣诺网络安全产品

数据链路采集 / 公共互联网安全治理系统

PRODUCT

INTRODUCTION

网络安全产品介绍

在信息安全领域，欣诺已发展成为国内网络安全领域少有的产品覆盖从分光、分流（硬件）到公共互联网安全治理系统（软件）的全产业链公司，产品包括：

1. 数据链路采集：从分光、光放、传输、分流以及服务器全系列硬件解决方案；
2. 公共互联网安全治理系统：主要包括IDC/ISP信息安全管理系统、5G DPI系统、5G恶意程序监控产品、5GC全流量产品等；
3. 分布式、一体式接入网特侦平台。

数据链路采集产品

分光光放 / 旁路器 / 分流汇聚

欣诺的数据链路采集产品主要包括分光放大和分流汇聚产品。分光放大产品是将需要采集的数据链路上的光信号先进行分光，然后对支路弱信号进行放大后多路复制输出。分流汇聚产品可对数据中心流量进行流量汇聚、流量过滤、分流/转发、负载均衡和复制输出，产品不仅可应用于数据中心的内容审计检测，还可以应用于移动互联网和城域网的信令采集、内容审计和电信增值业务等。

欣诺数据链路采集产品通过突破性的技术创新，在国内率先实现了智能分光、零误码串并切换并集成高速数据分类、感知和处理能力于一体，具有安全性高、稳定性好、处理能力强等优势。

OEO6504分光器

OEO6504是一款无源式分光器业务平台，该平台高为1U，共提供4个业务槽位，最大可支持24路1分2分光器模块/16路1分4分光器模块/8路1分8分光器模块，可根据客户需求定制分光比，特别适用于大型核心机房的分光采集和光放业务。

OEO6504

- 标准19英寸1U高设计，节省机房空间；
- 集成密度高，支持4个业务板卡插槽；
- 模块化设计、便于维护；
- 低插损、高反射、高波长隔离度；
- 分光比可由1:99到50:50；
- 支持平面光波导和熔融拉锥两种方式的分光器，分光器采用电信监控级分光器模块，具有可靠性好，分光比精确，带宽范围大，温度适应能力强等特性；

OEO6504分光器板卡

1分2分光器

1分2分光器业务卡支持2:8/3:7/5:5等各种分光比，每个业务卡支持4组1分2分光器

1分4分光器

1分4分光器业务卡支持7:1:1:1或均分等各种分光比，每个业务卡支持4组1分4分光器

1分3分光器

1分3分光器业务卡支持7:2:1/8:1:1等各种分光比，每个业务卡支持4组1分3分路

1分8分光器

1分8分光器业务卡支持2组8路均分分光

STN6200放大及安全系列

STN6200系列产品综合性强、集成度高、管理功能强大，提供基于SNMP协议的电信级图形化管理、配置灵活，通过混插不同的业务板卡同时实现OEO光放大、EDFA放大、SOA放大和集成放大分光等多业务的综合处理，提供丰富的速率接口类型，支持GE/2.5G/10G/ 40G/100G多种业务速率。

- 可插拔设计，所有板卡可以任意灵活搭配
- 双电源设计：双直流-48V，双交流220V或DC-48V和AC220V供电
- 双主控设计：支持主控1+1备份，网络管理更高可靠性
- 主控板支持SSH,Telnet,SNMP，ONE IP，Radius等功能，网管基于B/S设计，网维更灵活

STN6200 光放平台

STN6200光放大板卡

OEO放大卡

- 板卡型号：STN6200-OTU10A/OTU6FA
- 支持GE/10G/40G/100G OEO光信号放大

SOA放大卡

- 板卡型号：STN6200-SOA2 / SOA4 / SOA6
- 支持1310nm波长范围40G/100G链路信号放大

EDFA放大卡

- 板卡型号：STN6200-OA/OA1/OA2
- 支持1550nm波长范围40G/100G链路信号放大

集成放大分光

- 板卡型号：STN6200-SAX1/SAX2 / SSA2 /SAH/ SAH2 /SSAH
- 集成分光器和光放功能，支持GE/10G/40G/100G

光旁路器 OEO6500B

旁路器是针对光设备保护而专门设计的保护方案，当光设备故障或断电不能正常运行时，通过旁路器可直接跳过该节点进行通信，从而保证了整个通信系统的正常通信。旁路器是一种应用于光纤通信领域并能自动绕过故障的网络节点的光器件，能自动识别网络节点光信号状态，进行光路瞬时切换，从而能避免网络节点发生全阻障碍时，自动绕过故障的网络节点，保持系统连通正常。

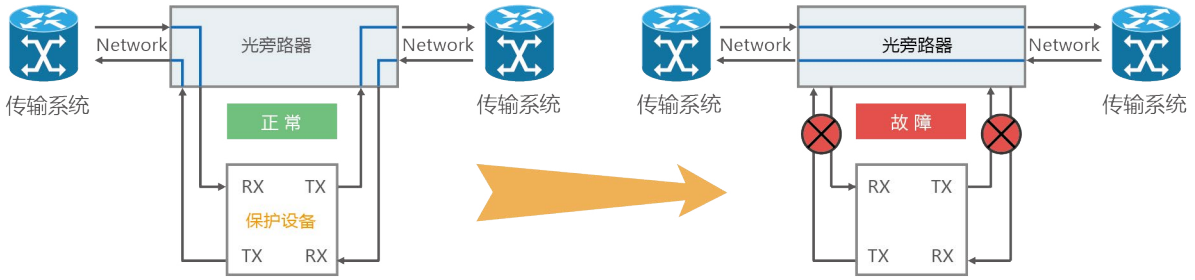
产品特点：

提供1U/2U标准19英寸机架可选，电源支持1+1备份，所有子卡支持热插拔，最大支持8条双向链路，支持异常掉电旁路，保证原始链路业务正常，支持心跳控制协议。与主流分流器厂商对接经验丰富，大批量实战部署，运行稳定。

- 无光旁路、掉电旁路
- 支持串口、网管、按键设置
- 插损小、切换快
- 内置心跳、智能检测

1U 旁路型 OEO6500B-BP

2U 旁路型 OEO6500B-BP



光单路Bypass

- 板卡型号：OEO6500-BP/BP-T/TBP
- 支持GE/10GE/100G光路Bypass保护，支持掉电旁路和心跳检测功能

多模旁路器/多模Bypass

- 板卡型号：OEO6500-BP-MM
- 支持GE/10GE光路Bypass保护，单卡支持主备设备接入，支持掉电旁路和心跳检测功能

智能光旁路器

10G Bypass-XGBP / 100G Bypass HGBP

全光口以太网Bypass交换设备，用于10G/100G以太网网络旁路保护，在内联系统出现故障或进行维护时保持网络连接的完整性，支持各类网关设备（如：防火墙、IDP、UTM、入侵防御系统、垃圾邮件网关、专用网络审计设备等）的智能切换。

与传统Bypass设备只支持纯硬切换功能相比，XGBP/HGBP支持更为灵活的切换方式，可将切换损伤降至最低。

支持串接接入(K2）、电旁路（K1）、光旁路（K0）三种工作模式
支持ACL规则过滤功能

10G Bypass_XGBP

100G Bypass_HGBP

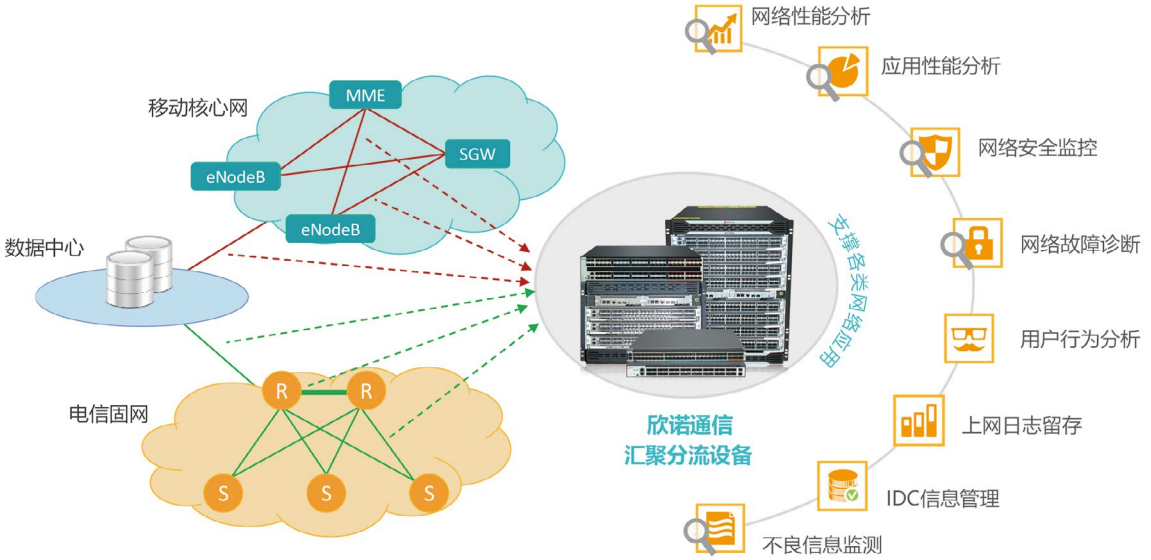
产品特点：

- HGBP支持4个光旁路保护组，最大可支持4条100G链路的串接保护；XGBP支持3块业务插槽，每块业务卡支持2个光旁路保护组，最大可支持6条10G链路的串接保护
- 支持分光镜像，在设备串接时能够分光原始数据
- 支持1对1的保护组级别心跳，支持多对1、多对多心跳保护，满足后端负载分担、冗余备份业务场景下的心跳保护机制
- 支持设备掉电旁路保护功能
- 支持串接链路的端口流量统计
- 支持K1和K2模式零丢包切换，无需中断业务的情况下无感知升级后端设备
- 支持warmboot升级设备
- 支持与10G、1G端口形态互联，可根据后端解析设备端口灵活配置接口形态
- 支持通过NMS9100实现统一的图形化界面管理。
- 友好的管理界面，提供完善的命令行管理、SNMP管理接口、UDP socket API接口
- 提供详细的系统日志记录

分流汇聚

SFC7000是欣诺面向大数据处理和网络流量分析处理的综合平台，主要应用于运营商、政企网、安网等领域，对网络流量进行复制、汇聚、分流、过滤、协转等方式实现自由导向输出，以满足各类流量监控系统的部署需求。

根据使用环境和网络流量的不同，SFC7000分别有盒式分流和正交分流解决方案。



盒式分流

SFC7000 系列盒式分流设备，将分路器、过滤分析设备、负载均衡设备合而为一，为网络安全、协议分析和信令检测系统提供了便捷高效的数据采集解决方案。能够适应多种应用环境，按照需要实时为网络信息监控、网络业务分析器、信令分析仪等设备提供网络通讯数据。

SFC7000 系列盒式分流设备支持强大的智能选流和多路监测功能，支持多端口数据标记、汇聚、过滤、数据包多份复制输出或者负载均衡分流输出，特别适合链路数量多、网络流量大、密集度高的复杂应用环境。

SFC7132T

- 高端口密度，提供 32个100GE接口和2个25G接口。100GE接口可以兼容40G/4x10G/4*25G接口模式，25G接口向下兼容10G速率和1G速率，线速能力可达3.2Tbps；
- 支持流量汇聚、规则过滤、流量镜像、负载均衡等功能；双路冗余电源；

SFC7132H（国产化方案）

- 高端口密度，提供 32 个 100GE接 口。100GE接口可以兼容40G/4x10G/4*25G接口模式；
- 支持流量汇聚、规则过滤、流量镜像、负载均衡等功能，双路冗余电源；

SFC7154

- 高端口密度，提供48个10GE 和6个100GE 接口。100G接口兼容40G或4x25G/10G速率，10G 接口兼容25G，整机线速处理能力可达1.8Tbps，高级处理功能可达400G；
- 支持流量汇聚、规则过滤、流量镜像、域名匹配、负载均衡、头部剥离、报文截短、报文去重、音视频过滤等功能，支持AC/DC电源1+1保护。

SFC7160

- 高端口密度，提供 52个25G/10G和 8个100GE接口；100G接口兼容40G或4x25G/10G速率，25G接口兼容10G；
- 支持流量汇聚、规则过滤、流量镜像、域名匹配、负载均衡、头部剥离、报文截短、报文去重、音视频过滤等功能，支持AC/DC电源1+1保护。

SFC7160E（国产化方案）

- 高端口密度，提供 48个10G和 8个100GE接口；100G接口兼容40G或4x25G/10G速率，10G接口向上兼容25G，向下兼容1G，整机线速处理能力可达2.0Tbps；
- 支持流量汇聚、规则过滤、流量镜像、负载均衡等功能；支持AC/DC电源1+1保护。

SFC7920

- 高端口密度，提供76个10G和 18个 100GE接口，100G接口兼容40G或4x25G/10G速率，其中24个10G接口兼容25G；
- 支持流量汇聚、规则过滤、流量镜像、负载均衡等功能；支持AC/DC电源1+1保护。

正交分流

欣诺正交汇聚分流设备是一款新型的 400G/200G/100G/40G/25G/10G 全光速率可接入的，具有端口密度高、工作模式丰富、高性能部署灵活、管理维护方便等特点，能够适应多种应用环境，按照需要实时为网络信息监控、网络业务分析器、信令分析仪等设备提供网络通讯数据。

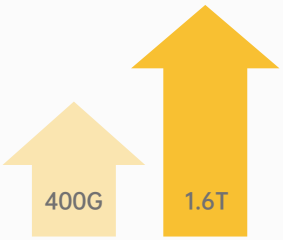
欣诺正交汇聚分流设备提供强大的智能选流和多路监测功能，支持多端口数据标记、汇聚、过滤、数据包多份复制输出或者负载均衡分流输出，特别适合链路数量多、网络流量大、密集度高的复杂应用环境，为网络安全、协议分析和信令检测系统提供了便捷高效的数据采集解决方案。

SFC7903

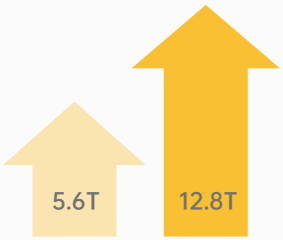
- 设备尺寸：5U 3 槽位正交机框；
- 交换能力：整机最大 4.8T；
- 端口密度：业务板卡可支持 24*100G/40G 和 36*25G/10G 接口，或支持 48*100G/40G 接口，或支持 4*400G 接口、20*100G 和 36*10/25G 接口；
- 电源：支持 2 路交流 / 高压直流电源或 3 路低压直流电源；
- 功耗：整机满配功耗小于 3500W；

SFC7908

- 设备尺寸：13U 8 槽位正交机框；
- 交换能力：整机最大 12.8T；
- 端口密度：业务板卡可支持 24*100G/40G 和 36*25G/10G 接口，或支持 48*100G/40G 接口，或支持 4*400G 接口、20*100G 和 36*10/25G 接口；
- 电源：支持 4 个可拔插的电源模块，3+1 冗余，支持交流 / 高压直流 / 直流 -48V 电源；
- 功耗：整机满配功耗小于 6500W；



单板接入能力升级



单机箱接入能力升级

交换能力升级

SFC7960SC-正交主控

- 支持对正交机箱各板卡、电源、风扇、应用的控制和管理功能；
- 支持自定义 IPMI 机箱管理功能；
- 支持2 个MGT（MGT0 和MGT1）管理网口、2个千兆光口和 2 个USB 接口；
- 正交机箱支持配置2块主控卡，1+1冗余。

SFC7964SW-正交交换卡

- 单板支持最大 6.4T 背板交换能力，为每块业务板卡提供 800G 的背板交换带宽；
- 正交机箱支持 2 块交换板卡，实现整机 12.8T业务交换能力；

SFC7960L-正交业务卡

- 支持 24 个 100G 和 36 个 10/25G LAN 接口的输入输出。其中 100G 接口兼容 40G，支持4*10G/4*25G 拆分；
- 单板采用1颗6.4T可编程交换芯片，最多可扩展4块多核高级业务处理模块；
- 支持3.3T流量接入能力和1.6T的背板交换能力；
- 支持1 个串口、1 个GE管理网口，实现对本板的本地和远程管理。

SFC7960Q-正交业务卡

- 支持4个400G接口、20个100G和36个10/25G接口，400G接口兼容100G/200G速率，100G 接口兼容 40G速率，支持4*10G/4*25G 拆分；
- 单板采用1颗12.8T可编程交换芯片，最多可扩展4块多核高级业务处理模块；
- 支持4.5T流量接入能力和1.6T的背板交换能力；
- 支持1 个串口、1 个GE管理网口，实现对本板的本地和远程管理。

SFC7948L-正交业务卡

- 支持 48个 100G 接口的输入输出， 100G 接口兼容 40G，支持4*10G/4*25G 拆分；
- 单板采用1颗6.4T可编程交换芯片；
- 单板支持4.8T流量接入能力和1.6T的背板交换能力；
- 支持1 个串口、1 个GE管理网口，实现对本板的本地和远程管理。

紧凑型正交分流

SFC7408 是一款正交架构的 10G/25G/100G 以太网汇聚分流设备，采用国产化交换方案，具有端口密度高、工作模式丰富、高性能部署灵活、管理维护方便等特点，能够适应多种应用环境，按照需要实时为网络信息监控、网络业务分析器、信令分析仪等设备提供网络通讯数据。

SFC7408 正交汇聚分流设备提供强大的智能选流和多路监测功能，支持多端口数据标记、汇聚、过滤、数据包多份复制输出或者负载均衡分流输出，特别适合链路数量多、网络流量大、密集度高的复杂应用环境，为网络安全、协议分析和信令检测系统提供了便捷高效的数据采集解决方案。

产品特点

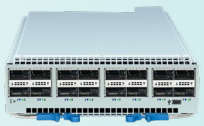
- 设备高度4U，支持8个业务槽位;
- 每槽位16个100G接口，单槽位支持1.6T背板带宽;
- 整机支持12.8Tbps基本分流处理能力;
- 可插拔风扇设计，支持4+1冗余;
- 可插拔电源设计，支持1+1冗余;
- 整机功耗不超过1600W.

SFC7408

板卡介绍

SFC7416CQ-业务接口卡

- 支持 16 个 100G LAN 接口的输入输出， 100G 接口兼容 40G，支持4*10G/4*25G 拆分;
- 支持1.6T流量接入能力和1.6T的背板交换能力
- 支持1 个串口可实现对本板的本地管理



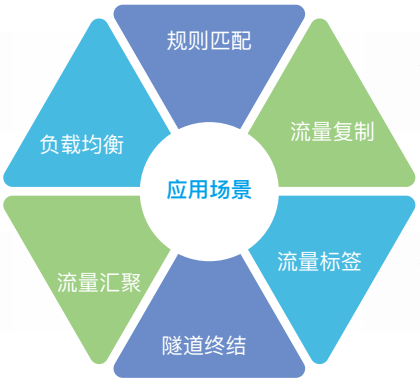
SFC7432X-业务接口卡

- 支持 32个 25G 接口的输入输出， 25G 接口向下兼容 10G和GE;
- 单板支持800G流量接入能力和800G的背板交换能力
- 支持1 个串口，可实现对本板的本地管理

基本分流功能

- 支持内层/外层的灵活和掩码五元组规则
- 支持MAC、VLAN、报文长度等匹配规则

- 支持输出组内的流量负载均衡输出，支持多种HASH方式



- 支持将流量复制多份，转发后端系统

- 支持GE/10G/25G/40G/100G等多种速率的流量接入汇聚

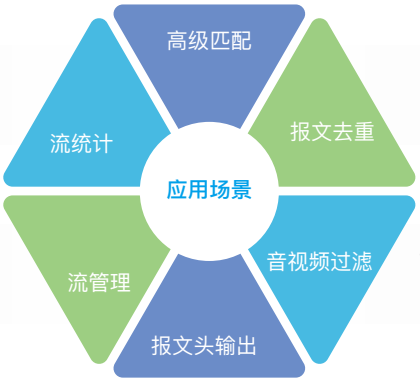
- 基于VLAN或MAC地址流量标签，转发后端系统

- 支持GRE隧道终结功能

高级分流功能

- 支持HOST/SNI/URL匹配规则

- 对输入流量进行Netflow统计，并输出统计信息



- 支持全包和L3以上重复报文去重

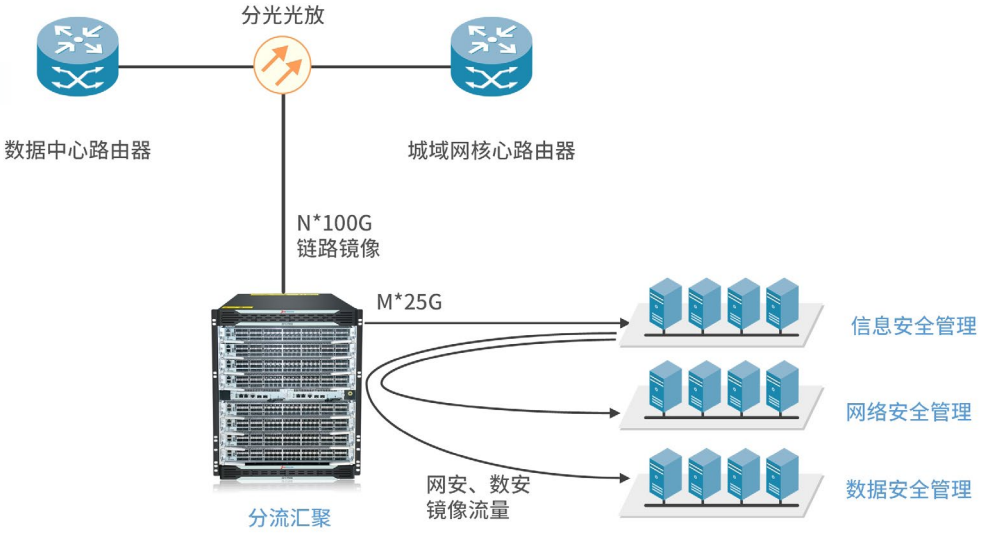
- 支持流表管理，输出每个会话前N个报文，支持流锁定功能

- 基于应用的五元组、协议、 Content-Type、URL特征实现音视频流量过滤

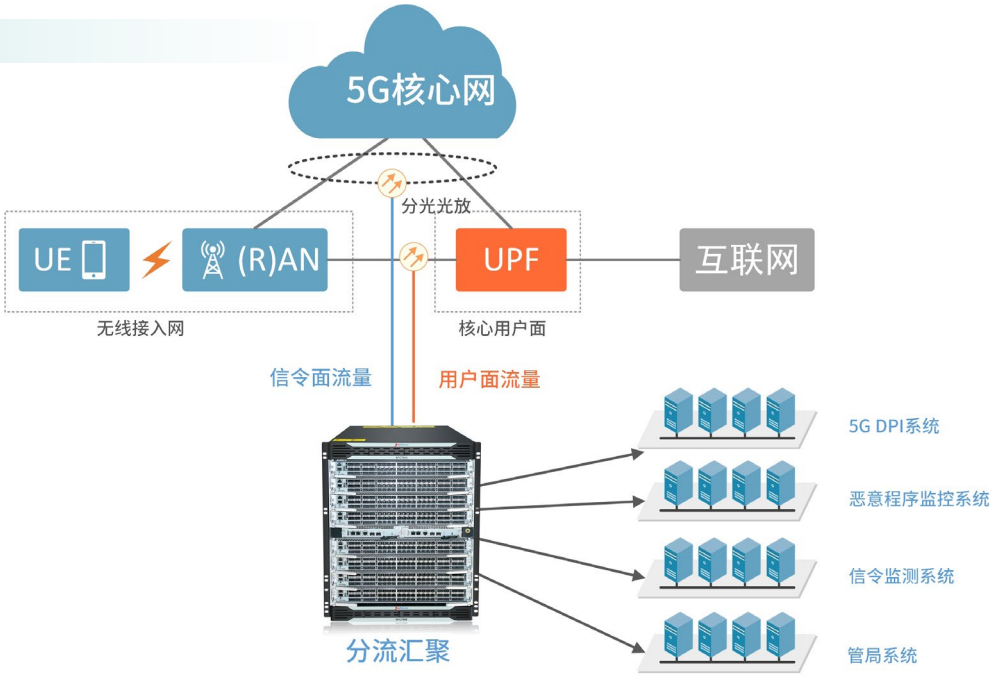
- 输出原始报文的网络层和传输层首部

应用场景

固网应用



移动网应用



公共互联网安全治理系统

IDC/ISP信息安全管理系统 / 5G DPI /恶意程序监控系统 /
5GC 全流量分析系统

欣诺公共互联网安全治理系统主要包括IDC/ISP信息安全管理系统、5G DPI系统、5G恶意程序监控产品、5GC全流量产品等。产品针对固网、移动网和数据中心等场景的网络安全、内容审计和增值业务需求，采用DPI（深度包解析）和DFI（深度流检测）技术，筑牢可信可控的数字安全屏障，切实维护网络安全，增强数据安全保障能力。

IDC/ISP信息安全管理系统

欣诺IDC/ISP 信息安全管理系统具有基础数据管理、访问日志管理、信息安全管理等功能的信息安全管理系统，以满足电信管理部门监管系统（SMMS）和 IDC/ISP 经营者的信息安全管理需求。

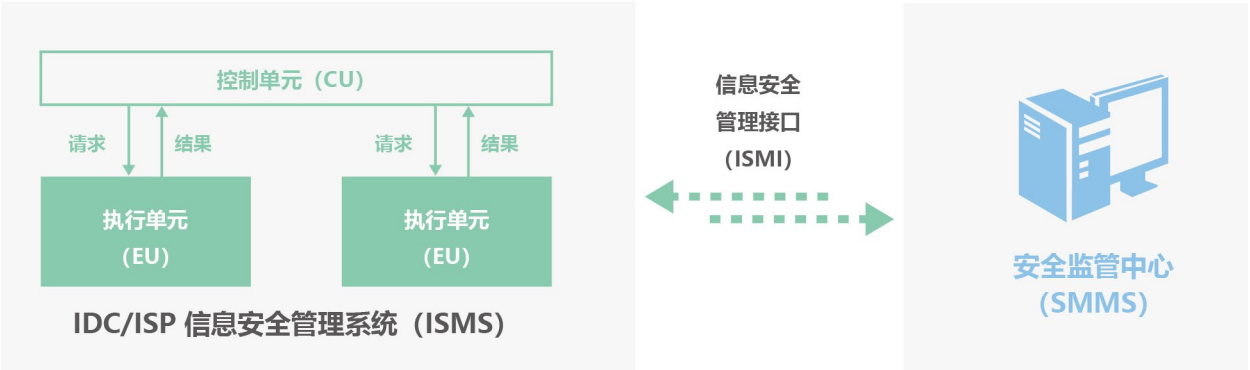
该系统是定位于运营商通信网络、数据中心等场景的深度报文检测和安全审计系统，满足工信部对电信运营商数据中心的监管要求，对电信运营商数据中心的双向网络大规模流量实时监测、采集、还原等，对违法违规信息实时阻断。

欣诺 IDC/ISP 信息安全管理系统服务器

该系统是一个承载在服务器上的信息安全软件系统，产品支持 X86 服务器，也支持国产化 ARM 架构的服务器。

控制单元（CU）：负责与通管局建设的安全监管系统（SMMS）进行通信，接收来自SMMS的管理指令，并根据要求向SMMS上报数据，同时还要实现对本单位各执行点的EU进行集中管理，完成管理指令的调度、转发和执行及数据的汇总、分析和预警。

执行单元（EU）：根据指令要求，实现IDC访问日志生成、违法信息监测发现、违法信息过滤处置，并将结果汇总到控制单元(CU)。



产品功能

信息安全管理

接收控制单元下发监测、过滤处置的指令并记录日志及时上报，实时调整信安管理策略，多维度多手段检测处置。

应用识别

支持20 多种业务大类和3500+ 应用小类；支持实时或者定期更新应用特征库；

日志审计

支持对所有访问日志进行审计记录并上报，支持灵活的日志定制模板

流量统计

支持IDC 流量流向分析统计；支持IP 地址流量TOPN，支持特定IP、IP 段的流量统计；支持统计网络攻击流量

流量镜像

支持基于用户、用户组、时间段等多维度组合的镜像策略

流量控制

支持基于APP、用户、用户组、qos 等多维度的流量控制

流量封堵

支持基于域名、URL、IP、端口、关键字的封堵策略；支持通过TCP 拆连、UDP 丢包、HTTP 页面重定向等多种手段封堵处置；支持和其他设备联动处置

网络安全

支持对网络攻击、恶意程序网络活动的监测；支持对网络异常行为监测和对恶意文件还原后的监测，包括对未知恶意程序进行沙箱、反编译等手段检测

数据安全

支持对包含数安内容的协议进行识别和还原，对还原的文件进行分级分类标记；支持控制单元下的数安巡查指令，并上报检测结果，对数据安全进行监测溯源；

产品特点

丰富的应用识别能力

- 支持互联网应用 20 多种大类、3500 余种业务小类的应用识别能力，针对常规互联网应用识别准确率达 95% 以上，且具备一定 AI 自学习特性不断扩展识别能力；

强大的规则匹配能力

- 全面满足国家通信管理部门关于信安系统中支持五元组、URL、域名、tcpflag、tos、vlan、关键词、IMSI 以及正则表达式等各类规则对流量进行匹配，并执行安全管理策略，最大可支持百万条规则；

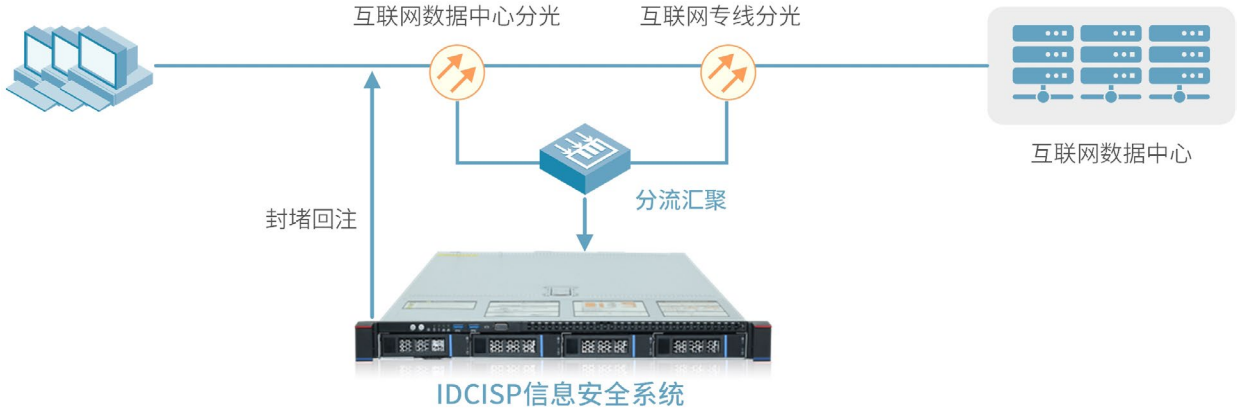
高集成度低能耗比

- 采用的 1U/2U 通用 x86 架构服务器或国产化 ARMv8 架构鲲鹏服务器，都具有低机柜、低电源占用的高集成度低能耗比特点；

良好的接口扩展性

- 物理接口方面，流量处理设备可灵活支持 100G、50G、25G、10G、GE 接口等多种线路接口进行流量采集接入。

典型应用场景



5G DPI 系统

欣诺5G DPI 系统应用于运营商移动网络场景中，可实现5G 网络信令面及用户面等信息的采集、识别、解析等功能；该系统是5G 网络可视化的核心支撑系统，是5G 网络的核心组成部分之一。

欣诺5G DPI 系统通过对5G 网络流量进行识别、采集与深度检测（DPI）等数据处理，实现识别、监测和统计5G 网络流量中的用户、业务，流量内容、运行质量等信息，并将分析完成的数据传递给下游应用。下游应用会以5G DPI 系统提供的数据为基础，可实现对网络流量及数据的智能化管控、商业智能以及信息安全等一系列目标。

欣诺 5G DPI 系统服务器

欣诺 5G DPI 系统是一个承载在服务器上的信息安全软件系统，产品支持 X86 服务器，也支持国产化 ARM 架构的服务器。5G DPI 系统根据应用场景和机框尺寸的不同分为 1U 设备和 2U 设备。

产品功能

支持全量原始数据控制处理

- 支持对 N1~N40 等 5GC 控制面接口全量原始数据进行控制处理，控制面原始数据解码、合成、各协议关联、用户信息回填；

支持对 N3 数据面接口进行深度报文解析识别

- 能够按照当个用户单次访问的颗粒度对移动网用户网页浏览、视频业务、即时通信、游戏等主要典型业务的开始时间、结束时间、URL、流量、关键质量信息等进行识别；

支持安全模式下的 NAS 消息解密

- kSeaf 密钥信息从 N12 接口提取，同时 N1/N2 解码过程与 N12 密钥提取进行联动，将 kSeaf 密钥用于相应的 N1/N2 接口 NAS 消息的解密；

具备 IPv4 和 IPv6 数据的解析识别能力

- 能够对所采集到的信令面及用户面的 IPv4、 IPv6 数据进行解析识别；

灵活的 xDR 输出模板快速调整输出字段集合，快速输出符合现场需求的 xDR 接口话单；

支持动态实时关联

- 可根据业务过程中各接口信令过程之间的相关性，对信令处理过程进行动态实时关联，并实时获取、存储和更新用户上下文信息并将无法直接从某过程消息中获取的用户信息（如 SUPI、GPSI、PEI、等）回填入 xDR 话单中；

生成网络 KPI 指标数据

- 能够解析识别的关键质量（KQI）指标信息，计算生成网络 KPI 指标数据；

支持信令原始码流的存储与分类上报，支持预设条件的信令原始码流抓取与导出。

产品特点

具有高集成度低能耗比的特点

- 采用高效数据采集解析引擎（UCPP），在提高采集和解析性能的同时，实现对于流量的准确识别，可实现在 1U 高度设备最大采集解析 120Gbps 5G 用户上网流量的处理性能，同时满足用户信息回填数据准确性不低于 99%，总体流量识别率不低于 99%，常规互联网应用识别准确率不低于 95% 的性能指标；

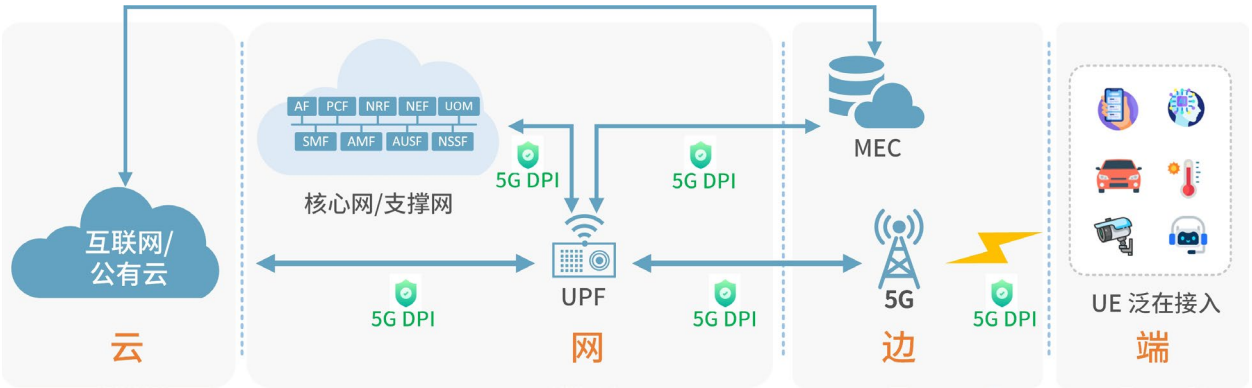
对于上级及三方应用的接口开放且丰富

- 可以支持 SDTP、FTP/SFTP、Socket/Kafka 等多种接口，可灵活配置加密 / 非加密、压缩 / 非压缩格式上传。同时，输出话单采用字段库设计模式，支持各种定制话单，可灵活输出不同格式话单；

运营商网络全覆盖

- 支持国内运营商 2G/3G/4G/5G/VoLTE/VoNR 各网络全接口的采集解码，并可提供符合运营商需求的识别能力和拓展能力。

典型应用场景



恶意程序监控系统

欣诺恶意程序监控系统由信令面解析模块、用户面解析模块、样本还原模块、样本扫描引擎、入侵检测引擎以及流量处置模块组成，支持对移动网络流量出现的安全攻击以及移动网恶意程序传播、控制事件的检测，生成事件话单记录，支持对恶意程序以及疑似恶意程序的样本文件进行捕获还原，并对安全事件进行识别、阻断处置。

该系统部署在运营商移动互联网的核心节点侧。适用于 4G/5G 等不同核心网网络流量的监测防护，主要服务于基础电信运营商及工信、网信等网络安全主管部门，满足工信部对运营商的考核要求 。

欣诺恶意程序监控系统服务器

欣诺恶意程序监控系统是一个承载在服务器上的信息安全软件系统，产品支持 X86 服务器，也支持国产化 ARM 架构的服务器。

产品功能

预处理

- 支持信令面流量 HTTP2,PFCP,GTPV2C 等协议解析；
- 支持用户面 GTP-U 协议解析；
- 支持物联网 MQTT,COAP 等协议解析；
- 支持 IPv6 协议解析；
- 支持内容监测信息提取：用户标识信息，位置信息，五元组信息，URL, HOST 等

检测分析

- 支持基于样本文件的恶意程序的检测，文件格式包括但不限于 SIS/SISX/EXE/JAR/APK/CAB/RAR/ZIP/IPA/COD/ALX/PRC/ELF 等；
- 支持网络入侵及攻击行为检测分析；
- 支持基于规则的恶意网站检测分析；
- 支持移动终端类型识别与分析；

样本还原

- 基于HTPP/FTP/EMAIL等多种文件传输协议的文件还原，文件格式包括但不限于SIS/SISX/EXE/JAR/APK/CAB/RAR/ZIP/IPA/COD/ALX/PRC/ELF等；
- 支持对还原的样本文件大小、文件格式类型、文件MD5值等多维度的匹配判定；
- 支持对文件中敏感词、关键字的匹配判定

封堵处置

- 支持恶意代码传播黑名单功能，具备根据恶意代码传播黑名单实施封堵；
- 支持根据URL对恶意代码传播，对受害终端（感染恶意代码的手机或PC等）异常流量等进行阻断；
- 支持多维度封堵，包括基于IP地址（IP地址段）、域名、URL、恶意代码特征、手机号码段的策略，实现特定用户的上网行为进行处置；

特征库管理

- 入侵检测特征库；
- 病毒样本特征库；
- 支持恶意特征库配置升级接口（IF_Config）

产品特点

协议识别及安全事件监测能力

- 支持对互联网、物联网、车联网、工业互联网相关协议进行解析，并支持深度提取报文中的相关设备类型、生产厂商、软硬件版本号等信息进行资产识别，通过安全监测引擎对主机受控、有害程序事件、网络攻击行为等恶意事件进行监测，并按需对恶意样本进行还原，同时输出相关恶意事件日志；

封堵处置能力

- 支持上级管理系统下发的策略进行封堵处置规则的定义和匹配，支持对基于TCP的协议、IP地址、域名、URL、端口、手机号码、用户标识（SUPI/IMSI）、手机硬件标识（PEI/IMEI）等规则等维度信息进行拆链和重定向的封堵处置，同时还支持具备恶意流量传播黑名单的功能，具备根据恶意流量传播黑名单实施封堵/解封；

高性能高检测率

- 具有高集成度低能耗比的特点，采用了高效数据采集解析引擎（UCPP），该引擎结合了零拷贝、无锁队列、大页等多项技术，使流量的采集和解析性能得到大幅提高，可在 1U 设备上实现最高 90Gbps 的处理能力；对移动互联网恶意样本产生的恶意事件（含主机受控、有害程序事件）检出成功率不低于 95%、网络攻击行为检出成功率不低于 85%、监测及处置的黑名单容量不低于 400 万条、URL、IP、域名、手机号的封堵成功率不低于 95%、实战精确率（Precision）、召回率（Recall）不低于 98%;

全流量通联关系发现

- 可实现基于链路特征的发现和关联，及对部分私有协议的解析，内置互联网通联关系模型，通过此模型可对 VoLTE、VoNR、CSFB、2/3G CS 域话单及 skype、微信、QQ 等 IM App 的流量话单进行关联识别，大幅提高对于电信诈骗团伙之间的通联关系、诈骗团伙和受害者之间的群组关系的识别能力。

典型应用场景

5GC 全流量分析系统

欣诺 5GC 全流量分析系统是定位于运营商移动互联网场景的深度报文检测系统，满足运营商在核心网领域的监管要求。5GC 全流量产品能够对核心网网元交互流量实时监控，根据全流量检测系统的威胁情报，提供核心网网元交互流量的分域防护、管控与安全清洗及防御功能。

欣诺 5GC 全流量分析系统服务器

欣诺 5GC 全流量分析系统是一个承载在服务器上的网络安全软件系统，产品支持 X86 服务器，也支持国产化 ARM 架构的服务器。

产品功能

数据采集和解析

- 支持 5G 信令解析，支持 NGAP、PFCP、GTPv2、HTTP2 等 5G 协议解析；
- 支持 IPv6 协议，能对 IPv6 数据包进行识别；

威胁检测与展示

- 支持特征事件检测、自定义检测、基于威胁情报检测、5G 信令安全检测、终端非法接入检测、网络攻击检测、Web 攻击检测、黑白名单检测，并将检测的事件结果可视化分类呈现

回溯分析

- 支持对事件回溯分析、码流回溯分析

资产管理

- 支持未知资产发现、失陷资产发现

威胁处置

- 支持计入日志、页面报警、发送邮件、发送 SNMP Trap 信息、发送 SYSLOG 信息等方式进行告警；
- 支持通过发送 RST 阻断报文；

产品特点

5G 协议全覆盖

- 支持 5G 核心网常用协议和 NGAP、PFCP、GTPv2、HTTP2 等 5G 协议的解析和还原，同时支持 5G 核心网信令面各接口的信令协议解析和还原，并支持工作在非默认端口下的常见服务的协议识别与协议分析能力；

对运营商 5G 核心网的信令面和管理面流量进行全面的安全检测和监控

- 可对运营商 5G 核心网的信令面和管理面流量进行全面的安全检测和监控，实现终端的恶意接入检测、漏洞和威胁利用行为检测、信令攻击检测、渗透入侵检测等功能，并能基于留存的全量数据进行攻击溯源、全流量关联和取证；

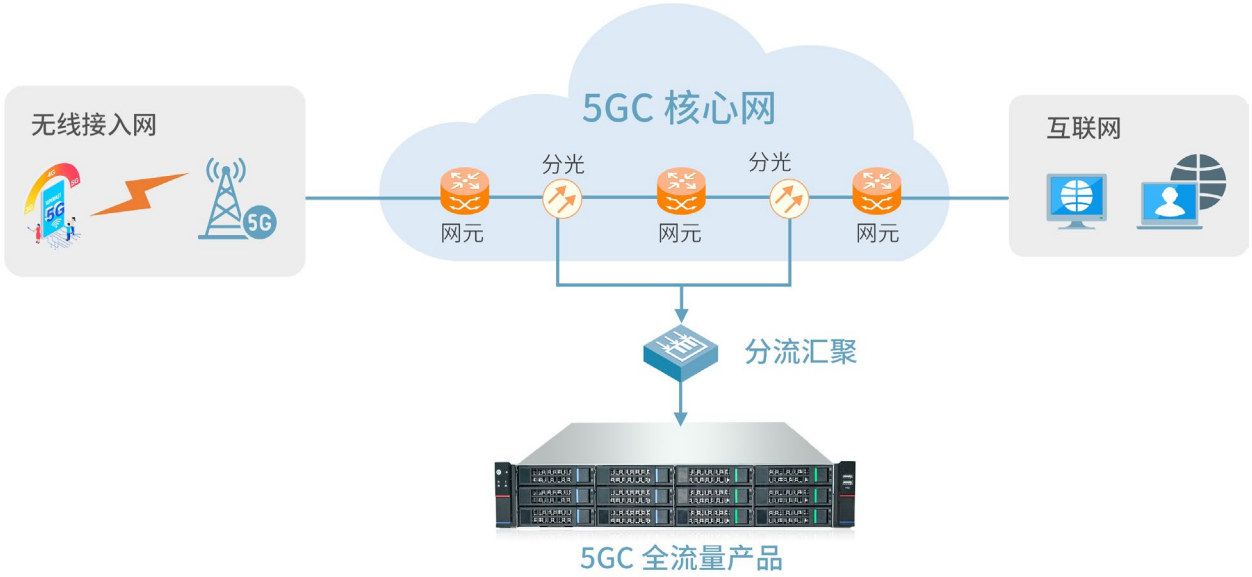
自动发现并上报

- 具备自动发现并上报网络资产及是否为暴露面资产信息的能力，支持提取网络资产的指纹信息，同时支持失陷资产监控和统计；

支持安全动态自监测功能

- 支持安全动态自监测功能，不会由于自身系统出现安全问题或故障导致 5GC 或网络链路引入安全风险。产品自身具备防止渗透攻击、反弹 shell、远程控制、暴力破解、行为异常、漏洞利用以及进行实时监测的功能，并支持通过分析平台进行统一展示。

典型应用场景



如上图所示，欣诺 5GC 全流量分析系统对 5G 核心网的流量进行安全检测分析，实现终端的恶意接入检测、资产识别、漏洞和威胁利用行为检测、信令攻击检测、业务渗透入侵检测和流量追溯取证等功能，检测 5G 核心网是否面临安全风险，提供安全、高效的网络保障和业务保障。

接入网数据采集平台

集成式数据采集平台：X1000EI / X1000EI-V / X3600LI
分布式数据采集平台：X1000LI

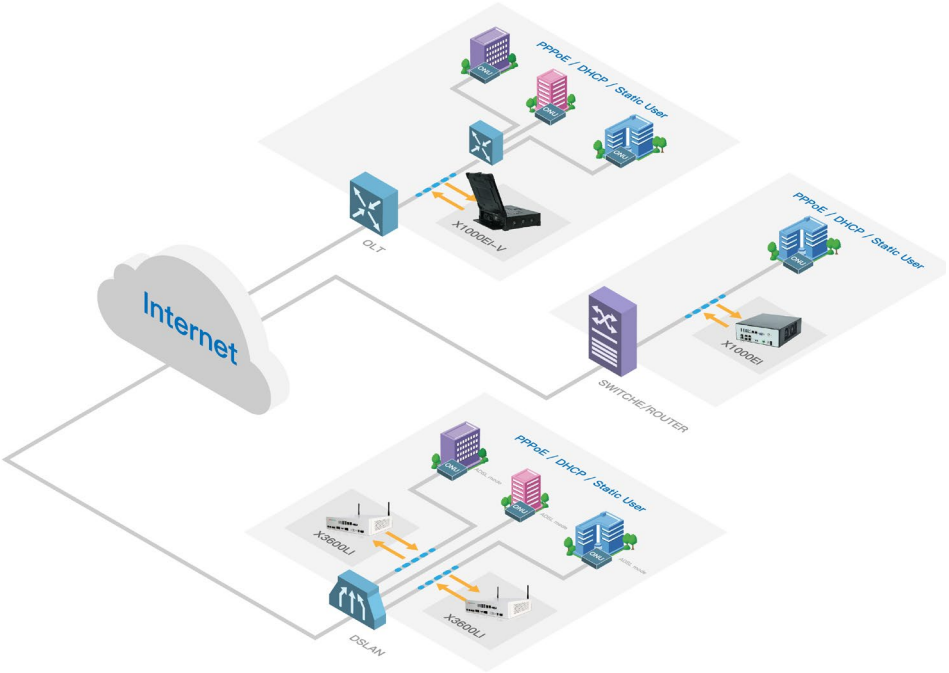
集成式数据采集平台

集成式数据采集平台是欣诺首创的全球领先的多业务接入网数据采集平台，内置高性能X86服务器，支持XGPON/10G EPON /GPON/EPON/ADSL/10G Ethernet/ WIFI等多种网络环境的数据采集，支持上行、下行用户报文的数据转发和镜像，通过镜像口提供镜像数据给软件分析。全系列产品支持断电链路保护和系统保护。

X1000EI-V

X1000EI

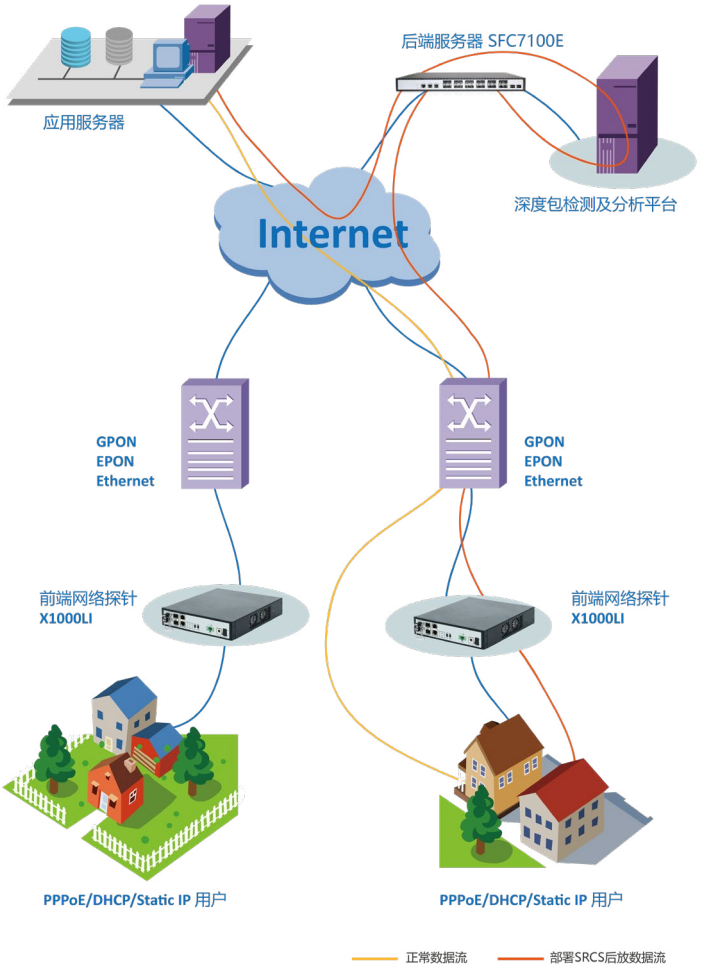
X3600LI



分布式数据采集平台

分布式远数据采集平台是一款多前端一后端的全功能远程数据采集系统，支持EPON、GPON、ETH光、ETH电四模接入，可接入在局端或者用户端。

分布式数据采集平台支持灵活的前端和后端的软件串并接组合，具有高效的上下行链路数据镜像和阻断功能，针对不同网络环境提供多种数据过滤规则，以及丰富统一的后台管理API，设备架设容易、管理方便，是网络安全产品中的一把利器。



X1000LI 前端探针

X1000LI，开创性地将互联网探针和处理平台分离，通过后置多核大数据处理平台统一汇聚处理各个节点部署的探针，方便了网络监管人员的日常工作，极大提升了工作效率。

SFC7100E 后端控制平台

后端控制平台SFC7100E主要功能是处理前端重定向过来的数据报文，并镜像一份到第三方解析平台，同时负责对前端设备进行统一管理。

上海欣诺通信技术股份有限公司

地址：上海市松江区文翔东路58号11幢

电话：400-827-8000

网址：www.sino-telecom.cn