守　望

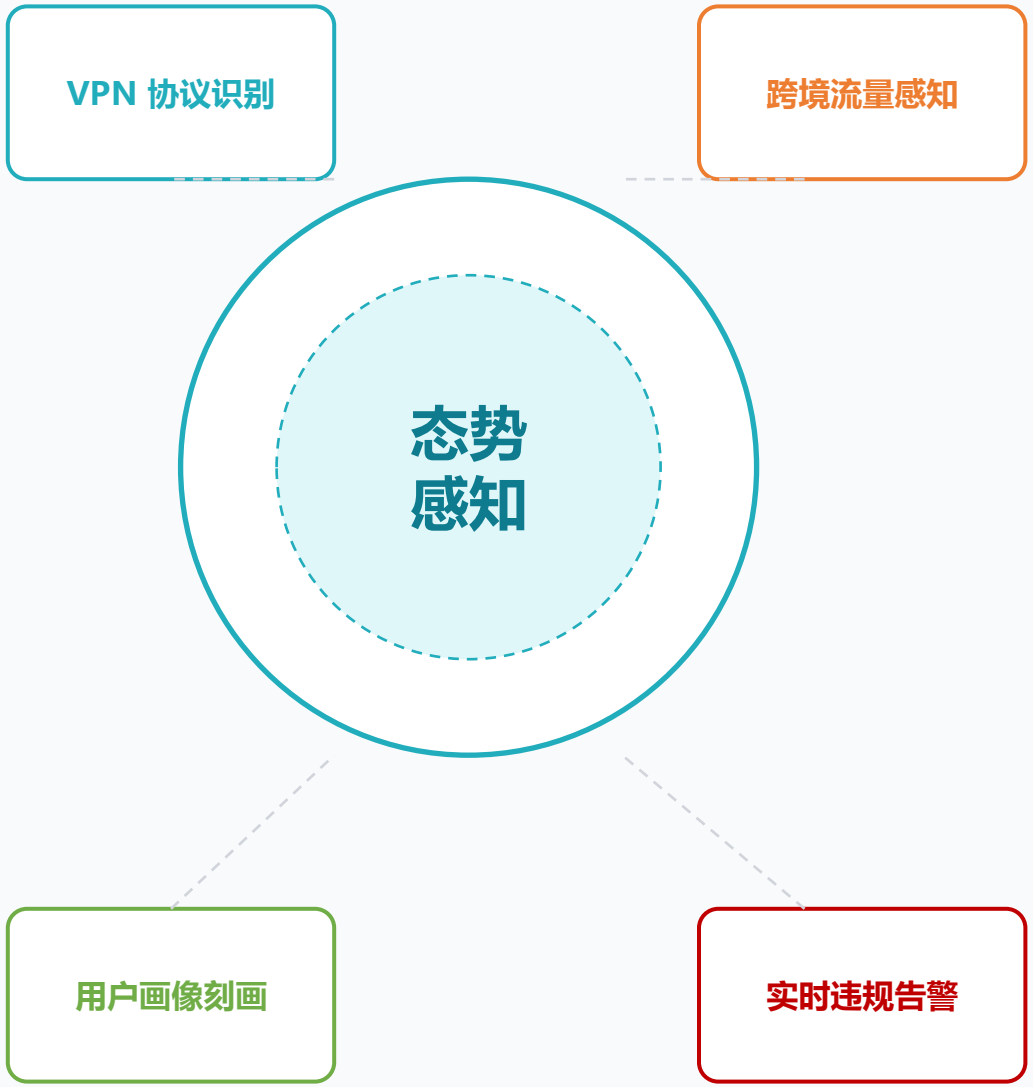
Sentinel

违规跨境态势分析系统

- 深度包检测 DPI ＋ AI 行为聚类
- 覆盖 10+ 类 VPN / 代理协议指纹
- 实时态势 + 长周期溯源取证

武汉博易讯信息科技有限公司

📍湖北省武汉市光谷科技港



boycent 网络安全

01

PART ONE

产品概述

PRODUCT OVERVIEW

基于深度包检测（DPI）与行为聚类引擎，洞察校园网跨境违规态势

校园网跨境违规：四类核心挑战

数据终端 · 视频监控 · 用户终端 · 数据中心

违规发现难

Shadowsocks/V2Ray/混淆协议
高度隐蔽
传统 ACL 与黑名单
易被绕过

溯源取证难

加密流量回溯
缺少元数据索引
事中无记录
事后难复盘

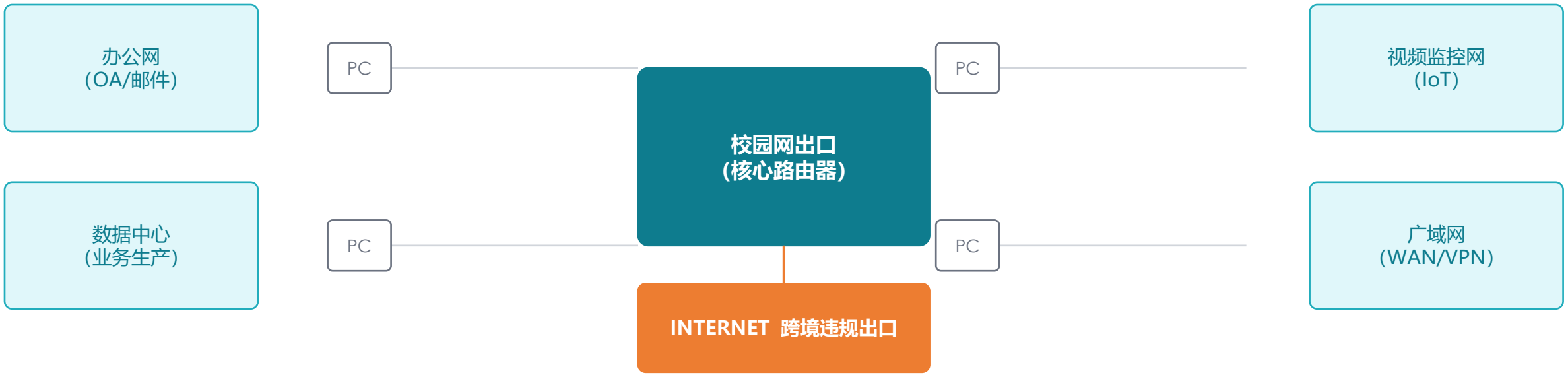
责任界定难

学生 / 教职工 / 实验室
身份归属不清
NAT 出口混杂
难以分责

合规管控难

教学/科研/外事
业务合法需求并存
一刀切封禁
影响正常业务

典型网络场景



产品概述：守望 — 跨境违规态势感知系统

面向高校 / 政企园区 / 科研单位的网络出口合规监测与溯源取证产品

产品定义

守望

Sentinel

面向 IT / 网络安全 / 保卫部门，运行在校园网、园区网出口的合规监测与违规溯源产品。

主要应用价值

- 实时识别 VPN/代理违规跨境流量
- 还原违规用户身份与责任归属
- 支持长周期数据回溯与安全取证
- 满足《数据出境安全评估》等合规要求

产品部署位置示意

用户终端层

办公终端 | 科研终端 | 视频终端 | 数据中心 | 物联网终端

核心交换层（旁路镜像）

Mirror → 守望 • 跨境违规态势感知系统

守望 • 跨境违规态势感知系统

实时识别	态势总览	违规发现
用户画像	告警响应	长周期取证

产品架构：四层分层设计

数据底座 → 数据处理 → 数据分析 → 数据共享

数据底座 DATA FOUNDATION	鲲鹏 ARM / 海光 / Intel / AMD 通用硬件 · openEuler / 麒麟 / 统信 / CentOS · TB 级原始报文与元数据双存储
数据处理 DATA PROCESSING	高性能实时解码引擎（DPI） · 1000+ 字段元数据提取 · 30+ 协议深度解析 · 安全 / 行为分析引擎
数据分析 DATA ANALYTICS	态势总览 · 违规跨境发现 · 跨境流量分析 · 跨境用户画像 · 检测规则 · 告警中心
数据共享 DATA SHARING	Syslog / Kafka / ZMQ / FTP / Email / REST API · 支持与态势感知、SIEM、审计系统对接

B/S 架构 · WEB 集中管理 · 支持分布式部署 · REST API 集成

硬件 + 软件 + 服务一体化交付 • 已适配国产化操作系统与芯片

02

PART TWO

核心功能

CORE CAPABILITIES

态势总览 · 违规跨境发现 · 跨境流量分析 · 跨境用户画像 · 检测规则 · 告警中心

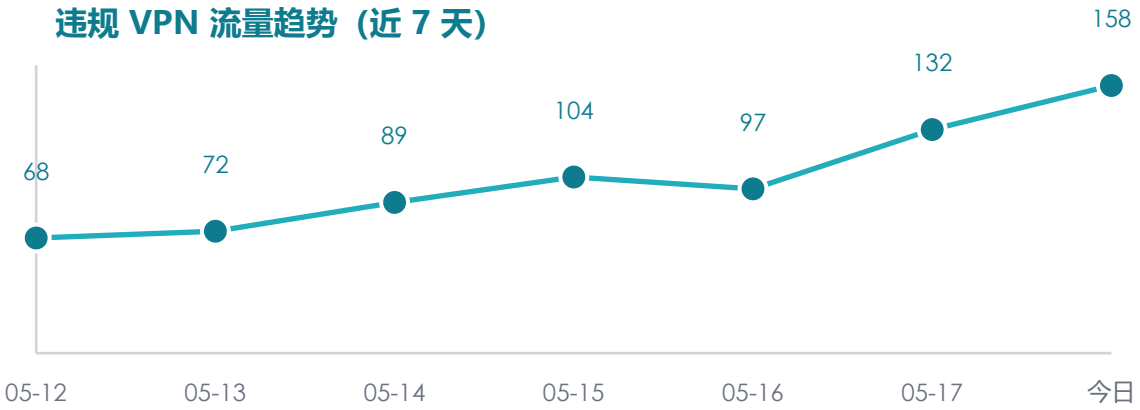
态势总览：跨境违规全景一张图

KPI 指标 · 流量趋势 · 协议分布 · TOP 国家 / 用户

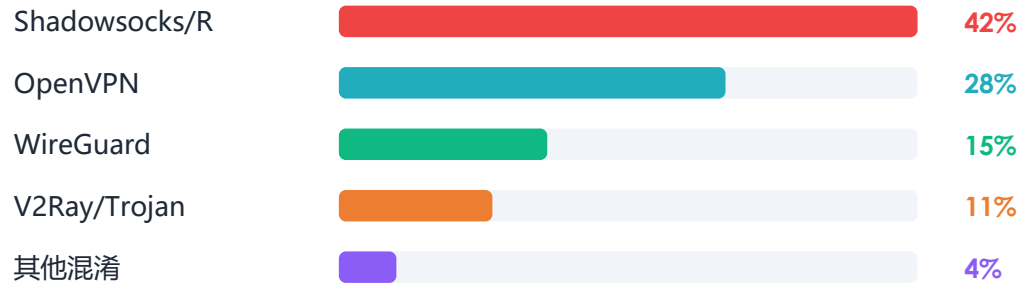
boycent 网络安全

活跃违规连接	新增违规事件	涉及 IP / 账户	跨境风险评分
128	47	86	87.6/100
+12% 较昨日	高峰时段 +5	-3% 压制有效	高危态势 建议立即处置

违规 VPN 流量趋势（近 7 天）



违规 VPN 协议类型分布



跨境流量目的地区 TOP5

美国	日本	新加坡	德国	英国
2.36 Gbps	1.22 Gbps	0.98 Gbps	0.57 Gbps	0.41 Gbps

高风险用户 / 资产 TOP5

10.12.34.102	持续 5 天	87 次连接
172.16.88.45	大流量出境	61 次
张** (研)	高频跨境	44 次

违规跨境发现：实时事件 + 多维筛选

时间 · 源 IP / 用户 · 目的地区 · VPN 类型 · 违规级别 · 处置状态

检测能力矩阵

1. **协议识别**
   10+ 类 VPN / 代理 / 混淆协议指纹
2. **行为聚类**
   AI 行为特征聚类，识别未知变种
3. **流量回溯**
   原始报文回查 + 元数据钻取
4. **多维告警**
   频率 / 阈值 / 时段 / 黑白名单
5. **证据固化**
   会话级证据包留存，支持链式哈希
6. **联动处置**
   对接 AC / 防火墙 / NAC 自动封禁

实时违规跨境 VPN 事件

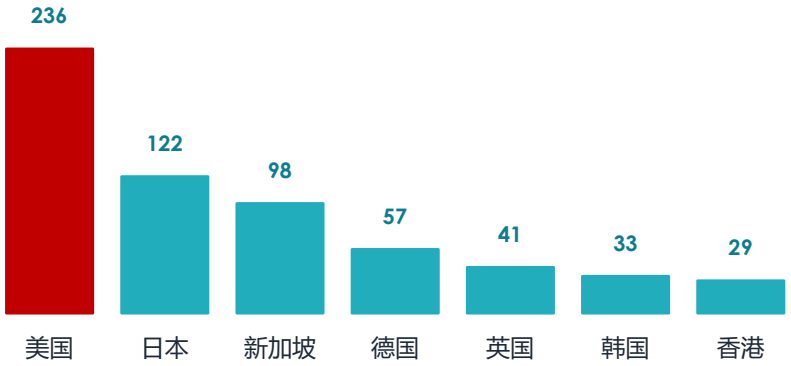
全部 | 高危 | 待处置 | 已处置

时间	源 IP / 用户	目的地区	VPN 类型	级别	处置状态
14:28:32	10.12.34.102	美国 · 加州	Shadowsocks	高危	未处置
14:21:15	172.16.88.45	新加坡	WireGuard	高危	告警中
14:15:03	10.88.32.12	日本	OpenVPN	中危	研判中
14:07:44	李** (教职工)	德国 · 法兰克福	V2Ray	高危	违规提醒
13:56:21	10.2.100.87	英国 · 伦敦	Trojan	中危	待封禁
13:41:09	172.18.200.56	香港 (跨境)	AnyConnect	中危	已封停
13:22:18	王** (学)	韩国 · 首尔	Shadowsocks/R	中危	研判中
12:55:40	10.5.220.36	美国 · 西雅图	V2Ray	高危	已封停

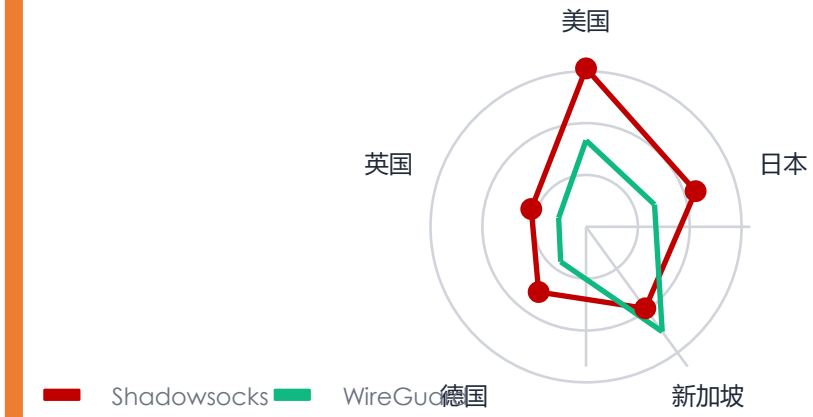
跨境流量分析：全球路由态势 + 协议分布

目的地区 · 协议类型 · 加密流量占比趋势

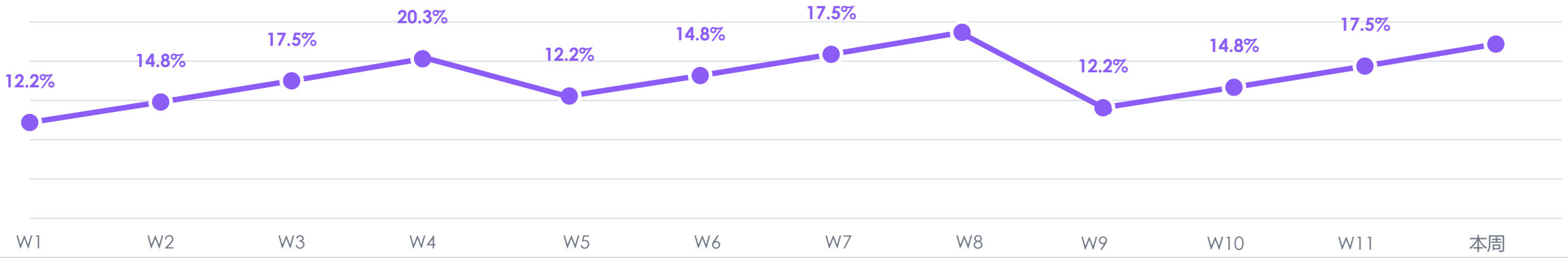
跨境流量目的地区 TOP7（Mbps）



VPN 协议 × 国家倾向



跨境加密流量占比趋势



跨境用户画像：从 IP 到责任主体的精准溯源

身份归属 · 行为画像 · 风险评分 · 处置建议

用户画像 · 五维模型

身份维度

姓名 / 学号 / 工号 / 部门 / 班级

网络维度

终端 IP / MAC / 接入位置 / 终端类型

行为维度

访问时间 / 频次 / 流量 / 协议 / 目的

风险维度

违规级别 / 持续时间 / 是否反复

责任维度

部门 / 学院 / 导师 / 班级 / 责任人

高风险用户处置名单（按风险评分排序）

姓名	身份	源 IP	违规特征	风险分	级别	建议处置
张**	研究生 · 计科	10.12.34.102	持续 5 天跨境	87	高危	重点约谈
王**	本科生 · 大三	172.16.88.45	大流量出境	81	高危	警示教育
李**	教职工 · 实验室	10.88.32.12	高频跨境	76	高危	通报约谈
陈**	本科生 · 大二	10.2.100.87	敏感时段违规	68	中危	批评教育
刘**	研究生 · 通信	172.18.200.56	已封停	52	中危	持续观察
孙**	本科生 · 大四	10.5.220.36	已封停	47	中危	持续观察

▲ 数据基于守望态势引擎 30 天滚动统计 · 支持导出 CSV / Excel

检测规则 & 告警中心：可编排 · 可运营 · 可观测

协议指纹库 · 行为规则 · 黑白名单 · 多通道告警

一、检测规则引擎

协议指纹

10+

Shadowsocks/R · V2Ray · Trojan · OpenVPN · WireGuard · AnyConnect

行为规则

30+

高频跨境 · 夜间活跃 · 长连接 · 大流量 · 异常协议组合

黑白名单

∞

支持 IP / 域名 / URL / 国家 / 协议多维度配置

策略组合

100+

支持 AND/OR/NOT 灵活编排 · 优先级 · 命中冷却

二、告警中心

- @ 邮件告警
- M 短信告警
- C 企微 / 钉钉
- S Syslog 输出
- K Kafka 对接
- W Webhook

告警运营闭环

检测发现 > 研判分析 > 通报处置 > 整改闭环 > 复盘总结

03

PART THREE

价值与优势

VALUE & ADVANTAGES

让跨境违规流量从不可见到可见、不可查到可查、不可控到可控

产品价值：让违规跨境流量清晰可见

流量可观测 · 性能可量化 · 溯源可取证

守望 基于 DPI + AI 行为聚类，将以往看不见的 VPN 加密流量变得清楚可见，复杂违规事件变得直观快速定位，分不清的责任变得清晰可查。

流量可观测

* 清晰了解已知合规流量
* 及时感知未知 VPN / 代理流量
* 分析流量合规性与异常行为

溯源可取证

* 长周期原始会话与数据包存储
* 会话级检索 / 数据挖掘 / 溯源
* 界定问题范围与责任界面

场景化价值：四大典型校园场景的差异化收益

保卫部门 · 网络信息中心 · 学工部门 · 科研管理

boycent 网络安全

01 COMPLIANCE 保卫部门

痛点

违规学生 VPN 访问境外资源，发现滞后，无法及时教育警示

收益

实时违规事件 + 高风险用户名单，支持一键通报保卫处分系统

02 OPERATIONS 网络信息中心

痛点

传统防火墙对 Shadowsocks / V2Ray 等混淆协议无识别能力

收益

10+ 协议指纹识别 + 行为聚类，分钟级发现违规跨境通道

03 STUDENT AFFAIRS 学工部门

痛点

学生使用违规工具访问有害信息，缺乏数据支撑处分

收益

完整证据链 + 用户画像，按学院 / 班级下钻，处置闭环可视化

04 RESEARCH 科研 / 外事

痛点

科研人员因合规查询 / 学术合作有合法跨境需求

收益

白名单 + 差异化策略，合法业务放行、违规访问阻断

产品优势：六位一体能力领先

高处理性能 · 全能一体化 · 长时间溯源 · 灵活集成 · 国产化适配

01

高处理性能

单机支持 1~40 Gbps 实时采集分析与原始报文落盘

02

丰富分析精度

1 秒 ~ 1 天多种流量分析精度；30+ 元数据 / 1000+ 字段提取

03

全能一体化

B/S 一体化架构，一机完成流量采集 / 回溯 / 跨境VPN监测 / 解码分析

04

长时间溯源

支持 180 天原始报文回溯；TB 级数据秒级检索；10 亿级会话秒级查询

05

灵活集成

REST API 集成调用；Syslog / Kafka / ZMQ / FTP 多方式数据共享

06

国产化适配

适配鲲鹏 / 海光 / 麒麟 / 统信等国产芯片与操作系统

boycent 网络安全

04

PART FOUR

部署与案例

DEPLOYMENT & CASES

硬件部署 · 云上部署 · 高校通管局案例 · 集团全链路案例

产品部署 - 硬件部署：三种网络规模

小型单台 / 中型集中管理 / 大型集中管理 + 外挂存储

小型网络 1~5 Gbps

单台集中式

前后端一体化单台设备，满足小型单位的网络监控、违规发现、性能分析与回溯取证

中型网络 10~20 Gbps

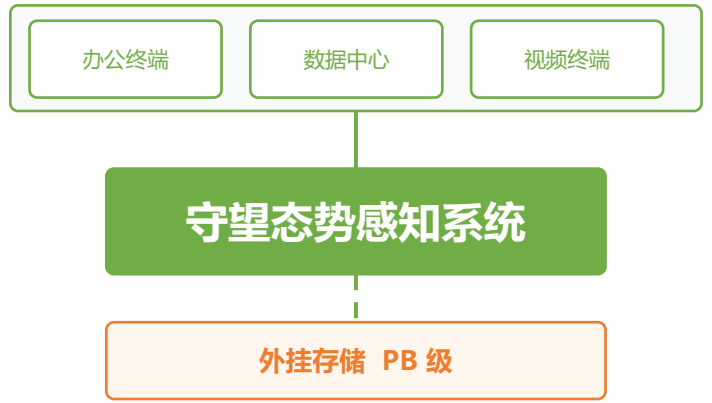
多台 + 集中管理

关键节点部署探针设备，管理平台集中管理，满足多个不同业务网络监控与违规分析

大型网络 40 Gbps+

集中管理 + 外挂存储

集中管理分析，关联分析，满足大型网络、大带宽、多层级管理与长周期取证需求



产品部署 - 云上部署：三种云上形态

云上业务回溯 / 云上+用户流量 / 云平台裸金属

云上业务回溯

Cloud Native

跨境VPN监测系统直接在云上运行，支持以端口镜像和 ERSPAN 方式将流量导入系统

▲ 云内业务流量全覆盖

云上 + 用户流量

Hybrid

云上业务流量通过镜像或 ERSPAN 方式导入，非云数据通过物理交换机端口镜像发送

▲ 云上+用户流量双采集

云平台裸金属

Bare-Metal

跨境VPN监测以裸金属形式被云平台纳管，出口所有流量通过端口镜像发送

▲ 出口全量纳管

案例 1：某省通管局 PB 级跨境违规流量监测

1 个统一管理 + 6 台前端分析节点 + 24 台 480TB 存储服务器

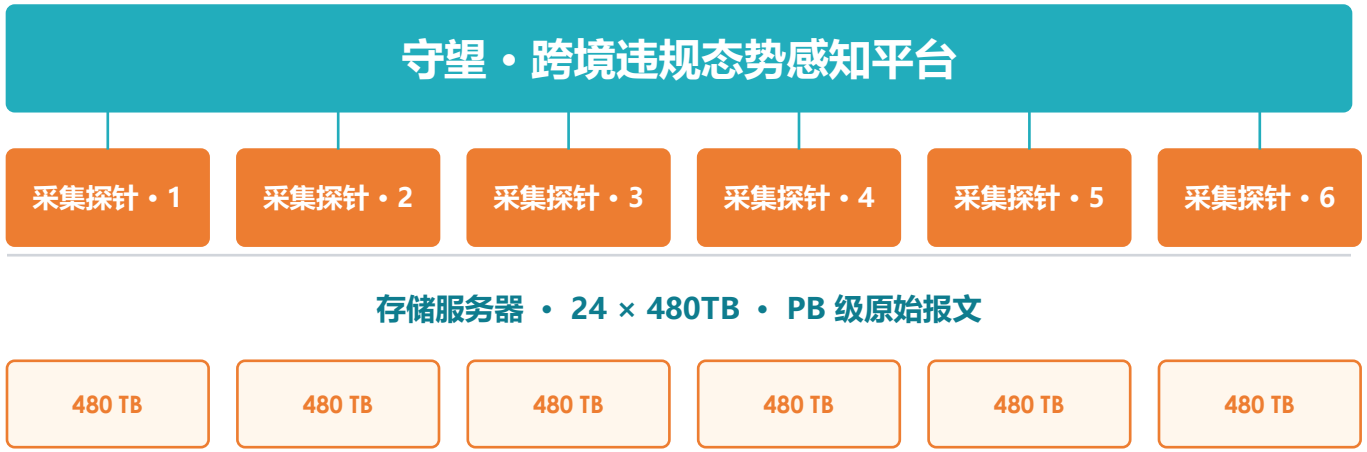
案例 · 客户背景

客户类型	**省级通信管理局**
监测范围	**全省跨境违规流量**
存储要求	**PB 级 原始报文存储**
部署架构	**集中管理 + 集中分析**
业务目标	**违规溯源 / 证据固化**

关键收益

违规跨境事件 90 天内发现率提升 87%；长周期证据链固化，支持监管部门执法

PB 级存储 · 集中管理 + 集中分析平台



6	24	40 Gbps+	11 PB+
前端 NTA 节点	存储服务器	单台处理带宽	在线报文存储

案例 2：某高校园区全链路跨境违规监测

总部数据中心部署分析平台 + 各园区 / 教学楼出口部署采集探针

客户场景：某高校业务系统部署在总部机房，各校区 / 教学楼通过专线或互联网访问业务。守望在总部数据中心部署分析平台，在各出口节点旁路部署采集探针，统一集中分析，快速定位违规节点。

高校园区跨境违规态势监测拓扑

3+	15+	180 天	< 5 分钟	85%
校区 / 教学楼覆盖	链路 / 出口采集	原始报文回溯	违规事件发现	违规处置效率提升

THANKS

Thank you for your attention

武汉博易讯信息科技有限公司 · 湖北省武汉市光谷科技港

销售热线 / 邮箱 / 微信公众号 请与对口销售经理联系