CLOUDFLARE

解决方案简述

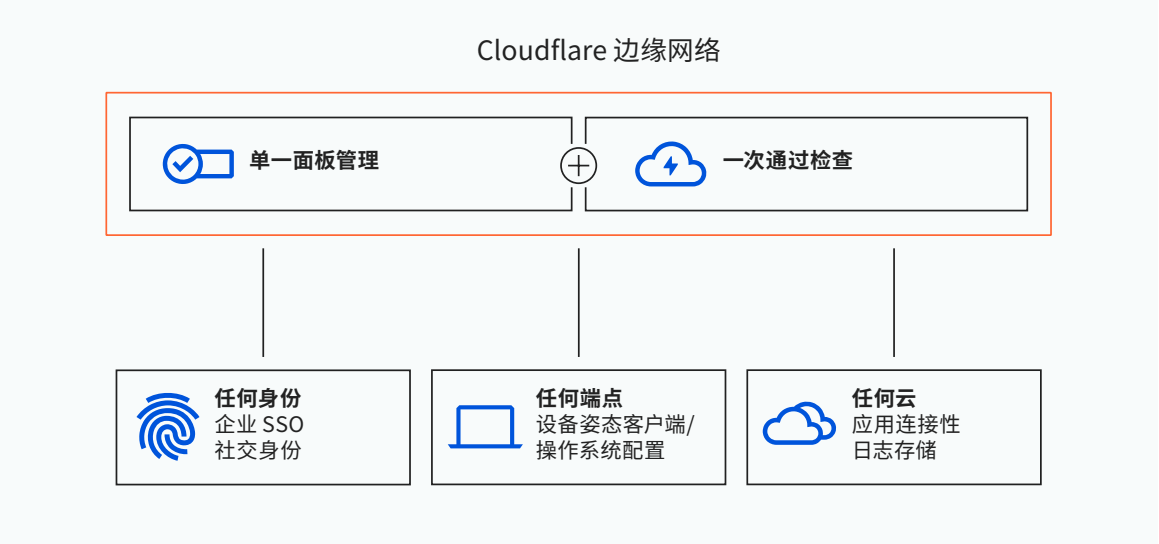
Cloudflare 的 Zero Trust 集成

建立在您已经使用的身份、端点和云提供商之上

在一个组织内部处理多个身份、端点和云提供商是不可避免的，但不必成为麻烦。Cloudflare 的目标是以最容易使用的方式为您的组织提供最强健的安全。与其他供应商不同，我们对您目前或将来与哪些特定的供应商合作没有任何既得利益。

我们是通用的。 因此，我们的长期战略是将 Cloudflare Zero Trust 设计成与尽可能多的解决方案集成。

通过集成，Cloudflare 聚合来自多个提供商的信号，并通过单一控制面板提供服务，以便在我们的全球网络中执行上下文丰富的细粒度策略。此外，这些集成不需要研究密集的技术文档；它们被预先构建为工作流，以实现更加无缝的“单面板”管理。



在此，我们强调所遵循的三个原则，以满足客户的实际需求：

- **身份无关：** 跨多个身份提供者类型对用户执行身份验证，以实现所有用户的无摩擦访问，且无需任何麻烦的配置。
- **端点无关：** 同时使用来自您最偏好的端点供应商和我们的设备客户端的信号，以更细粒度和自适应的方式丰富您的设备姿态检查。
- **云无关：** 保护任何公有或私有(本地)云上的应用程序，以避免长期供应商锁定。

将多个身份聚合到 Cloudflare

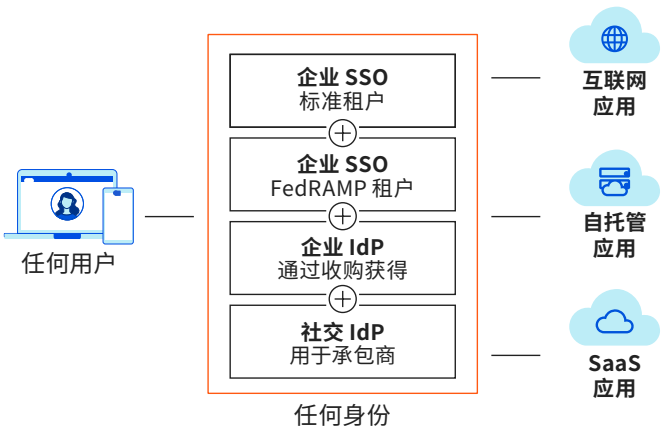
多个 SSO

Cloudflare 打造了首批同时支持多个身份提供商 (IdP) 的 Zero Trust 访问解决方案之一。今天，我们集成了领先的企业 IdP (如 Okta 或 Azure AD)，社交身份(如 LinkedIn 或 Github) 和开源标准(如 SAML 或 OIDC)。此外，我们支持同一个 IdP 的多个实例：例如，Okta 的 FedRAMP 和非 FedRAMP 使用。

同时联合多个身份

我们具备跨多个身份提供商 (IdP) 整合身份的能力，帮助启动构建身份感知策略的过程。组织不再需要在其 IdP 之间构建自定义集成。

对信息安全人员有限的成长期组织而言，联合可能是一个特别强有力的工具，无需费心整合单一集中式目录即可扩展到 Zero Trust 模式。



关键功能

- Cloudflare 同时集成多个 IdP，均为个中佼佼者。
- 集成多个身份提供商或同一提供商的多个实例
- 更快加入第三方用户和并购合作伙伴

使用案例：

让第三方用户享受一等公民待遇

Cloudflare 采用与身份无关的方法，在与组织外部的第三方(如承包商、收购企业或合作伙伴)协作方面特别方便。仅需几分钟，即可基于这些用户带来的身份设置最低特权访问规则。

这种毫不麻烦的灵活性避免了发放 SSO 许可证、部署 VPN、或创建一次性权限的低效率和安全风险。

一流的端点保护合作伙伴

合作伙伴关系

Cloudflare 与 CrowdStrike、SentinelOne、VMware Carbon Black、Tanium、Uptycs 和 Microsoft Intune 建立了合作关系。

客户可以同时使用多个端点保护提供商，并利用这些解决方案的安全信号和风险评估功能。

配置

通过预先构建的工作流程，在 Cloudflare 仪表板中点击数下，即可完成这些提供商的配置。设置完成后，Cloudflare 可以在允许或拒绝访问受保护的应用程序之前，检查设备是否正在运行您首选的端点软件，以提供对恶意软件和其他威胁的持续监控。

由我们的设备客户端(WARP)增强的集成

升级安全性通常需要设备客户端，它可以用附加属性来丰富设备态势检查。我们的产品经过专门优化，以便于灵活和轻松采用。

部署到大部分操作系统

- 我们的企业客户端 —— WARP ——兼容越来越多最流行的操作系统（例如Windows、macOS、Linux、iOS、ChromeOS 和 Android）。
- 我们的现代 WireGuard 架构仅需要极少的操作系统特定代码调整。
- 我们的企业客户端有一个消费者版本，每天被全球数百万人使用。如此大量个人用户的测试意味着，WARP 比大多数用于 Zero Trust 的客户端做好了更充分的实战准备。

托管或自助注册选项

- 对于托管设备，我们用任何基于脚本的方法在流行的移动设备管理（MDM）软件中记录部署情况。
- WARP 的自助注册对第三方用户非常有用，任何桌面或移动设备都只需要几分钟时间。

避免云提供商锁定

问题

一些较为独立的供应商主要关注如何让您增加其云服务的消费，尤其是在存储和计算层。

毫无疑问，他们的附加安全解决方案与其他云提供商的集成并不会那么顺利。文档化较弱、程序错误等小麻烦接连不断。技术堆栈锁定会让您的信息技术团队更加头疼。

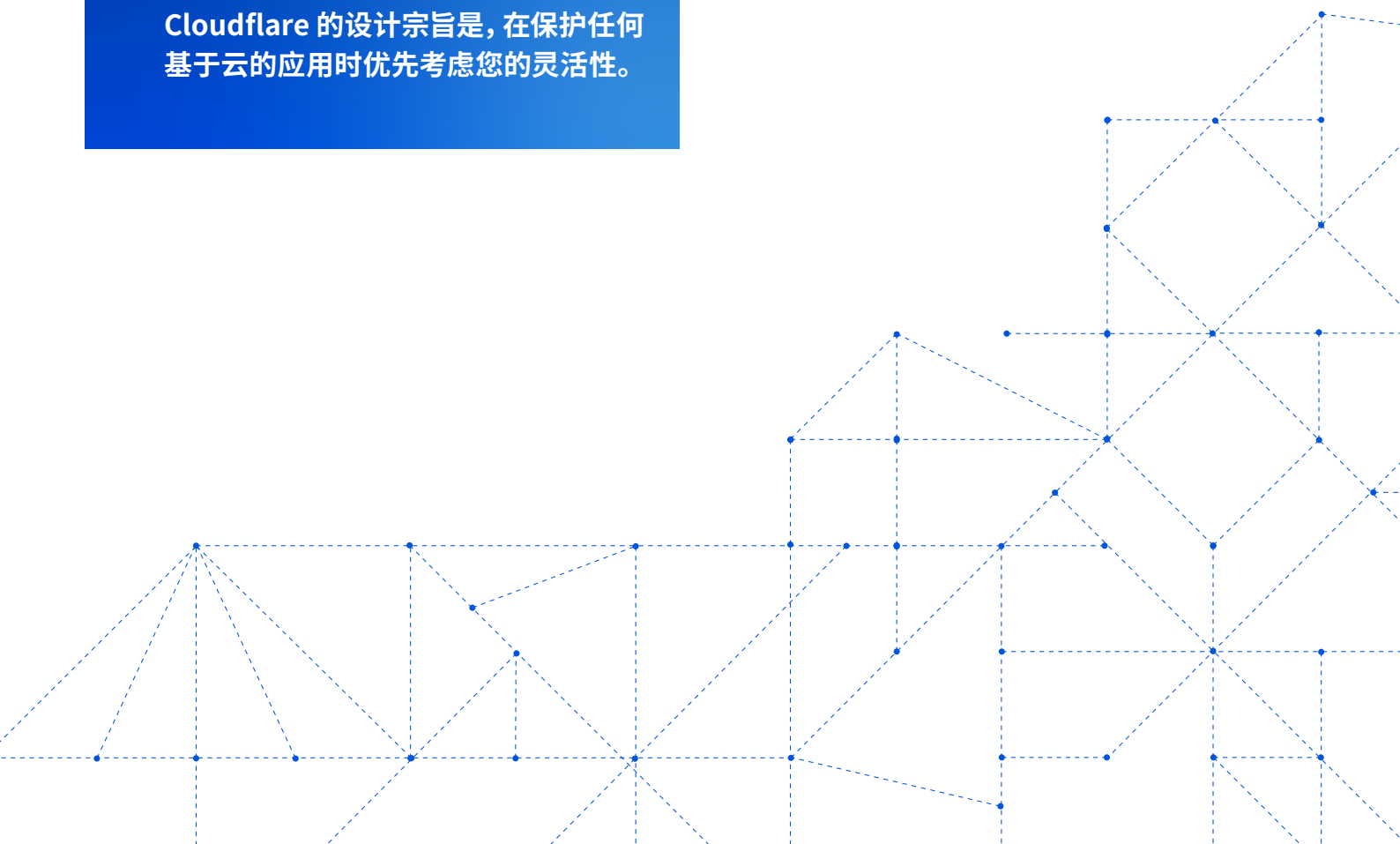
解决方案

相比之下，我们的战略重点是您的安全，而不是您的云消费。Cloudflare 与云无关：我们保护对任何公有、私有或 SaaS 云环境中任何资源的访问。

关键功能

- 跨公有、私有和 SaaS 云环境的 Zero Trust 访问
- 不锁定云计算或存储服务提供商
- 提供应用连接器、网络入口合作伙伴和存储集成，使您可以轻松地与任何云中的应用进行交互

Cloudflare 的设计宗旨是，在保护任何基于云的应用时优先考虑您的灵活性。



Cloudflare 的优势

将连接扩展到任何云中的应用

我们的轻量级应用连接器能在任何云中工作

- 在 Linux 和其他操作系统上以服务形式运行命令行工具
- 预先打包为 Docker 容器
- 对现代 Kubernetes 环境的副本支持
- 可通过用户界面配置和监控隧道

与云提供商的广泛互连

- 我们的网络与其他云提供商建立了 1.1 万个互连，其中 50 个为与 Microsoft、Amazon 和 Google 数据中心之间的专用互连，从而实现用户的快速连接

多样化的网络入口合作伙伴，不受云平台限制

- 使用您现有的 SD-WAN 路由方法 (例如 VMware)，或在超过 1600 个共置提供商地点建立专用互连 (例如 Equinix)，轻松将任何公有和私有云环境连接到我们的网络

推送日志数据到任何云

日志数据可存储到任何云，或直接发送到分析提供商

- 内置支持一个或多个存储目的地，包括 AWS、Azure、Google Cloud 和任何 S3 兼容的 API (例如 Digital Ocean Spaces)
- 内置分析和 SIEM 工具集成，例如 Sumo Logic、Splunk 和 Datadog

跨任何公有或私有云的安全性

Zero Trust 集成合作伙伴名单

随着时间的推移，Cloudflare 将从更广泛的首选供应商名单中聚合信号，
并由我们的 Zero Trust 平台和全球网络提供的情报予以增强。

身份提供商

企业 SSO

- Centrify
- Citrix ADC©
- Google Workspace
- Jumpcloud
- Microsoft Azure Active Directory (AD)
- Okta
- OneLogin
- PingIdentity

社交网络账号

- Facebook
- Github
- Google
- LinkedIn
- Yandex

开源

- OIDC
- SAML 2.0

端点提供商

端点保护提供商

(设备安全态势)

- Crowdstrike
- Microsoft Endpoint Manager
- SentinelOne
- Tanium
- Uptycs
- VMWare Carbon Black

端点管理提供商

(客户端部署)

- Hexnode
- Ivanti
- Jamf
- Jumpcloud
- Kandji
- Microsoft Intune

网络入口合作伙伴

物理互联合作伙伴

- 365 Data Centers
- BBIX
- CoreSite
- Cyxtera
- Databank
- Digital Realty
- EdgeConneX
- Equinix
- Netrality Data Centers
- Teraco
- Zayo

结构互联合作伙伴

- Console Connect / PCCW
- CoreSite
- Epsilon Infiny
- Equinix Fabric
- Megaport
- PacketFabric

SD-WAN

- Aruba (Silverpeak)
- Cisco
- VMWare (Velocloud)

云提供商

云储存目的地

- AWS S3
- Google 云存储
- Microsoft Azure Blob Storage
- 其他使用 S3 兼容 API 的供应商

云分析与 SIEM 合作伙伴

- Azure Sentinel
- Data Dog
- Elastic
- Google Cloud
- Graylog
- IBM QRadar
- Looker
- New Relic
- Splunk
- Sumologic

要进一步了解Cloudflare Zero Trust，并向销售代表请求演示或概念验证（POC），
请访问：https://www.cloudflare.com/products/zero-trust。

010 8524 1783 | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES-3795.2022SEP26