CLOUDFLARE

产品简介

Cloudflare Zero Trust

最快的 Zero Trust 浏览和应用访问平台

边界以外的风险

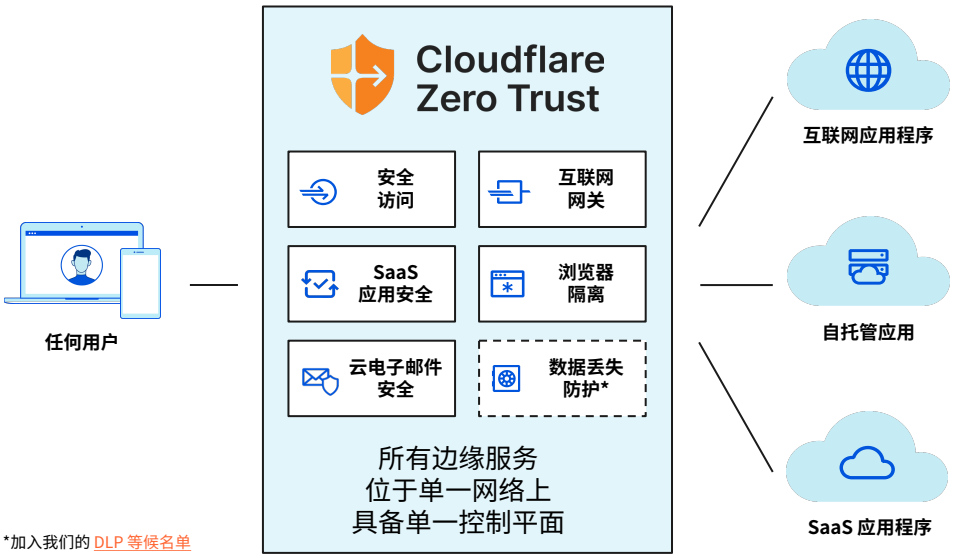
应用和服务离开企业边界后，安全团队不得不在如何保障数据安全方面做出妥协。以位置为中心保护流量的方法（例如 VPN、防火墙和 Web 代理）已经不堪重负并崩溃，使组织面临有限的可见性、互相冲突的配置和过度的风险。

鉴于风险现已无处不在，组织正在转向通过云交付的 Zero Trust 来予以应对。

采用互联网原生的 Zero Trust

Cloudflare Zero Trust 是一个安全平台，在远程和办公室员工连接到应用程序和互联网时，增加可见性、消除复杂性并降低风险。采用单次通过架构，对流量进行验证、过滤和检查，并隔离威胁。

该平台运行在世界最快的 Anycast 网络上，覆盖 100+ 国家/地区的 275+ 城市，部署速度和性能均傲视同侪。



*加入我们的 DLP 等候名单

VPN 替代品
简化并保护，连接任何用户到任何资源

互联网保护
保障数据安全，防御来自任何端口和协议的威胁

SaaS 安全
就包括电子邮件在内的应用获得可见性和管控

安全现代化
提高生产力，简化运营，减少攻击面

商业效益

减少过度信任

通过基于身份和上下文的 Zero Trust 规则保护应用。阻止勒索软件、钓鱼和其他在线威胁。通过在远离设备的地方执行不可信的 Web 代码来保护端点免受风险威胁。

消除复杂性

减少对传统点产品的依赖，对所有流量应用标准的安全控制，无论连接如何开始，或其处于网络堆栈的什么位置。

恢复可见性

覆盖 DNS、HTTP、SSH、网络和影子 IT 活动的全面日志。监控所有应用的用户活动。将日志发送到多个首选云存储和分析工具。

VPN 替代与增强 (ZTNA)

以更快、更容易、更安全的方式将远程用户连接到应用

挑战：缓慢、复杂和存在风险的 VPN

传统 VPN 日益成为负担。缓慢性能损害最终用户生产力。管理员努力应对笨拙的配置。此外，VPN 让恶意软件得以在网络中肆意横向移动。

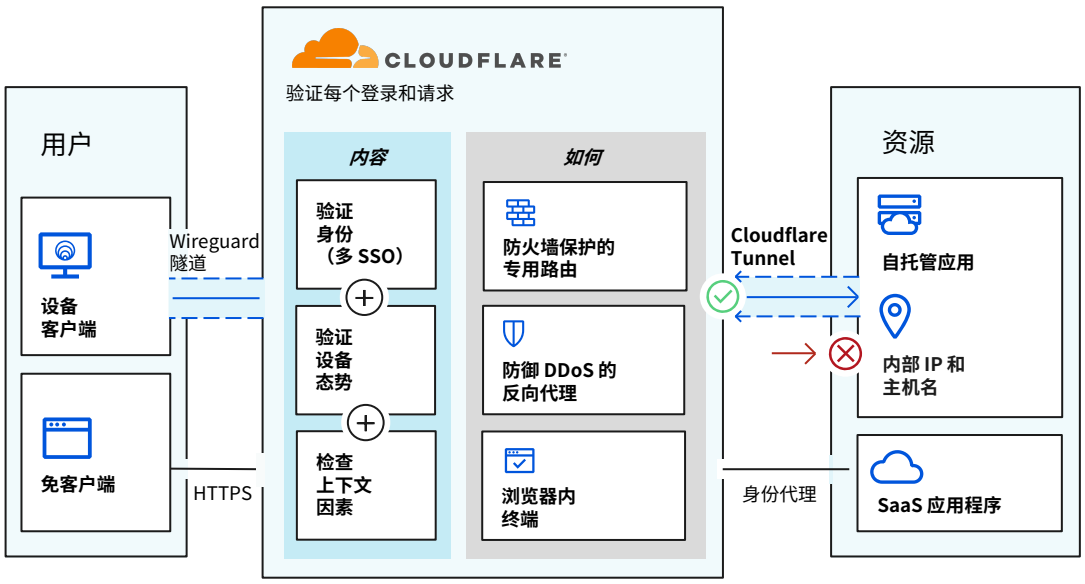
加速上云和混合办公进一步暴露了以上缺陷，使 VPN 更易受到攻击。

Zero Trust 网络访问 (ZTNA)

Cloudflare Access 是我们的 ZTNA 服务，通过保护任何本地网络、公共云或 SaaS 环境中的任何应用程序来增强或取代 VPN 客户端。

Access 与身份提供商和端点保护平台协同工作，执行默认拒绝的 Zero Trust 规则，限制对企业应用、私有 IP 空间和主机名的访问。

了解详情



无客户端部署
通过浏览器访问基于 Web、SSH 或 VNC 的自托管应用。

通过 Cloudflare 设备客户端部署
来连接到内部 IP、主机名和非 Web 应用。

关键用例

支持远程办公和 BYOD 倡议

根据身份、设备态势、认证方法和其他上下文因素，验证所有用户的访问，无论他们位于何处。

为混合办公团队实施这些 Zero Trust 策略。通过保护受管和非受管设备，支持自带设备 (BYOD) 倡议。

灵活地简化第三方访问

加快承包商、供应商、代理和协作者等的访问设置。

一次性加入多个身份提供商。根据已经使用的身份提供商设定最低特权规则。

避免配置 SSO 许可证、部署 VPN 或创建一次性权限。

简化管理配置和支持

短短几分钟即可添加新用户、身份提供商或 Zero Trust 规则。

通过减少员工加入时间 (eTeacher Group) 和淘汰基于 IP 的访问配置 (BlockFi) 来释放新生产力。无需雇佣专职人员来管理 VPN (ezCater)。

互联网威胁和数据保护（SWG 与 RBI）

对前往互联网的流量进行过滤、检测和隔离

挑战：不断演变的威胁形势

提高安全性并维持用户的生产力比以往任何时候都要棘手。远程办公意味着更多未受管设备在本地存储更多敏感数据。与此同时，勒索软件、网络钓鱼、影子 IT 和其他基于互联网的威胁在数量和复杂性上均呈爆炸式增长。

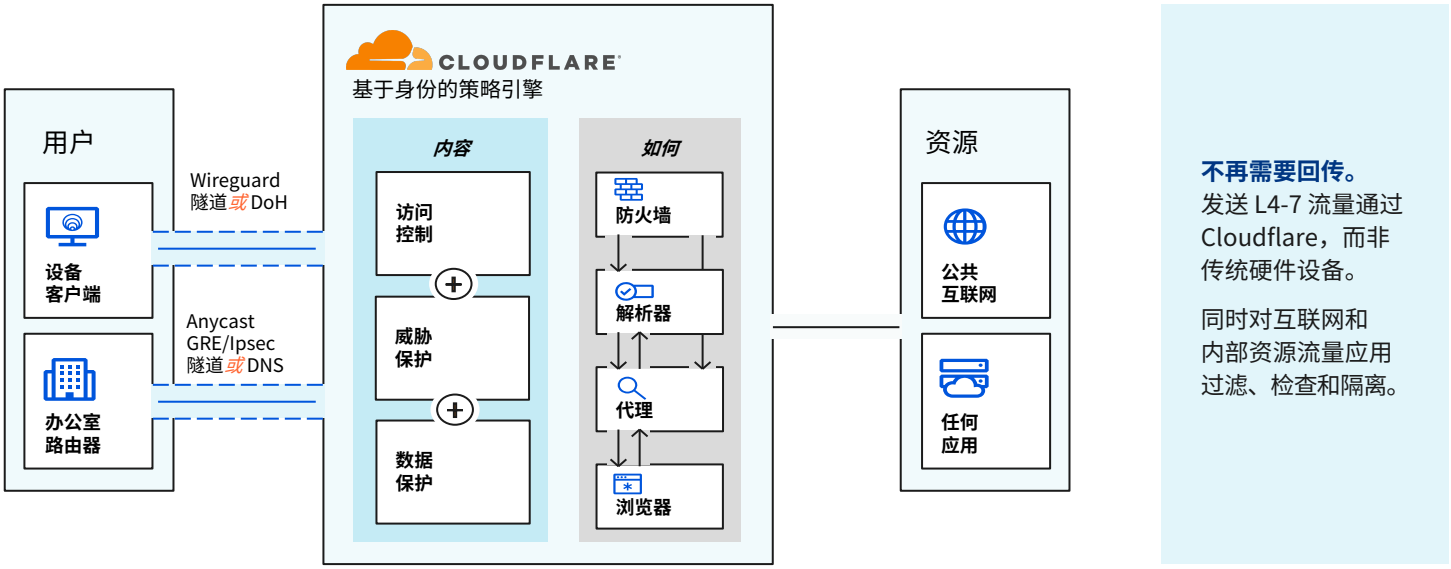
依赖传统点产品和数据备份来防范下一次恶意软件威胁是一种有风险的策略。

SWG + Zero Trust 浏览

Cloudflare Gateway 是我们的安全 Web 网关 (SWG) 产品，它使用基于身份的 Web 过滤加原生集成的远程浏览器隔离 (RBI) 来保护用户。

首先部署 DNS 过滤，为远程或办公室用户快速实现价值。其次，应用更全面的 HTTPS 检查；最后，扩展 RBI 控制来为所有互联网流量活动实施 Zero Trust。

了解详情



不再需要回传。
发送 L4-7 流量通过 Cloudflare，而非传统硬件设备。

同时对互联网和内部资源流量应用过滤、检查和隔离。

关键用例

阻止勒索软件

根据我们的全球网络情报阻止恶意软件站点和域。在有风险的站点隔离浏览以增强保护。

将 SWG 过滤和 RBI 与默认拒绝的 ZTNA 结合起来，缓解恶意软件感染在网络内部横向传播和提升权限的风险。

阻止网络钓鱼

过滤已知或“新”/“新发现”的网络钓鱼域。隔离浏览以阻止有害代码在本地执行。通过 RBI 的键盘输入控制阻止在可疑的钓鱼网站上提交敏感信息。

此外，不久后，管理员将能一键启用 Area 1 驱动的电子邮件过滤功能。

防止数据泄露

实施数据丢失防护 (DLP)，使用文件类型控件来阻止用户将文件上传到站点。

部署 Zero Trust 浏览，以控制和保护 Web 应用中的数据。管控用户在浏览器中的操作，例如下载、上传、复制/粘贴、键盘输入和打印功能。

SaaS 安全 (CASB)

简化 SaaS 安全以获得更多可见性和控制，减少开销

挑战：SaaS 应用使用激增

现代办公对 SaaS 应用的依赖达到前所未见的程度。然而， SaaS 应用的配置各不相同，要求不同的安全考虑，并且在传统边界的保护范围以外运行。

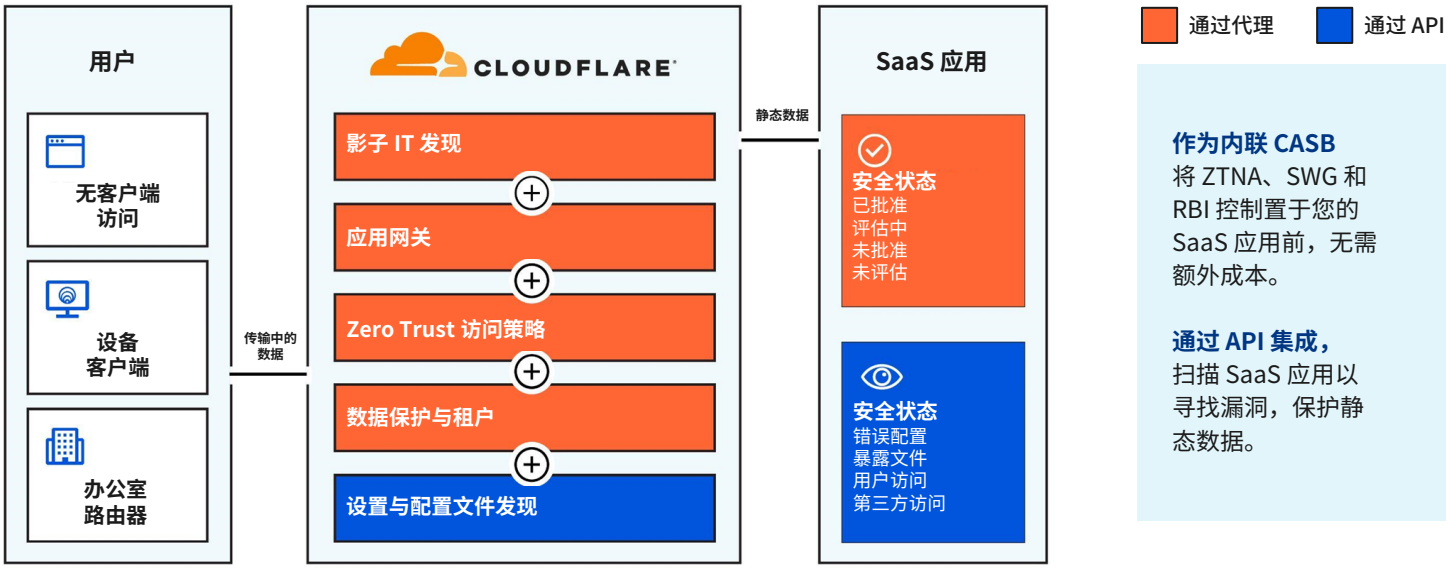
随着组织采用数十乃至数百个 SaaS 应用，维持一致的安全、可见性和性能变得日益困难。

云访问安全代理 (CASB)

Cloudflare 的 CASB 服务提供对 SaaS 应用的全面可见性和管控，以便您能轻松预防数据泄露和不合规行为。

阻止内部威胁、有风险的数据分享和恶意行为者。记录每一个 HTTP 请求，以发现未经批准的 SaaS 应用。扫描 SaaS 应用以检测错误配置和可疑活动。

了解详情



作为内联 CASB
将 ZTNA、SWG 和 RBI 控制置于您的 SaaS 应用前，无需额外成本。

通过 API 集成，
扫描 SaaS 应用以寻找漏洞，保护静态数据。

关键用例

应用租户和数据保护控制

通过 HTTP 网关策略应用租户控制，防止用户无意或恶意地在流行 SaaS 应用程序的错误版本中访问或存储数据。

控制 Web SaaS 应用中的用户操作（例如复制/粘贴、下载、打印等），以最大限度减少数据丢失风险。

缓解并管控影子 IT

最大限度减少未经批准的 SaaS 应用带来的风险。

Cloudflare 根据应用类型聚合并自动分类我们活动日志中的所有 HTTP 请求。据此，管理员可以设置状态并跟踪组织中已批准和未批准应用的使用情况。

识别新的威胁和错误配置

通过 API 连接到流行的 SaaS 应用（Google Workspace、Microsoft 365 等）并扫描风险。

让您的 IT 和安全团队获得对权限、错误配置、不当访问和控制问题的可见性，这些问题可能会使其数据和员工面临风险。

即将加入 Zero Trust：云电子邮件安全 (CES)

将 Zero Trust 扩展到电子邮件

CLOUDFLARE®
AREA 1 SECURITY

2022 年 4 月 1 日，Cloudflare 完成对 Area 1 Security 的收购。后者是一家领先的云原生电子邮件安全公司，保护用户免受电子邮件、Web 和网络环境中的钓鱼攻击。查看公告。

挑战：电子邮件是头等威胁手段

电子邮件是团队通信的最主要方式，但也是攻击者的第一大手段。事实上，近期一项研究发现，91% 的网络攻击都是从网络钓鱼邮件开始的。

电子邮件是每个人都成为内部攻击来源，甚至包括来自组织以外的人员，例如供应商、合作伙伴和客户。

最基本的问题是：电子邮件被授予太多隐式信任，被攻击者加以利用，欺骗日常商业流程（例如密码重设、文件共享通知）或可信实体（例如CEO、供应商/合作伙伴发送发票）等。

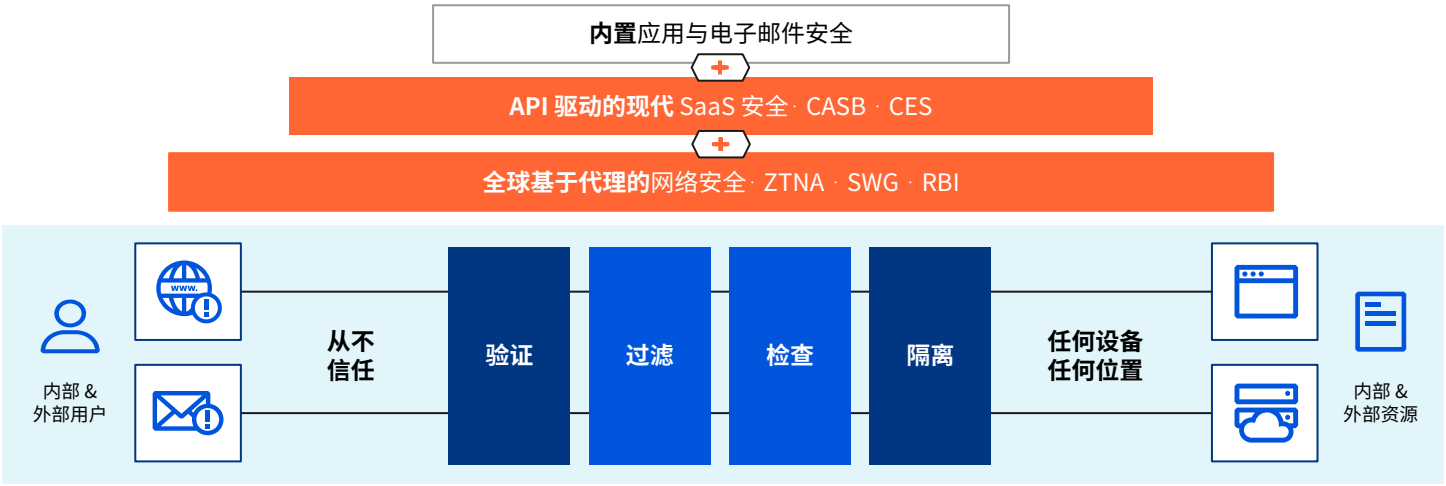
集成云原生电子安全

将 Area 1 加入 Cloudflare Zero Trust，消除了对电子邮件的隐式信任，以先发制人的方式阻止网络钓鱼和商业电子邮件攻击 (BEC)。同时，还可以节省用于创建和调优电子邮件威胁策略的时间。

通过从不信任发件人，包括电子邮件在内的所有流量均得到验证、过滤、检查，免受来自互联网的威胁。Area 1 帮助客户阻止高级威胁，采取主动积极的安全态势，将网络钓鱼时间响应时间缩短 90%。

电子邮件安全将被整合到我们的 Zero Trust 服务中，与 RBI、CASB 等成为一个强大的组合。例如，你是否对电子邮件中的一个链接持怀疑态度，但又不想直接屏蔽它？在隔离浏览器中打开链接，并阻止文本输入，以防万一。

工作原理：针对所有内部与外部网络、Web 和电子邮件流量的 Zero Trust



安全现代化：Cloudflare 的独到之处

安全现代化的强大基础

部署简易性

Cloudflare 交付单个统一、可组合的平台，易于设置和操作。通过纯软件连接器和一次性集成，我们的 Cloudflare 入口和边缘服务均可协同工作。

这为您的 IT 从业人员和最终用户都提供更佳体验。

网络韧性

我们的端到端自动化确保可靠、可扩展的网络连接，从任何位置都提供一致的保护。

不同于其他安全提供商，Cloudflare 构建的每项边缘服务运行于每一个网络位置，对每一位客户可用。

创新速度

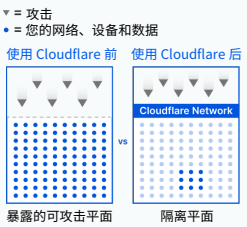
我们拥有面向未来的架构，能够快速构建并交付新的安全和网络功能。

无论是快速采用新的互联网和安全标准，还是构建以客户为主导的用例，我们的技术实力发展历程有目共睹，我们的基础提供了高度可选择性。

Zero Trust 为企业节省时间与金钱的五种方法

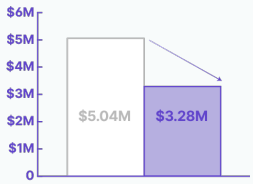
攻击面减少

91% ↓



泄露成本减少

35% ↓



员工加入提速

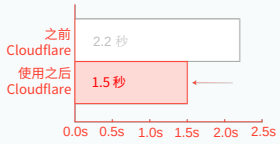
60% ↑

IT 工单负担减轻

80% ↓

用户延迟降低

39% ↓



为可用性优化

统一管理界面

利用原生构建的仪表板简化对应用和互联网访问策略的配置。

使用单一仪表板与身份提供商、端点保护和网络入口集成。

统一集成平台

淘汰拼凑而成的 VPN 客户端、本地防火墙和其他点产品解决方案，代之以单一平台和单一控制平面。

将安全性迁移到边缘，降低成本和复杂性。

无以伦比的用户体验

Cloudflare 拥有庞大的 Anycast 网络，覆盖全球 100 多个国家/地区的 275+ 城市，更加靠近您的用户和服务，并能利用经过优化、情报驱动的路径更快地路由请求。

加速您的 Zero Trust 旅程

马上试试吧　联系我们