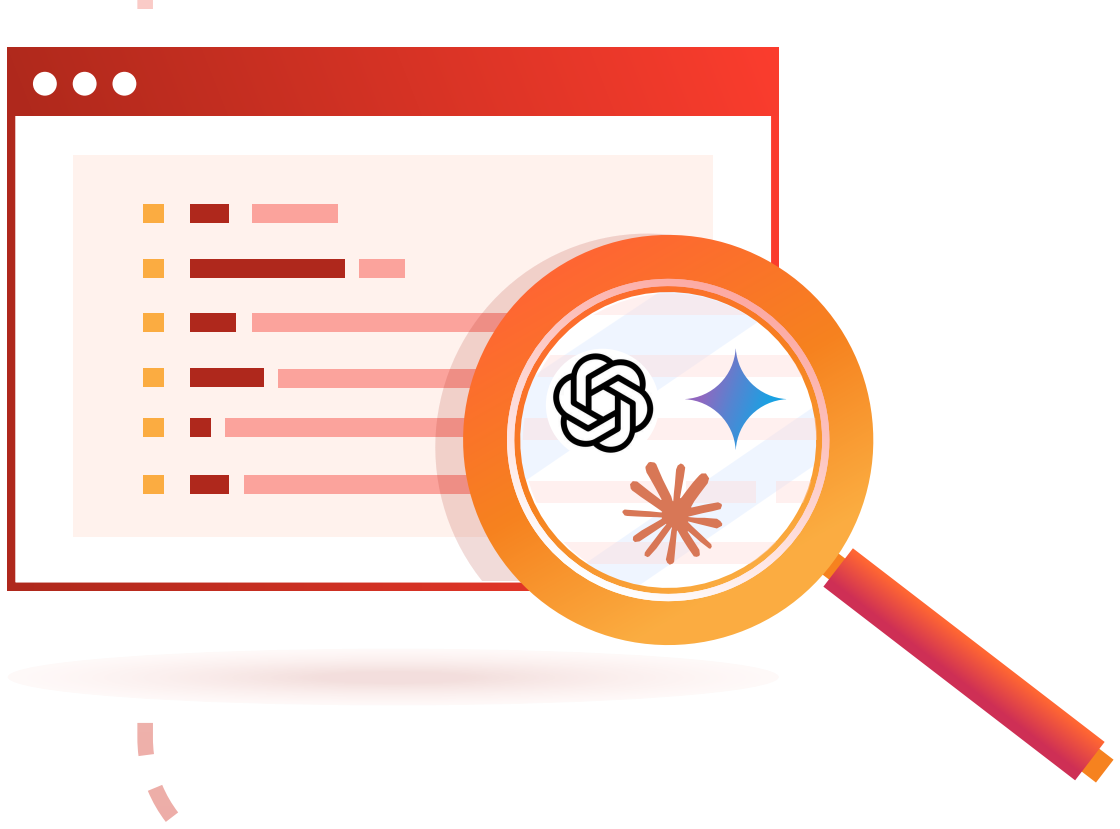
CLOUDFLARE

以安全设计加速 AI 应用落地

AI 时代已至，传统安全模式已然落伍

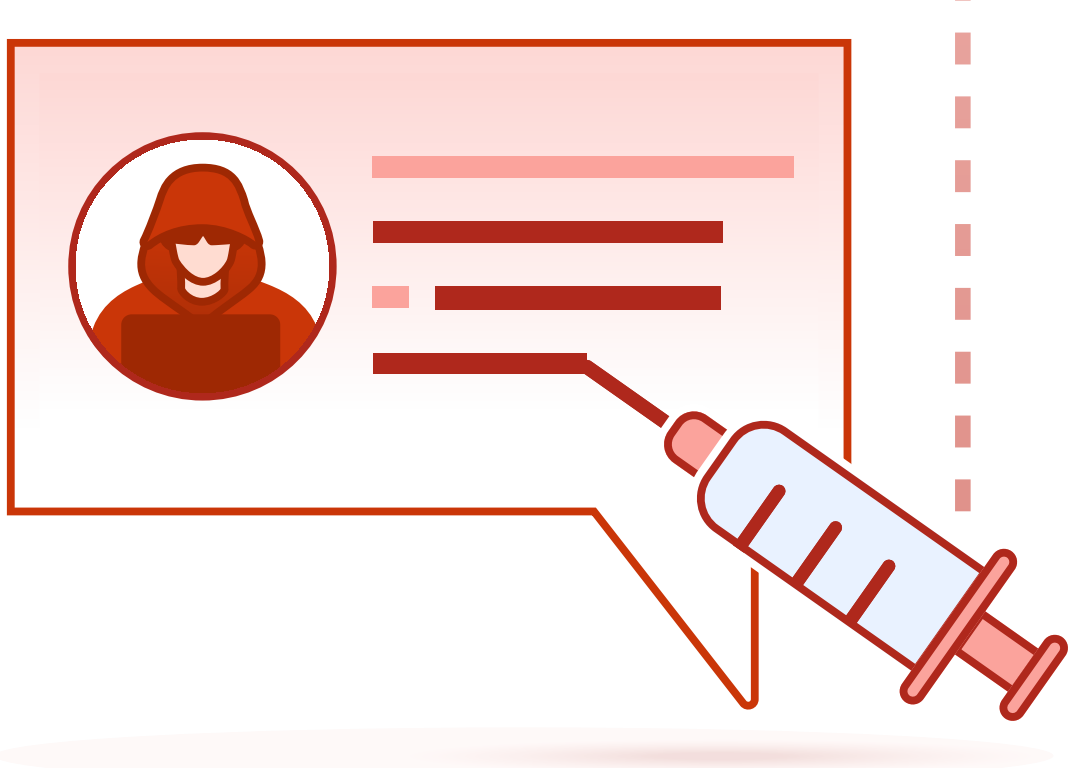


98%

98% 的组织存在未经批准的应用，包括影子 AI。这些盲点会带来数据暴露和违规风险。[1]

50%

提示词注入攻击成功率达到 50%，在 OWASP LLM 应用十大安全威胁中排名第一。[2]



97%

在经历过 AI 相关安全事件的组织中，97% 缺乏适当的 AI 访问控制。[3]

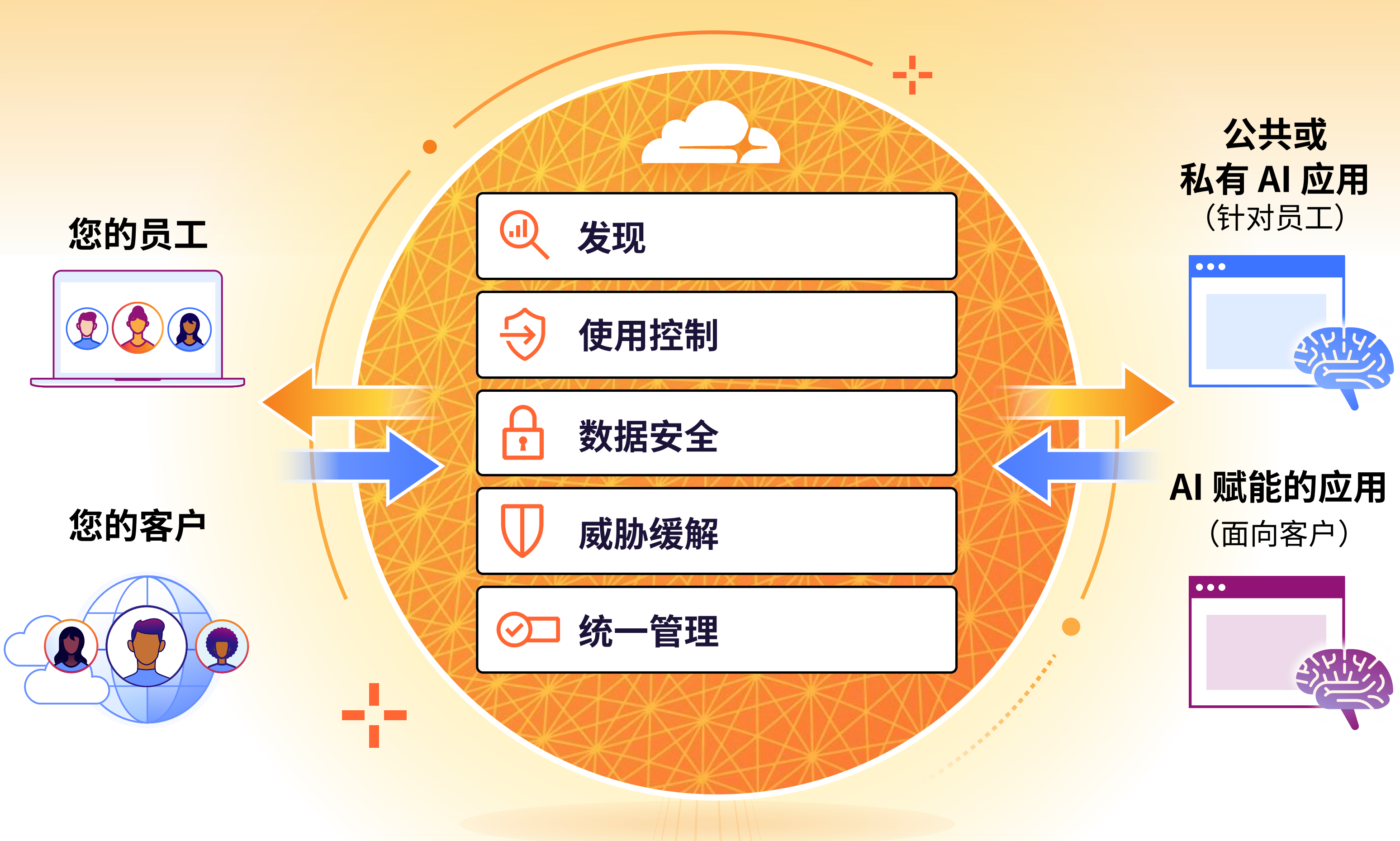
93%

93% 的员工承认曾在未经批准的情况下将信息输入到 AI 工具。[4]

使用 Cloudflare 保障 AI 生命周期安全

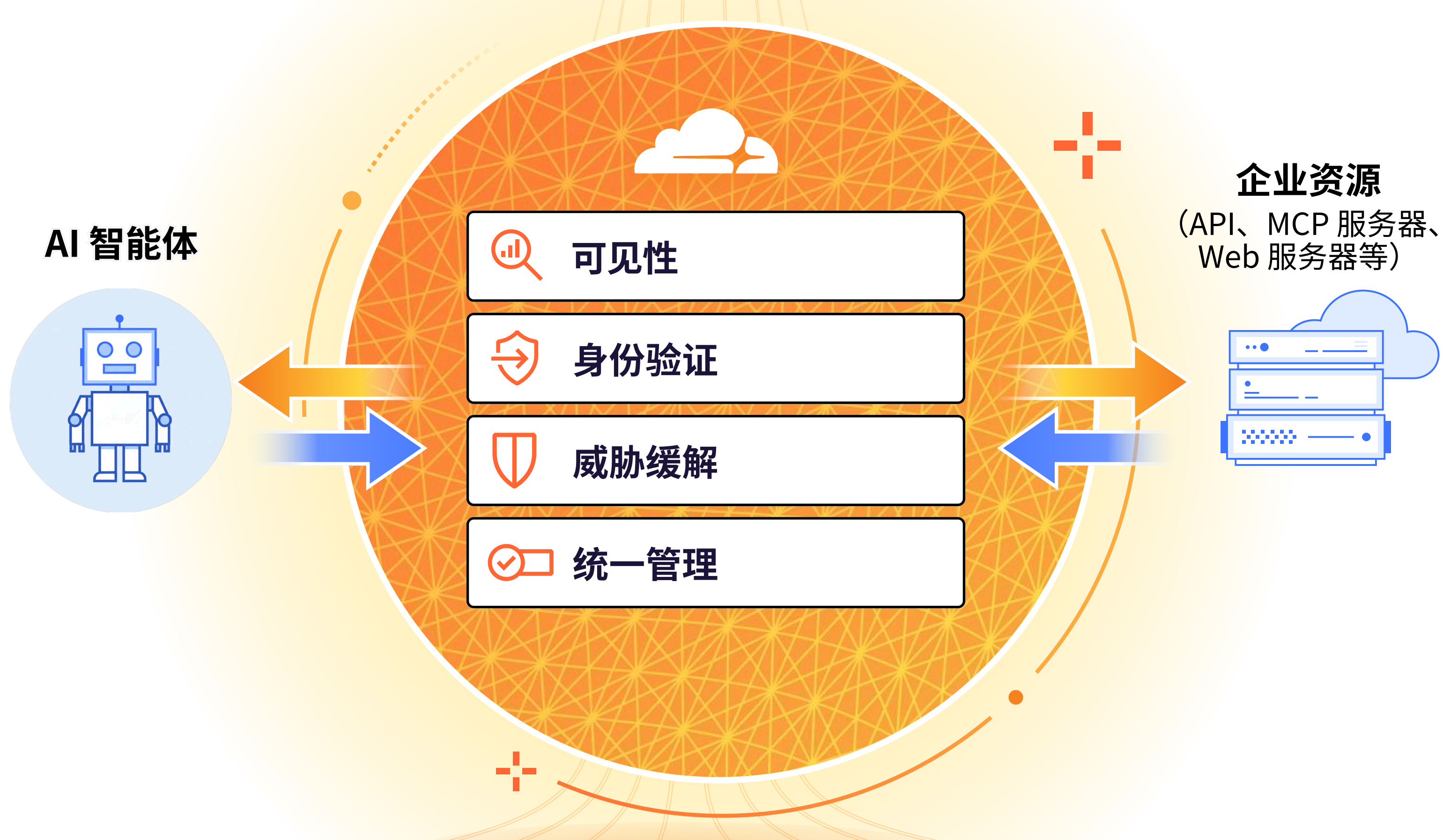
包括生成式 AI 与智能体式 AI

人类-AI 交互安全



- 发现
- 使用控制
- 数据安全
- 威胁缓解
- 统一管理

智能体式 AI 安全



- 可见性
- 身份验证
- 威胁缓解
- 统一管理

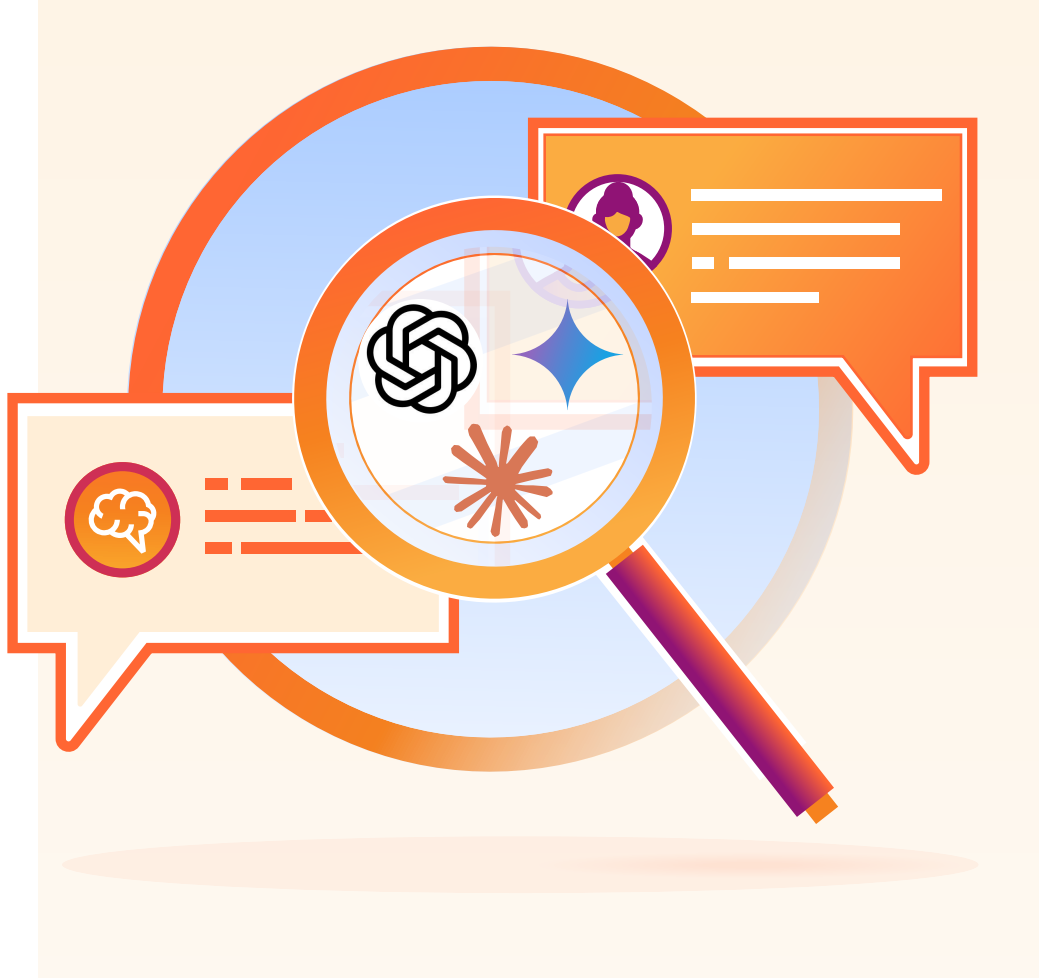
扩展可见性
覆盖 AI 应用、API 端点以及 AI 智能体和 MCP 连接

管理风险
通过防护机制、态势控制和实时威胁缓解

保护数据
通过针对员工和 AI 智能体的提示词保护和访问控制

内置安全保护

在 Cloudflare 上开发 AI



保护员工使用生成式 AI 的安全

- 发现影子 AI
- 评估 AI 应用的风险
- 管理 AI 应用态势
- 限制敏感数据输入
- 在提示词和响应中实施防护措施

保护 AI 驱动的应用和工作负载

- 发现影子 AI 端点
- 保护 AI 模型和训练数据以防滥用
- 防止提示词和响应中泄露 PII
- 执行内容审核

保护您构建的内容

- 构建内置身份验证/授权的 MCP 服务器
- 记录并限制 AI 模型的请求/响应、令牌使用和成本
- 通过模型回退和速率限制防止服务中断

Cloudflare 的不同之处

全面的 AI 生命周期保护
统一平台保护从开发到部署的用户与 AI 及 AI 与资源间的通信安全。

实时内联 AI 安全防护
通过覆盖公共和私有 AI 环境的控制措施，实时保护 AI 提示词和响应安全。

面向未来的全球 AI 架构
利用我们的全球网络实现一致的边缘执行，满足 AI 所需的规模和性能。

模型中立部署
安全控制适用于组织环境中的所有 AI 模型，为 AI 部署治理提供统一方法。

客户案例研究

indeed
世界第一求职网站
识别和控制影子 AI
同步推进远程访问现代化项目

AI 赋能的 SaaS 公司
保护 PII
防止客户向公共生成式 AI 端点提交敏感信息

Cyndx
AI 驱动的金融科技公司
推理成本降低 95%
采用 Cloudflare 缓存并运行来自 AI 模型提供者的响应

了解 Cloudflare 如何保护您的 AI 应用安全

探索用例

---

1. Varonis，2025 年数据安全现状
2. Liu, S.、Wang, Z.、Chen, Y.、Deng, G.、Liu, Y. & Liu, Y. (2024)。针对大语言模型的自动和通用提示注入攻击。
3. IBM，2025 年数据泄露的成本
4. ManageEngine, 企业影子 AI 激增

1 888 99 FLARE | enterprise@cloudflare.com | enterprise@cloudflare.com Cloudflare.com

REV:BDES-8274.2025OCT13

CLOUDFLARE