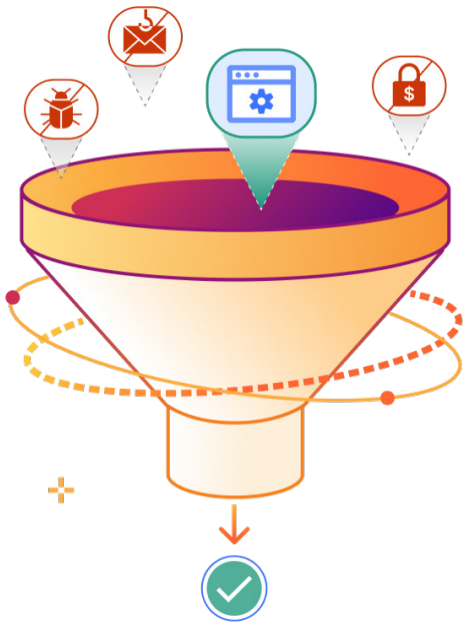
安全 Web 网关 (SWG)

Cloudflare Gateway 是 Cloudflare One 中的一项可组合服务，通过身份感知互联网过滤保护用户和数据免受网络威胁。



简单、现代的威胁防御

取代复杂的传统 Web 安全

网络威胁无处不在，并继续利用组织不断扩大的攻击面中的漏洞。同时使用多个单点解决方案（例如 DNS 解析器、Web 网关和网络防火墙）只会增加成本、复杂性和风险。

Cloudflare Gateway 为针对互联网和内部资源的访问提供一致的保护和可见性，从而简化安全性。通过身份感知策略降低网络风险，帮助组织：

- **阻止互联网威胁**，例如勒索软件、网络钓鱼、命令与控制等
- 通过 DNS、HTTP 网络和浏览器隔离规则**控制和监控 L4-7 层流量**
- 对远程和办公室内人员**实施适当使用策略**

采用一次通过架构，对所有流量进行验证、过滤和检查并隔离威胁。

今天是 SWG，明天是安全服务边缘 (SSE)

现代化 SWG 控制是通过 SSE 架构整合安全性和采用 Zero Trust 最佳实践的常见步骤。

探索使用 Cloudflare 完成这个过程的效果。

为什么选择 Cloudflare?

统一的安全性

1 个网络

和控制平面覆盖所有服务，包括安全服务边缘 (SSE)、Web 应用程序和 API 保护 (WAAP)、电子邮件安全和其他领域。

大规模威胁情报

2 万亿

次 DNS 查询/天。这种覆盖新注册、新发现和有风险域的实时可见性驱动基于 AI/ML 的威胁搜寻模型。

为规模而建

310+

网络节点，遍布 120+ 国家/地区。每个 SWG 和 Zero Trust / SSE 功能都可供客户在每个节点运行，实现始终快速、一致的策略执行。

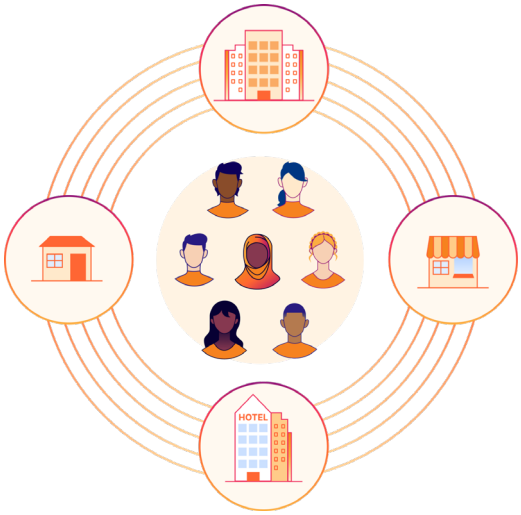
用例：适用于远程员工和办公室的威胁防御

问题

混合办公扩大了您的攻击面，管理不同工具带来安全漏洞，使勒索软件、网络钓鱼和其他网络威胁更容易损害您的收入和品牌声誉。

解决方案

Cloudflare 的 SWG 为远程和办公室员工提供一致的 Web 安全性。大多数组织从 DNS 过滤开始以快速实现价值，然后针对所有互联网活动实施更全面的检查和控制。



立即开始

将流量发送到 Cloudflare 的网络：首先进行 DNS 解析（然后执行完整的 HTTP 检查）

执行 DNS 过滤：根据远程办公人员的身份/设备或办公室位置

叠加更细粒度的控制：包括 HTTP、网络和浏览器隔离规则

部署云电子邮件安全，包括 MX 内联，通过 API 或两者兼有（多模式）

首先，确保网络内外用户的安全 Web 浏览

其次叠加电子邮件安全措施

降低风险并提高团队生产力

简单、灵活的部署

使用网络路由器进行 DNS 解析。通过 GRE/IPsec 隧道、WAN 连接器或现有 SD-WAN 发送 L3 流量。

或者部署我们的设备客户端来转发代理流量。

快速、一致的保护

在我们的网络中执行一次通过检查，在任何地方快速、一致地执行策略。

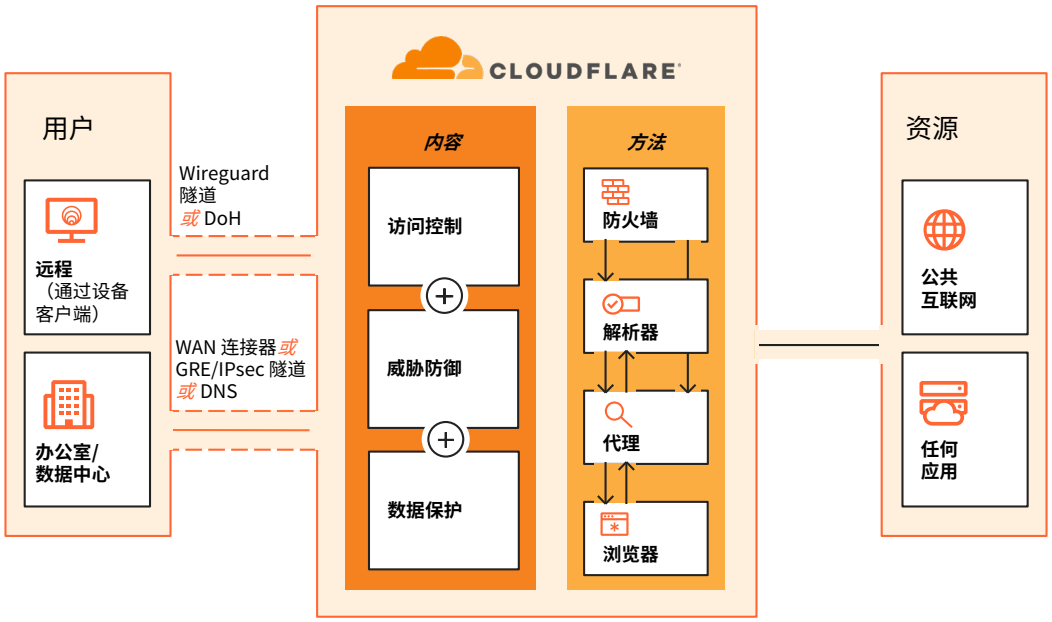
证明比 Zscaler、Netskope 和 Palo Alto Networks 等供应商更快。

加速 Zero Trust 采用

统一控制平面，单一策略管理器，覆盖可组合的安全服务。

从 Web 和电子邮件安全开始，然后按自己的节奏增加其他 Zero Trust 控制。

SWG 的工作原理



简化安全。

对访问互联网和内部资源流量均应用防火墙、解析器代理和浏览器控制。

从一个策略管理器构建策略。

在 SWG 基础上叠加 SSE 控制

通过转发代理流量通过 Cloudflare 的 SWG，以便组织利用我们原生集成和可组合的 SSE 服务的丰富功能，进一步扩展安全控制和可见性。

使用 RBI 保护 Web 和应用活动

- 在 Cloudflare 的全球网络上低延迟运行所有浏览器代码，防止本地设备受到恶意软件侵害
- 通过 DLP 扫描和浏览器控制（例如阻止复制-粘贴、限制上传/下载、打印 — 使用或不使用设备客户端均可）隔离应用以保护数据

使用多模式 DLP 和 CASB 保护数据

- 通过检测和阻止 HTTP(S) 流量中的敏感数据以及预定义文件（例如财务/健康数据）或自定义配置文件（例如精确数据匹配）
- 扫描 SaaS 套件的错误配置，使用集成 DLP 检测敏感数据，并采取规范步骤以进行补救

使用 ZTNA 扩展身份感知访问策略

- 执行 Zero Trust 规则，限制对自托管企业应用程序、SaaS 应用程序和专用网络 IP 或主机名的访问
- 一次性集成身份和端点保护提供商，并使用相同的规则构建器对互联网和应用程序访问规则应用态势检查

增加可见性

- 在受管和非受管设备上维护详细的审计日志（在各合约计划中，DNS 日志存储 6 个月，HTTP 和 网络日志存储 30 天）
- 推送日志到首选的 SIEM 以进行关联和进一步分析

Gateway 功能

威胁防御与安全访问	
安全与应用程序类别	全面覆盖勒索软件、网络钓鱼、DGA 域、 DNS 隧道技术、新注册/新发现的域、C2 和僵尸网络以及其他安全风险。内联 CASB 覆盖 25 个应用类别，包括 AI。
递归式 DNS 过滤	按安全或内容类别允许/阻止/覆盖域和 IP 地址。DNS 过滤器可通过我们的租户 API 进行管理以实现父子可配置性。
HTTP(S) 过滤和检查	基于源、目的地、域、HTTP 方法、URL 等控制流量 。HTTP1/2/3 检查支持 AV 和 DLP 扫描、文件控制、设备态势、租户、远程浏览器隔离等。
无限 TLS 1.3 检查	默认无限 TLS 1.3 检查。所有 HTTPS 流量均被解密、应用策略并使用我们的证书或用户的自定义证书重新加密请求—全部具备市场领先的低延迟。支持 DNS over TLS (DoT) 和 DNS over HTTP (DoH) 标准。仅启用符合 FIPS 140-2 标准的加密套件。
L4 FWaaS	L4 网络策略应用于所有公共/私有 TCP/UDP 数据包，根据检测到的协议、地理位置、SNI 域等控制对非 HTTP 资源的访问。审计端口 22 上的 SSH 流量。（L3 FWaaS 功能内置于 WAN 网络服务中。）
防病毒检查	扫描上传/下载的各种类型（PDF、ZIP、RAR 等）文件以检查病毒扫描 。
身份和设备态势检查	基于所有主流企业身份提供商、社交身份或 SAML 和 OIDC 标准设置策略。通过设备客户端或您的第三方端点保护提供商验证设备姿势。
集成威胁情报	威胁情报基于我们自己的 AI/ML 模型和第三方源。第一方情报源自作为最大权威递归 DNS 解析器之一（2T+ 查询/天）的全球遥测数据。我们的 Web 爬网程序还每隔几周对整个 Web + 页面编制索引以发现新出现的恶意活动基础设施。此外，支持自定义威胁源和特征（IP 、URL 和域等）。
网络	
使用设备客户端	利用我们的设备客户端 (WARP)，通过完全的 WireGuard 隧道或通过 DoH 转发代理流量。 自行注册或通过 MDM 部署。启用设备态势检查。检测设备是否在网络上。
无客户端选项	选项包括：网络路由来自客户位置的 DNS查询；Anycast GRE/IPsec 隧道；WAN 连接器，通过 PAC 文件的代理端点；以及通过重写 URL 的无客户端 Web 隔离。
IPv4 和 IPv6 支持	所有功能均可用于 IPv4 和 IPv6 连接（纯 IPv6 或双堆栈）。
流量路由	
专用出口 IP 和出口策略	专用的静态 IP 范围（IPv4 或 IPv6），可用于基于源 IP 的允许流量。 使用出口策略选择使用哪个出口 IP，根据诸如身份、地理位置或设备态势等属性。每个出口 IP 均为账户专用，不会被其他客户使用。
解析器策略	将 DNS 请求路由到自定义 DNS 解析器以到达非公共可路由域，例如专用网络服务和内部应用程序。（默认情况下，DNS 请求使用 Cloudflare 自己的公共 DNS 解析器 1.1.1.1——世界上最快、最可靠的解析器之一。）
隧道拆分	排除/包含 IP 地址或域以用于专用网络或与 VPN 一起使用 。
可见性和可扩展性	
日志记录	完整日志记录，包括所有 DNS 查询、L4 网络数据包和通过任何端口检查的 HTTP 请求。使用日志推送或 API 以集成现有 SIEM 、编排和分析工具。管理员可以选择排除和/或删除各用户的个人可识别信息 (PII) 集合。
影子 IT 发现	跟踪、审查和批准最终用户通过内联 CASB 访问的 SaaS 和专用网络源服务器。
页面自定义	上传自定义 HTTP 阻止页面以贴合您的品牌或传达说明以提供更好的用户体验。
自动化	直观的 API 和 Terraform 提供商用于以编程方式管理 SSE/Zero Trust 实现的所有方面。也提供无用户的服务令牌以支持自动化服务。

客户如何使用我们的 SWG

Cloudflare 和 Accenture 为美国网络安全和基础设施安全局 (CISA) 保护互联网访问

100+ **美国民事机构**
使用 Cloudflare 的 DNS 过滤功能保护其办公地点

了解更多

北欧 IT 和数字通信咨询公司

“我们依赖 Cloudflare 保护我们的端口、过滤威胁并清理我们的流量，从而减少了攻击面。”

— Victor Persson，安全运营负责人
阅读案例研究

日本云集成商和咨询公司

4K **每周阻止的请求数**
防止数百名员工访问有害和无用的互联网内容

阅读案例研究

与 Zscaler 的竞争比较示例

标准	Cloudflare Gateway	Zscaler 互联网访问
架构	一个云平台，一个控制平面	多个分散的云，多个控制平面
管理界面	单一界面覆盖所有 SSE	不同界面 SWG 和 ZTNA 分离
一次通过检查	是适用于所有 SSE 服务	否
仅支持 IPv6	是	否
正常运行时间 SLA	100%（所有服务）	99.999%（大多数服务）99.9%（DNS 解析器）

继续比较 Cloudflare 与 Zscaler

更快的保护

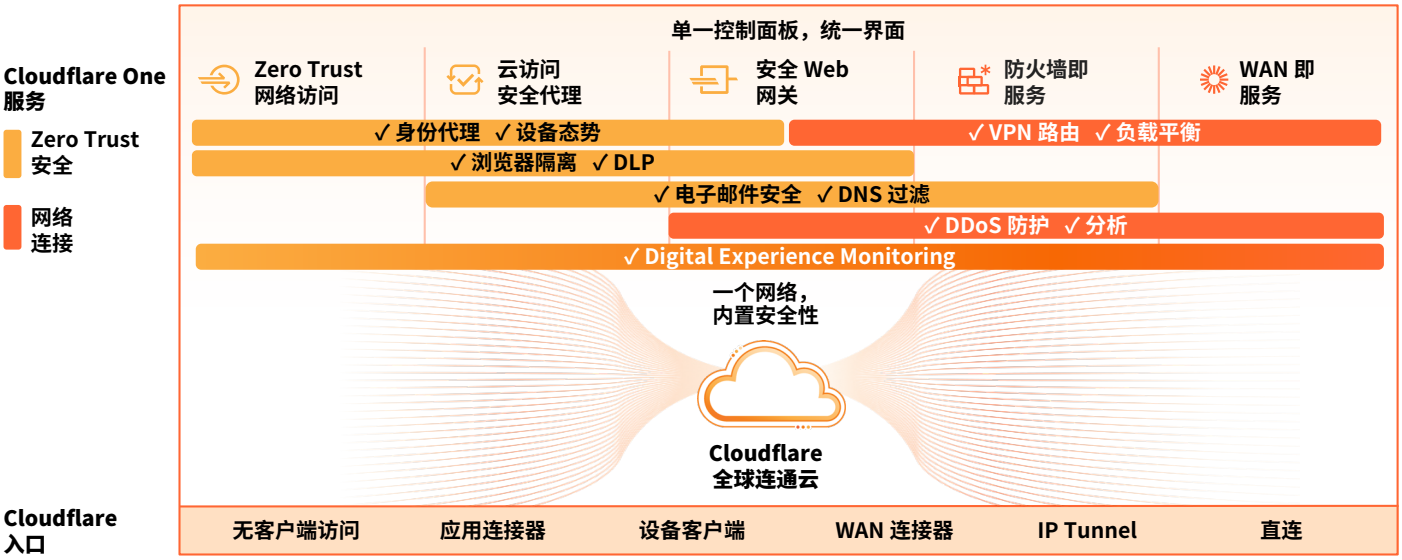
13-58%
更快的安全 Web Gateway (SWG)

45-64%
更快的远程浏览器隔离 (RBI)

基于第一方测试和第三方测试

使用 Cloudflare 的 SSE 平台实现安全现代化

Cloudflare Gateway 是 Cloudflare One （我们的 SSE 平台）中的一项可组合服务。利用 Cloudflare One 跨 Web、SaaS 和私有应用环境的可互操作安全功能在您的 SWG 基础上构建并扩展可见性和控制。



统一平台

- **安全访问** — 验证和分隔任何用户对任何资源的访问
- **威胁防御** — 使用网络驱动的 AI/ML 和威胁情报覆盖所有渠道
- **数据保护** — 增加对传输中、静态和使用中数据的可见性和控制

一个可编程的网络

- **更有效** — 简化连接和策略管理
- **提高生产力** — 确保在任何地方提供快速、可靠和一致的用户体验
- **更敏捷** — 快速创新以满足您不断变化的安全需求

还未准备好进行实时对话？

欢迎阅读我们的 SASE 参考架构以了解更多信息，或者在我们的 Zero Trust 平台观看交互式演示以了解其如何工作。