保护员工的生成式与智能体式 AI 使用

通过 Cloudflare 的 SASE 平台提供的保护措施，助力您的团队安全地使用任何 AI 工具。

重获控制并释放生产力

快速采用 AI 带来一系列不断增加的风险，包括数据泄露、监管违规和攻击面扩大。完全禁止 AI 只会牺牲您的竞争优势，而使用单点解决方案只会增加复杂性。

Cloudflare 通过在所有 AI 环境扩展可见性、降低风险并全面保护数据，有效确保组织的 AI 使用安全：

- **发现影子 AI** 并管理针对所有已批准和未批准 AI 工具的策略。
- **加强 AI 治理**——利用基于身份的访问控制和态势管理。
- 通过屏蔽用户提示词中的敏感信息，实施主题防护措施，并扫描 AI 工具中的错误配置，有效**防止数据丢失**。

扩展 Cloudflare 以安全地采用 AI。无论您的 AI 策略是将使用限制于特定应用内，还是尝试更广泛的各种工具。

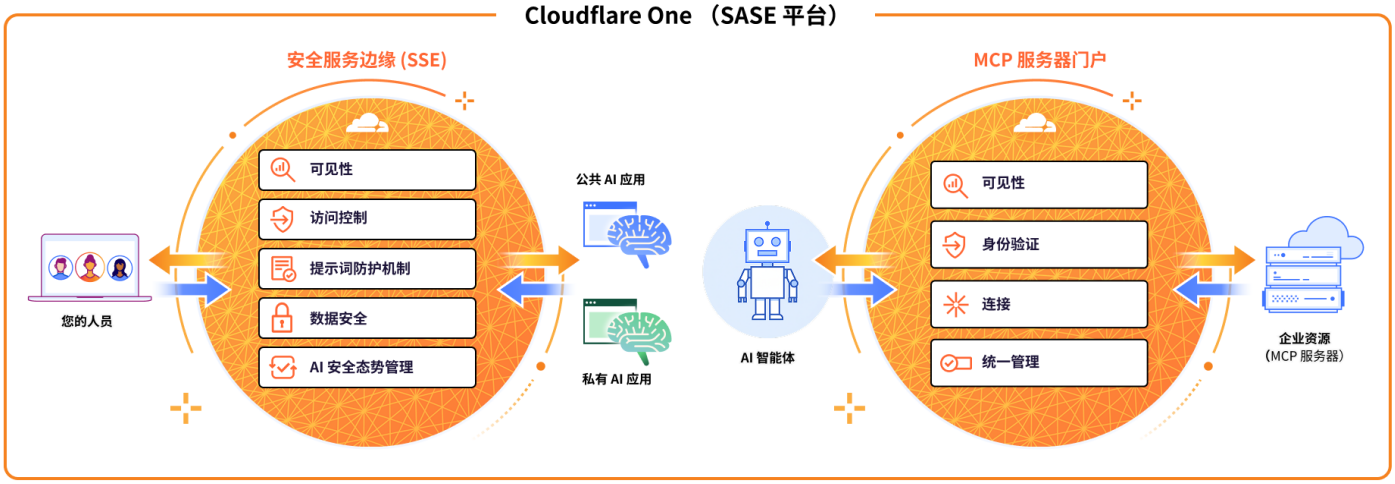
为什么选择 SASE 来保护员工使用 AI 的安全

Cloudflare 的安全访问服务边缘 (SASE) 平台位于您的员工和 AI 工具之间。这使得 SASE 成为许多企业安全地开始使用 AI 的理想起点。

无论是员工使用 ChatGPT 聊天，还是 AI 智能体在企业资源中收集信息，Cloudflare 的 SASE 平台都能执行一致的安全控制。

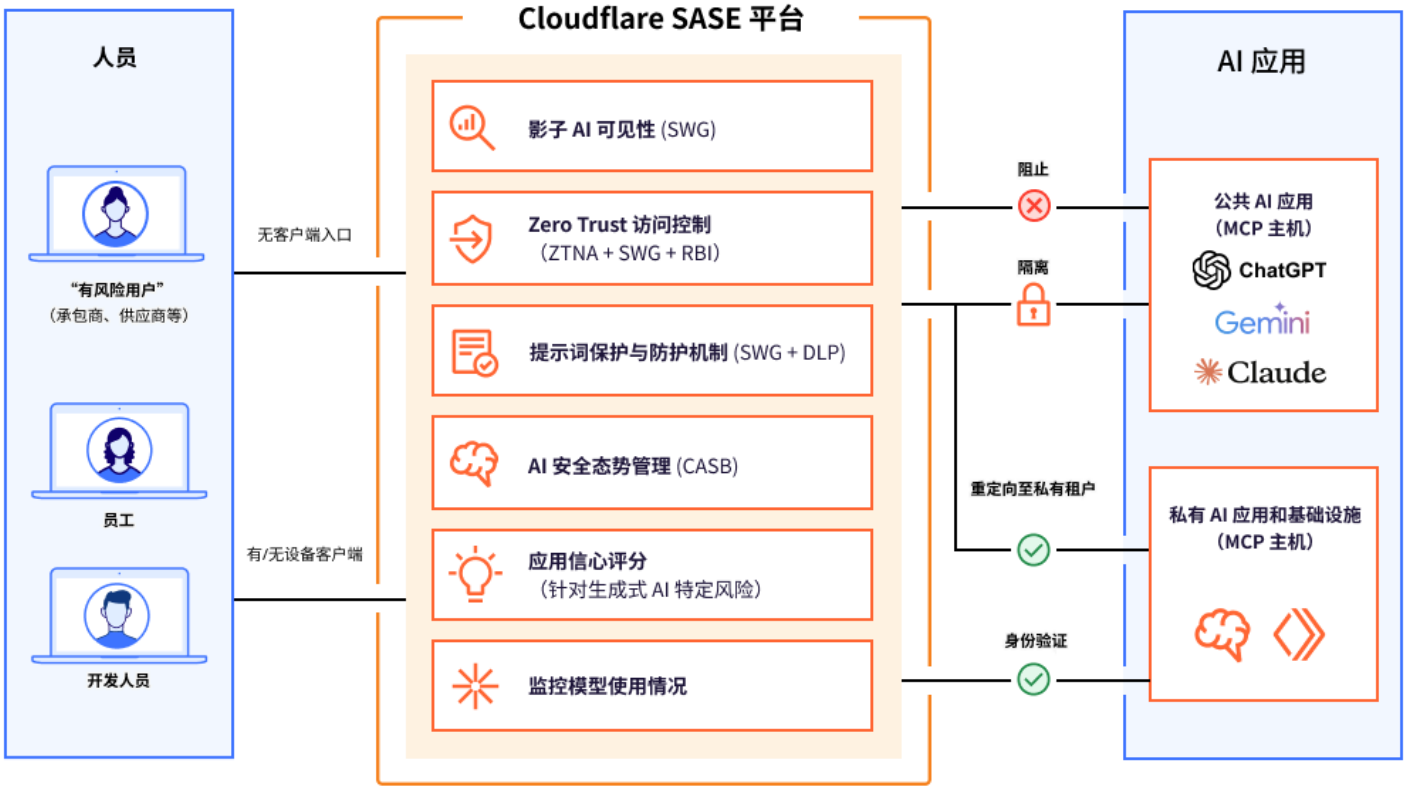
保护生成式 AI 与智能体式 AI 通信安全

Cloudflare 的 SASE 平台提供统一的仪表板和控制平面，以便轻松管理整个组织的人员与 AI 的交互以及机器与机器交互。



与其他 SASE 供应商不同，Cloudflare 还可以帮助连接和保护面向公众的 AI 驱动应用和工作负载（例如您网站上的 AI 聊天机器人或推荐引擎）。

通过 Cloudflare 的 SASE 平台上的 AI **使用控制，保护用户与生成式 AI 应用的通信安全**



- **可见性：**通过内联流量检查，发现并分析影子 AI 的使用。通过透明度评分评估这些 AI 应用带来的风险。
- **访问控制：**阻止、隔离、重定向或允许用户连接。按应用强制执行基于身份的 Zero Trust 规则。
- **提示词保护和防护措施：**根据意图（例如，越狱尝试、代码滥用、个人身份信息请求等），检测并阻止用户提示词。
- **数据安全：**利用 AI 驱动的数据丢失防护 (DLP) 检测，阻止 PII、源代码等敏感数据泄露。
- **AI 安全态势管理：**通过 API 与生成式 AI 工具集成（现已可用于 ChatGPT、Claude 和 Google Gemini），使用我们的云访问安全代理 (CASB) 扫描配置错误。

客户成果

世界第一大求职网站

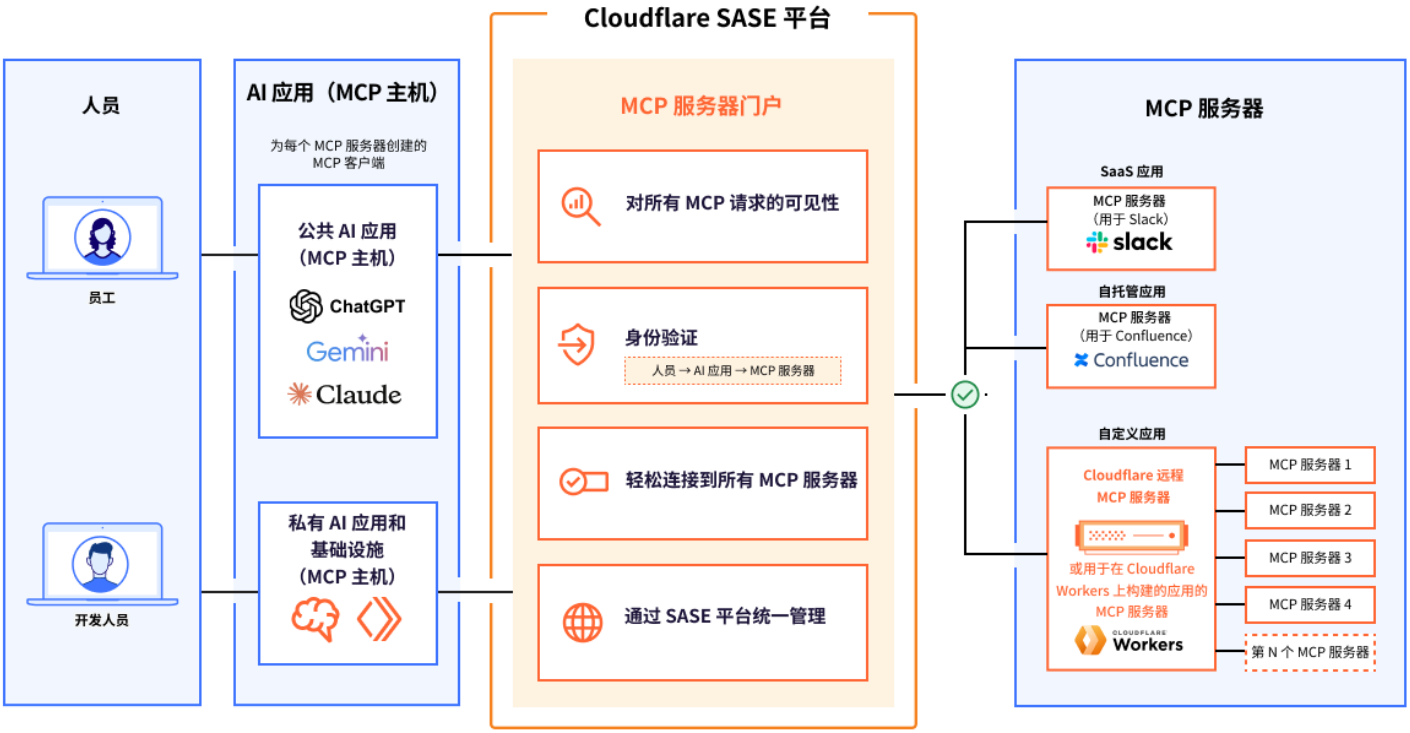
在开展 VPN 替代项目的同时**识别并控制影子 AI**

保险科技公司

隔离 ChatGPT 等公共生成式 AI 工具 以阻止复制粘贴敏感数据

 | 010 8524 1783 | enterprise@cloudflare.com | www.cloudflare.com/zh-cn/

通过 Cloudflare SASE 平台上的 MCP 服务器门户，**保护智能体式 AI 通讯（AI-资源）安全**



- **可见性：**聚合所有 MCP 请求日志，用于审计和分析。在添加到门户之前，审核并批准每个 MCP 服务器。
- **身份验证：**对访问门户的用户进行身份验证。根据最小权限原则限制对 MCP 服务器的访问范围。
- **连接：**使用单个 URL 连接所有可访问的 MCP 服务器，无需单独配置每个 MCP 服务器。
- **统一管理：**对 AI 连接实施与人类用户相同的细粒度访问策略。
- **自定义每个门户的工具：**选择每个用户可用的特定工具和提示词模板。

注意：Cloudflare 的 MCP 服务器门户支持任何 MCP 服务器，包括（但不限于）在 Cloudflare 上构建或部署的任何远程 MCP 服务器。此功能以 Zero Trust 网络访问 (ZTNA) 控制形式提供。

参阅此博客以详细了解我们的愿景。

准备好了解 Cloudflare 如何保护您的 AI 使用了吗？

申请研讨会

