腾讯云T-Sec高级威胁检测系统-威胁检测

产品名称	腾讯云T-Sec高级威胁检测系统-威胁检测
公司名称	昆山昱唯网络科技有限公司
价格	51400.00/年
规格参数	品牌:腾讯云 产品:T-Sec高级威胁检测系
公司地址	花桥国际商务城曹新路70号
联系电话	17601404160

产品详情

什么是高级威胁检测系统

腾讯云高级威胁检测系统通过镜像方式采集企业网络边界流量，对流量进行解析、还原文件。通过入侵规则、威胁情报匹配和沙箱文件分析等技术手段识别威胁，保障企业系统安全。同时，系统将对流量日志及告警报文进行存储，方便事故后追踪溯源。

产品优势行为覆盖与平台监控

高级威胁检测系统自研的沙箱模块，其行为覆盖具有全面性。经过腾讯多年的安全经验积累，高级威胁检测系统的沙箱模块当前拥有500多个 Windows 平台监控点、100多个 Android 行为监控点。

漏洞攻击检测

基于特征的漏洞检测技术，仅能应对历史漏洞扫描和攻击，而高级威胁检测系统拥有面向攻击链的检测方式和深入全面的动态分析技术，使其能灵活应对 0day
漏洞攻击。同时，基于腾讯反病毒实验室在浏览器漏洞、操作系统漏洞及 Office

漏洞等方面的丰富经验，研制出了全面的检测方法和模型。

腾讯威胁情报集合

高级威胁检测系统集成腾讯安全大数据中心采集的海量样本，及哈勃分析集群产生的大量分析数据，可生成威胁情报，通过在线或离线升级服务的方式，输送到各个子系统。

攻击链视角与大数据分析

高级威胁检测系统拥有多重威胁感知方法，并以攻击链视角统一呈现威胁数据。同时融合大数据分析，对攻击事件进行时序串接，对攻击者、受害者进行深度画像。并且可以对企业网络边界进行全流量日志大数据框架存储，快速返回海量数据查询结果。

高级威胁发现

攻击者在目标对象处，通过带有恶意附件的电子邮件进行窃取数据活动，使得关键信息基础设施面临高级持续性威胁（APT）。高级威胁检测系统集成腾讯哈勃沙箱分析系统，支持多种文件格式和虚拟环境，能对恶意文件进行精准识别。

网络入侵检测

木马、蠕虫及漏洞利用等攻击手段在网络入侵中仍占据很大比例，高级威胁检测系统提供完善的网络入侵规则集，高度覆盖已知入侵场景。

威胁情报失陷感知

黑客往往会通过远程控制已攻陷的系统，挂马企业信息资产，此类行为会使外联 C&C 服务器产生相应的网络流量。因此，网络边界是从全局感知失陷资产的极佳位置。高级威胁检测系统基于腾讯的威胁情报，可精准识别网络主机产生的失陷流量。

全流量数据溯源分析

在攻击发生后，用户往往要对安全事件进行溯源分析，了解安全事件的来龙去脉，对于较

大的安全事件，甚至需要进行深入复盘。高级威胁检测系统提供流量日志存储功能，通过“检索”可进行流量日志交互式分析，回溯攻击发生时刻的流量信息，同时还可提供告警流量的 PCAP 包下载功能。

单点部署

当边界流量小于3G时，推荐使用单点部署模式，此时高级威胁检测系统的分析平台、沙箱和流量探针可部署在单台服务器上。

多探针部署

当有多个边界点的流量需要采集，且总分析流量小于10G时，可采用多探针部署模式。此时多个探针分别部署在各节点交换机旁，采集到的流量日志将输送到统一的高级威胁检测系统及沙箱处分析。

多探针、平台集群化部署

当流量大于10G时，平台将采用集群化部署，支持硬件设备按需平行扩展，灵活应对10G以上大流量。