API访问管理

API的权限漏洞已经成为企业重要的风险之一

安全

保护端到端的身份

数据安全与合规

数据隔离和保障身份数据安全与隐私合规

权限与API

发现越权漏洞与提供修复方案

高度灵活端模型支持

威胁发现

建立与威胁情报端连接，AI工作流自动化响应

通过API授权服务器，将访问策略设计节省到几分钟

1天

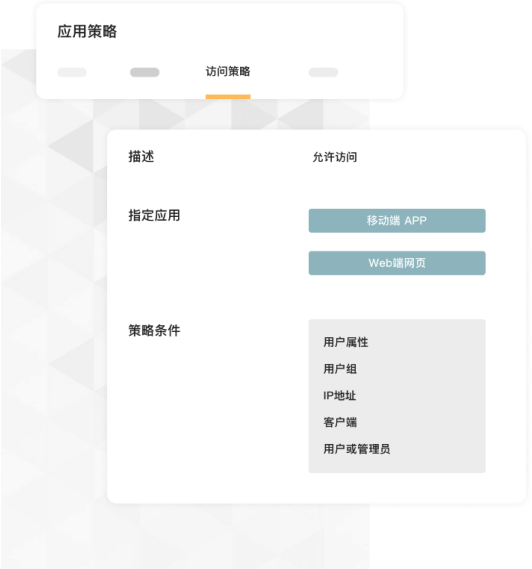
API的权限的集成从数周缩短到1天

2小时

为合作伙伴提供API的周期缩短到小时

35分钟

通过可视化视图调整API权限策略缩短到分钟级别



将身份验证和授权策略扩展到 API

已经对应用进行了访问控制，足够了么？这只完成了第一步，还需要对API进行保护

防止 API 违规

API安全漏洞已经影响到所有行业和组织。API的安全隐藏在应用程序的候端，但对于攻击者来说，缺乏保护的API是最容易攻击的目标。

现代 API 安全性

轻松实施 API 安全最佳实践和 OAuth 等现代身份框架。根据应用程序、用户上下文和组成员身份创建 API 授权策略，以确保只有合适的人才能访问。

从一个中央控制点 查看、管理和保护您的 API访问

无需在 API、网关和应用程序之间传播策略，而是集中管理它们

安全和开发，完美结合

将您的安全和开发团队团结在一个集中的地方，以实现您的所有 API 授权策略。

简化的授权策略

简化您的策略创建、维护和审核，让您的安全团队的生活变得更加轻松。随着授权策略随时间变化，他们可以集中调整它们，所有下游应用程序都可以使用修改后的权限。

更多的开发时间

开发者可以将用户管理、API授权相关的复杂设计完全交给XAuth，从而将节约的时间更加专注在核心的业务开发上