安全加速 SCDN

产品简介

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2025 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】

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或95716。

文档目录

产品简介
- 产品概述
- 产品优势
- 应用场景
- 使用限制

版权所有：腾讯云计算（北京）有限责任公司

产品简介
产品概述

最近更新时间：2023-11-03 11:32:11

什么是安全加速?

安全加速（Secure Content Delivery Network，SCDN），在为用户业务提供快速稳定的内容分发服务的基础上，提供全面的网络攻击防护能力。已接入并开启腾讯云 内容分发网络（Content Delivery Network，CDN）或 全站加速网络（Enterprise Content Delivery Network，ECDN）服务的域名，可一键开启 SCDN 安全加速，对 DDoS 攻击、CC 攻击、Web 攻击、BOT 爬虫等网络攻击类型进行全方位防护，为业务安全保驾护航。

> **说明：**
> 安全加速 SCDN 现已全面升级为边缘安全加速平台（TencentCloud EdgeOne，简称 EdgeOne），如您同时有内容分发加速与安全防护需求，请前往 选购 EdgeOne 产品 。

SCDN 有效解决了网络加速场景中的以下问题：

1. 在仅使用 CDN/ECDN 服务的情况下，依赖 CDN/ECDN 带宽抵挡大规模 DDoS、CC 攻击产生的攻击流量和请求，会产生大量非业务计费流量与请求，进而可能产生不必要的费用消耗。
2. CDN/ECDN 服务本身提供有限的安全、访问控制能力（例如 IP 限频、访问鉴权等），但在面对日益复杂的网络威胁和攻击时，需要结合使用其他云上安全产品，才能全方位防护各类攻击，且需要分别配置服务，在网络传输架构中添加额外层级。

SCDN 接入简单，您无需对现有 CDN/ECDN 配置和域名解析做任何调整，即可开启域名安全加速服务，并按实际业务需求，调整各类安全设置。

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：2023-11-03 11:32:11

功能丰富

腾讯云安全加速（SCDN）在为用户提供快速、稳定的内容分发加速服务的基础上，支持一键开启安全一体化解决方案，集成 Web 攻击防护、DDoS 防护、CC 防护等多项安全功能，全面提升加速网络的安全防护能力。

分布式 DDoS 攻击防护

SCDN DDoS 攻击防护，基于先进的特征识别算法对流量进行统一精确清洗，抵御 SYN Flood、UDP Flood、ICMP Flood 等各种大流量攻击，保障正常服务平稳运行。
SCDN 安全节点网络基于分布式架构搭建，智能调度全局负载均衡，当受攻击流量到达清洗阈值时，调度流量至 SCDN 高防集群，应对超大流量 DDoS 攻击，保障突发攻击时的业务访问流畅稳定。
腾讯云 SCDN 全网最大可抵御 20Tbps 的 DDoS 攻击，单个安全节点最大可抵御 1Tbps 的 DDoS 攻击。

CC 攻击防护

SCDN CC 攻击防护，通过内核级拦截、机器学习算法，配合人机识别等手段智能识别并拦截 CC 攻击。
SCDN 单个安全节点最大可抵御60万 QPS 的 CC 攻击，避免用户服务受异常高频访问影响瞬间崩溃。在分布式架构下，安全加速同时能够通过智能调度均衡节点间负载，抵抗大型攻击。

Web 应用层攻击防护

SCDN Web 攻击防护，基于腾讯云 Web 应用防火墙能力构建，通过腾讯海量 Web 攻击样本库和 AI+ 规则，智能识别常见 Web 攻击，精准有效地防御如 SQL 注入、非授权访问、XSS 跨站脚本、CSRF 跨站请求伪造、Webshell 木马上传等威胁，具有防绕过、低漏报、低误报的特性。
主动监测并响应突发网络安全事件，24小时内下发高危 Web 漏洞，0day 漏洞防护虚拟补丁，使受保护站点远离突发 Web 漏洞隐患。

> **注意**
> SCDN Web 攻击防护已全新上线，并限时免费！

爬虫对抗（BOT 防护）

SCDN BOT 防护基于 AI+ 策略引擎和规则库，直接对知名和公开的机器行为和爬虫（包括网页爬虫，搜索引擎，内容聚合工具等超过1000种公开爬虫行为）进行识别、监控和阻断，协助企业规避恶意 BOT 行为带来的站点用户数据泄露、内容侵权、竞争比价、库存查取、黑产 SEO、商业策略外泄等业务风险问题。
对于未被公开策略识别的 BOT 攻击，支持设置匹配 UA、referrer、速率、路径和特殊参数，通过行为观察，特征提取 ，业务调整的方式不断进行动态对抗。

> **注意**

版权所有：腾讯云计算（北京）有限责任公司

> SCDN BOT 防护能力正在内测中。

自定义防护规则

除 CDN 所支持的基础 IP、referer、UA 黑白名单等基础访问控制能力外，SCDN 支持用户自定义复杂访问控制规则，即指定客户端 IP、URI、Referer、User-Agent、Params 等字段进行等于、包含、不包含等规则匹配，根据业务场景进行对请求的多条件组合过滤。

海量资源储备

腾讯云安全加速依托于腾讯云 CDN/ECDN 节点网络构建，在加速内容分发、传输的同时，全方位防护 Web 攻击，DDoS 攻击，CC 攻击等网络攻击类型，为业务安全保驾护航。腾讯云 CDN 节点网络在中国境内拥有1100+个加速节点，境内总储备带宽 100Tbps+。境内安全加速节点均为腾讯高规格、高安全性自建机房，享受运营商高质量网络。

智能调度

腾讯云安全加速通过对全网链路进行实时监控，结合自研的 GSLB 调度体系和智能路由技术，将访问流量调度至最优的安全加速节点进行服务，保证正常业务请求被最快速响应。在遭受大流量攻击时，安全加速能够智能调度节点间负载均衡，保证业务的高可用性。

一键接入

在腾讯云 CDN/ECDN 基础上使用腾讯云 SCDN，无需对现有 CDN 配置和域名解析做任何调整，即可开启域名安全加速服务，接入流程简单快捷。
将需要安全服务的域名接入腾讯云 CDN/ECDN 后，用户只需要在安全加速控制台开启域名安全服务并按业务需求对各类安全设置进行配置，静待5分钟左右，域名相关安全配置会下发至全网安全加速节点，整个过程当中加速服务不会中断，不会对现网业务造成任何影响。

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：2023-11-03 11:32:11

场景概述

腾讯云 SCDN 可结合多项安全能力，针对各行业不同的网络威胁，为各行业的内容分发、网页应用安全提供全面保障。

应用行业	行业安全风险	SCDN 安全能力	腾讯云 SCDN 方案优势
政企、传媒	政企传媒类网站、APP 是政府机关实现政务信息公开，企业单位、媒体进行信息传播，并与社会公众、互动交流的重要窗口。政企传媒网站或信息系统受攻击导致服务不可用，或内容被篡改，影响政企单位形象，干扰信息正常传播，更有造成 PR 问题的风险。	Web 攻击防护 DDoS/CC 攻击防护 HTTPS	保障政企类网站、APP 应用的高可用性，抵御 Web 攻击，防止网站内容造攻击而被篡改，而引发 PR 风险。
金融	金融领域类别众多，包括但不限于银行、证券、基金、股票等，是黑客攻击的主要目标领域之一。金融业务对可用性要求非常高，当攻击消耗系统和网络资源造成业务中断时，正常用户无法进行交易下单，将造成严重的经济损失。同时金融业务源站存储有大量敏感数据，如源站被攻破导致信息泄露，会导致更大影响和损失。	Web 攻击防护 DDoS/CC 攻击防护 HTTPS	保障金融应用的稳定性和高可用，抵御 Web 攻击，降低源站内容、数据泄露风险。
游戏、流媒体	游戏、视频行业竞争激烈，一直是 DDoS 攻击行为的高发地。2017 年以来，棋牌类游戏、在线视频等进入到大爆发阶段，大量资本和用户涌入，同业竞争引发行业恶性竞争，网络流量攻击层出不穷，DDoS 攻击迅猛，不乏上 T 级流量的攻	DDoS 攻击防护 Web 攻击防护 HTTPS	保证游戏内容、资源包下载，和流媒体传输的稳定性。行业恶意竞争频繁，帮助避免由大流量攻击导致服务不可用，造成用户流失。

	击。对于相关行业来说，保证业务的高可用性，低卡顿是留住玩家、用户的前提。		
电商	电商行业在业务高峰期，尤其是年中、年末等多个活动周期，易因同行恶意竞争，或黑客勒索等原因，遭到 DDoS、CC 和 Web 攻击，导致服务不可用等事故，造成商家信誉受损，商家、用户流失，造成巨额经济损失。	DDoS/CC 攻击防护 Web 攻击防护 HTTPS	抵御 DDoS、CC、Web 攻击，避免尤其是在活动高峰期间的攻击造成的服务不可用。

使用限制

最近更新时间：2025-03-27 15:55:22

- 接入安全加速

接入腾讯云 SCDN 的域名需要首先接入腾讯云 CDN/ECDN，且开通 SCDN 的服务地域，需要同时启动 CDN/ECDN 服务。使用 CDN 服务，接入域名的相关限制，请参考 CDN 使用限制 。

安全加速服务

类型	限制说明
安全加速域名	• 安全加速套餐内含 20 个基础防护域名数量。如需增加上限，需购买域名扩展包，提升上限为120个。 • 安全加速域名，在 CDN 的对应服务区域的状态需要为“已启动”。如关闭对应区域 CDN 服务，安全加速服务也会关闭。 • 暂不支持泛域名接入。
数据统计	默认提供近 1 年的整体攻击数据查询，部分特别说明的数据项除外。
事件日志	• 支持查询近 7 天的攻击事件日志。 • 创建成功的日志下载任务保留 7 天。 • 单个任务最多支持下载 1000 条日志。 • 每日允许创建 100 个下载任务。

版权所有：腾讯云计算（北京）有限责任公司