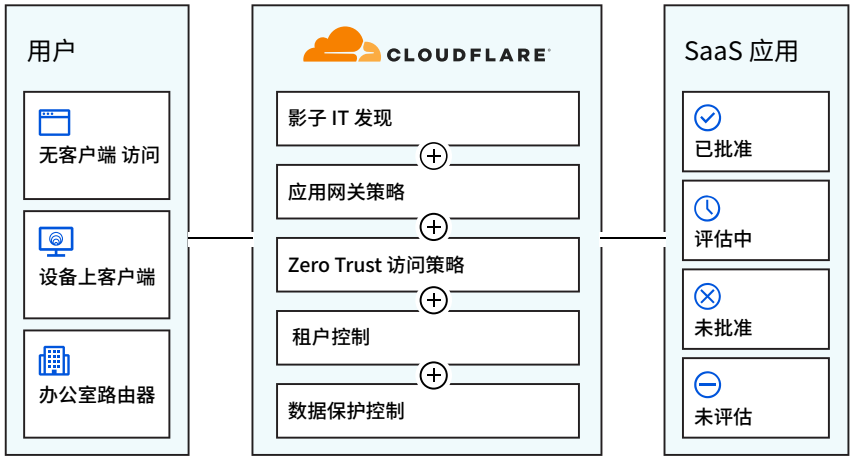
解决方案简介

CLOUDFLARE

SaaS 应用程序的 Zero Trust 可见性和管控解决方案

SaaS 应用程序能显著提高团队的工作效率，但在获得灵活性和自由的同时，这些应用程序也给员工带来了安全风险、可见性挑战和访问控制障碍。

Cloudflare 不但能提供保护数据和员工所需的工具，还能允许员工使用那些能帮助他们高效完成工作的应用。



发现和控制影子 IT

如果对员工所用的应用程序缺乏可见性，企业就无法管控如何将敏感数据储存、分享和提供给第三方。Cloudflare 帮助您发现、分类和控制企业内所有已批准和未批准的应用程序，并在一个集中的位置记录每一次连接和请求。

应用 Zero Trust 访问策略

SaaS 应用程序是托管于企业网络之外的，对于用户如何访问这些应用程序,以及如何在这些应用中存取数据，企业安全团队往往力所不逮。Cloudflare 在您的 SaaS 应用程序前加上一层 Zero Trust 安全措施，对合法用户进行身份验证，并防止未经授权的用户或存在风险的设备访问您的文件和数据。

应用租户和数据保护控制

在员工访问错误的应用实例时，他们有可能将数据储存于错误的地方，为潜在的数据泄露和其他安全风险打开了大门。Cloudflare 帮助您控制企业数据的分享和储存，无论是在通过我们的网络传输时，还是在我们的远程浏览器中。现在，您可以构建和部署 Zero Trust 浏览策略来保护存在于任何 SaaS 租户中的数据，同时防止您的员工访问错误的应用程序或已批准的应用程序的错误租户。

发现和控制影子 IT

评估员工使用的应用程序

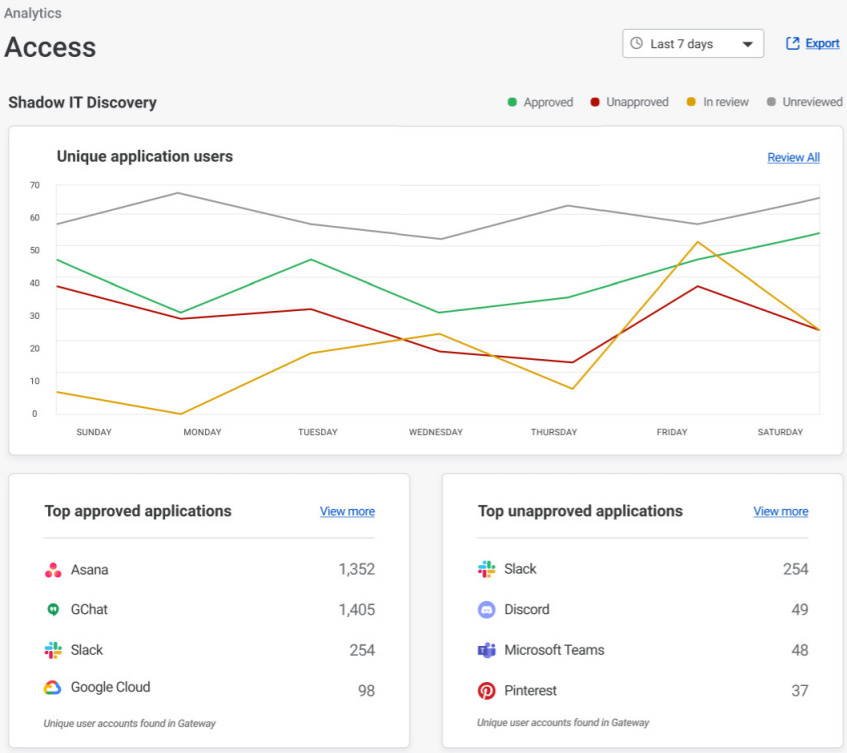
如果 IT 团队看不到您的员工正在使用的应用程序，他们就无法控制这些应用程序中的数据发生了什么。Cloudflare 根据应用程序类型聚集并自动分类我们活动日志中的所有 HTTP 请求。据此，您可以设置状态并跟踪整个组织中已批准和未批准的应用程序的使用情况。

记录每个连接和请求

员工访问未经批准的应用程序，或使用不受管理的设备来访问敏感信息时，就会给组织带来风险，而 Cloudflare 能帮助缓解这种风险。每个连接和请求都会记录到一个中心位置，因此您可以看到正在使用的应用程序以及用户在其中执行的操作。管理员还能够阻止和允许对 SaaS 应用程序的请求，防止用户绕过重要的安全控制，对组织内部应用程序、资源和数据进行未经授权的访问。

重要功能

- 自动跟踪哪些应用程序已经受到 Cloudflare 保护
- 在 Cloudflare 网络中保留最长 6 个月的日志
- 将日志推送到一个或多个云日志存储和 SIEM 服务



对您的 SaaS 应用程序应用 Zero Trust 访问策略

通过 Cloudflare 的身份验证代理来保护 SaaS 访问

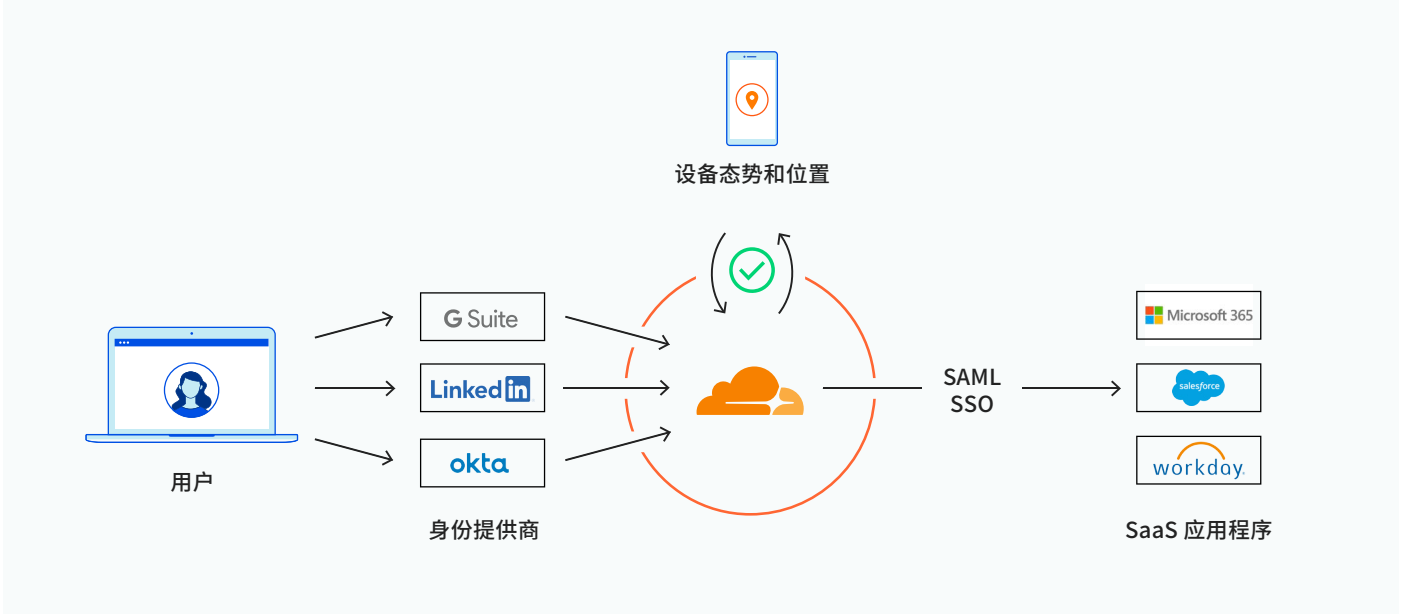
SaaS 应用程序托管于第三方并通常由业务部门管理，这意味着您的 IT 团队对用户如何访问这些应用程序往往几乎没有任何发言权。Cloudflare 位于您的身份提供商和您的 SaaS 应用程序之间，使您能够在登录过程中构建和应用身份敏感、上下文驱动的 Zero Trust 规则——全程不会干扰最终用户体验。

判断用户设备的应用程序权限

您的 IT 部门需要对企业管理设备对 SaaS 应用程序的登录实行精细化管理。Cloudflare 将 Zero Trust 规则插入到所有支持 SAML 身份验证的应用程序的单点登录过程中。用户首先通过其身份提供者进行验证；然后，Cloudflare 会根据设备态势和位置检查请求，再授权对任何 SaaS 应用的访问——这是通过持续验证的灵活会话管理完成的。安全管理员也可创建特定于设备的策略，使用户仅能通过满足既定安全要求的设备（包括 mTLS 证书）来访问应用程序。

重要功能

- 集成多个身份提供商或同一提供商的多个实例
- 通过针对每个应用的规则来验证用户身份（例如MFA 要求硬件密钥）
- 通过针对每个应用的规则来验证设备态势（例如已实施的 SWG 策略，已安装的 EPP，mTLS 证书、磁盘加密）和位置
- Cloudflare 的应用程序启动器门户允许用户查看和访问所有已获得批准的 SaaS 应用程序



对任何 SaaS 应用程序实施租户和数据保护控制

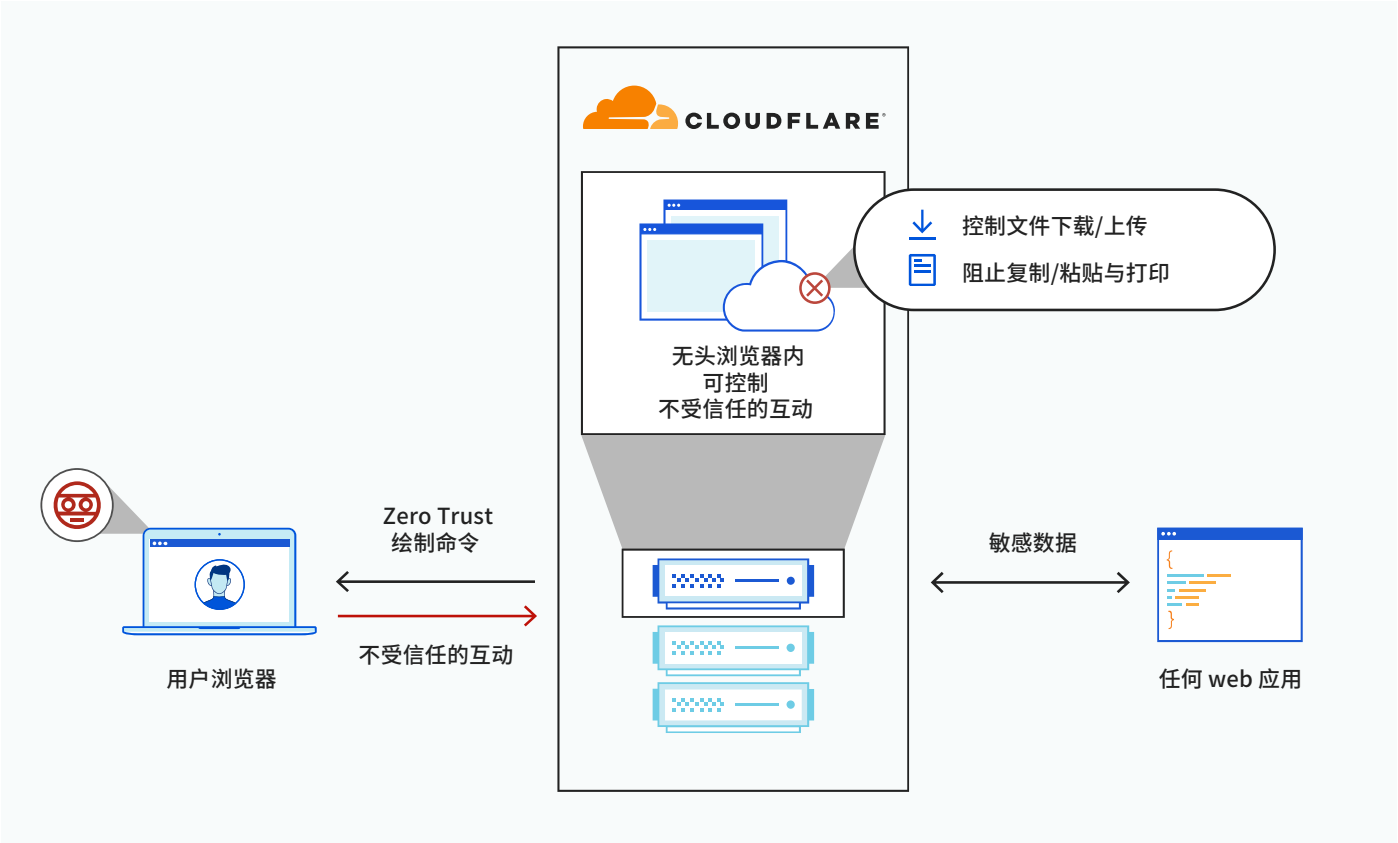
限制对任何非企业应用程序实例的访问

Cloudflare支持通过 HTTP 网关策略来控制租户，可以通过配置这些策略来阻止用户访问应用程序的消费者版本。Cloudflare 不是通过企业 VPN 使用本地代理服务器来执行这些策略，而是通过一个庞大的全球数据中心网络来过滤和检查所有流量和请求——因此您的用户不会体验到延迟增加或性能下降。**防止企业数据离开您的租户**

Cloudflare 使企业能轻松构建和部署 Zero Trust 浏览策略，以控制和保护 web 应用程序中的数据。所有应用程序代码都是在一个安全的远程无头浏览器中执行的，而该浏览器在我们庞大的全球网络中运行，而不是在终端设备上运行，从而杜绝遭入侵或不可信设备和零日威胁，避免敏感数据泄露。管理员保留对用户如何访问和共享数据的控制，因此能够最大限度地降低意外数据丢失或更严重的数据泄露风险。

重要功能

- 根据多种条件来允许或阻止浏览器行为，包括应用程序、应用程序类型、主机名、用户身份和安全风险
- 控制浏览器内的用户操作：下载、上传、复制粘贴、键盘输入和打印功能



Cloudflare 的独特优势

覆盖广泛

Cloudflare 将 Zero Trust 访问（ZTNA）、网关（SWG）和浏览器（RBI）置于 SaaS 应用程序前，不需您的IT团队配置和运行专门的 CASB 产品。

从零构建

Cloudflare 的 CASB 能力与我们的 ZTNA、SWG 和 RBI 服务无缝协作，因为所有这些服务都是从头构建的，无需使用多个独立产品来保护您的应用程序和团队。

单一控制面板

Cloudflare 让企业通过单一仪表板设置策略并管理应用程序的访问和使用——所有请求和许可一览无余。

Cloudflare 提供一整套原生集成的零信任安全能力，帮助团队监测、保护和控制 SaaS 应用程序。

了解更多