安全运营中心（专有云）

产品简介

产品文档

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2021 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【商标声明】

腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

文档目录

产品简介
产品概述

最近更新时间：2022-01-14 17:18:34

什么是安全运营中心（专有云）

安全运营中心（专有云）是腾讯安全面向政府以及金融、制造业、医疗、教育等大型企事业单位推出的一款以安全大数据分析和可视化为基础的智能化安全运营平台。安全运营中心（专有云）围绕安全运营和风险管理，构建了以安全检测为核心、以事件分析和腾讯威胁情报为重点、以可视化为特色、以可靠服务为保障，可针对企业面临的外部攻击和内部潜在风险进行深度检测，为企业提供及时的安全告警。通过对海量数据进行多维度分析、及时预警，并且对威胁及时做出智能处置，实现企业全网安全态势可知、可见、可控的闭环。

主要功能

腾讯云安全运营中心（专有云）提供态势总览、资产感知、威胁发现、风险预警、溯源分析等功能。

监测中心

通过仪表板态势大屏，总览全企业范围内的资产安全状况、最新待处理威胁、风险事件、安全事件趋势等值得关注的安全信息。支持仪表板自定义。

资产中心

为用户提供资产可视功能，从资产角度了解安全态势，盘点现有资产，对资产进行编辑管理，同时方便运维人员对企业内网资产进行管理。支持通过多种渠道发现资产，支持资产分组管理。

漏洞管理

实时收集互联网最新安全漏洞情报，扫描内网资产安全状况，发现并生成漏洞事件，方便运维跟踪处理。

告警与事件

将接收的日志归一化为事件，支持多源日志关联、日志与漏洞信息关联匹配，生成高确信安全告警。

行为分析

通过采集全方位多维度的安全事件信息、用户信息和资产信息等数据，进行行为基线分析和群体异常分析、用户实体画像分析、结合智能 AI 机器学习异常检测模型，基于动态评分技术，能够快速发现高风险用户和设备，并能够通过时间线查看异常事件的上下文信息，提高风险定位和详情查看以及快速响应的能力。

调查中心

提供事件日志、告警日志、漏洞记录等全量数据信息的复杂查询检索。提供调查任务管理功能，方便集中收集人工判断相关联的证据信息。

响应中心

- 支持安全运营工单，支持人工和自动处置工单，与 SOAR 系统对接。
- 提供攻击事件、漏洞事件的工单流转、通知消息提醒、威胁阻断等的响应处置功能。

报表中心

可根据用户实际需求制定并输出安全报表，方便安全运维人员总结一段时间内的安全工作成果，提供向上汇报，内部总结分析的材料支撑。

安全专题

提供域名安全、邮件安全、账号安全、数据泄露和攻击 IP 分析的分析场景，基于腾讯安全运营经验，内置各专题的安全分析视图。

安全智能

通过对流量日志进行基于深度学习的 AI 智能检测，能够进行安全检测与分析。

系统管理

提供日志接入、系统版本管理、审计管理、账号权限、对接平台、API 密钥管理等系统运行支撑功能。

版权所有：腾讯云计算（北京）有限责任公司

产品优势

最近更新时间：2022-01-14 17:16:58

大数据平台支撑技术

海量数据处理

腾讯多年的大数据分析处理能力赋能到安全运营中心（专有云）平台中，使得本产品在以下几个方面优势明显：

海量数据处理能力

专有云 SOC 支持 PB 级别的数据分析与存储。

数据处理性能

流量处理能力达到10Gbps，并可支持平行扩展。

多种数据聚合

安全运营中心（专有云）具备支持不同来源、不同类型、不同格式的数据聚合能力。具体数据源包括以下几方面：

网络流量

通过将核心交换或其他网络节点上的流量旁路到智能态势感知平台的流量探针。

设备、主机和系统日志

支持主流网络设备日志、Windows 系统日志、Linux 系统日志等。

业务及应用的日志

支持 Web 服务器日志（IIS 日志、nginx 等常见 Web 日志）、代理服务器日志、FTP 日志、VPN 日志、RDP 日志、主流数据库日志等。

安全设备事件日志（告警日志）

支持安全设备、安全软件的安全事件日志（例如：蜜罐、哈勃沙箱的分析日志）、防火墙、WAF 的拦截日志以及终端安全软件日志。

无代码扩展安全检测能力

安全运营中心（专有云）的 AI 引擎运用了基于 AI 的分析和检测技术，将腾讯在 AI 方面的探索应用于网络安全，使用传统规则引擎与机器学习智能算法相结合的分析技术，配合丰富的业务场景与安全场景，最终实现风险发现和威胁检测的能力，即安全感知。

安全监测手段

- 基于特征、统计及关联规则的威胁感知。
- 基于威胁情报匹配的威胁感知。
- 基于机器学习的流量异常感知。

覆盖的部分典型场景

内部威胁

能够有效识别异常的主机行为、用户行为（例如：发现对关键资产的异常访问、敏感数据的外发等），进而识别口令失窃、越权访问、内鬼等企业内部的安全威胁。

横向移动

黑客在攻陷某一主机后，为扩大控制范围会尝试横向移动（例如：扫描、爆破、文件感染、流量代理等）。安全运营中心（专有云）能够检测到攻击者的这类横向移动行为。

黑客牟利

能够检测到典型的黑客牟利手段和对应恶意行为（例如：外发垃圾邮件、对外扫描、爆破、刷广告、挖矿等）。

隐蔽通道检测

能够检测 DGA 等较为隐蔽的 C2 方法，能够检测 DNS 隧道、文件类型伪造等用于隐蔽数据传输的方法。

恶意流量识别

能够使用不基于特征的智能检测模型从网络流量中识别到恶意软件的通信流量，进而识别出疑似失陷主机和 C2 服务器。

APT 攻击

能够对来路不明的对象（例如：邮件附件、可疑链接等），结合沙箱进行深度分析，判定其恶意性，进而提升 APT 攻击的对抗能力。

异常行为风险检测能力

通过采集全方位多维度的安全事件信息、用户信息和资产信息等数据，进行行为基线分析和群体异常分析、用户实体画像分析、结合智能AI机器学习异常检测模型，基于动态评分技术，能够快速发现高风险用户和设备，并能够通过时间线查看异常事件的上下文信息，提高风险定位和详情查看以及快速响应的能力。

- 支持基于用户实体行为分析的威胁发现能力，对 VPN、堡垒机、Linux、终端和安全设备等多种数据源日志，通过风险检测引擎实现对账号失陷、凭证盗用、横向移动等场景的检测分析能力。
- 使用企业内部人员的 HR 数据、资产数据、业务访问数据和登录活动等信息，能够监测内部人员风险行为，并能够结合 AI 引擎来识别用户合法登录后的风险行为，包含资源过度访问、数据量过量下载/外发、账号权限授权和异常使用、僵尸账户发现等场景。

安全编排与自动化响应（SOAR）

高效率的安全运营离不开安全编排与自动化响应（Security Orchestration, Automation and Response，SOAR）。腾讯 SOAR 积累了腾讯安全丰富的运营经验与安全运营中心（专有云）对接，为用户提供不一样的安全运营视角：

- 原子化安全设备动作，按照一定的顺序和逻辑进行组合，形成剧本。
- 通过编排好的安全剧本执行自动化调度和联动安全设备。
- 开展快速的标准化、自动化的应急响应处置，提升 MTTR 水平。

响应联动处置能力

与安全运营中心（专有云）联动的网络入侵防护系统，是一款依靠旁路部署实现旁路阻断和 IP 封禁的设备，同时提供阻断 API 与高级威胁检测系统进行联动，实现安全威胁的闭环处置，在不影响企业业务的情况下，实现快速封禁和阻断。

威胁情报能力

百亿级恶意文件样本库、数亿级 IP 信誉库、域名信誉库、木马病毒样本、日均新增100W+、数千万级恶意网址、高质量情报云查、数十万级漏洞情报等安全运营中心（专有云）内置的威胁情报关联能力，在关联分析中能够将系统采集到的流量、各种安全日志和事件与威胁情报进行碰撞比对。

生动酷炫的态势感知大屏

基于对用户心理、交互行为和安全的理解，安全运营中心（专有云）的可视化呈现方式引入了腾讯在大屏展示方面的优势，利用先进的可视化技术打造了 3D 可视大屏，用户很容易看清业务、看见风险和威胁。

同时，安全运营中心（专有云）提供高度自定义视图模式，能够让安全运营管理人员更高效地进行风险、威胁处置和溯源分析。

版权所有：腾讯云计算（北京）有限责任公司

应用场景

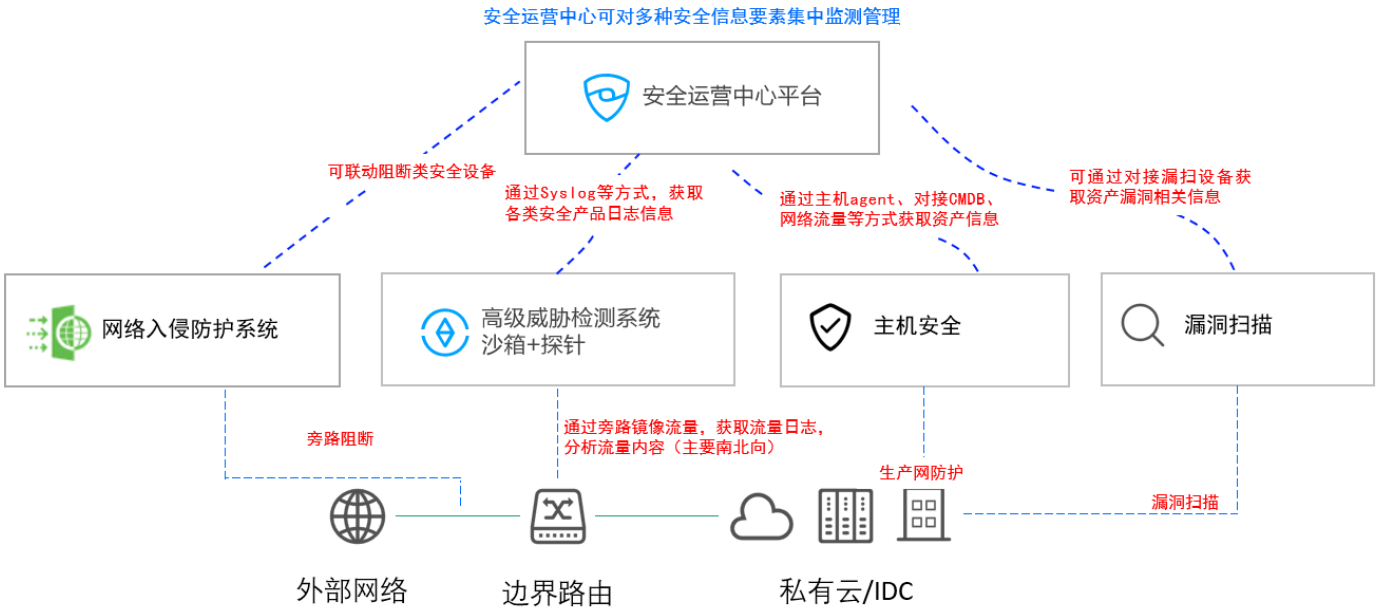
最近更新时间：2022-01-14 17:46:05

安全等保合规

对安全事件、漏洞、资产等安全要素全方面运营，满足等保2.0关于安全管理、日志审计等合规需求。

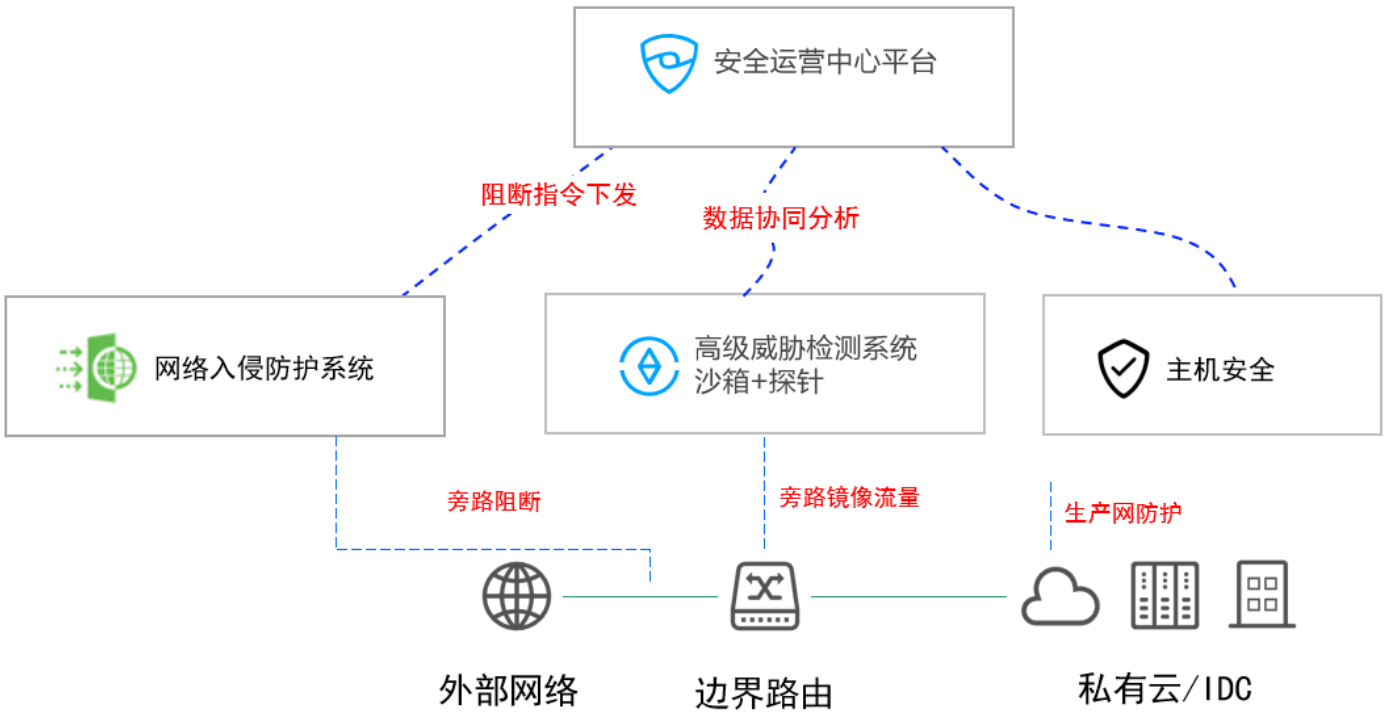
安全运营态势感知

云中心建设过程中需要构建端、管、云统一协同安全整体方案，实现覆盖端（主机侧）、管（网络侧）、云（综合分析大脑）的态势感知系统。



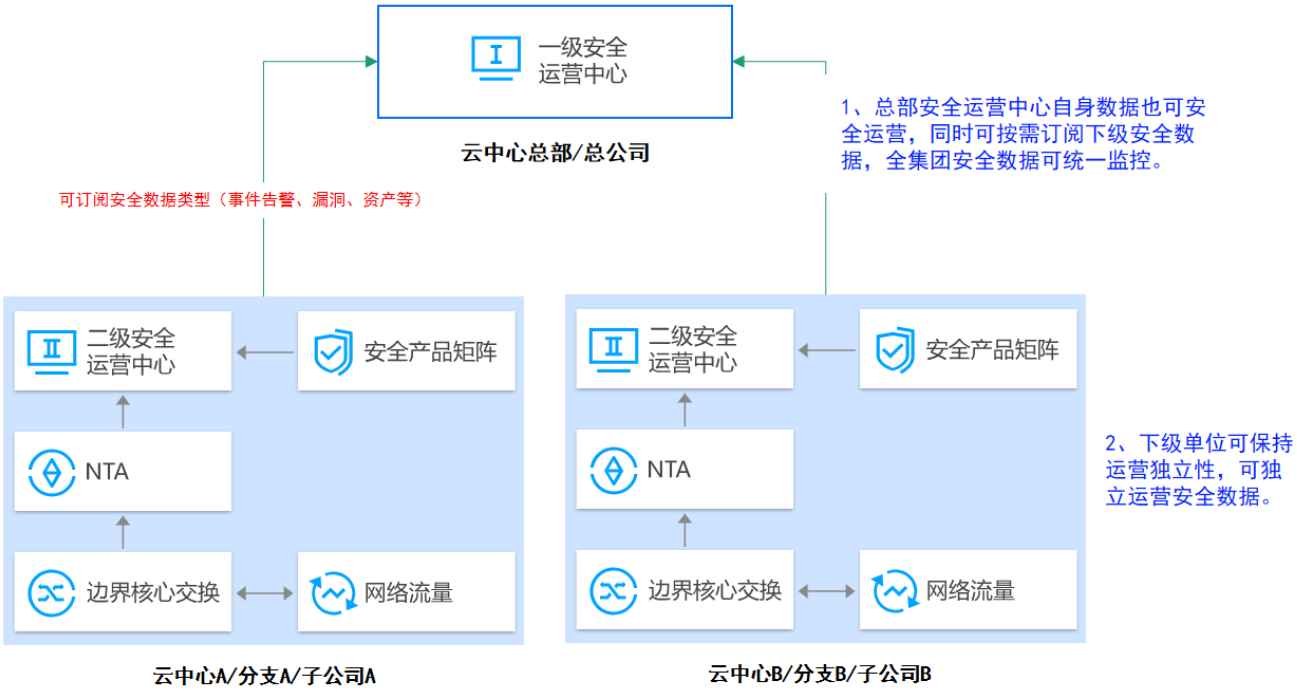
重保场景方案

支持用于重保强攻防对抗场景，拥有检测全、阻断快等特点，确保攻防对抗下能看得清、防得住。



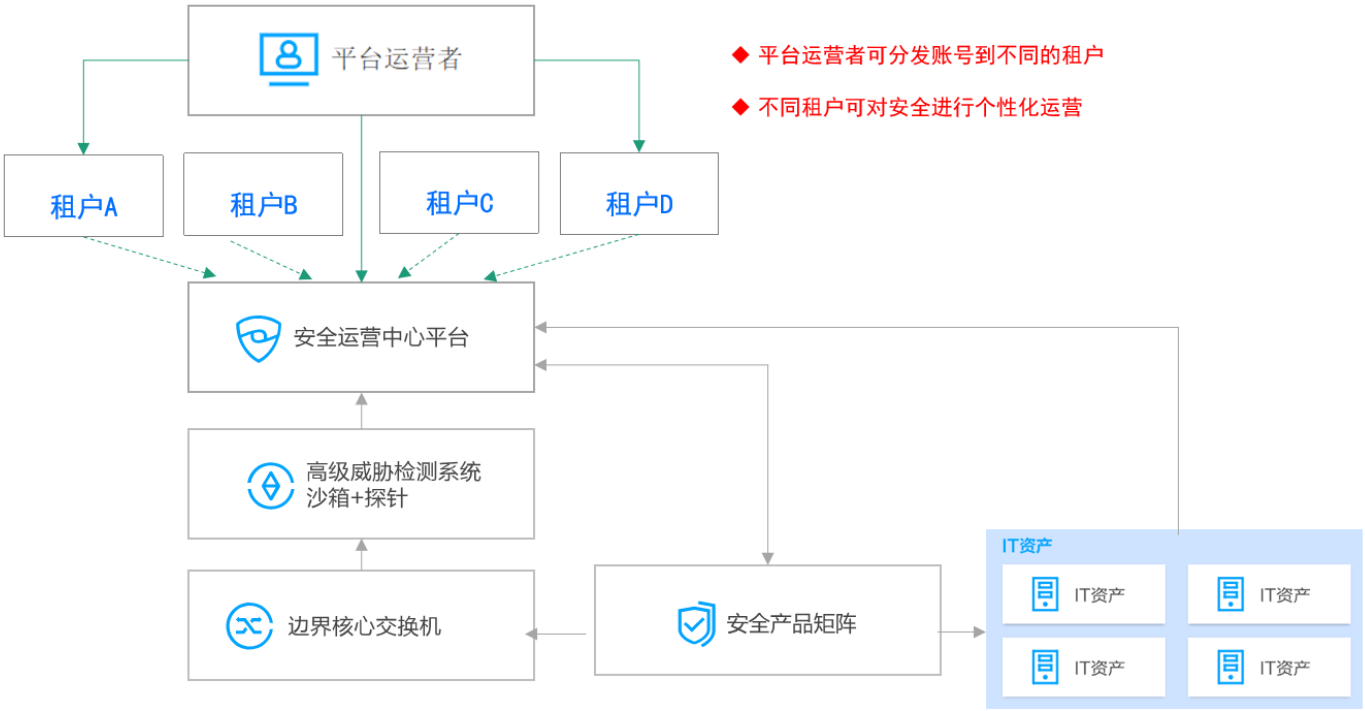
多级统一安全态势感知

支持用于大型集团或行业安全运营情况监管场景，上级单位可以对下级的安全情况有统一的了解。



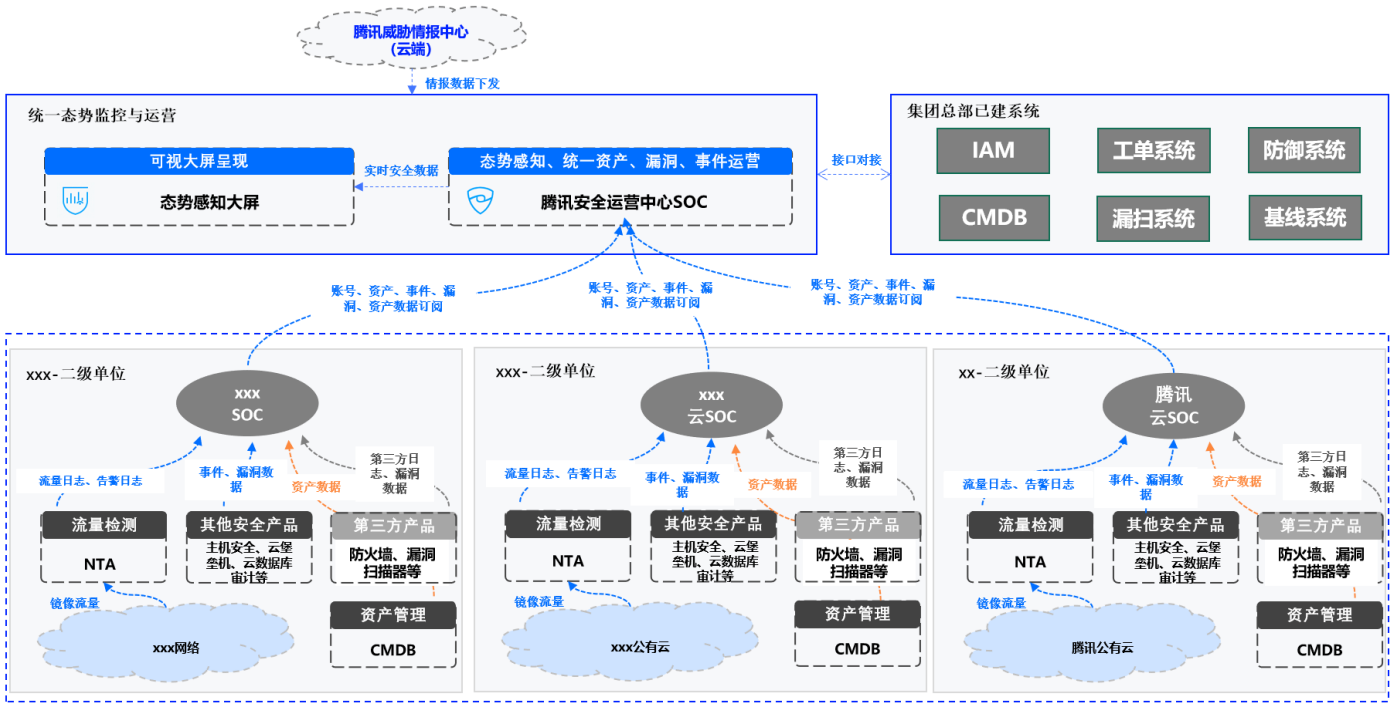
云中心多租户安全运营（云 MSSP）

支持在平台上创建租户账号，并分发给下属单位。下属单位通过账号登录系统，实现自服务。



集团安全运营中心解决方案

支持创建统一监控与运营管理平台，并与集团总部已建系统对接，实现多级统一安全态势感知。



版权所有：腾讯云计算（北京）有限责任公司