安全治理

产品简介

产品文档

腾讯云

文档目录

产品简介
产品概述

最近更新时间：2019-04-26 16:25:52

腾讯天幕安全治理（Platform Security Governance，PSG）基于腾讯近二十年安全技术的积累，通过旁路部署方式，无变更无侵入地对网络4层会话进行实时阻断，并提供了阻断 API，方便其他安全检测类产品调用；此外，安全治理（腾讯天幕）提供全量网络日志存储和检索、安全告警、可视化大屏等功能，帮助客户解决等保合规、日志审计、行政监管、以及云平台管控等问题。

产品功能

安全治理（腾讯天幕）的主要功能，如下表所示：

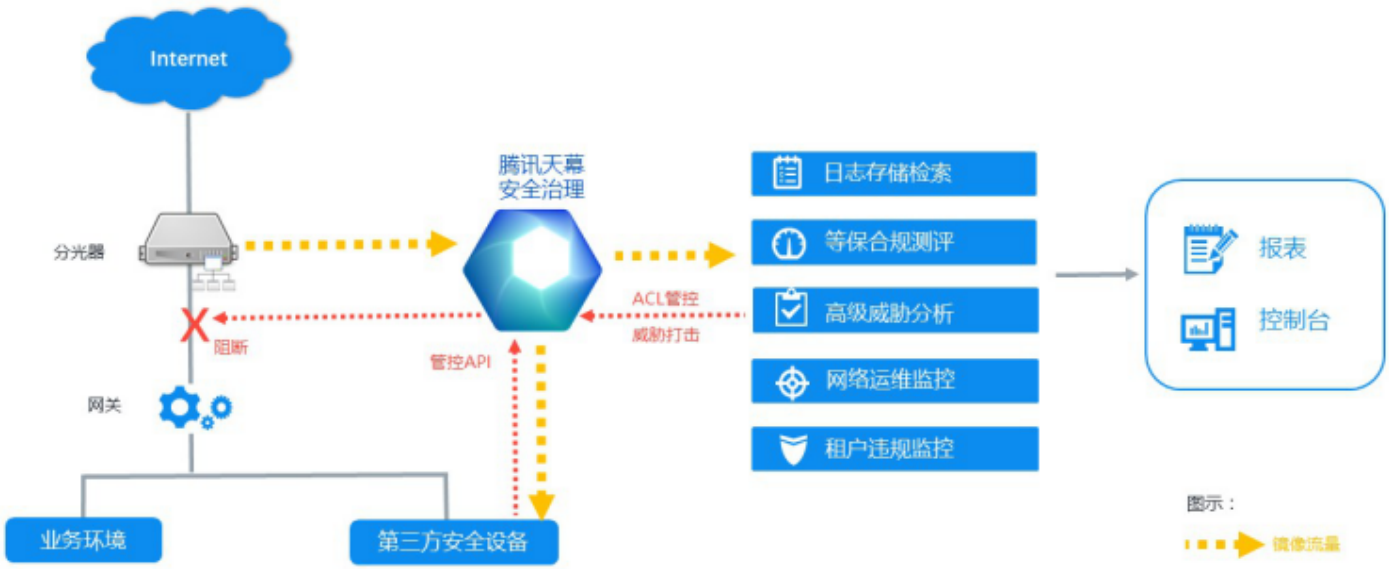
功能	功能描述
黑白名单配置	用户可基于 IP、域名、URL 等维度对网络流量进行管控。
威胁分析与合规审计	内置数十种检测和分析模型，识别各类针对业务和平台的基础和新型威胁。
网络攻击防护	对网络中的常见攻击流量进行识别和打击。
风险资产隔离	支持违规和被篡改页面隔离、特殊时段网站访问隔离、风险主机隔离等快速处置。
告警与分析报表	提供安全告警、流量带宽、网络日志审计等丰富报表。
网络日志审计	提供 Web 访问、安全告警、近180天网络会话五元组等日志检索。

产品架构

最近更新时间：2019-04-26 16:25:58

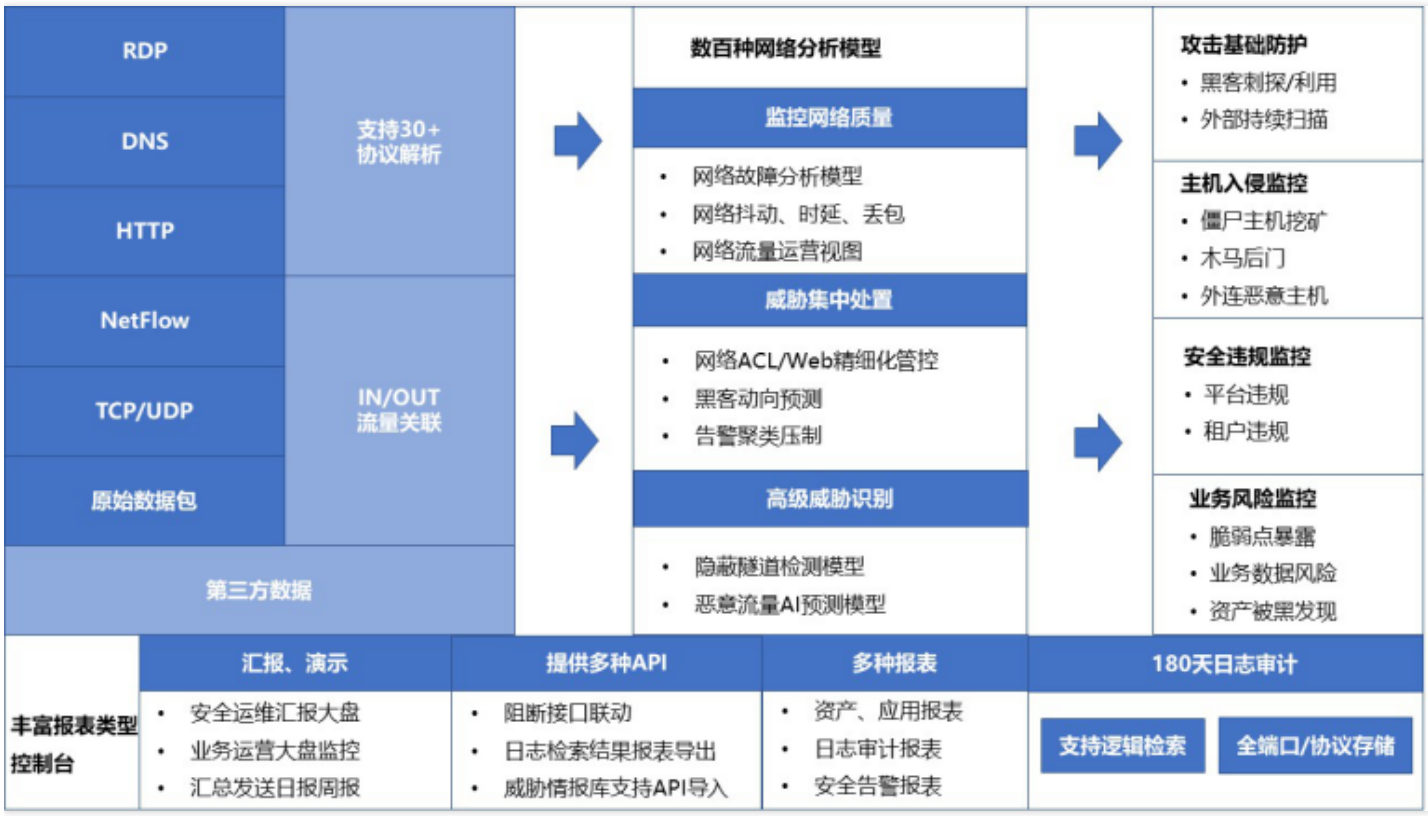
整体示意图

整体结构示意图如下所示：



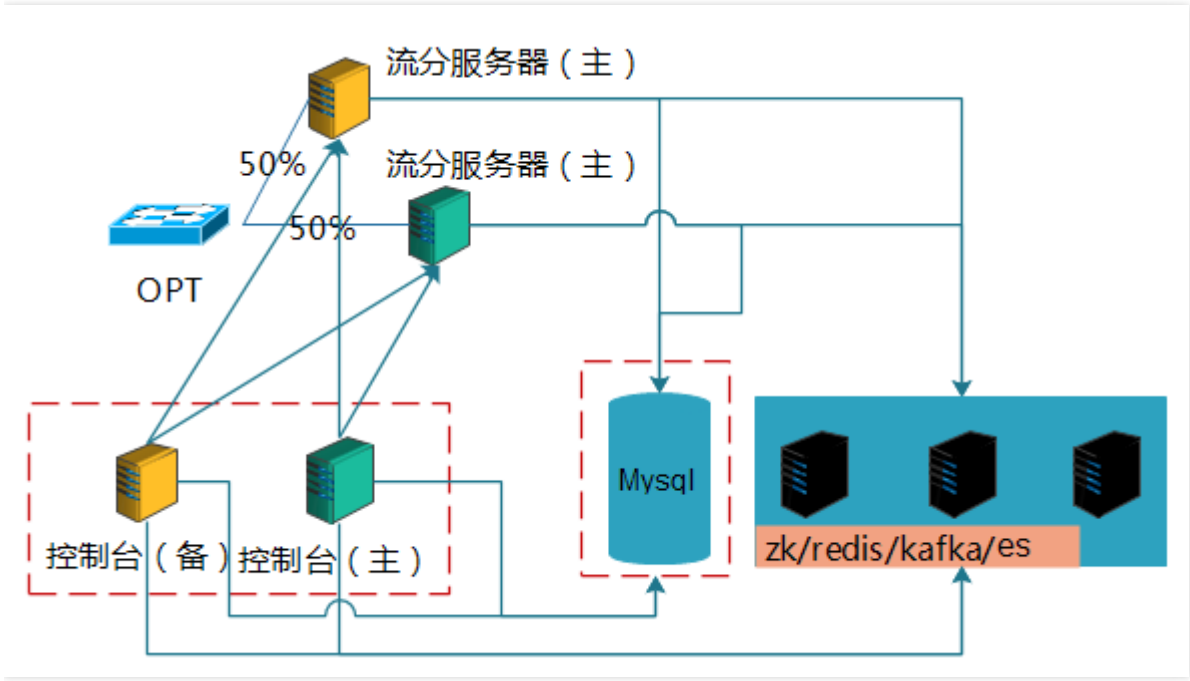
系统架构

系统架构示意图如下所示：



高可用部署

高可用部署方式示意图如下所示：



- **流分服务器**：用于流量数据分析、阻断，支持多主部署模式，由 OPT 镜像分配流量。当某台机器故障，网络链路自动与其断开，并将流量切换至另外一条链路，保证流量分析服务不受影响。
- **控制台**：主备模式部署，当主机故障时，自动切换备机对外服务，配合虚拟 IP 使用，可达到自动切换。
- **存储**：包括 mysql，redis，zookeeper，kafka，elasticsearch。
  - mysql，热备部署模式，当 mysql 主机故障，程序自动切换到备机，保证业务数据传输不中断。
  - redis，zookeeper，kafka，elasticsearch，至少3节点的集群模式部署。任意一台机器故障均不会影响程序正常运行，且支持横向扩容。

产品优势

最近更新时间：2019-04-26 16:26:05

- **安全治理（腾讯天幕）核心优势：**

1. 支持跨 Region 的 Tb 级双向流量镜像，具备微秒级网络协议解析和毫秒级流量分析能力；
2. 腾讯近二十年护网对抗与实践经验内置其中，实时流式检测与大数据机器学习新型威胁分析模型结合，提供成熟的基础防护能力；
3. 对业务网络架构无侵入的同时提供高阻断率；
4. 管控和打击能力 API 化，方便企业集成到现有安全系统中联动响应与处置，提升整体安全防御效果。

- **安全治理（腾讯天幕）与其他安全治理产品的优势对比，如下表所示：**

产品优势	安全治理（腾讯天幕）	其他安全治理产品
网络流量管控	支持网络层和应用层的双向实时检测和阻断，提供 IP、域名、URL 等多维度管控。	仅支持网络日志存储，无法进行阻断。
威胁分析与合规审计	内置数十种常见业务威胁和平台违规场景的分析模型，如攻击基础防护、主机入侵监控、安全违规监控、业务风险监控等。	无威胁模型，仅支持网络五元组会话级解析。
部署方式	旁路部署，对业务网络架构无侵入。	串行部署，容易因为设备故障引起业务中断。
HTTPS 解包	支持。	不支持。

应用场景

最近更新时间：2019-04-26 16:26:11

合规护网保障

问题场景：

- 针对内外部红蓝对抗、网络安全评测等行动，如“等保测评”、“护网行动”，需要日志审计和全局攻击源封禁功能。
- 提供 IP 封禁 API，给其他检测类产品调用。

解决方案：

通过双向流量镜像和网络多层多协议解析，威胁实时检测与离线分析预测模型关联判定，挖掘流量中多种风险场景，结合坏人的行为恶意度和业务风险等级，准确、灵活、分级进行多维打击和管控。

安全能力连接协同

问题场景：

现有的安全产品不能完成阻断，可联动腾讯天幕 API 完成对攻击的阻断。

解决方案：

通过核心网络管控能力 API 化，方便客户盘活联动已有第三方检测能力，进而提升整体安全防御效果。

平台安全管控

问题场景：

- 执行国家监管部门下发的行政命令，屏蔽某违规页面。
- 切断平台中涉政、涉黄暴恐等页面及未备案域名的访问。

解决方案：

提供 IP、URL、域名黑名单设置、访问规则配置、一键断网及页面防篡改功能，帮助企业实现有效的平台安全管控，同时快速响应国家监管部门的行政命令，一键阻断访问，避免在国家重大事件及会议期间发生不可控事件。

租户违规监控

问题场景：

- 租户利用云平台服务器偷偷挖矿，资源被浪费。
- 租户对外发送垃圾邮件，导致外网 IP 被列入黑名单。
- 租户被黑客入侵，被动对外发动攻击，导致云平台违规。
- 租户在服务器上部署提供违规外连服务。

解决方案：
对租户违规行为进行监控和审计，识别租户主动或被动对外进行攻击、扫描、DDoS、暴力破解等违规行为，并能对违规主机进行自动或手动 IP 封禁，切断网络通信或进行网络隔离，同时也提供事件日志 API，方便客户导入工单系统统一管理。

网络运维监控

问题场景：

- 流量暴涨，出口拥塞，被 DDoS 还是爆款现象？
- 带宽闲置或带宽损耗，如何才能合理有效利用？

解决方案：
实时监控网络抖动、时延、丢包率，采用 QoS 策略与流量调整，确保特定数据的优先传输，解决流量拥塞难题。
实时监控带宽利用率，根据历史数据比对，合理有效分配带宽资源，提前做好机房容量规划。