高级威胁检测系统（NTA）

腾讯云高级威胁检测系统（Network Traffic Analysis System，NTA）通过镜像方式采集企业网络边界流量，结合腾讯多年积累的海量安全数据，运用数据模型、安全模型、感知算法模型识别网络攻击及高级威胁（APT）。同时，对事件告警原始流量进行留存，方便事后追溯，可极大提升云环境下的威胁感知能力。

产品特性

非侵入式安全

高级威胁检测系统采用镜像流量旁路检测，对原有网络业务无干扰影响；提供多种版本适配不同流量环境。探针、沙箱、分析平台一体化部署方案，轻松、高效对接用户环境。

深度检测

传统检测手法对高级威胁基本无效。高级威胁检测系统大量应用人工智能、机器学习，行为分析，统计模型等高级检测方法来识别网络中潜伏的威胁。检测效果明显优于传统检测方法，有效识别高级威胁、未知威胁。

失陷感知

边界是对用户网络中失陷流量进行感知的极佳位置，高级威胁检测系统集成腾讯威胁情报，通过情报匹配，能协助用户精准定位失陷资产，第一时间感知资产受害信息。

大数据持续分析

定向的攻击不是一步就完成的，因此需要持续跟踪。针对特定威胁，高级威胁检测系统依靠大数据模型，对多维度数据进行长时间跟踪分析，呈现给用户的不只是独立的告警，而是安全事件的结论。

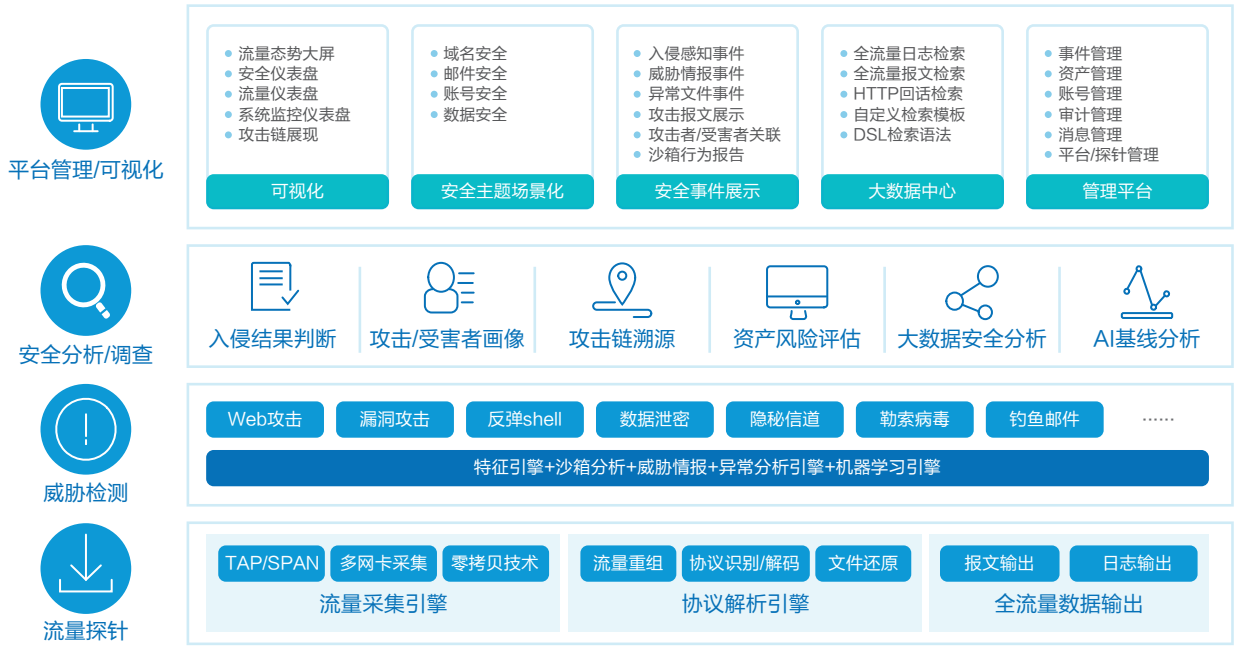
全场景调查

提供先进安全交互分析工具，内置腾讯域名解析、邮件安全、账号安全等丰富内网安全运营调查模板，让安全调查分析有的放矢。

安全大脑

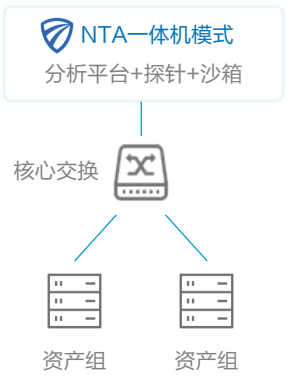
腾讯云端超级安全大脑持续输送安全能力，并提供威胁云查、联动分析，威胁追溯平台等安全分析服务及工具，让用户时刻处于腾讯安全能力环绕中。

产品模块或架构



典型应用场景

一体机部署



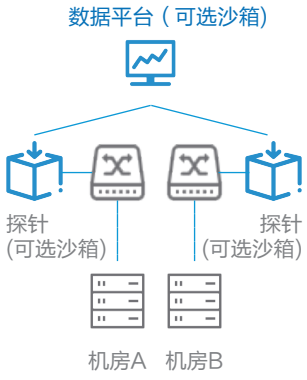
适应场景：

流量采集点<=2
整体流量<3Gbps

模式特点：

轻量低成本，单台服务器即可完成所有模块部署

多探针部署



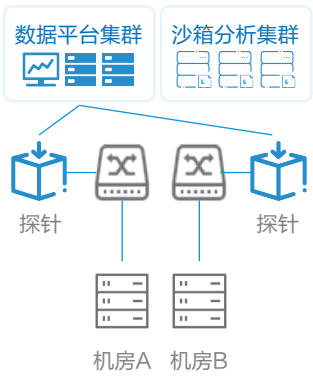
适应场景：

多个流量采集点
整体流量<10Gbps

模式特点：

流量探针可平行扩容，沙箱可部署在探针服务器或分析平台服务器上

集群部署模式



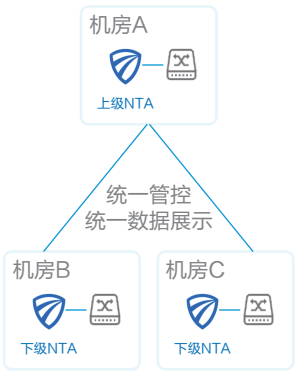
适应场景：

高可用，多个流量采集点
文件分析量大
整体流量>10Gbps

模式特点：

数据平台服务器至少3台，可平行扩容，沙箱和探针服务器可分别按需平行扩容

级联部署模式



适应场景：

多区域部署统一管理

模式特点：

多套NTA产品可进行上下级配置，由上级NTA统一进行管理与告警查看等