适用于资料保护的 Cloudflare One

更佳的网络架构，实现更有效、更高效和更敏捷的数据保护。

统一保护数据

现代数据风险要求现代安全措施

今天，数据的容量、种类和速度都在爆炸式增长，组织面临着不断升级的风险，来自：

庞杂分散的云和 SaaS 环境
↳ 包括诸如 ChatGPT 那样不透明的新兴 AI 工具
↳ 导致宝贵的源代码被暴露

Cloudflare One 的数据保护套件正是为应对这些现代特有的风险而打造的。

通过将点解决方案统一到单一平台和网络上，Cloudflare 提供具备如下特性的数据保护：

- **更有效**— 简化连接和策略管理
- **更高效** — 确保在任何地方均提供快速、可靠、一致的用户体验
- **更敏捷** — 快速创新以满足您不断变化的安全需求

一个安全服务边缘(SSE)用于保护 Web、SaaS 和私有应用的数据

在您的 SSE 旅程中逐步采用 Cloudflar，以便：

1. 通过 Zero Trust 保护对数据的访问
2. 阻止网络钓鱼和勒索软件等威胁
3. 检测并锁定您最敏感的信息

应对不断升级的数据风险……

不断扩散的 SaaS 足迹

82%

的泄露涉及存储于云环境的数据。[1]

当然，数据泄露的成本也在持续上升——在过去 3 年里上升了 15%。[1]

多种多样的监管法规

71%

的国家已经实施保护数据和隐私的法规。[2]

在美国，**11 个州**现在已有全面的数据保护法律 —— 而 2021 年仅为 3 个。[3]

数字化转型

89%

的 CISO 表示，快速推进数字化转型计划在保护企业数据方面带来不可预见的风险[4]

用例 #1：保护开发人员代码

问题
代码会在许多开发工具中被暴露或成为盗窃的目标，包括公共代码库等明显的位置。

解决方案
扫描并修复配置错误而可能泄露代码的公共存储库，例如 GitHub。检测上传/下载中的源代码并应用控制措施。

→ GitHub
→ GitLab
→ Bitbucket

用例 #2：数据暴露可见性和风险管理

→ OpenAI
→ Bard
→ GitHub Copilot

问题
数据跨越不同的 SaaS 和云环境、未经批准的影子 IT 以及 ChatGPT 等新兴 AI 具，增加了泄露的风险。

解决方案
扫描SaaS套件是否存在配置错误，集成 DLP 检测敏感数据。获得对未批准应用使用情况的可见性，然后允许、阻止、隔离或通过 Zero Trust 控制访问。

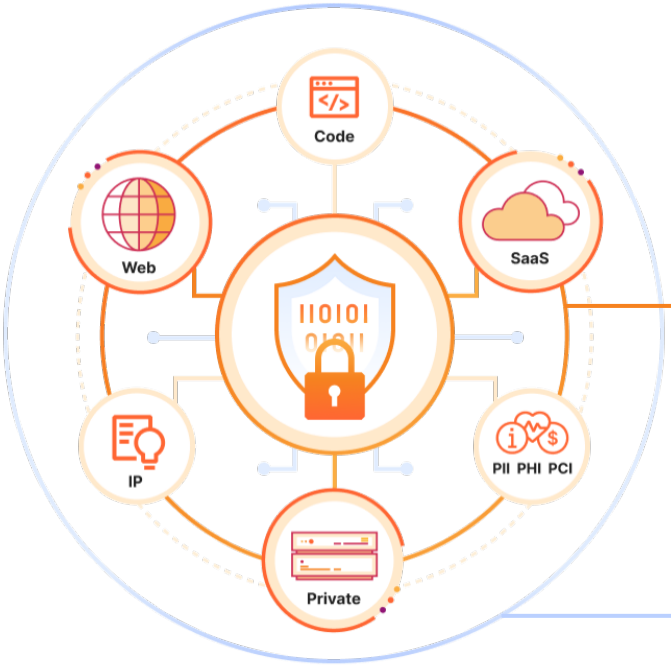
用例 #3：遵守法规

问题
企业面临更严格、更广泛的法律要求，以保证数据的安全和隐私，违规行为的罚款也在增加。

解决方案
识别并应用对受监管数据类别(PII、健康状况、财务信息)的控制。通过日志和进一步的 SIEM 分析维护详细的审计跟踪。通过全面的 Zero Trust 安全态势减少攻击面。

- ✓ GDPR
- ✓ DPDP
- ✓ CCPA
- ✓ CPRA
- ✓ GLBA
- ✓ PCI DSS
- ✓ HIPAA
- ✓ ISO
- ✓ 还有更多！

工作方式



统一平台

Cloudflare 将针对 DLP、CASB、ZTNA、SWG、RBI 和电子邮件安全服务的可见性和控制汇集到单一平台上，简化了管理。

一个可编程的网络

单一控制面板，包含基于我们自有开发人员平台打造的服务，对传输中、使用中和静态存储的数据实施控制，覆盖所有执行点，包括 Web、SaaS 和私有应用环境。

使用可组合服务进行控制的示例

对传输中数据应用 DLP，保护访问

- 扫描流量和文件中的敏感数据，通过 DLP 配置阻止策略。
- 使用 CASB 发现和管理影子 IT。
- 使用 ZTNA 保护对应用中的数据的访问。
- 阻止 SaaS 应用的个人租户，以防止数据泄露。

隔离应用以保护使用中的数据

- 阻止复制/粘贴、上传/下载、打印，键盘输入 —— 无需安装设备客户端。
- 无客户端部署非常适合非受管设备、第三方用户和 ChatGPT 等 AI 工具。
- 在独立的应用程序中应用 DLP 策略。

保护 SaaS 应用中的静态数据

- 扫描 SaaS 应用中的可疑活动、错误配置和敏感数据。
- 采取预防性措施，通过 SWG 策略纠正风险。

集成以简化合规和控制

- Logpush 到首选 SIEM 以供关联和审计
- 与 18 个最流行的 SaaS 套件集成，进行基于 API 的 CASB 扫描。
- 为您的 DLP 策略持续同步 Microsoft 信息保护标签。

Cloudflare 提供更佳的数据保护

更有效
— 降低复杂性

通过许多灵活的选项简化连接，将流量发送到 Cloudflare 供执行控制。

使用基于 API 的扫描检查 SaaS 套件，或 ZTNA 和 RBI 的无客户端模式，保护对应用的访问。对于转发代理流量，使用设备客户端，或跨安全服务的广域网入口。

更高效
— 改善用户体验

我们的网络无处不在，确保在靠近最终用户和数据的地方通过单次通过检查执行控制。

可靠且无干扰的最终用户体验意味着执行数据控制绝不打断工作。实证比同类 SSE 更快。

更敏捷
— 快速创新

我们拥有可编程的网络架构，能够快速构建各种功能，帮助您灵活地应对新风险。

我们迅速采用新的安全标准和协议（例如纯 IPv6 连接或 HTTP/3 加密），使数据保护始终最新。

客户感言

“今天，Cloudflare One 帮助防止我们的用户与 ChatGPT和 Bard 等工具共享敏感数据和代码，使我们能够安全地利用人工智能……展望未来，我们对 Cloudflare 为保护数据而进行的持续创新感到兴奋，尤其是他们有关数据丢失防护(DLP)和云应用安全代理(CASB)等服务的愿景和规划。”

Tanner Randolph
首席信息安全官(CISO)

Applied Systems
阅读案例研究

其他用例

- **财富 500 强天然气公司**保护承包商的数据访问
- **美国大型求职网站**保护代码和个人信息
- **美国地区航空公司**降低暴露客户数据的风险
- **澳大利亚医疗保健公司**保护受监管的医疗数据
- **美国医疗器械制造商**简化 HIPAA 合规

常见的采用路径

立即开始

了解……

不断升级的数据风险，请查看信息图

了解……

平台如何工作，请观看演示

证明……

价值，请预约一次咨询

1. IBM《2023 年度数据泄漏成本报告》
2. 联合国贸易和发展会议
3. 国际隐私专业人士协会(IAPP)
4. 《2023 年“CISO 现状”》报告