云安全中心

产品简介

腾讯云

【版权声明】

【商标声明】

【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或95716。

文档目录

产品简介
产品概述

最近更新时间：2024-09-05 10:12:51

什么是云安全中心

云安全中心（Cloud Security Center，CSC）是腾讯云一站式安全管理平台，通过资产中心、风险中心、告警中心、高级安全管理，帮助用户实现事前威胁检测、事中响应处置、事后溯源分析的安全运营闭环，一键搞定安全问题。

- 资产中心：支持管理34种云上资产。
- 风险中心：一键检测漏洞、配置不当等6大风险。
- 告警中心：聚合、关联分析日志和处置响应。
- 高级安全管理：集团账号统一纳管、模拟攻击防护验证。

产品功能

资产中心

腾讯云公有云上自研的最全资产管理系统，支持自动同步腾讯云的34种云上资产，手动添加非腾讯云 IP、非腾讯云域名进行统一管理。

风险中心

创建资产体检任务，检测端口风险、漏洞风险、弱口令风险、内容风险、云资源配置风险和服务暴露六大风险，并将以上风险信息分类进行管理。支持发起定时任务、周期任务，持续监测企业安全情况。

告警中心

云安全中心统一接入了云防火墙、Web 应用防火墙、主机安全、容器安全服务的日志数据，基于对告警日志的分析和聚合，将三道防线的告警统一展示，可以在告警中心统一处置以上产品的告警信息。

待办事项

为提升安全运营的效率，云安全中心智能分析和汇总了资产中心、风险中心和告警中心的信息，并整理为待办；单击待办可以进一步在各个产品进行处理。

体检任务

管理资产体检任务，对资产体检任务进行编辑、暂停、删除。

报告下载

对于已经完成的资产体检任务，云安全中心会自动生成 PDF 格式的安全报告，提供预览或下载。

模拟攻击

根据用户授权，通过模拟攻击者的思考和工作方式，基于 MITRE ATT&CK 框架自动化模拟战技、战术 ，从攻击视角看待各种云上安全威胁，帮助用户识别可能被攻击的不同路径和影响力较大的安全威胁，发现安全防护产品的不足及对应安全策略是否配置得当，合理利用安全资源、降低云上风险。

日志审计

云安全中心原生接入云防火墙、Web 应用防火墙、主机安全、容器安全服务的日志，可以在日志审计页面根据日志字段，一站式检索以上安全产品的日志。

多账号管理

对于腾讯云集团账号用户，云安全中心支持通过多账号管理切换登录各账号、集中管理各账号的资产、告警、风险等信息。集团管理者有效掌握集团安全信息，实现集团安全管理上的透明化与可视化，实时掌握各成员账号云上业务的安全防护状态、风险等信息。

应用场景

最近更新时间：2024-05-23 17:08:31

云上安全预防

适用场景

业务上云之后，由于公有云自身的特点以及业务上频繁的变更可能会带来很多威胁，例如云上服务器直接面向公网开放了 Telnet 访问；又例如云上数据库直接面向公网开放了服务访问，同时还未加密码验证。针对此类问题，需要对云上的各种安全情况进行集中的安全预防与检查。而云安全中心则集成了此类功能，可为客户提供完整的云上安全预防能力。

解决方案

云安全中心提供泄露监测、互联网攻击面测绘、云安全配置管理、漏洞管理四类功能对客户云上资源做集中的安全预防管理，分别覆盖云 API 密钥和关键信息泄露、云上服务暴露、云资源的配置风险、云服务器的漏洞问题四类云上主要安全问题。同时结合集中的云上资产管理能力，可以为客户提供全局的资产风险管理视角。

统一威胁运营

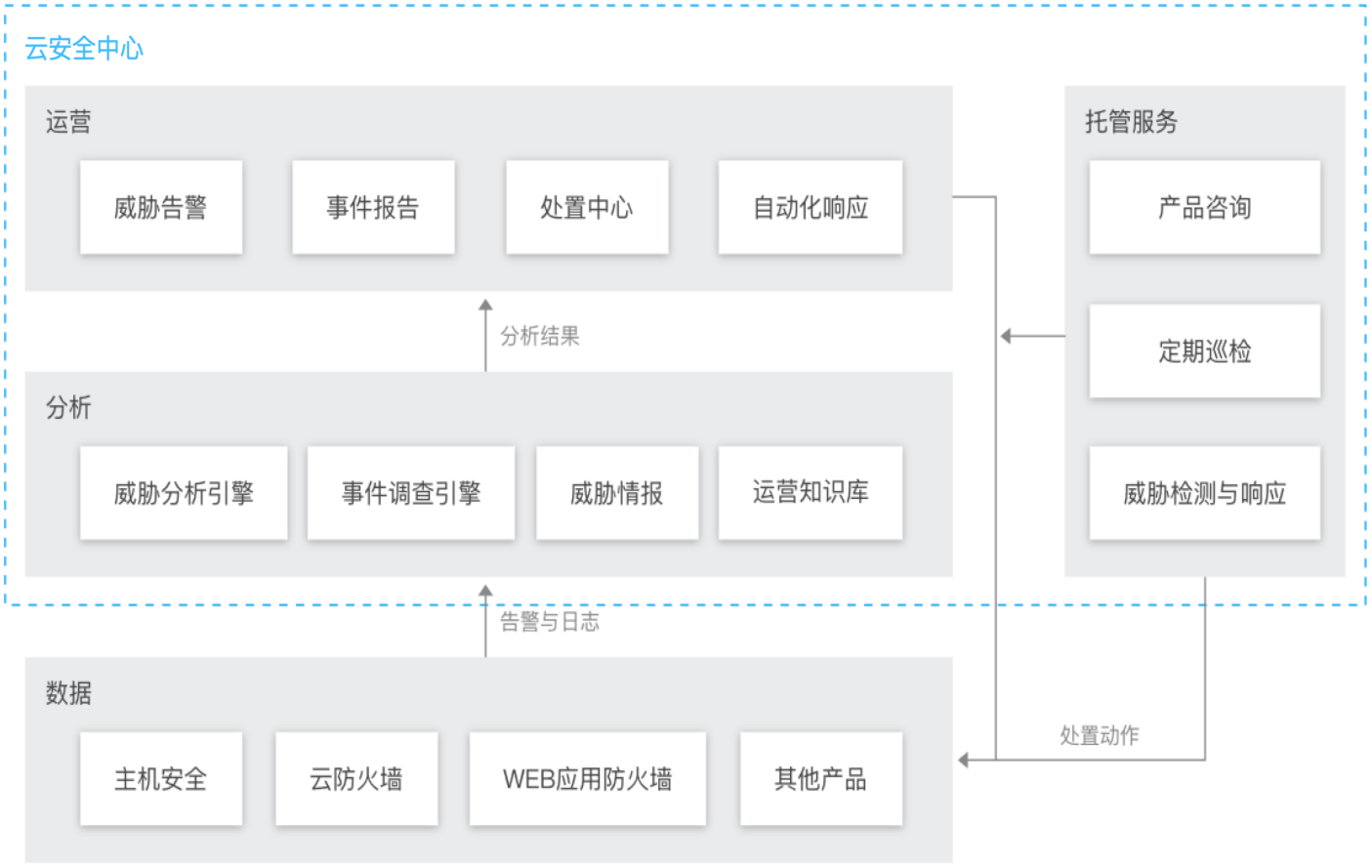
适用场景

云上威胁可能通过网络入侵、主机入侵等各种手段进入企业云上资产并造成进一步损失。为防御和检测威胁，主机安全、云防火墙、Web 应用防火墙往往是企业上云的必然选择，但也由此带来诸多问题：如告警众多并且管理分散、

处置和封禁入口多样、无法有效进行处置、告警关系缺失导致无法按照攻击事件完整还原攻击过程等。这些问题都将直接造成威胁运营效率低下。
针对上述问题，腾讯云安全中心整合腾讯云主机安全、网络安全多方数据与能力，并将腾讯多年威胁分析经验和威胁情报数据应用于帮助客户进行威胁运营，解决威胁运营中的各类问题。

解决方案

威胁运营方案将以云安全中心为核心平台，采集并整合分析主机安全、云防火墙、Web 应用防火墙各类告警与日志，通过告警定性、事件调查、威胁情报分析等手段对告警进行集中分析，筛选高价值告警，针对失陷告警生成事件报告回溯整个攻击过程。
同时依靠云原生能力，云安全中心整合了主机安全、云防火墙、Web 应用防火墙、安全组等各类产品的处置与封禁能力，可以为企业客户提供集中处置、一键处置、自动处置，极大的提升威胁响应效率。腾讯云还可以提供云上威胁托管运营服务，帮助缺少运营人力和能力的客户进行实时威胁监测与响应。



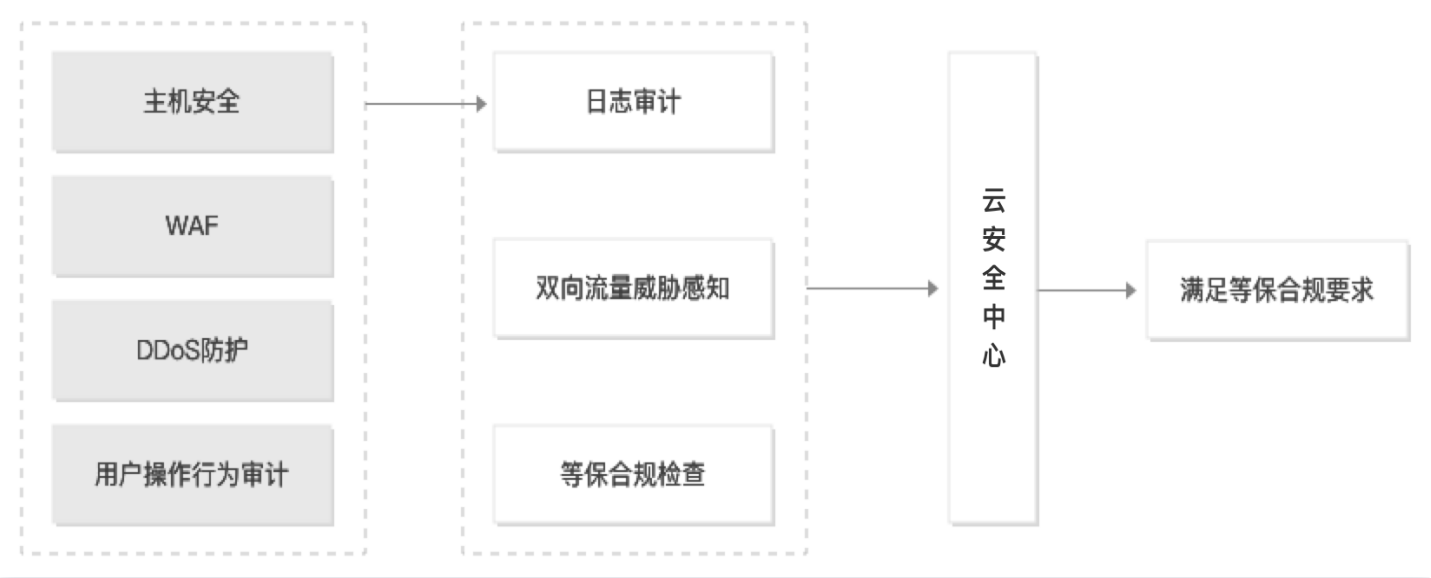
等保合规

适用场景

等级保护2.0标准正式实施后，以“一个中心三重防护”为核心框架针对云上合规的要求进行了进一步细化，对云上资产对外发起的攻击检测、日志审计及集中管理等要求都需要客户采取相应技术措施进行满足。同时针对安全管理方面提出的各项管理要求，也需要有相应的工具和产品帮助客户更容易更有效地落地。

解决方案

云安全中心提供的等保自查、网络入侵检测、日志审计等功能，可以帮助客户有效满足等级保护合规要求。同时云安全中心可帮助客户实现等级保护标准要求中的安全管理中心相关要求的落地，在满足等保要求的基础上，切实提升客户云上安全水平。



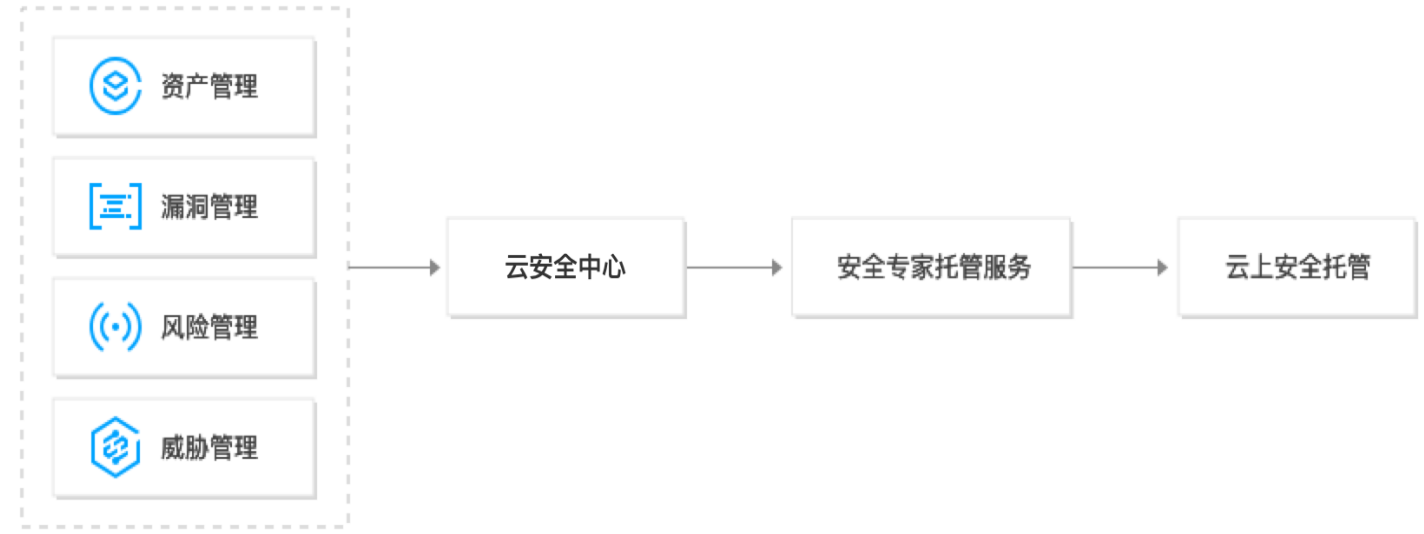
云上安全托管

适用场景

随着攻击手段的不断升级和安全监管要求的不断提高，客户面临的安全形势日益严峻，对客户的安全运营管理也提出了越来越高的要求，需要专业的托管服务实现安全体系的建设与运营管理。

解决方案

腾讯云可为客户提供云安全中心安全托管服务，以云安全中心为核心载体，腾讯安全工程师可为客户提供云安全中心不间断值守、应急处置及定期巡检服务。客户只需聚焦整体安全体系规划和整体安全管理，即可轻松获得云上业务的安全运行。


资产管理
漏洞管理
风险管理
威胁管理
云安全中心
安全专家托管服务
云上安全托管