安全运营中心

产品简介

产品文档

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。

文档目录

产品简介
产品概述

最近更新时间：2021-02-22 10:43:35

什么是安全运营中心

安全运营中心（Security Operation Center，SOC）是腾讯云原生的统一安全运营与管理平台，提供资产自动化盘点、互联网攻击面测绘、云安全配置风险检查、合规风险评估、流量威胁感知、泄漏监测、日志审计与检索调查、安全编排与自动化响应及安全可视化等能力，帮助云上用户实现事前安全预防，事中事件监测与威胁检测，事后响应处置的一站式、可视化及自动化的云上安全运营管理。

产品功能

互联网流量威胁感知

针对互联网流量进行威胁感知，帮助客户实现互联网对内攻击及内部资产向互联网异常外联行为的检测，检测内容包括漏洞利用攻击、命令注入攻击、暴力破解攻击、僵尸网络主机、主机挖矿行为、代理隧道行为等多种威胁。

资产安全中心

帮助客户实现云上资产的自动化动态盘点，盘点内容包括云服务器、对象存储、云数据库及云负载均衡等多种资产。同时通过云配置风险、漏洞及安全事件等多种安全维度，对资产安全风险进行统一管理，降低云上“影子IT”（IT 管理员未知的 IT 资产）风险。

云安全配置管理

为云产品配置风险提供自动化检查评估功能，覆盖云服务器、对象存储、云数据库及负载均衡等多种云产品，帮助客户降低因云产品使用中的错误安全配置带来的安全风险，提升整体云上安全水平。

互联网攻击面测绘

针对向互联网暴露的云上资产，提供互联网攻击面测绘功能，帮助用户快速识别云上资产的暴露端口、暴露服务及暴露组件等潜在攻击面，防患于未然。

安全事件统一运营

将云上各个安全产品检测出的安全事件进行统一采集与存储，帮助客户实现云上安全事件的便捷统一运营管理。

日志审计与检索调查

统一采集云安全产品告警数据、云资产配置变更数据、云上用户操作行为数据及部分云产品日志数据等各类云上安全相关数据，并提供统一检索调查平台，帮助用户实现全面的云上日志审计与检索调查。

安全可视化

通过安全仪表盘、安全大屏及安全报表中心实现云上安全的全局可视化，帮助客户实现安全态势的实时监测及安全建设成果的直观可视化呈现。

安全编排与自动化响应

提供安全编排及自动化响应功能，通过内置的安全编排剧本，可针对多种安全事件实现自动化的响应处置，提升云上安全事件响应处置效率。

合规管理

针对等级保护2.0中的部分合规要求，安全运营中心提供了自动化的动态合规评估功能，并提供相应的加固建议，客户可按需对云上资产的合规风险进行持续监测与评估。

Cloud UBA

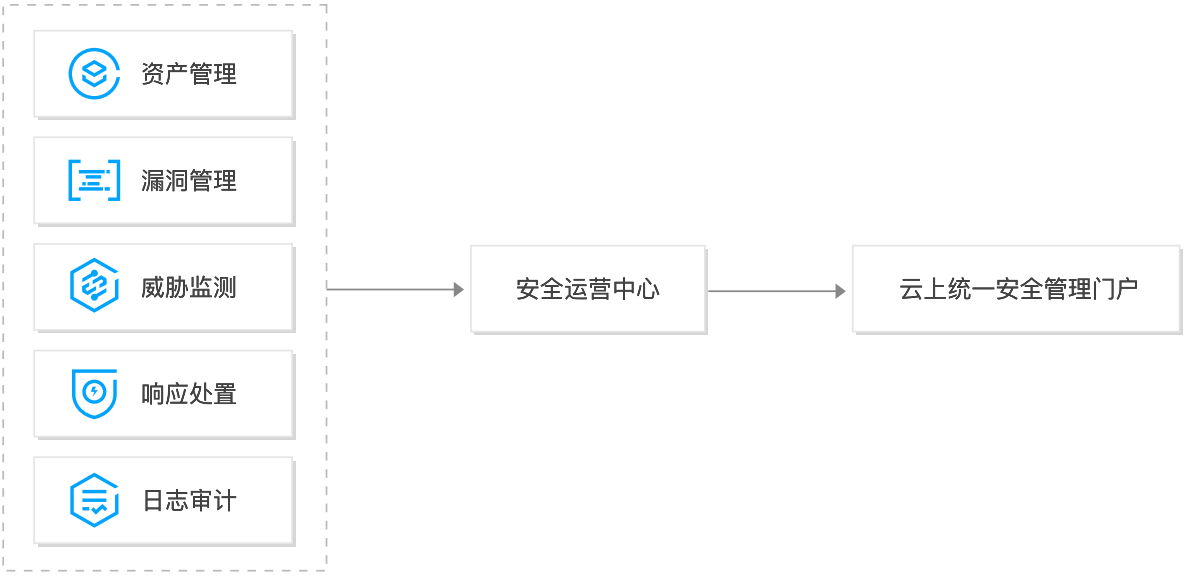
为云用户操作行为及云 API 调用提供可视化审计与监测，并针对敏感操作和风险操作进行检测告警，识别因用户异常行为及风险 API 调用等造成的安全风险。

应用场景

最近更新时间：2020-11-17 15:17:49

统一安全管理

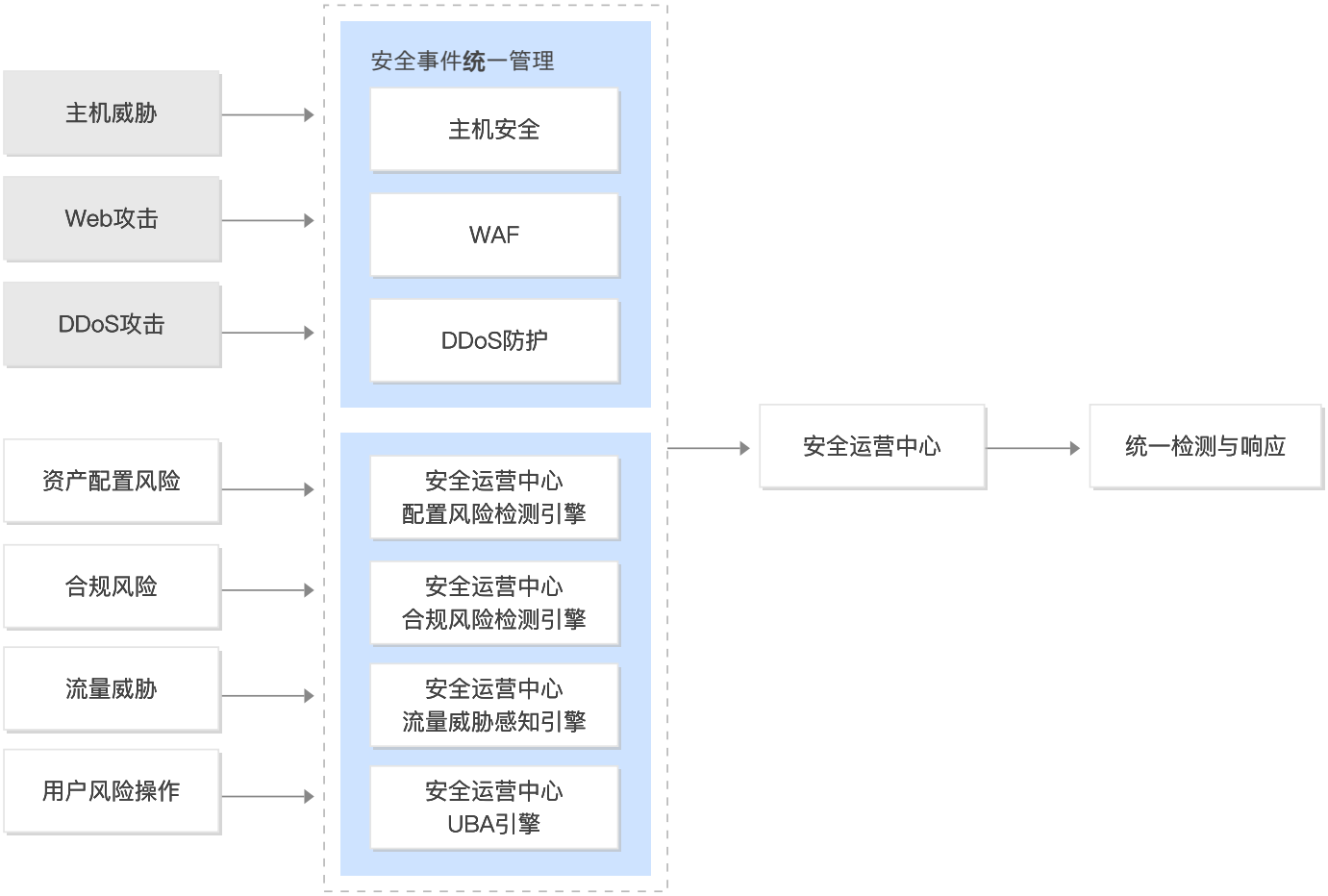
- **适用场景**：云上业务众多，若同时使用多种安全产品，需要构建云上统一安全运营管理平台，提升整体云上安全管理效率。
- **解决方案**：安全运营中心以云上资产中心为基础，打通云上各类安全相关数据，为客户构建覆盖事前、事中及事后各个环节的统一安全运营管理平台。



统一威胁检测与响应

- **适用场景**：业务上云后，除了面对传统的主机安全威胁、网络安全威胁及应用安全威胁外，客户也需要面对云上特有的新的威胁类型，例如云上用户操作行为风险及异常 API 调用等。各类安全威胁的检测与响应处置分散在各个安全产品上，造成安全事件处置效率低下，大大增加了云上安全风险。
- **解决方案**：安全运营中心提供流量威胁感知功能，为腾讯云现有安全产品提供了有效的流量威胁检测能力补充，同时帮助客户实现云上流量由外到内及由内到外的双向攻击检测。安全运营中心可针对云上特有的云产品配置风险、异常用户行为及异常 API 调用等进行检测，全面覆盖云上新增的各类安全风险及威胁。同时安全运营中心打通云上各类安全产品检测的威胁数据，并通过统一的响应中心实现对威胁统一的响应处置，针对部分威胁事件可

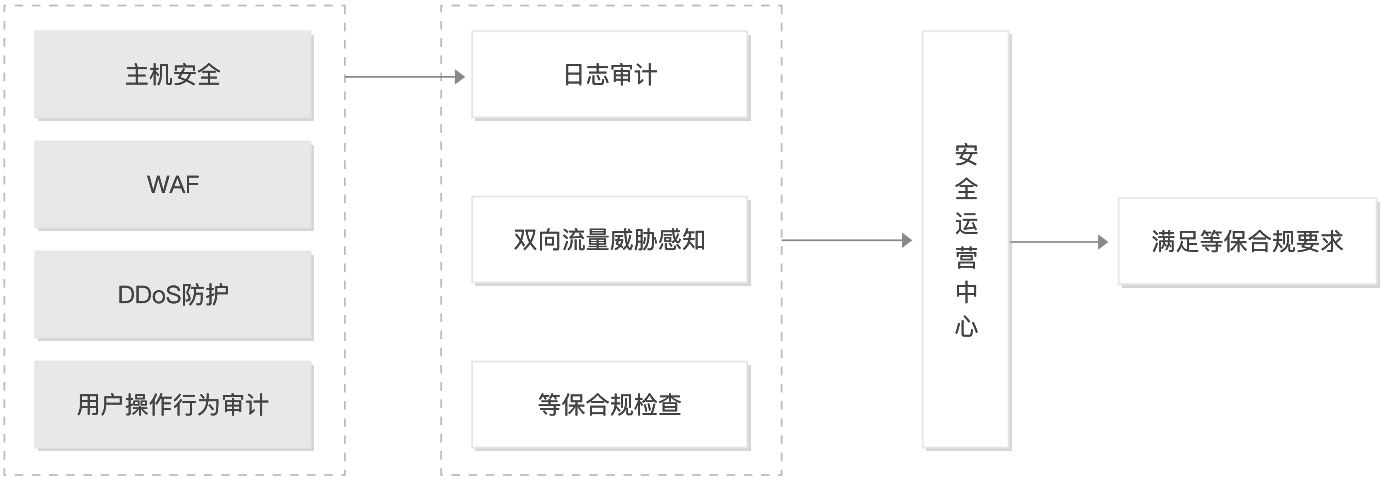
通过内置的安全编排功能实现自动化响应处置，简化威胁管理难度，提升响应处置效率。



等保合规建设

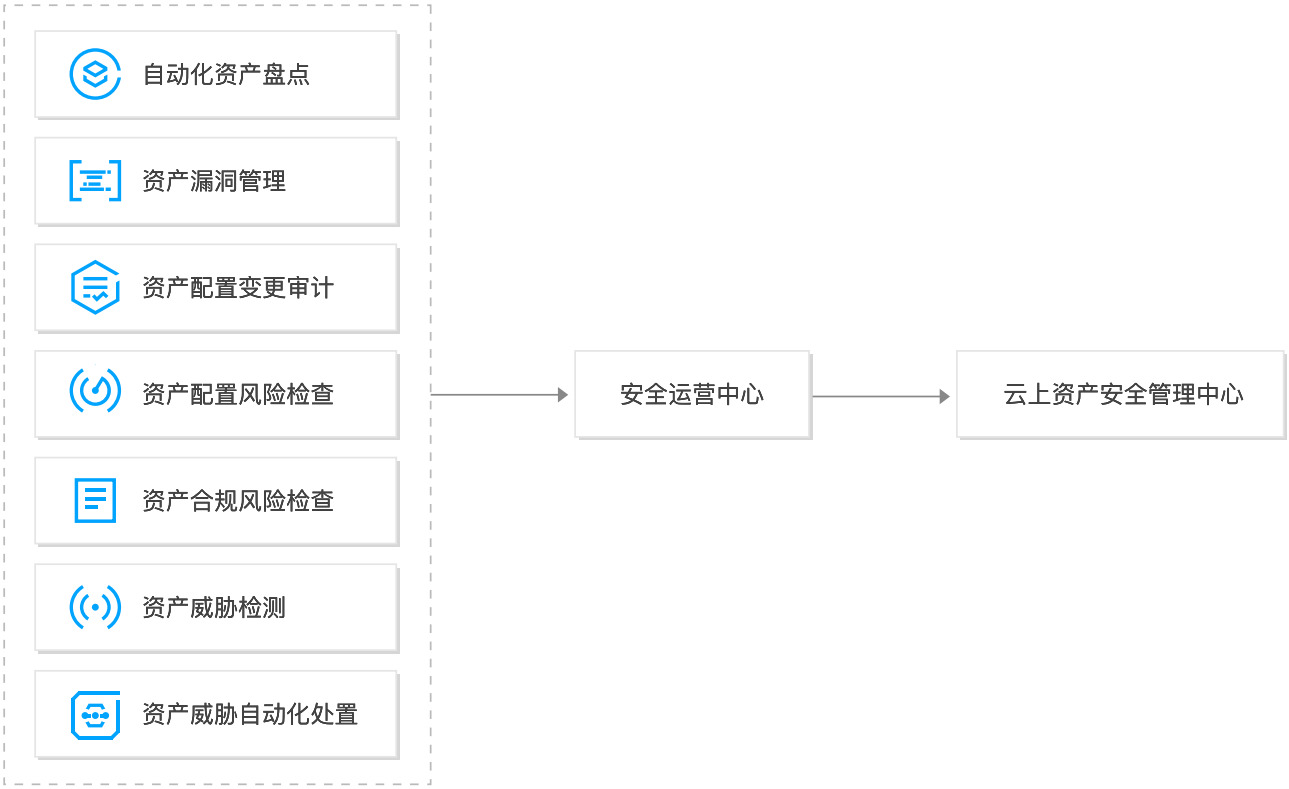
- **适用场景**：等级保护2.0标准正式实施后，针对云上合规要求进行了进一步细化，云上资产对外发起的攻击检测、日志审计及集中管理等都需要客户采取相应技术措施进行满足。同时针对安全管理方面提出的各项管理要求，也需要有相应的工具和产品帮助客户更容易、更有效地落地。
- **解决方案**：安全运营中心提供的流量威胁感知、UBA 、日志审计与检索等功能，可以帮助客户有效满足等级保护合规要求，同时安全运营中心可帮助客户实现等级保护标准要求中关于安全管理中心相关的要求，在满足等保要

求的基础上，切实提升客户云上安全水平。



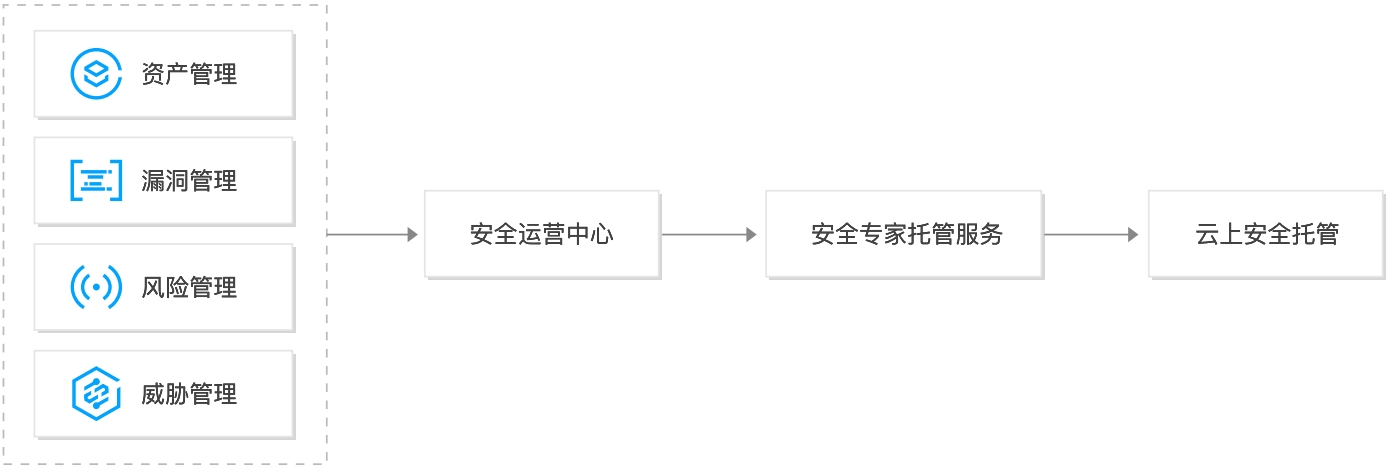
资产安全管理中心

- **适用场景**：公有云上的业务更加弹性灵活，云资产的变化更加频繁，对资产的安全运营和管理要求更高，需要通过自动化的方式实现资产的统一安全管理。
- **解决方案**：安全运营中心可为客户提供云上资产全流程的安全管理平台。从资产的自动化盘点，到资产各类安全风险的检测识别，再到资产安全风险的自动化响应处置，客户可建立以资产为中心的统一安全管理平台，提升云上整体安全水平。



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安全运营中心安全托管服务，以安全运营中心为核心载体，腾讯安全工程师可为客户提供安全运营中心不间断值守、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。



自动编排响应（SOAR）

- **适用场景**：针对大量安全事件，面临溯源调查过程繁琐、响应速度过慢、运营知识随人员的流动而流失，所造成的安全能力断层等问题，需要缩短 MTTR（平均修复时间）、释放人力压力、安全运营流程标准化、避免能力断层，提升整体云上安全事件响应效率的场景。
- **解决方案**：腾讯云安全运营中心为客户提供云原生的安全编排与自动化响应处置功能，可针对云上安全事件为客户提供安全编排剧本，实现高效的自动化响应处置。