云安全中心

实践教程

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

实践教程
等保合规

最近更新时间：2026-04-30 14:08:13

等级保护测评解读

云安全中心产品符合等级保护2.0标准体系主要标准。根据《网络安全等级保护基本要求》（GB/T 22239-2019），云安全中心（需单独购买日志分析功能）可协助客户满足第三级的以下安全要求：

序号	等保标准章节	等保标准序号	等保标准内容	对应功能描述
1	安全区域边界-边界防护	8.1.3.1 c）	应能够对内部用户非授权联到外部网络的行为进行检查和限制。	云安全中心支持对云服务器非授权外联到外部恶意域名，IP 地址的行为进行检测和拦截。
2	安全区域边界-入侵防范	8.1.3.3 a）	应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。	云安全中心支持检测和阻断暴破攻击，并能对常见的网络攻击进行检测，部分漏洞支持一键漏洞防御。
3	安全区域边界-入侵防范	8.1.3.3 b）	应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。	云安全中心可检测云服务器系统层和应用层的主动外联和攻击行为，对进程、命令等异常行为进行告警。
4	安全区域边界-入侵防范	8.1.3.3 c）	应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。	云安全中心支持基于主机、网络、云平台的安全数据进行分析，实现对挖矿、勒索、木马、蠕虫等新型攻击进行检测告警。
5	安全区域边界-入侵防范	8.1.3.3 d）	当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。	云安全中心在检测到爆破攻击时，会记录来源 IP、来源地、被攻击服务器 IP/名称、端口、协议、用户名、时间、破解状态、阻断状态并进行告警。
6	安全区域边界-安全审计	8.1.3.5 b）	审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	云安全中心支持服务器登录审计，记录信息包括来源 IP、来源地、服务器 IP/名称、登录用户名、登录时间、状态、危险等级。

7	安全计算环境-身份鉴别	8.1.4.1 a）	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。	云安全中心基线检查能力支持对云服务客户登录配置和密码复杂度进行定期安全检查，对风险项进行预警并提供安全建议。
8	安全计算环境-身份鉴别	8.1.4.1 b）	应启用登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。	云安全中心支持主机登录失败防御配置，可灵活设定在一定时间段内多次登录失败后锁定用户的规则。
9	安全计算环境-身份鉴别	8.1.4.1 c）	当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	云安全中心支持对远程管理的不当配置进行检查，如包含禁止使用 Telnet 基线检查。
10	安全计算环境-访问控制	8.1.4.2 b）	应重命名或删除默认账户，修改默认账户的默认口令。	云安全中心支持对账户权限配置检查，资产管理支持展示所有可登录账号，支持默认弱口令安全检查，发现风险时进行告警并提供修复建议。
11	安全计算环境-访问控制	8.1.4.2 c）	应及时删除或停用多余的、过期的账户，避免共享账户的存在。	云安全中心支持对云服务器账户进行安全配置检查，资产管理支持展示所有登录账号，支持账户登录 IP 异常时进行告警，避免共享账户的存在。
12	安全计算环境-安全审计	8.1.4.3 a）	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。	云安全中心支持对云服务器账户登录操作进行记录，以及高危命令、高危操作的审计。
13	安全计算环境-安全审计	8.1.4.3 b）	审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	云安全中心日志记录包括主机 IP、主机实例 ID、账户、源 IP、目的 IP、进程 ID 端口、事件类型、发生时间、动作策略等内容。
14	安全计算环境-安全审计	8.1.4.3 c）	应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	云安全中心产品支持日志审计存储功能，可存储至少6个月内的日志数据，不同租户使用完全独立的日志空间，日志数据有多副本备份机制。
15	安全计算环境-入侵防范	8.1.4.4 b）	应关闭不需要的系统服务、默认共享和高危端口。	云安全中心资产管理支持对云服务器上运行的服务、进程、开放的端口进行统一管控。

16	安全计算环境-入侵防范	8.1.4.4 c）	应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。	云安全中心支持添加主机登录 IP 地址白名单，非白名单内用户登录将被拦截。配合安全组实现云上网络管理和限制。
17	安全计算环境-入侵防范	8.1.4.4 e）	应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	云安全中心支持检测 Linux 软件漏洞、Windows 系统漏洞、Web-CMS、应用漏洞、应急漏洞，评估风险级别并提供修复建议。
18	安全计算环境-入侵防范	8.1.4.4 f）	应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	云安全中心支持检测重要节点的入侵行为，主要包括恶意文件，异常登录，密码破解，恶意请求，高危命令，反弹 Shell，本地提权，文件篡改等，提供告警及部分主动阻断能力。
19	安全计算环境-恶意代码防范	8.1.4.5	应采用免疫恶意代码攻击的技术措施或采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。	云安全中心支持恶意文件查杀，实时监测木马、病毒等，并自动隔离。
20	安全管理中心-安全管理	8.1.5.3 a）	应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计。	云安全中心支持通过控制台对云资源进行安全管理操作，能对登录行为、高危命令进行审计。
21	安全管理中心-安全管理	8.1.5.3 b）	应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。	云安全中心支持通过控制台对系统中的安全策略进行配置。
22	安全管理中心-集中管控	8.1.5.4 e)	应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。	云安全中心支持漏洞集中管理，恶意代码检测和隔离功能。

等保合规基线策略

云安全中心支持对等级保护安全要求基线检测项的定期检测和一键检测，帮助了解基线通过率及风险情况，提供基线和检测项的风险等级和修复建议，有助于您快速整改，满足等保合规要求。以下为等保合规支持检测项：

基线分类	基线名称	包含的检查项数量
等保二级	等保二级-CentOS 6安全基线检查	16

	等保二级-CentOS 7安全基线检查	18
	等保二级-CentOS 8安全基线检查	16
	等保二级-Ubuntu 14安全基线检查	19
	等保二级-Ubuntu 16安全基线检查	19
	等保二级-Ubuntu 18安全基线检查	21
	等保二级-Ubuntu 20安全基线检查	29
等保三级	等保三级-CentOS 6安全基线检查	27
	等保三级-CentOS 7安全基线检查	31
	等保三级-CentOS 8安全基线检查	36
	等保三级-Ubuntu 14安全基线检查	35
	等保三级-Ubuntu 16安全基线检查	33
	等保三级-Ubuntu 18安全基线检查	40
	等保三级-Ubuntu 20安全基线检查	48
	等保三级-Windows 2008安全基线检查	19
	等保三级-Windows 2012安全基线检查	19
	等保三级-Windows 2016安全基线检查	19

等保合规日志及告警

云安全中心产品符合等级保护2.0标准体系主要标准。根据《网络安全等级保护基本要求》（GB/T 22239-2019），云安全中心（需单独购买日志分析功能）可协助客户满足第三级的以下安全要求：

序号	等保标准章节	等保标准序号	等保标准内容	云安全中心对应功能	功能解读
1	安全区域边界-安全审计	8.1.3.5 a)	应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重	日志审计	云安全中心可集中存储一定时间的日志数据，包含主机安全告警、Web 应用防火墙告警、DDoS 防护

			要安全事件进行审计		告警、云用户操作行为等安全相关日志数据
2	安全区域边界-安全审计	8.1.3.5 b)	审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息	日志审计	云安全中心日志审计模块可审计相关告警事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息
3	安全区域边界-安全审计	8.1.3.5 c)	应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等	日志审计	云安全中心日志通过多副本实时存储多份，保障用户日志在其存储周期内不丢失、可恢复
4	安全计算环境-安全审计	8.1.4.3 a)	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计	日志审计	云安全中心日志审计模块可审计相关告警事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息
5	安全计算环境-安全审计	8.1.4.3 b)	审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息	日志审计	云安全中心日志审计模块可审计相关告警事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息
6	安全计算环境-安全审计	8.1.4.3 c)	应对审计记录进行保护，定期备份，避免	日志审计	云安全中心日志通过多副本实时存储，保

			受到未预期的删除、修改或覆盖等		障用户日志在其存储周期内不丢失、可恢复
7	安全区域边界-集中管控	8.1.5.4 f)	应能对网络中发生的各类安全事件进行识别、报警和分析	威胁告警	云安全中心可通过威胁分析将客户使用的不同安全产品识别的告警进行分析，并结合威胁情报及事件调查能力，将告警串联起来，形成事件攻击链，帮助安全管理员更好的判断与处置问题