RUNXUN 润迅

Refract 洞流

洞流 Refract 系统 V1.0

产品白皮书

版本 v1.0 | 编制：产品部 | 编制日期：2026-08-26

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

官网：www.runxun.com

目录

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

官网：www.runxun.com

地址: 广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话: 400-854-5566

官网: www.runxun.com

1.公司介绍

润迅从 1992 年就开始做企业通信和信息化基础设施，持有 IDC/ISP 运营资质。是扎根华南、深耕二十余年的 IDC 及云计算服务商，为政府、金融、互联网、教育等行业客户，提供数据中心承载、网络与地址资源、AI 交付与长期运维服务。自建并运营前海云与田心两大数据中心，并在华南、华东、华北、香港布局合作机房，合计数万机柜（含合作）。

做数据中心这些年，润迅一直在跟镜像接入、NAT 溯源、加密流量暴涨、IP 异常使用（翻墙/挖矿）这些实打实的问题打交道。洞流 Refract 就是在这样的场景里一点点打磨出来的产品——它把流量接入、分层研判、调查下钻、证据复核、工单处置到系统运维串成一条完整的线。

关于公司背景（https://www.runxun.com/about/company）、发展历程和资质、产品网站，可前往润迅官网对应页面查阅。

2. 产品定位

2.1 一句话定位

Refract 洞流是面向服务运维、安全与合规团队的加密流量被动旁路观测与取证平台。

这款产品部署于交换机镜像口或光分路器之后，以只读、不解密、不阻断、不进业务链路的方式，从加密流量中识别 VPN/代理/隧道与算力滥用行为，为每个来源生成带证据、可复核、可导出的判定报告，处置决策与执行权留给客户自身。

2.2 客户痛点

客户问题	Refract 的机制	可验证结果
用户数据流量加密以后看不清在做什么，是否存在违规行为。	协议握手、TLS/QUIC 元数据、连接行为和多源情报	从普通加密流量中筛出值得调查的隧道、代理和挖矿风险。
平台上抓取到终端用户的 IP 数据是否真实可信。	分层信号、确定性锚点、双置信度与"为什么判定"	用户能看到信号来源、强弱、时间和关联流量。
当获取到终端用户 IP 违规信息时，如何快速完成调查和交接。	加密数据检测、取证、检索、行为画像、拓扑、工单、CSV/STIX/MISP/SIEM 导出	发现模块支撑 IP 加密数据检测以及取证； 调查模块支撑检索页查 IP 行为画像以及拓扑溯源； 处置模块支撑工单页处置留痕。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

官网：www.runxun.com

怎么证明系统当时判定这个 IP 违规是合理的。	JSON/PDF/PCAP、实体重算、哈希账本与制品 provenance	用户可以对数据、切片和规则版本进行复核。

2.3 核心价值

价值	Refract 的机制	产品证据
用户看得见	从大量普通加密连接里筛出值得调查的隧道、代理和挖矿风险	握手、TLS/QUIC、CONNECT/SOCKS、行为和情报分层
用户看得懂	不只给标签，还解释主体、对端、协议和证据强弱	IP 详情、为什么判定、节点画像、关系图、访问日志
用户交得清	把发现变成工单、报告和可复核证据	工单、JSON/PDF/PCAP、哈希账本、CSV/STIX/MISP/SIEM

3.整体架构

下图从部署架构与平台能力两个视角，描绘了 Refract 这款产品在客户机房的典型交付形态及其核心能力全景。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

4. 产品能力详解

4.1 取证与审计 — 解决"违规通报无凭据"

痛点场景：上级单位在通报业务 IP 违规时，下发到 IDC 运营商往往只有"IP + 端口"，无法给出经得起复核的违规通知。

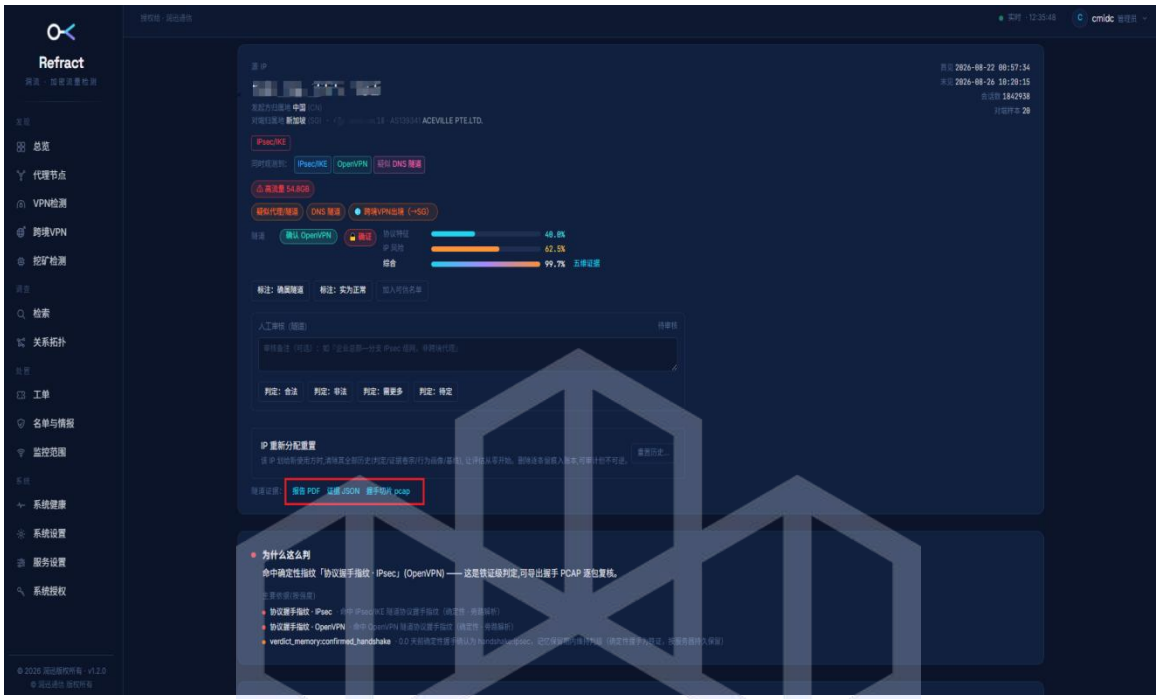
解决路径：

1. **证据交叉验证**（多维特征·相互印证）— 结合 IP/ASN、协议、TLS 握手、JA4+、流量节奏与封装特征，识别 VPN、代理、隧道及算力滥用。
2. **风险定级**（四级判断·人工复核）— 输出分级与判定理由，区分正常 VPN、疑似、可能和高置信违规，减少误报带来的客户争议。
3. **证据交付**（取证包·审计报告）— 自动沉淀流量摘要、PCAP 证据切片、命中特征和判定理由，形成可导出的审计报告，让客户通知可复核，可追溯。

功能实现：

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

图一是洞流平台根据算法逻辑匹配后生成得用户 IP 相关信息，红框标注位置为取证报告的入口：



图二是洞流平台自主生成的单 IP 取证 pdf 报告：

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

Refract 洞流 — 取证证据报告

被动旁路检测 · 只读不阻断 · 概率判定需人工复核

出具对象：润迅

源 IP：[redacted] 检测类别：隧道 判定：高度疑似隧道 置信度：[redacted]

生成时间：2026-08-26 10:48:32 会话数：[redacted] 对端数：[redacted]

一、结论速读（非技术人员阅读本节即可）

监测系统发现：内网 IP [redacted] 很可能正在使用 VPN/加密隧道。

这一结论是概率性判断，系统的把握约为 [redacted]%（依据同等强度的证据，历史上绝大多数判断正确）；建议人工核实后再处置。

系统为什么这么判（通俗解释，技术细节见第二节）：

· 它连接的对端地址在已知的 VPN/代理服务器名单上

[redacted]

建议下一步：

1. 由技术人员按本报告第二节复核证据，确认后按已确认流程处置；
2. 暂不建议仅凭本报告直接处罚，先与使用人/租户核实业务背景。

二、信号分解（为什么判它 · 技术复核）

层	信号	置信度	权重	确定性	证据
L1_ip_intel	v[redacted]een_as[redacted]ky	[redacted]	0.75	否	曾于 0.0 天前确认为代理（forward_proxy:socks），记忆保留期内按衰减维持判组（绝不直升为「确认」）
L_dns_tunnel	d[redacted]ly-edge.com	[redacted]	0.80	否	DNS 隧道特征 @ google.fastly-edge.com：20 查询/1 唯一子域（唯一率5%）、子域熵4.0、最长 label 32、NXDOMAIN 0%、TXT/N
L_dns_tunnel	d[redacted]m	25.0%	0.80	否	DNS 隧道特征 @ ksyuncs.com：37 查询/1 唯一子域（唯一率3%）、子域熵4.1、最长 label 18、NXDOMAIN 0%、TXT/NULL 0%；命中[高
L_dns_tunnel	d[redacted]	25.0%	0.80	否	DNS 隧道特征 @ ksyun.com：38 查询/1 唯一子域（唯一率3%）、子域熵4.1、最长 label 18、NXDOMAIN 0%、TXT/NULL 0%；命中[高熵子
L_dns_tunnel	d[redacted]m	25.0%	0.80	否	DNS 隧道特征 @ jddebug.com：26 查询/7 唯一子域（唯一率27%）、子域熵3.4、最长 label 32、NXDOMAIN 0%、TXT/NULL 0%；命中[

三、涉事会话（取证 flows，最多 15 条）

[redacted]

四、握手原始证据（铁证）

握手 PCAP 切片 SHA-256：

[redacted]

可下载 slice.pcap 用 Wireshark 打开，核对真实握手包。

五、取证完整性与可复核

卷宗内容 SHA-256（payload_hash）：

[redacted]

系统版本：Refract 洞流 v1.2.0 构建 cea40c57fd11 · 2026-08-26（取证复现内部留 [redacted]）

核验方式：① 重算 payload_hash 比对；② verify_ledger 校验只追加哈希链并交叉核对本案卷；③ recheck 按记录信号 + 钉死引擎版本重跑打分，复现同一判定。

六、声明（判定分级与不可确证范围）

· 确定性信号（L3 协议握手）配握手切片 → 铁证，可定隧道确认。

· 概率性信号（L4 TLS / L5 熵）为校准后置信度，非确定，需人工复核。

· VLESS+Reality / WARP-MASQUE / iCloud Private Relay 等被动视角无法确证，不予 confirm。

· 本平台纯被动只读，不阻断、不解密；仅用于部署方自有基础设施合规检测。

4.2 挖矿连接检测 — 解决"隐蔽挖矿"

痛点场景：机房内服务器或员工终端被植入挖矿程序，连接外部矿池跑算力。资源被滥用、电力成本上升。传统监控只能看到"有加密出向流量"，分辨不出是挖矿还是正常业务。

解决路径：

1. **协议精准识别**— 协议指纹比对，从海量流量里筛出像矿池的连接。
2. **行为画像**— 行为画像交叉验证，排除伪装，锁定真正的挖矿行为。

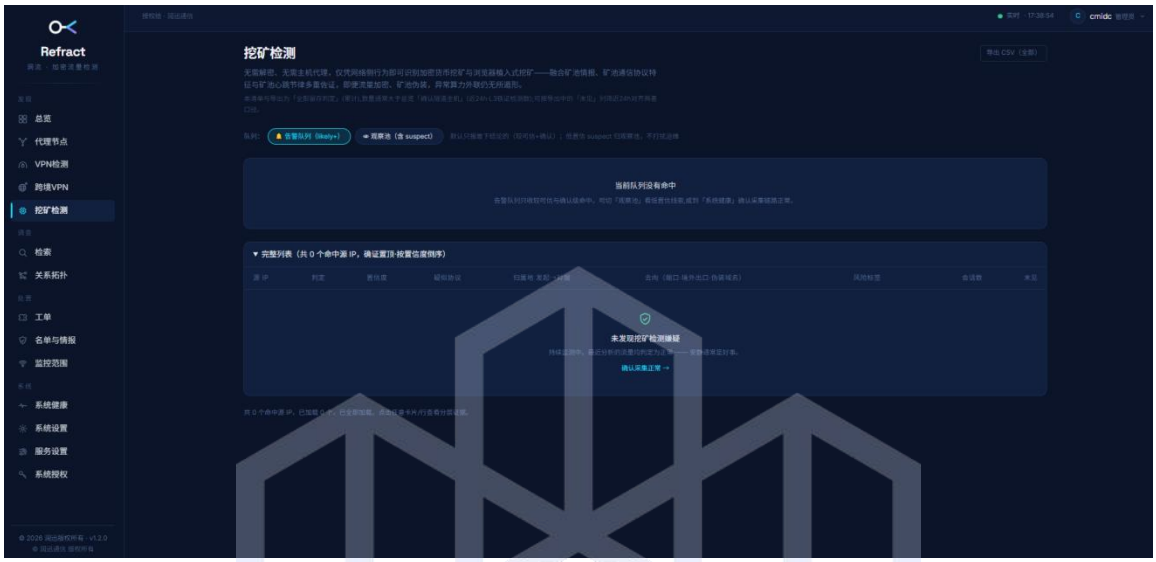
地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

官网：www.runxun.com

3. **证据落地**— 自动沉淀取证包，直接导出可处置的审计报告。

功能实现：



4.3 被动旁路采集 — 解决"串联拖慢业务"

痛点场景：传统安全设备串联部署在出口或核心交换机端口，业务流量必须主动经过设备才能被分析。添加检测设备后，故障域扩大、业务响应变慢、甚至因规则过严误断正常通信，运维压力陡增。

解决路径：

1. **镜像挂载**（SPAN/TAP·不进主链路）— 挂在交换机 SPAN/RSPAN 镜像口或光分路器后，只取流量副本，业务原始链路保持不变。

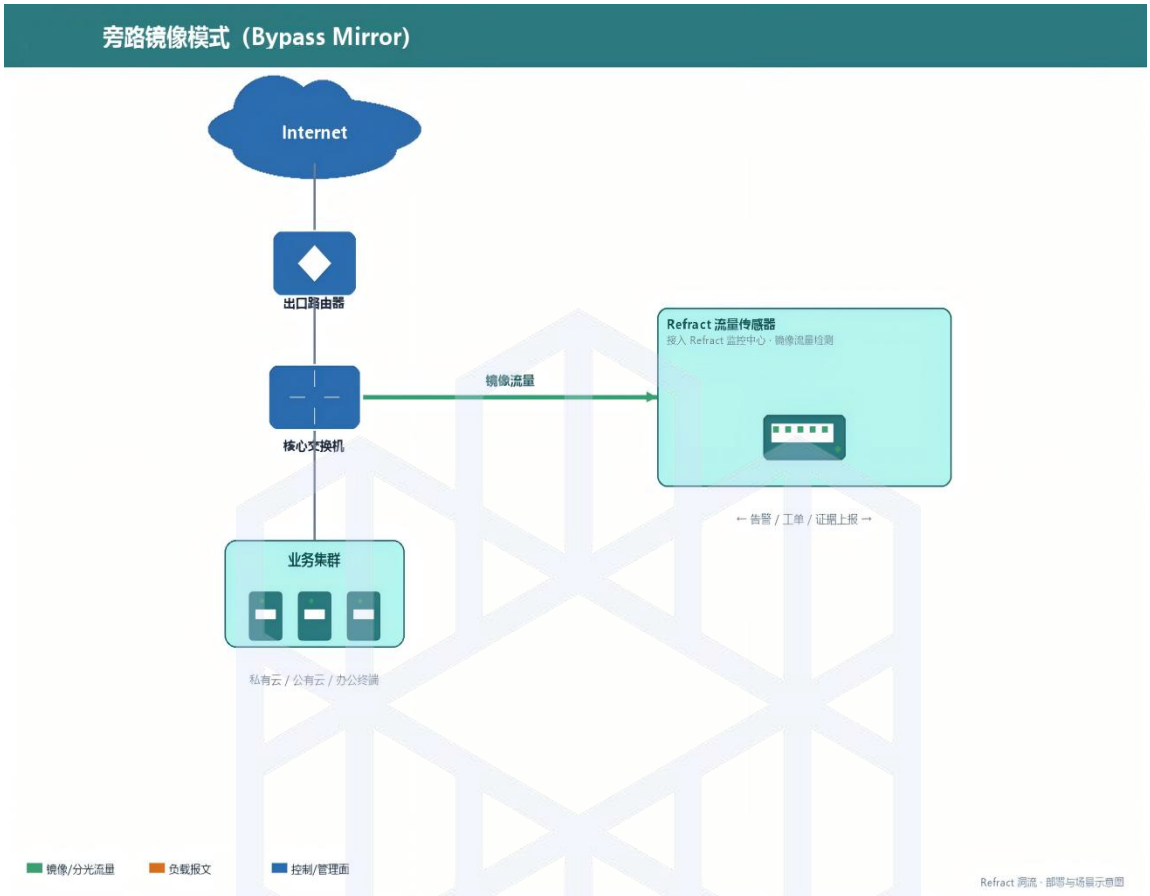
2. **被动监听**（零单点故障）— 洞流产品容器进程异常时对业务网段零影响，不参与数据包转发，不会成为网络瓶颈。

3. **元数据特征检测**（不解包·不阻断）— 洞流产品只截取加密流量的元数据特征做检测，不解包、不下发封堵指令，不引发策略误伤。

功能实现：

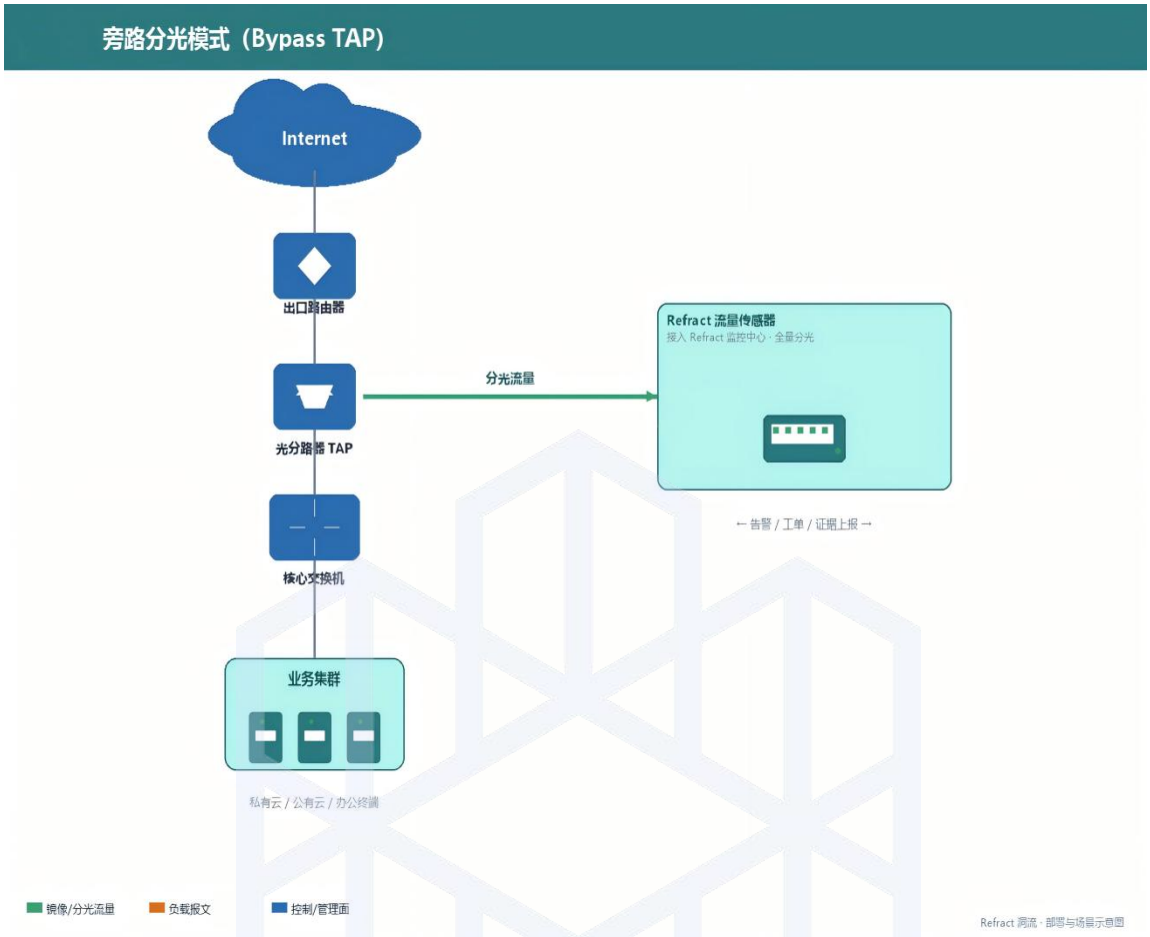
地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

图一是通过交换机端口镜像（SPAN / RSPAN）将目标链路流量复制到检测口。部署简单、无需改动物理链路，适合大多数园区与数据中心接入场景。



图二是通过光分路器（TAP）对光纤链路做物理分光，检测口获取与业务完全一致的副本。高保真、不依赖交换机配置，适合核心链路与对采集完整性要求极高的场景。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

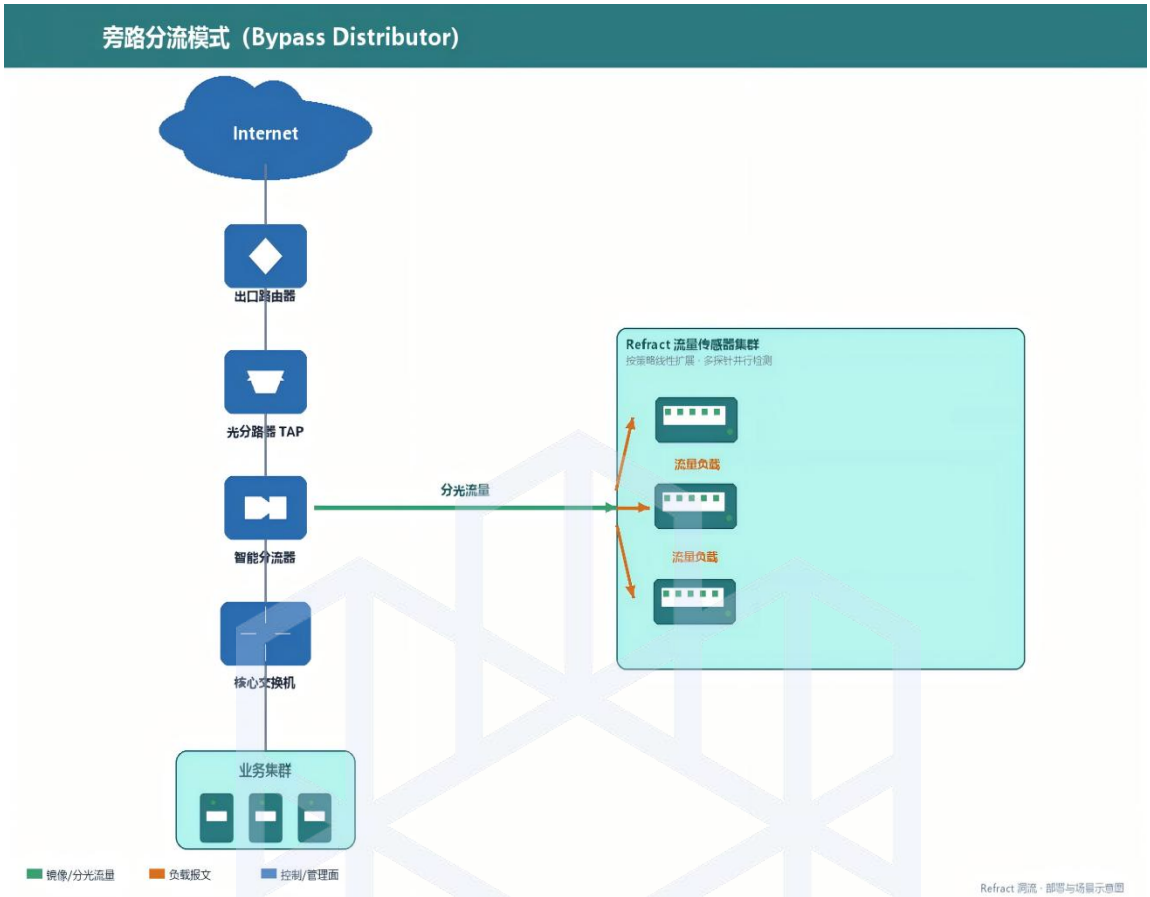


图三是针对超大流量按策略分流到多台传感器，线性扩展检测吞吐，适配高带宽、大并发的云数据中心场景。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

官网：www.runxun.com



4.4 隧道与代理检测 — 解决"VPN 藏在 HTTPS"

痛点场景：数据中心租户私自搭建 VPN 代理节点翻墙，违规连接伪装成正常 HTTPS 流量。传统防火墙只看端口和 SNI，分辨不出哪些是正常业务、哪些是翻墙代理，违规行为长期潜伏。

解决路径：

1. **多维采集**（IP·端口·握手·时序·熵值）— 洞流产品从 IP 情报库匹配、端口真实用途、TLS 握手指纹、流量时序节奏、加密熵值五个维度同步采集，每个维度独立打分。
2. **交叉印证**（多维度互相对照）— 洞流产品通过多个维度的评分交叉对照，只有多个维度同时指向同一结论时才升级判定，避免单一特征导致的误判。
3. **证据链定级**（凑齐才下结论）— 洞流产品的证据链完整度决定判定等级，证据越充分等级越高。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

4. **精准锁定**（区分正常与违规）— 洞流产品针对正常 HTTPS 业务和翻墙代理在多维特征上表现不同，精准区分，锁定违规代理连接。

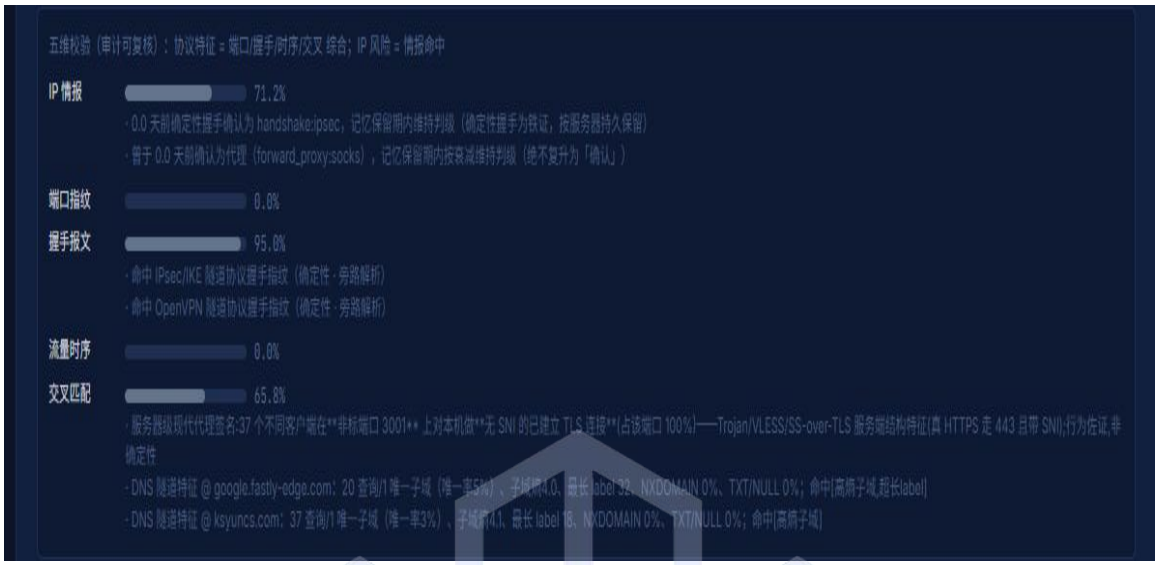
功能实现：

洞流使用 L1–L6 六层分层证据：

层级	证据维度	典型信号	证据性质
L1	基础设施与情报	IP、ASN、机场/代理/IDC 情报	概率信号
L2	端口与协议	常见端口、IP 协议号、非标准端口上下文	概率信号
L3	握手锚点	WireGuard、IPsec、OpenVPN 等可解析握手	**确定性锚点**
L4	TLS/QUIC 特征	JA4+、证书/SNI、QUIC Initial、TLS-in-TLS、包长与 RTT	概率/行为信号
L5	加密与混淆行为	全加密结构、长流、方向与时序	概率/行为信号
L6	跨流行为	周期回连、指纹扇出、服务器聚合和双端关联	概率/行为信号

下图为洞流平台配图，后台通过算法逻辑匹配，将每一层的匹配度按照百分比的形式呈现给用户：

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com



4.5 纯本地化部署 — 解决"数据出境合规"

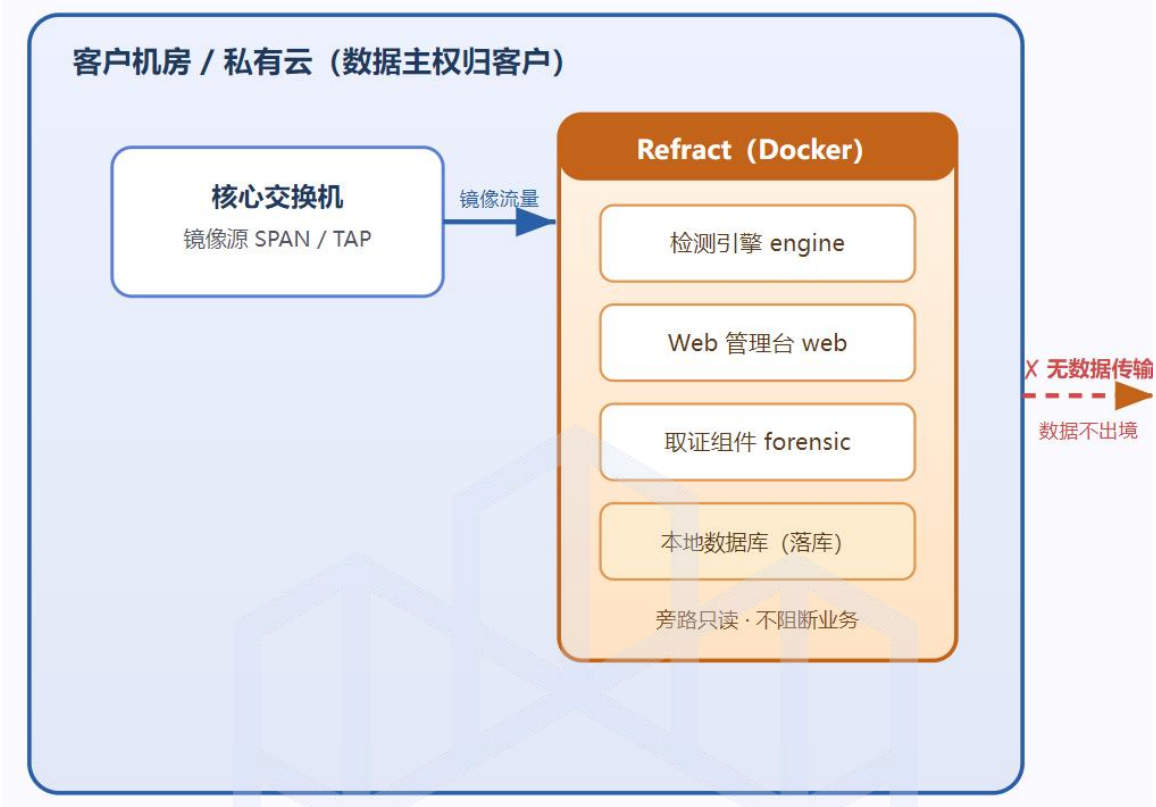
痛点场景：很多流量分析产品以 SaaS 或公有云方式提供，流量明细、行为画像、审计报告要传到厂商云端计算，存在敏感数据外泄风险。

解决路径：

1. **源头阻断：**— 采用容器化本地部署，流量、告警报告全部留存于客户环境内，数据全程不外泄，从源头阻断流量外溢风险。
2. **按需升级：**— 支持物理隔离或可信 VPC 部署，网络隔离级别由客户自主定义，可根据防护要求灵活调整升级。
3. **数据主权：**— 厂商零接触、零留存客户任何监测数据，数据管控、销毁权限完全归属客户，保障客户完整的数据主权。

功能实现：

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com



4.6 四级判定与误报抑制 — 解决"正常 VPN 被误报"

痛点场景：企业合法使用商业 VPN 远程办公或分支组网，被传统规则粗暴识别为"违规 VPN/代理"误报频繁，业务方投诉不断，运维疲于核实。

解决路径：

1. **多维证据**（多维特征·交叉印证）— 结合 IP/ASN、协议指纹、TLS 握手、JA4+、流量节奏、加密熵值多维特征做交叉分析，识别准确度大幅提升。
2. **区分合法与违规**（商业 VPN vs 私翻墙）— 用企业 VPN 服务商名单、合规自建隧道特征区分合法使用与个人违规翻墙，不再误伤业务连接。
3. **四级判定**（confirmed/likely/suspect/clean）— 证据链完整度对应不同等级，疑似异常走人工复核通道。
4. **申诉可复核**（判定理由透明）— 每条判定附触发该维度的评分明细，业务方申诉时可逐条解释，运维判定不再靠拍脑袋。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

功能实现：

洞流产品通过算法逻辑匹配过后，将所有监控 IP 分为以下四个等级：

等级	含义
clean	当前可见证据未达到风险阈值
suspect	单一弱信号或有限异常
likely	多层或较强概率证据
confirmed	确定性协议锚点或确认门槛

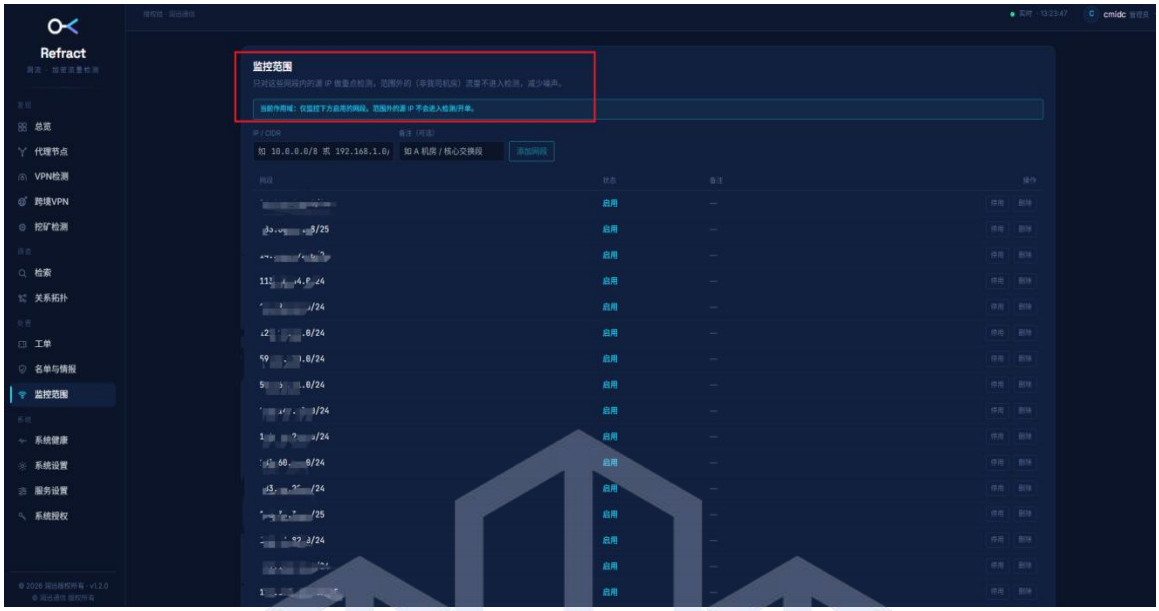
同时为了继续降低误报率，洞流产品还具备相应的降噪功能：

降噪功能	适用场景	证据影响
监控范围 CIDR	只让纳管范围进入重点检测	部署前必须确认观测方向
IP/CIDR/ASN 白名单	稳定基础设施	硬抑制：命中后不进入检测
SNI/域名白名单	可伪造的域名	软抑制：只压弱信号，强握手证据仍保留
临时抑制	临时降噪	只停开单，不删原始观测

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

官网：www.runxun.com



地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

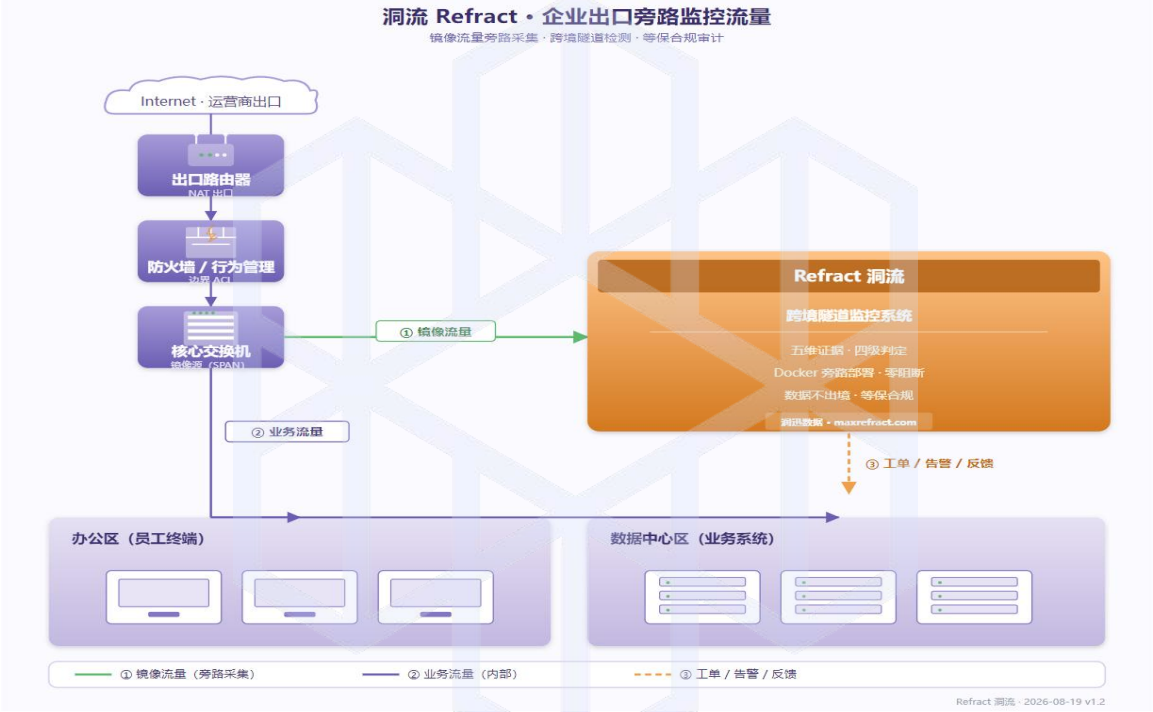
官网：www.runxun.com

5. 典型应用场景

5.1 政府/企业园区应用场景

需求背景：政府/企业业务网络内监测到存在利用非法翻墙工具访问境外违规站点的行为，此类外联行为不可控，存在较大网络安全与合规监管风险。

解决方案：在政府/企业业务网络出口侧做镜像，接入洞流 refract，查找“境内 → 境外”的违规出境行为。结合跨境 VPN 定向视图与可信名单，快速定位违规主机、降低重复研判，把合规检查结果从“看不到”变为“证得清”。

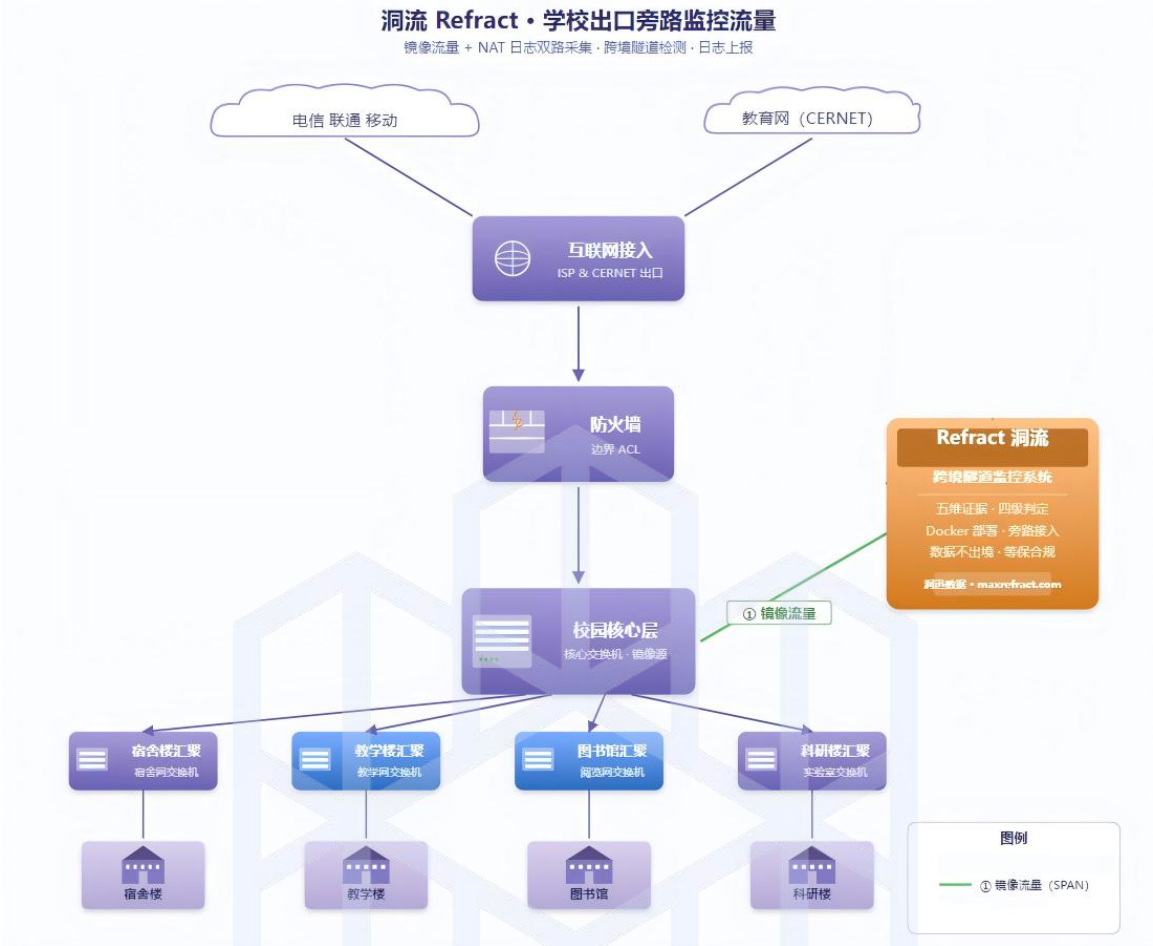


5.2 学校等教育行业应用场景

需求背景：学校的传统安全设备防御重心集中在外部入侵攻击、恶意病毒防范等层面，无法有效识别隐蔽的跨境 VPN 隧道流量。由于违规外联通道具备极强的隐蔽性，从而形成了网络监管盲区。

解决方案：在校园网出口侧做镜像，接入洞流 refract，实现校园网内终端设备跨境 VPN 行为的监测与取证。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

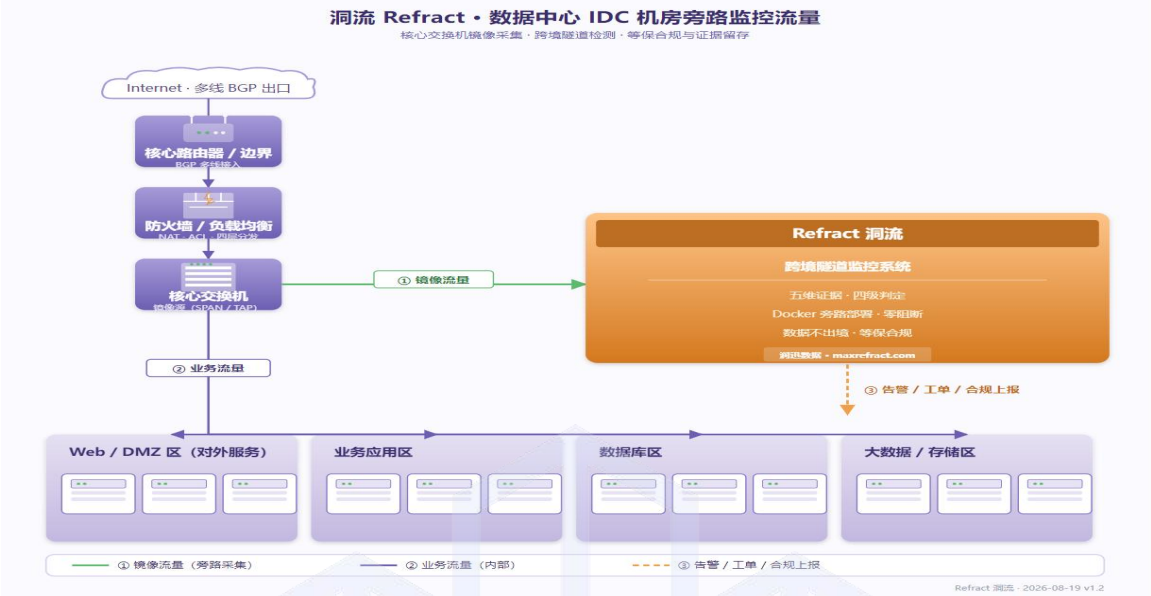


5.3 数据中心应用场景

需求背景：数据中心的传统边界防护设备以外部攻击、病毒防御为主，对主机私建跨境 VPN 产生的加密隧道流量识别能力不足，存在较大安全监管风险。

解决方案：在数据中心出口侧做镜像，接入洞流 refract，实现数据中心网内客户跨境 VPN 代理行为的监测与取证。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com



6. 交付标准

6.1 交付形态

1. 交付形态：洞流 Refract 安装包、服务包

洞流 Refract 以标准化离线安装包为载体，内含版本化部署文件与脚本以及组件镜像，并附配套产品手册。

服务项目	说明
软件版本升级	服务期内所有功能迭代与版本更新
远程技术支持	电话、邮件、在线工单
Bug 修复与安全补丁	紧急修复与安全加固

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

服务项目	说明
其他增值服务	其他

2. 部署方式：SSH 远程 / 远程指导 / 人到线下

标准流程统一为：系统环境准备→导入校验镜像 → 安全配置 → 起栈 → 基础验收 → 绑定镜像采集口 → 激活授权。

按实施在场方式分三种：SSH 远程部署（工程师登录客户服务器远程执行）；远程指导部署（客户根据产品手册自操作、我方在线指导）；人到线下部署（赴现场联调培训，适合物理隔离 / 等保高安全 / 复杂拓扑）。

3. 授权机制：离线签名 + 机器绑定

部署完成后，以离线申请码经安全渠道换取厂商签发的数字证书（token / 离线签名）并上传激活。

7. 客户价值

洞流 Refract 产品为客户业务经营提供了以下价值：

7.1 满足监管合规要求

通过四级判定与全量可回溯告警记录，将加密流量监测纳入日常审计流程，从而满足监管要求。

7.2 守护数据主权，防止数据出域

基于纯本地化部署，流量明细、行为画像、取证报告全部本地落库，零外部传输、零外部 API 调用，规避合规风险，让数据主权牢牢掌握在客户手中。

7.3 立体化加密流量监测，遏制衍生风险

以"五维证据交叉印证"识别非法隧道协议、挖矿连接等异常流量，以 PCAP 切片保留完整证据链，支撑事后审计与司法举证，从源头遏止利用加密通道衍生的黑灰产行为。

7.4 完整的取证数据，让判定更有依据

很多同类产品提供的数据有限，客户需要审计举证时拿不出硬材料。洞流给每条可疑连接配三样取证材料：一份取证报告 PDF、一份证据 JSON、一段握手切片 PCAP。客户可以通过这些材料进行报送、举证和复盘。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

官网：www.runxun.com

8. 附录

8.1 协议覆盖表

协议/维度	洞流 Refract v1.0
WireGuard	L3 握手锚点
IPsec	L3 握手锚点
OpenVPN	L3 握手锚点
HTTP CONNECT	正向代理控制面
SOCKS	正向代理控制面
TLS/QUIC 指纹	L4 JA4+ + 证书/SNI + TLS-in-TLS
跨流行为	L6 周期回连/指纹扇出/服务器聚合
DNS/ICMP/DoH/DoT 隧道	独立模块 + 启发式
Stratum 挖矿	M3 明文首包签名/ M4 TLS / M5 节律
Clash/Shadowrocket/V2ray	L4/L5 特征匹配
REALITY/混淆	概率验证
自动阻断	旁路只读

8.2 术语表

术语	含义
被动旁路	不在业务转发路径上，不主动阻断或改写流量；不等于"不处理任何明文字段"
不解密	不解密 TLS/QUIC 应用数据；系统会处理 IP、端口、DNS、SNI、证书等协议控制面和握手元数据
置信度	规则、校准和融合后的风险评分；在没有独立未知集前，不能称为真实世界概率
确认（confirmed）	仅代表产品规则中的确定性协议锚点或达到

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

	确认门槛，处置仍需人工复核
观测主体	默认是镜像点可见的 IP；NAT 后不能天然归因到具体终端
L1–L6	隧道/代理六层证据：基础设施与情报/端口与协议/握手锚点/TLS·QUIC 特征/加密与混淆行为/跨流行为
M1–M5	挖矿五轴证据：矿池情报/端口/明文 Stratum/TLS 矿池指向/心跳节律
JA4+	TLS/QUIC 客户端指纹体系（替代 JA3/JA3-S），用于 L4 层概率信号
XDP	eBPF Extended Data Path，内核态包处理；用于大象流卸流降低解析成本
noisy-OR	概率融合模型：同层取强后独立证据做 OR 融合
transactional outbox	工单意图与事件在同一数据库事务中写入，重试使用幂等键
哈希账本	对实体字段、关联流和 PCAP 切片计算 SHA-256 并追加账本，用于发现篡改
Ed25519	离线授权签名算法；machine-id 绑定，到期/宽限/硬停状态机
fail-closed	生产环境登录锁不可由数据库开关关闭；未认证请求一律拒绝
token_version	每请求与数据库比对；改密/删用户/降权后旧 JWT 自动失效
expansion-only	版本迁移只增不删策略；允许回退到 N-1 兼容镜像

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com