CLOUDFLARE

解决方案简介

保护您的敏感数据

更佳的网络架构，实现更有效、更高效和更敏捷的数据保护。

统一保护无处不在的数据

数据保护并非新的强制要求，但向混合云架构的转变以及快速采用 AI 带来了新的挑战：

- **93% 的员工**承认在未经批准的情况下将信息输入 AI 工具[1]
- **79%** 的国家/地区已实施数据隐私法规[2]

Cloudflare 在数据的整个生命周期中执行一致的控制：

- **在任何地方提供保护：**对 Web、SaaS、电子邮件和云流量执行一致的控制。
- **阻止 AI 泄露数据：**分析生成式 AI 提示词以阻止敏感数据泄露并管控 AI 使用。
- **管控数据风险：**发现和管理影子 IT/AI，并使用 CASB 扫描 SaaS/云应用。

“这些未经授权的 AI 工具崛起使我们重新审视自己的安全策略。我们正在研究 SASE。”
*——信息安全主管**AllSaints***

为何选择 SASE 而非企业 DLP?

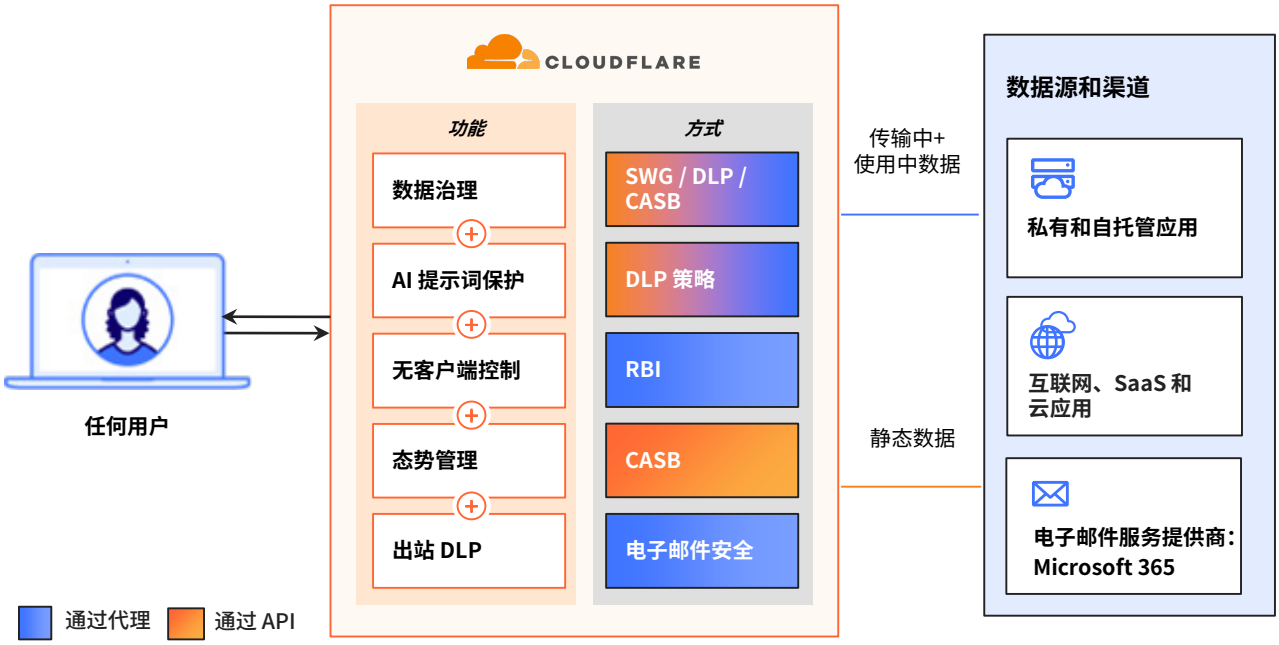
Cloudflare 的安全访问服务边缘 (SASE) 平台设计为位于您的员工与所有应用及数据源之间。这使得 SASE 成为许多企业安全保护数据的理想起点。

无论员工是访问 SaaS 应用中的数据、下载敏感文件，还是使用生成式 AI 工具聊天，Cloudflare 的 SASE 平台都能在所有数据交互中执行一致的安全管控。

工作原理

Cloudflare 的 SASE 平台部署于您的员工与资源之间，以统一可见性与管控。

通过 Cloudflare 的 SASE 平台，实现 AI 驱动的数据保护，
覆盖网络、SaaS、电子邮件和云流量



实时、内联数据保护

- **细粒度数据丢失防护 (DLP)：**通过上下文感知检测阻止 PII、源代码、客户数据等敏感数据泄露。
- **出站电子邮件 DLP：**自动标记出站电子邮件中的敏感数据，防止意外数据泄露。
- **提示词保护：**根据意图检测并阻止存在风险的 AI 提示词和响应（例如，越狱尝试、代码滥用、PII 请求）。

安全访问和客户端控制

- **安全应用访问：** 跨所有企业应用执行 Zero Trust 网络访问 (ZTNA) 规则，例如针对智能体 AI 连接的细粒度 DLP 防护扫描。
- **设备态势检查：**根据细粒度态势检查（例如磁盘加密和启用端点 DLP）控制访问。
- **无客户端控制：**采用基于浏览器的数据控制，以保障第三方访问和员工自带设备 (BYOD) 安全。

影子 IT 与态势风险

- **影子 IT 和 AI 发现：**发现和管理整个环境中的影子 IT/AI。使用应用置信度评分和数据传输指标量化风险，以快速缓解暴露。
- **态势管理：**扫描 SaaS 应用和云环境中的态势风险。采取规范性措施以修复安全检测发现的问题。
- **租户控制：**阻止 SaaS 应用的个人租户，以防止数据泄露。

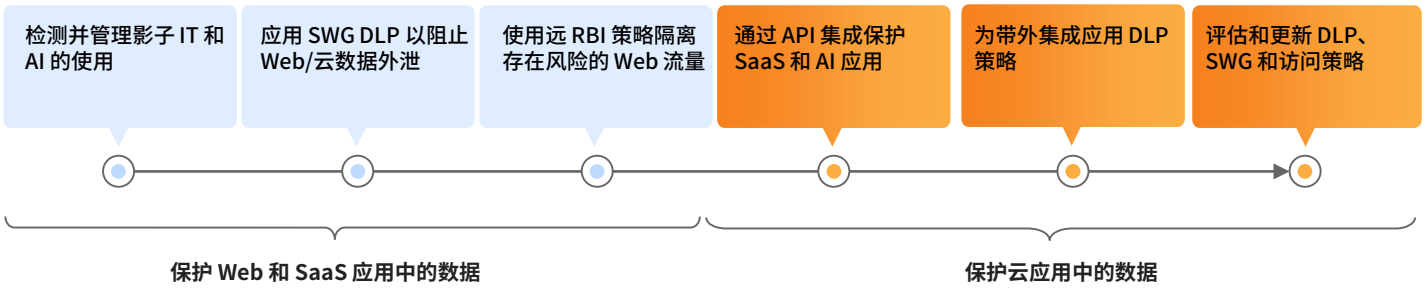
集成与报告

- **CASB 集成：**与领先的 SaaS 和 AI 平台 （包括 Microsoft 365、Google Workspace 和 ChatGPT）无缝集成，进行基于 API 的 CASB 扫描。
- **Microsoft MIP 集成：**与 Microsoft 信息保护 (MIP) 标签持续同步，以执行一致的 DLP 策略。
- **可观测性与取证：**将数据安全记录到您首选的安全信息和事件管理 (SIEM) 系统中以进行审计，或通过仪表盘或 API 即时分析日志。

数据保护历程示例

从发现影子 IT 和 AI 使用情况入手，掌握攻击面可见性。在 SWG 上配置基础 DLP 策略，以阻止来自未受管控云应用的高风险数据泄露，并对未批准的 Web 流量部署 RBI。

然后，部署 CASB，通过纠正错误配置和实施内部共享策略来保护获得批准的 SaaS 和 AI 应用。优化和集成跨 SWG、电子邮件和 CASB 的细粒度 DLP 和访问策略，针对所有主要数据流实现自动、统一的防护。



示例初始使用场景

- 在所有未经批准的通信和存储渠道**实时阻止 PII/PHI 泄露**。
- **保护源代码和知识产权 (IP)**，以防内部盗窃和未经授权的分发。
- **对生成式 AI 应用执行提示词保护策略**，以防止敏感数据暴露和模型污染。
- 针对所有 SaaS 和 AI 应用**防止错误配置**，并实施细粒度访问控制。

客户成果

EESTI RAUDTEE

基础设施提供者
阅读案例研究

缓解数据丢失和 SaaS 漏洞

通过识别数据泄露和错误配置。

APPLIED

保险科技公司
阅读案例研究

隔离 ChatGPT 等公共生成式 AI 工具

以阻止复制-粘贴敏感数据。

Flo

领先健康应用
阅读案例研究

保护患者数据

并通过电子邮件安全解决方案和 zero trust 实现合规。

CREDIT SAISON INDIA

非银行金融公司贷款机构
阅读案例研究

保护 PII 并实现合规

防止不必要的数据出站。

准备好讨论您的数据保护需求了吗？ 申请研讨会

1. 2025 年 Manage Engine 研究：来源
2. 2025 年联合国贸易和发展大会：来源

