CLOUDFLARE

解决方案简述

云和本地基础设施的特权访问

简化对基础设施目标的访问 (authN/authZ/audit)——而不干扰开发人员的工作流程。

过度特权问题

虽然很多组织已经采用了 Zero Trust 倡议来现代化应用和网络的安全访问，但基础设施安全或特权访问管理 (PAM) 策略大多依然是孤立、过于复杂或无效的。

- **风险太大：**长期存在和共享的密钥极易被滥用，增加过度权限和横向移动相关风险
- **过于笨拙：**手动凭据轮换，可见性差，影响管理员生产力

将 Zero Trust 控制扩展到基础设施

不再采用传统的 PAM 工具或构建自行开发的服务器访问或密钥管理解决方案，而是重新利用团队在 Zero Trust 网络访问 (ZTNA) 和相关 VPN 替代计划中已经使用的相同思维方式。

以应用访问的相同方式验证基础设施访问——利用现有的身份提供者组，使用单点登录 (SSO)、MFA 和设备上下文来构建策略。确保正确的用户才能访问正确的基础设施资源，并将全程一切活动记录到日志。

Cloudflare 的整合式方法

利用 ZTNA 融合特权访问

Cloudflare 充当聚合层，比其他安全访问服务边缘 (SASE) 供应商更进一步扩展了现代身份和访问管理 (IAM) 工具以及细粒度、基于上下文的验证。这意味着：

- 将 VPN 替代的范围扩展到组织最敏感的基础设施资源，而不仅限于应用和网络
- 通过整合特权开发人员访问和一般员工/承包商访问来降低总拥有成本

Cloudflare 现代化基础设施的特权访问

降低风险

防止 SSH 密钥泄漏，并消除可能暴露基础设施的过度特权风险。

简化运营

避免传统 PAM 或 DIY 解决方案的复杂性，内置简单、细粒度的策略编辑器和审计日志功能。

支持开发人员工作流程

实施不会干扰开发人员、DevOps 或站点可靠性工程 (SRE) 团队原生工作流程的 Zero Trust 控制措施。

架构概述

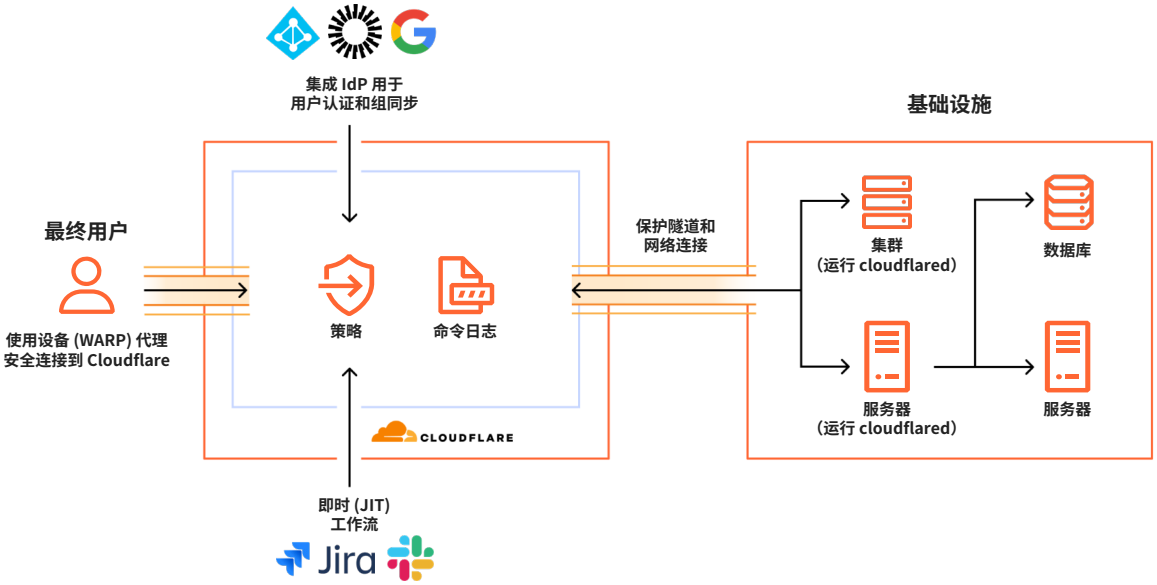

图 1：本图显示从 BastionZero 获得的技术被原生重新集成到 Cloudflare 的 ZTNA 服务中。有关当前已实现的支持功能的列表，请参阅“基础设施访问”技术文档。

工作方式

就针对目标而非网络的特权访问进行身份验证、授权和审计

- 为目标机器创建 Zero Trust 访问策略，并指定端口、协议和用户连接上下文（例如，*root* 或 *ec2-user*）。
- 融入开发人员现有工作流程——无需特殊 CLI 或命令，避免对开发人员造成任何干扰。
- 使用单点登录 (SSO)、多因素身份验证 (MFA)、设备态势和其他上下文进行身份验证。
- 提供清晰的可见性并记录每个最终用户命令，以支持合规审计要求。

为什么选择 Cloudflare 来管理基础设施访问?

市场上最全面的 ZTNA 解决方案

没有其他 SSE/SASE 供应商能在提供常规用户对应用访问的同时，就基础设施访问提供对 DevOps 友好的 Zero Trust 控制。同时，各式各样的基础设施访问初创公司都不过在吹捧另一个单点解决方案。

Cloudflare 的 ZTNA 服务帮助组织将传统的 PAM 或自建服务器访问能力整合到一个更广泛的 VPN 替代计划或 SASE 架构实施过程中。全部通过 Cloudflare 的全球连通云——世界最大、最快、最可靠的网络之一。

想要了解更多？查看我们的分步技术文档，或请求一次对话。

