

# 领先的身份互联网解决方案提供商

企业的下一代 IT 身份基础设施

## Q当前场景面临挑战

..

01

身份体系分散，统一治理难

02

账密分散，安全漏洞多

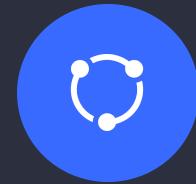
03

身份和业务紧密耦合  
难以适应快速变化的业务

04

用户登录体验欠佳  
IT 管理效率普遍不高

## 传统系统存在的问题



运营能力弱，传统 IAM 账号中心的运营能力较弱，难以满足大型组织在业务方面的需求，例如，筛选出六个月内未登录过的用户，并向他们发送营销短信；或找到那些高频使用的用户并交由客户经理转化商机。



缺乏伸缩性和扩展性，当企业的用户量不断上升时，用户系统承载的压力也会不断增加，传统的 IAM 主要靠堆积服务器和设置负载均衡来优化，但登录失败的次数总是随着用户量的增长而增长，这对企业和用户来说都是灾难。



运维费用高，大多数 IAM 专家难以雇佣并且费用高昂。而且当企业计划将内部员工训练成专家时，他们面临着将训练好的员工流失到咨询公司或竞争对手那边。



安全性欠佳，数据资产正在逐渐超越实体资产成为企业最有价值的核心。而针对数据资产的盗窃和攻击也呈不断上升趋势。传统的 IAM 在本地构建，难以保障混合云环境下的企业安全，权限管理颗粒度较粗，访问控制策略单一。



难以更新换代，大多数企业的 IAM 系统需要消耗巨大的人力物力去更新换代，而当企业耗尽千辛万苦将系统更新好了之后，市面上又出现了新的技术和系统。

# 构建统一内外用户体系



不带业务属性



统一数字身份 (UID)

姓名 | 身份证号 | 手机号 | 邮箱 | 生物特征

# Authing 如何拓展传统 IAM





# 云原生架构

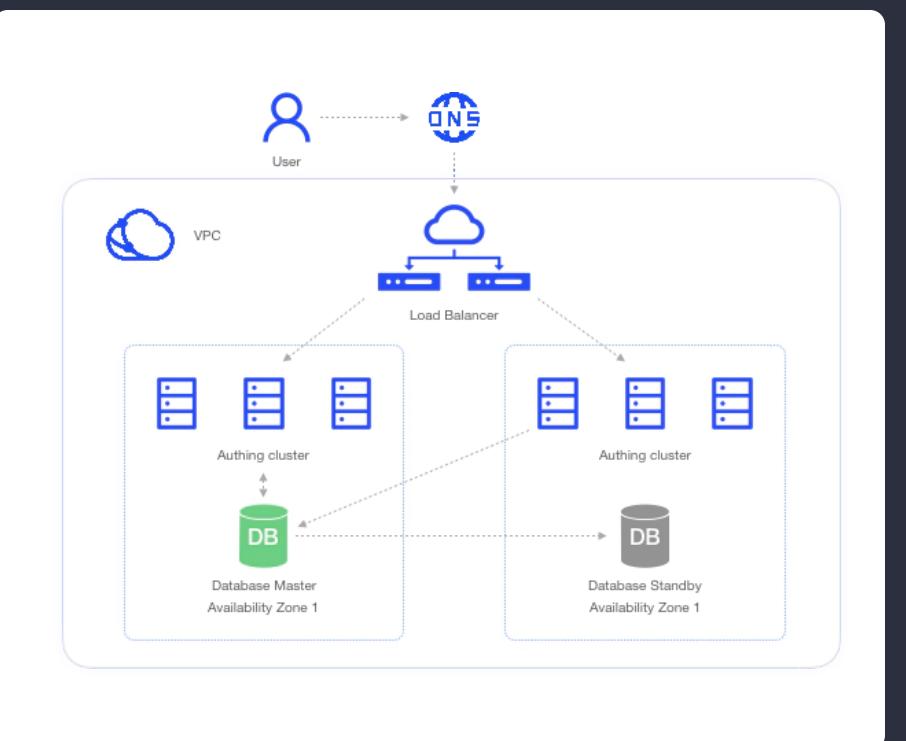
a.

伸缩性



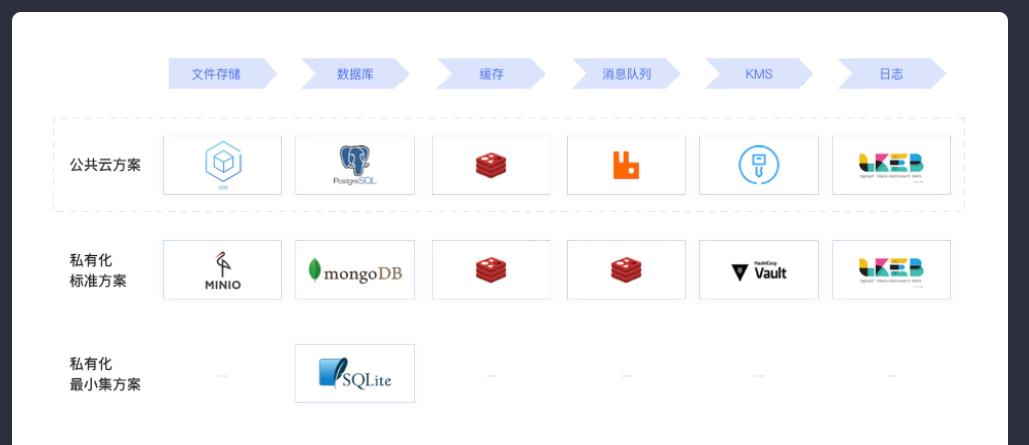
b.

高可用



c.

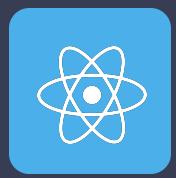
多云化部署



a.

## 新系统开发

### API / SDK



React Native



JavaScript



Android



Java / Kotlin



Swift



Node.js



Python



.NET



Flutter



鸿蒙 OS



PHP



微信小程序



GO

b.

## 旧系统集成

### 应用集成网关

老旧系统无需改动或仅需要做较少的改动，即可集成到 Authing 中来，既拥有多样化的认证方式，又拥有强大的基于策略的动态权限判定功能。

### 自定义数据库

自定义数据库支持

使用自己的数据库保存用户数据

惰性迁移用户到 Authing

### 自定义密码加密

此功能适用于以下场景：

- 你将所有用户迁移进了 Authing，但不想让用户修改密码；
- 你想使用自己的密码加密算法；

# 统一登录认证

· · ·

a.

## 单点登录



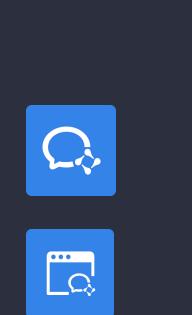
b.

## 20+ 社会化登录方式

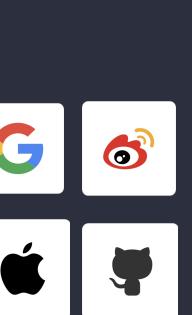
微信生态



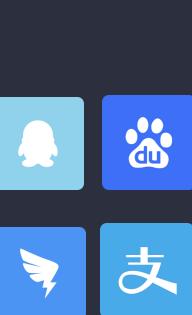
企业微信



Web 端登



移动端登录



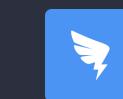
c.

## 企业身份源认证

企业微信



钉钉



LDAP



OIDC



CAS



Windows AD



SAML

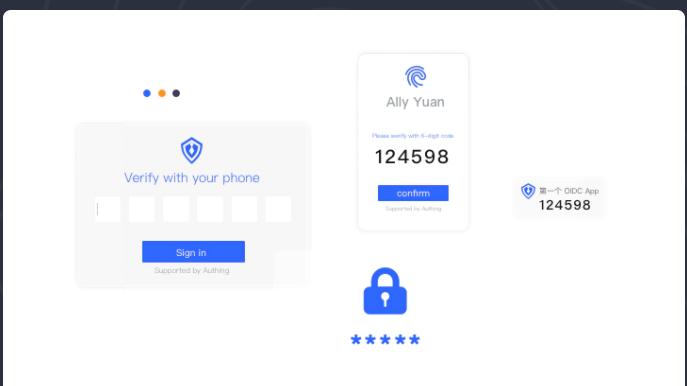


Azure AD



d.

## 自适应多因素认证



e.

## 对认证流程进行扩展

1. 自定义数据库
2. Authing Pipeline
3. Authing Webhook



# 管理用户账号目录

a.

## 用户管理

The screenshot shows a user profile for 'Aaron Kelly' with the following details:

- 基本信息: 手机号 131-4967-9860, 邮箱 kile@gohvut.kr, 最后登录时间 2021-01-17 12:52:50, 登录次数 2。
- 权限信息: 包含权限管理、授权管理、子账号、原生 JSON 数据和历史记录。
- 详细信息: 显示姓名 方锐, 职称 如花, 部门 一部门, 手机 18922475415, 邮箱 tida@hapohit.rs, 生日 1994-01-21。
- 拓展信息: 空白。

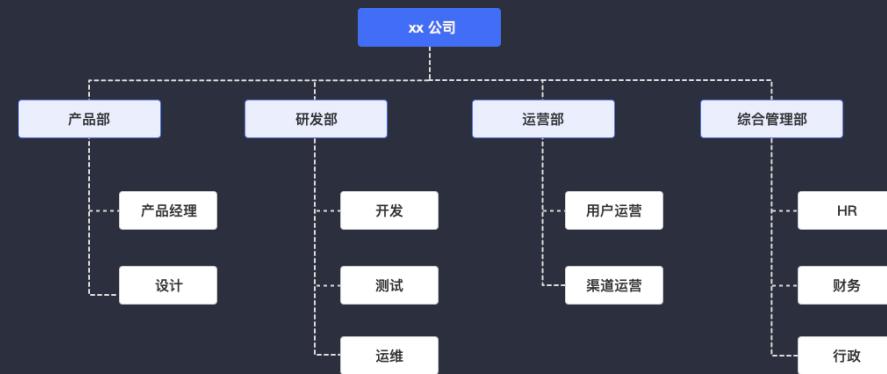
b.

## 生命周期管理



c.

## 组织管理



d.

## 应用管理

The screenshot shows a list of connected applications under the '应用' (Application) tab:

- 腾讯企业邮箱 (Tencent Enterprise Mail)
- 阿里云 (Aliyun)
- Zabbix
- Authing
- Aliyun SAML Demo
- Huawei cloud SAML IdP demo
- 后台管理系统 (Backend Management System)
- LDAP demo

e.

## 同步中心/身份供应



# 权限管理与授权

a.

## 应用授权

The screenshot shows the 'Wecom demo' application configuration page. The '应用访问控制' (Application Access Control) tab is selected. It displays a section for '默认权限' (Default Permissions) where '允许所有用户访问' (Allow all users to access) is selected. Below this, there's a table for '应用授权类型' (Application Authorization Types) showing two entries: 'Intern' and 'Authing 助手', both with '拒绝' (Deny) selected for '授权作用' (Authorization Effect). There are also '编辑' (Edit) and '删除' (Delete) buttons for each row.

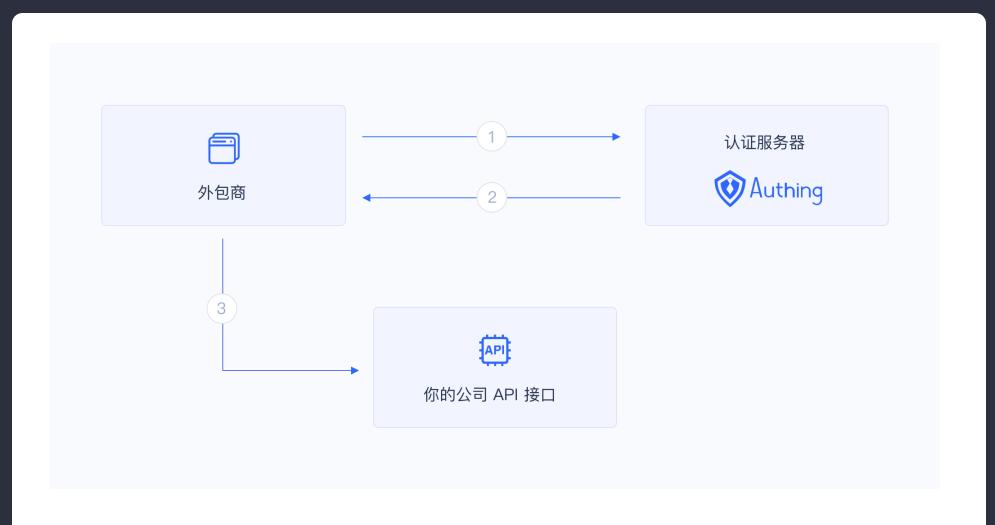
b.

## RBAC、ABAC 基于属性的权限控制

The screenshot shows a configuration interface for RBAC or ABAC. It includes sections for '当前请求用户是否开启了 MFA 认证' (Current request user has MFA authentication enabled), '客户端浏览器' (Client Browser), '客户端设备 ID' (Client Device ID), '客户端操作系统' (Client Operating System), '当前请求来源国家' (Current Request Source Country), and '当前请求来源省份' (Current Request Source Province). At the bottom, there are dropdown menus for conditions: '当前请求用户是否...' (Current request user is...), '值为 True 或者 Fa...' (Value is True or False), and '是' (Yes).

c.

## M2M 对机器授权



粗

← → 细



## 数据存储安全

所有数据存储在云端，关键数据使用「KMS」完成多重保护



## 数据传输安全

所有数据传输过程中使用非对称加密，通过 SSL/TLS 协议加密传输，搭配严格的访问控制策略，保障数据高效传输不泄漏



## 审计

Authing 提供操作审计功能以帮助企业  
和组织在业务不断增长的同时保持安  
全与合规。

用户可以通过「应用市场」快速集成 Authing 已经预集成的应用，包括 Salesforce、Slack、AD、飞书、企微等。

用户也可以通过标准协议，如 Oauth2.0、OIDC、SAML 等集成应用，快速实现单点登录。

OIDC



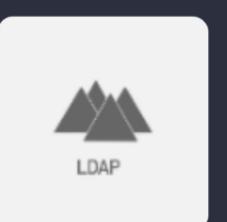
SAML



CAS



LDAP



OAuth 2.0



应用市场

在应用市场中寻找可以帮助你的企业的单点登录集成。用户登录第一个应用程序后，无论平台，技术或领域如何，都无需再次输入凭据即可访问其他应用程序。

全部 28 办公 16 云计算 5 CRM 2 财务 0 项目管理 6 搜索单点登录集成应用 搜索

Discourse discourse	Slack slack	WordPress wordpress
Discourse 是一个简洁、平面化的论坛,回复就像瀑布一样线性显示在页...	Slack 是一个适用于业务沟通的消息发送应用程序，它将人们与他们需...	全球最热门的网站构建器。42% 的网页在 WordPress 上构建。越来越...
Seafile seafile	Kibana kibana	Jenkins jenkins
Seafile 是一款开源的企业云盘，注重可靠性和性能。支持 Windows, Ma...	Kibana 是一个免费且开放的用户界面，能够让您对 Elasticsearch 数据...	构建伟大，无所不能。Jenkins 是开源 CI&CD 软件领导者，提供超过...
Teambition teambition	Salesforce salesforce	JFrog jfrog
包括项目空间、网盘、文档、待办、日历等新一代工具，帮助你把想法...	Salesforce 是一款可将公司和客户联系在一起的客户关系管理解决方案...	JFrog Artifactory 是目前全球唯一一个支持所有开发语言，任意维度的...

< 1 2 3 4 >

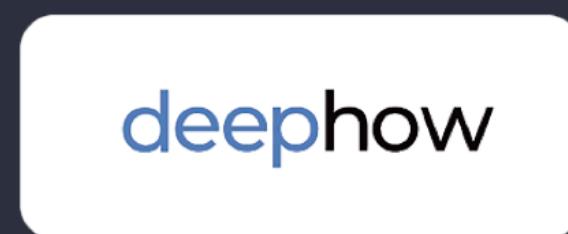
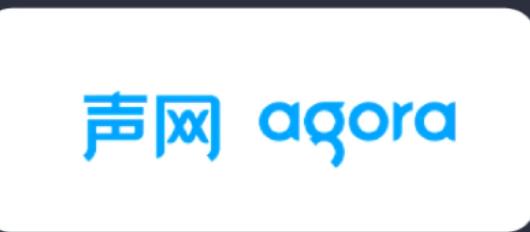
# 预期价值





Authing 是国内首家提供用户身份管理和员工身份管理（CIAM & EIAM）解决方案的云服务，凭借安全、完善、易用的用户认证和管理平台，Authing 已帮助全球 **10000+** 企业和开发者构建标准化的用户身份体系，每月支持近亿用户安全登录数万系统，成为新一代身份基础设施。

Authing 已经帮助全球 10000+ 开发者和企业解决复杂的身份管理问题



# 典型客户：外部用户身份管理案例示例

• :



定位：媒体出版

外部用户数：3500 万用户

集成软件数量：100+ 个

安全研发投入：千万级/年

## 客户需求

- 研发 100 多个业务网站的 3500 万用户的统一身份系统
- 需要跨品牌、跨平台的单点登录，优质、无缝的用户体验设计
- 需要防欺诈保护、安全保障

## 解决方案

- 多云部署解决方案，3小时两个人即完成部署测试，轻松集成千万用户
- 提供基于微服务架构、高度产品化的身份管理服务，满足企业灵活多变的身份管理需求
- 提供多语言轻量级 SDK 集成套件，仅需几行代码即安全地实现单点登录，省去老旧系统接口定制开发烦恼
- 联通企业内部复杂应用集成

## 方案效果

- 加速了产品研发，加快业务上线
- 对冲了开发过程与使用过程的安全风险
- 集中管理所有来源的用户
- 创造交叉销售机会
- 完备的应用集成适配方案

50%  
开发工时降低

200 小时  
运营管理时间减少

# 典型客户：外部员工身份管理案例示例

• :



定位：汽车厂商

外部用户数：百万用户

内部软件数量：数十个

安全研发投入：千万级/年

## 客户需求

- 为支撑开发 B2C 租车业务应用，统一身份认证功能开发周期长、拖累核心应用开发进度，需要统一规范的身份体系来支撑快速交付。
- 原有应用身份认证系统不能复用到新应用中，新旧应用身份集成存在困难。
- 新应用万级以上用户身份认证和管理，给运维带来极大工作量。
- 用户数据安全问题，现有的用户管理流程不够清晰，覆盖不全面，存在一些管理薄弱点及落实不到位问题，无法满足行业监管审计的要求。

## 解决方案

- Authing 提供的 SaaS 标准化身份云产品，提供身份供应源。
- 接入企业现有应用系统，完成身份账号同步、单点登录和访问授权问题。
- Authing 的自适应多因素认证功能，提升用户完全登录，提升信息安全，强化风险控制，安全合规，提升身份治理水平。

## 方案效果

- 帮助丰田研发团队快速部署身份安全管理平台，缩短新应用研发的周期。
- 满足丰田后续开发新应用中的身份登录及 C 端用户万级用户的流量问题。
- 无需重新构建或重复构建身份登录体系，快速集成我们的新老应用，大大减缩减了新应用的研发周期和上市时间。

# 典型客户：内部员工身份管理案例示例

• :



定位：大集团部门

员工数：2000 个

内部软件数量：近百个

安全研发投入：千万级/年

## 客户需求

- 旗下某研究所总计千余人，使用的软件服务 100 余个，IT 管理复杂
- 希望实现成员使用公司账号即可登录所有软件，然而业务系统老旧，安全、认证创新困难
- 核心功能研发已耗时许久，然而用户验证功能一直未处理完善，希望加速研发周期

## 解决方案

- 提供完善的单点登录平台，为旗下 Web 和 App 快速实现用户验证和访问管理功能
- 提供全套的 C# SDK，满足中国石油快速接入其研发系统
- 在中国石油重点关注的移动端单点登录上，Authing 具备「自动检测同一设备上关联应用的登录状态」、「唤起关联 App 以交换用户信息」，方便依据场景做选择

## 方案效果

- 消除了本地 IAM 的维护、运营和安全成本
- 提高了集团 WPF 应用的员工访问安全和合规性
- 实现了使用「石油集团」登录的开放功能，轻松与其他公司合作

2000 个  
协同员工处理数量

# 典型客户：内部用户身份管理案例示例

• :



定位：新零售

员工数：5000 个

内部软件数量：几十个

安全研发投入：千万级/年

## 客户需求

- 随着员工的不断增长，传统 IAM 难以解决不断扩容的问题，如何使用通用登录来管理内部用户的角色和权限，确保安全内置到每个员工对应的级别系统，是目前运维人员管理的难点。
- 内部几十个应用系统的集成，与身份体系的打通，自研力度较大，时间周期长。
- 希望解决不断增长的应用和员工规模，应对企业未来不断扩张带来可持续的增长和高效率。

## 解决方案

- 实现员工一个账号密码登录所有应用，并统一管控身份权限。
- 与飞书产品层面的打通，为元气森林提供身份供应，实现基于飞书组织架构下的不同权限不同访问级别，轻松在后台实现分配和更改不同应用的权限，保护企业数据安全，节省运维人员 80% 的工作量。
- 提供一站式团队应用平台，实现成员和集中管控访问权限，提供身份供应。

## 方案效果

- 为企业提供身份源能力
- 打通企业内部应用
- 节省了大量的研发人力、费用和周期

# 典型客户：政务服务身份管理案例示例



定位：政务服务

员工数：20000 个

外部用户数：120 万用户

内部软件数量：数千个

安全研发投入：千万级/年

## 客户需求

- 政务内外部身份体系割裂，身份治理难，IT 管理复杂
- 政务服务应用太多，账户密码过于分散，用户需要记住大量的密码以登录不同应用，导致认证困难
- 不同业务系统身份和权限体系无法打通，统一运营困难重重

## 解决方案

- 提供了完善的单点登录平台，让公民通过一个账号访问所有系统
- 在 Authing 控制台的用户管理可以做到所有公民和办事人员的身份信息的集中管理
- 使用用户行为审计，保证每个用户的每个行为都被记录下来
- 通过多重安全防护策略进行防护，保障数据安全

## 方案效果

- 打通了内部外部，业务应用间的身份，使统一管控变得非常轻松
- 消除了本地 IAM 的维护、运营和安全成本
- 提高了政务员工和市民访问安全和合规性

122万 个

协同终端用户处理数量

# 为不同企业定制化解决方案

工作事项	工作内容	交付文件
初步沟通需求	首次沟通，明确公司需求背景，并对产品做初步介绍	《首次沟通纪要》 《公司、产品白皮书》
需求方案匹配	具体、细化需求，演示demo并探讨项目框架	《PoC 建议书》
协助测试与报价	协助公司进行 PoC，并提供项目正式报价	《项目报价详情单》
签署服务协议	双方明确合作协议并完成签约立项	《服务合作协议》



# Thank You

联系我们

公司地址：北京市海淀区中关村东路1号院7号楼威盛大厦6层

联系方式：158 1077 0445

电子邮箱：[marketing@authing.cn](mailto:marketing@authing.cn)

北京蒸汽记忆科技有限公司