云安全中心

快速入门

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。

快速入门

最近更新时间：2026-04-30 14:08:12

步骤1：进入云安全中心，查看安全分

1. 登录 云安全中心控制台 ，在左侧导览中，选择**概览**。
2. 在概览页面，查看核心指标：

指标	说明
安全评分	• 0~100 分，综合反映当前云上整体安全水位。 • **安全分越低，说明当前风险越集中**，优先处理高危待办项可快速提升安全评分。

步骤2：基于安全分引导，处理高危风险

1. 在概览页面，单击**高危待办**的数字或**查看全部风险**。
2. 系统自动按**风险等级排序**，优先展示严重和高危风险。
3. 针对每条高危风险，单击进入详情页：
   - 查看**风险描述**：了解该风险的危害和影响范围。
   - 查看**受影响资产**：确认哪些主机或云产品受影响。
   - 单击**立即处理**：跟随引导完成修复操作。

> **说明：**
> 建议优先处理**暴露在公网的资产**上的高危风险，这类风险被攻击的概率最高。

步骤3：进入漏洞治理，修复系统漏洞

入口：登录 云安全中心控制台 ，在左侧导览中，选择**风险治理 > 漏洞治理**。

3.1 查看漏洞列表

系统按优先级自动排序，重点关注：

优先级	颜色	处理建议
严重		立即修复

3.2 执行漏洞修复

主机安全（专业版）产品支持一键修复系统漏洞。

修复小技巧：可按**主机**筛选，集中处理同一台主机上的全部漏洞，减少重复登录操作。

步骤4：检查云产品配置风险并修复

入口：登录 云安全中心控制台，在左侧导览中，选择**风险治理** > **云安全态势管理** > **云资源配置检查**。

4.1 查看配置检查结果

系统自动扫描存储桶、安全组、数据库等云产品的安全配置，重点关注高危状态的检查项：

状态	说明	操作
高危	配置存在安全风险，需立即整改	单击**配置项名称**参考修复建议进行调整

4.2 优先处理高危配置风险

重点关注以下类型的**不合规**项：

风险类型	典型案例	危害
存储桶公开访问	COS 存储桶设置为公开可读	数据泄露
安全组过度放开	0.0.0.0/0 开放高危端口	暴露攻击面
数据库公网暴露	数据库实例绑定公网 IP	直接攻击风险
访问密钥权限过大	子账号具有全量管理权限	权限滥用风险

4.3 按引导完成配置修复

1. 单击不合规项的**配置项名称**，查看**修复建议**。
2. 按步骤在对应云产品控制台完成配置修改。
3. 返回云资源配置检查页面，单击**立即检查**验证是否已通过。

步骤5：下一步推荐

目标	入口
处理入侵告警，响应安全事件	检测响应 > 告警中心
开展合规检查	风险治理 > 云安全态势管理 > 云资源配置检查
开启日志分析，留存安全审计日志	安全运营 > 日志分析