助力零信任安全架构的下一代IAM

中通快递 信息安全负责人 | 伏明明

目录

业务背景

国内业务量最大

业务规模世界第一

连续两年稳居行业第一

2017年业务量达到62.2亿件

中通人
30万+

网络合作伙伴
9400+

服务网点
29500+

覆盖区县
98%+

覆盖乡镇
85.24%+

生态中通

——中通集团的
多元化经营战略

目录

面临的安全风险

业务系统众多和异构

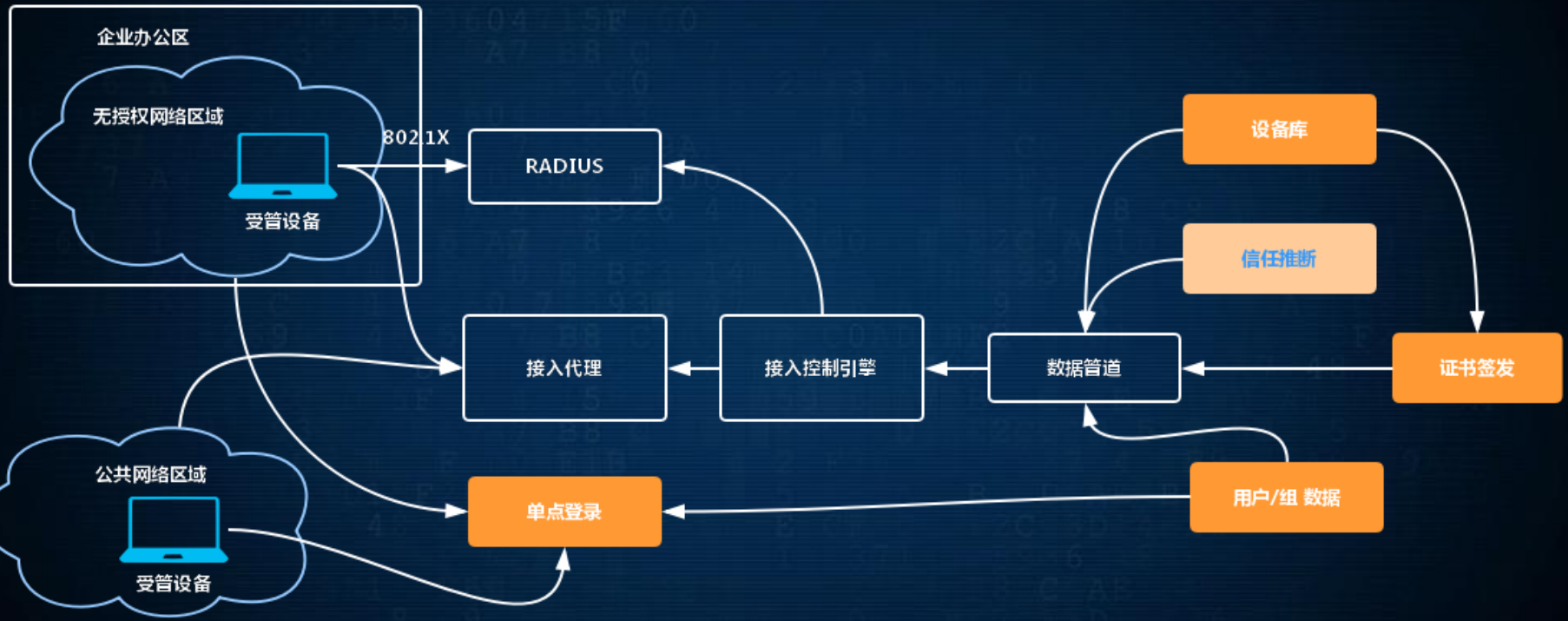
组织人员和设备变动

敏感数据参与业务

开放平台API管理

目录

下一代IAM——零信任安全架构（Google BeyondCorp）及其中的IAM组件



下一代IAM——设计目标

全面身份化支持

1. 使用通用安全身份框架SPIFFE，实现支持万物互联的身份认证技术
2. 将客观世界的对象抽象成逻辑上具备不同属性的身份，如人员、设备、应用、API等

云原生支持

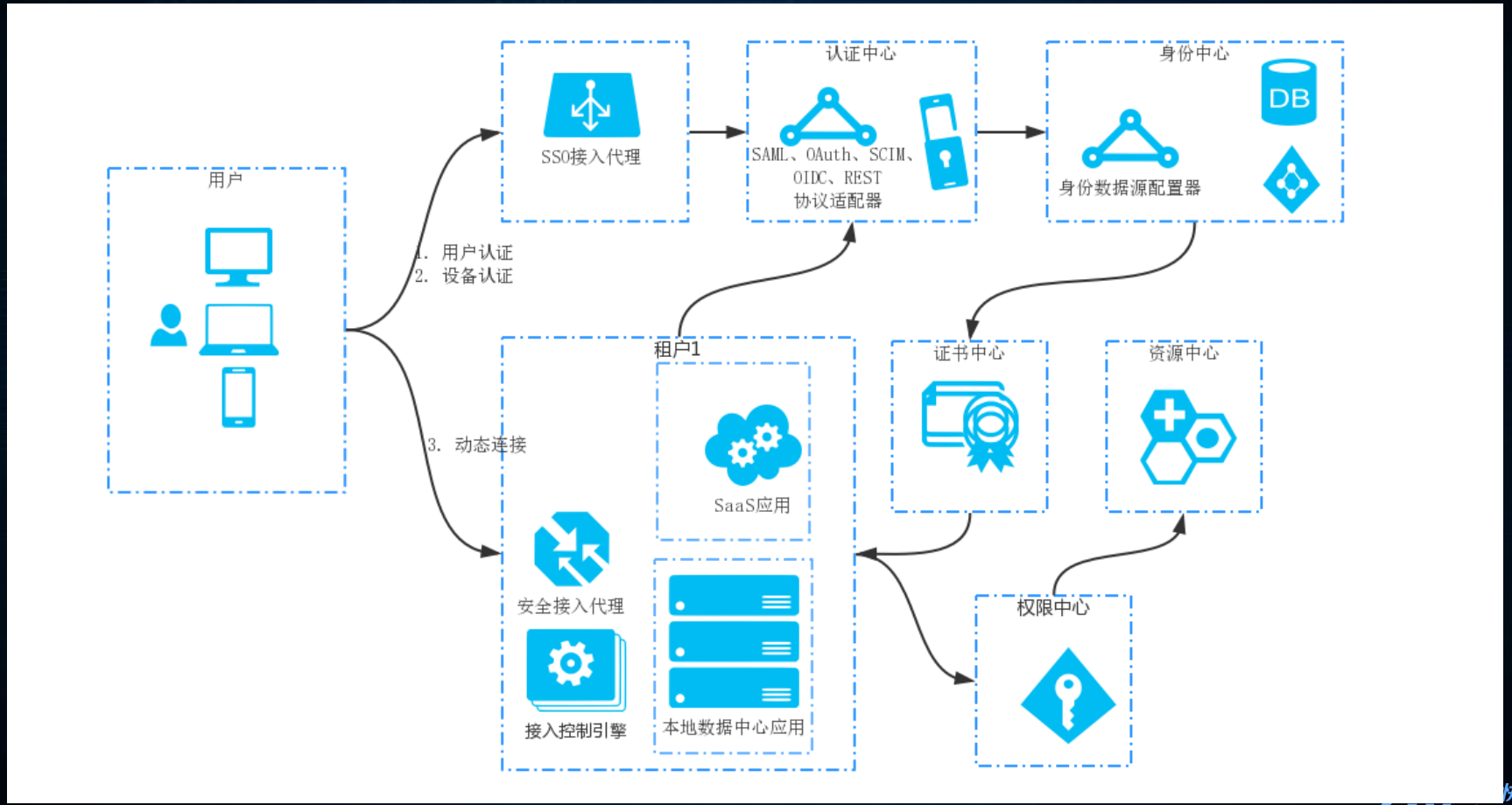
1. 真正打通本地/云/办公等网络边界，全面从网络层访问控制升级为应用层动态智能深度检测和控制
2. 使用容器、微服务、服务网格、编排等技术实现灵活的水平扩展、异构系统互操作支持和端到端的安全加密

复杂组织的支持

1. 跨租户、跨帐号体系、跨端、跨用户渠道、跨应用、跨生态的支持
2. 应用和身份数据分离的联邦和多协议的支持
3. 在资源层面对所有操作进行分类分级及自动化审计

下一代IAM——功能全景视图

下一代IAM——总体工作流程



下一代IAM——本质上是对资源操作更灵活及更细粒度的管控

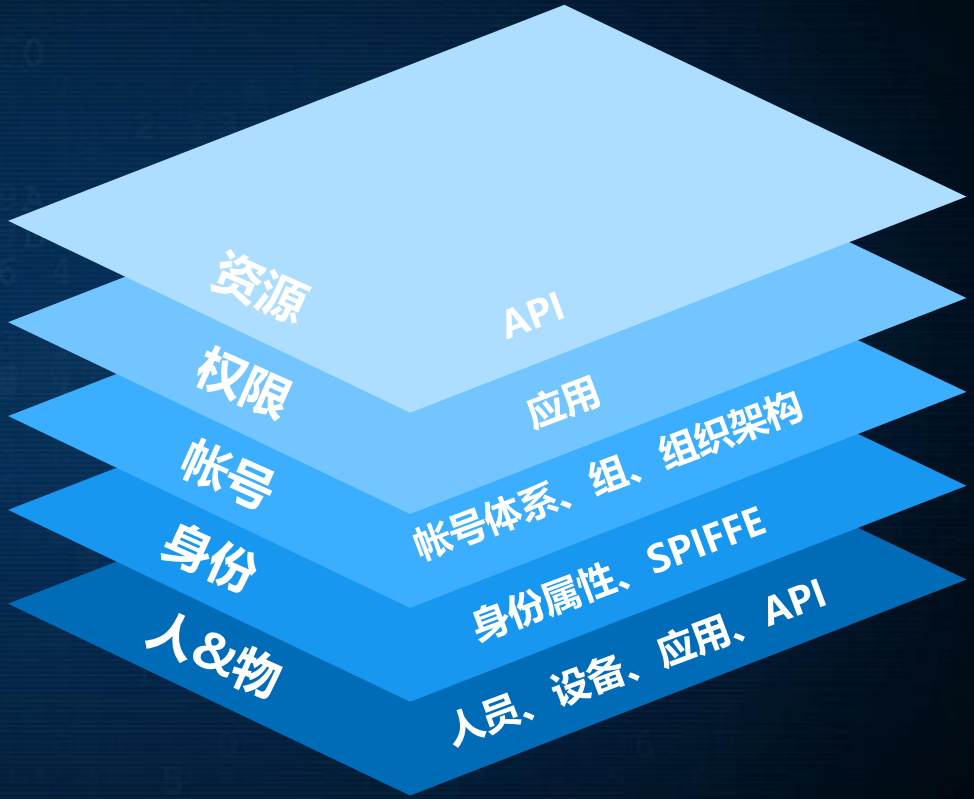
下一代IAM——身份空间

资源操作

权限授予

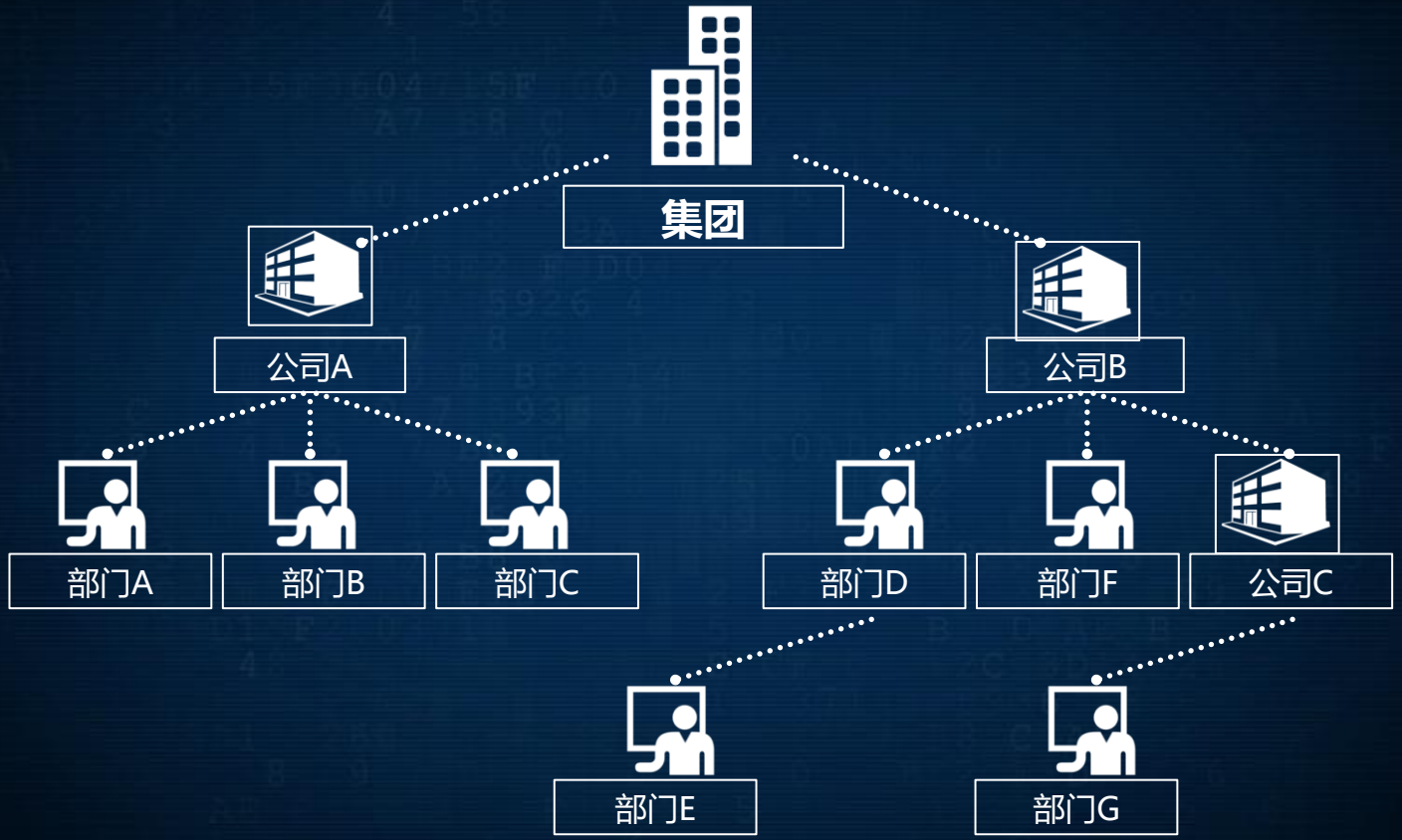
一对多归属

生命周期管理

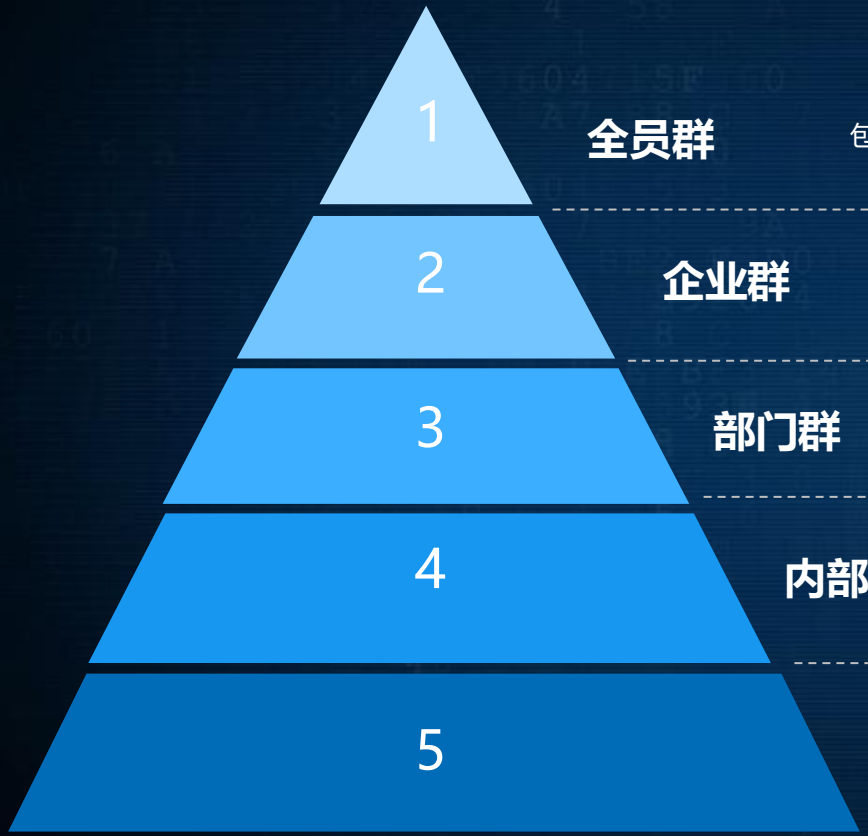


下一代IAM——帐号、帐号组、帐号体系

下一代IAM——组织架构



下一代IAM——组织架构群组



全员群　包含集团下所有员工的群

企业群　集团下某个公司下的所有员工的群

部门群　组织架构的最底层，隶属于某个公司下，它可以是一个大的部门，也可以是部门下的一个小部门。

内部群　集团下跨部门跨企业不少于三个员工创建的群

特殊群　合作群：集团员工与外部联系人创建的群
普通群：非同一集团下的员工建立的群

下一代IAM——系统集成

下一代IAM——授权

权限模型

ACL

RBAC

ABAC

授权方式

基于身份的

基于资源的

访问控制策略

添加权限边界

授权过程

定义 Resource

定义每个Resource 上的Action

定义 Identity实体

定义 Policy 语法/权限/角色

解析 Policy 给出裁决结果

下一代IAM——自定义授权请求DSL

授权本质

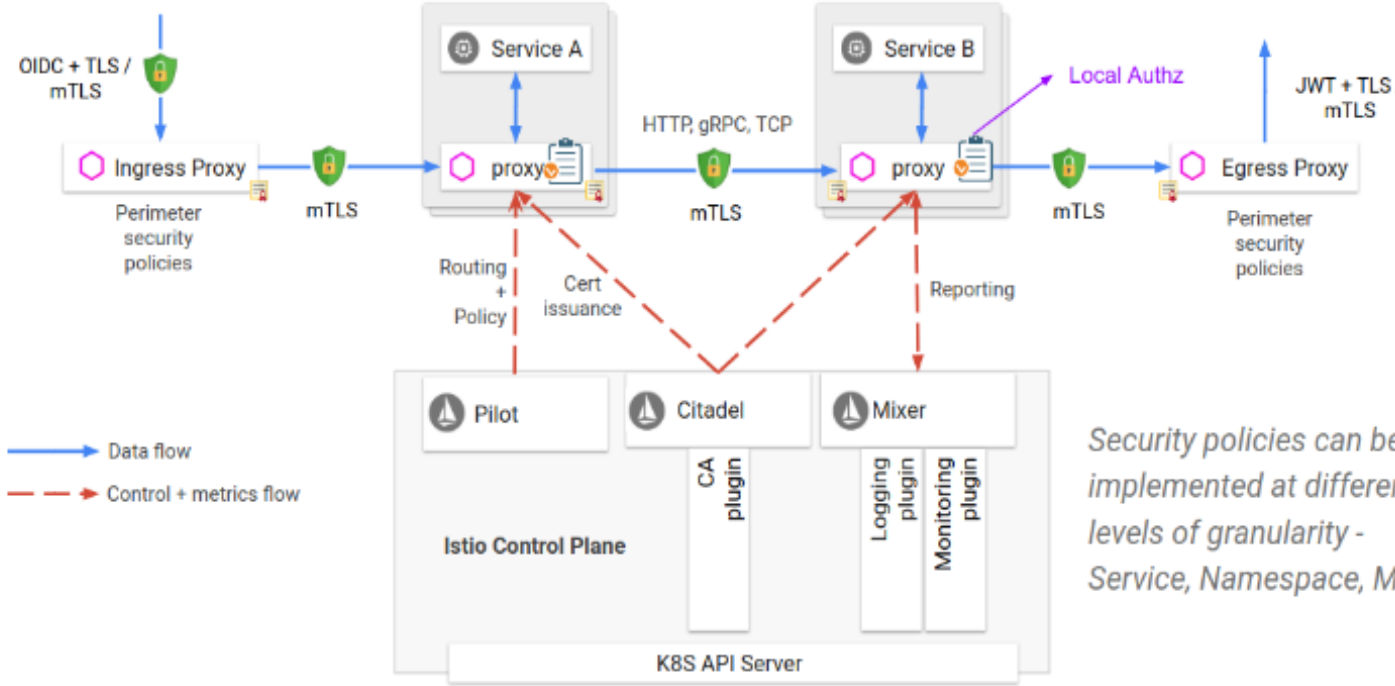
谁
能不能
在什么样的上下文
对什么样的资源
做什么样的操作

DSL语法

```
{
"appid":"eihxiidhh23s","user":"jack","action":"getArticleID","resource":"resources:articles:zto","context":{"remoteIP":"192.168.0.5","trustScore":"90"}
}

{
"allowed": true   //裁决结果
"options": {"id": 11 }  //数据权限
}
```

下一代IAM——微服务安全架构（双向认证、加密、隔离）



Istio Security Architecture

下一代IAM——证书签发、轮换和吊销机制

下一代IAM——自动化审计

安全审计概念

➢跟踪记录谁在什么时间什么地点以什么样的方式做了什么

➢聚焦在及时发现异常和处理上

自动化

➢对所有资源进行分类

➢对所有资源和操作对分级

➢根据分类分级和权限过滤异常

➢与其它系统集成自动过滤异常

交付物

➢主动及时汇报和确认异常以推动策略实施及问题解决

➢确保审计对象得到合理准确的处理和合规

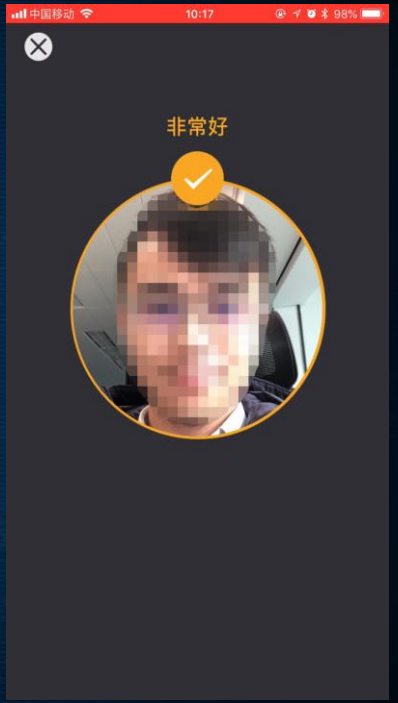
➢对企业内审计对象进行关联性分析并得到综合性的报告

下一代IAM——移动端APP

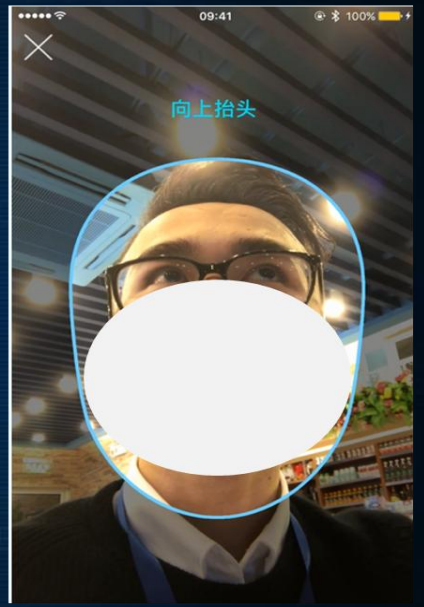
安全模块	吉信模块	应用模块	工具模块
风控解锁	单聊	应用Portal	个人资料维护
移动SSO	群聊	事件流推送	中通邮箱激活
扫码	好友	帐号申请审批	实人认证
动态码	通讯录	权限申请	系统设置
推送	文件		
安全评估	公告		

目录

实践总结——SSO支持多种认证方式（密码/短信/TOTP/推送/扫码/刷脸/会话代理等）



实践总结——身份管理支持实人认证（人、证、帐号、设备合一）



实践总结——敏感操作审计（刷脸认证日志）

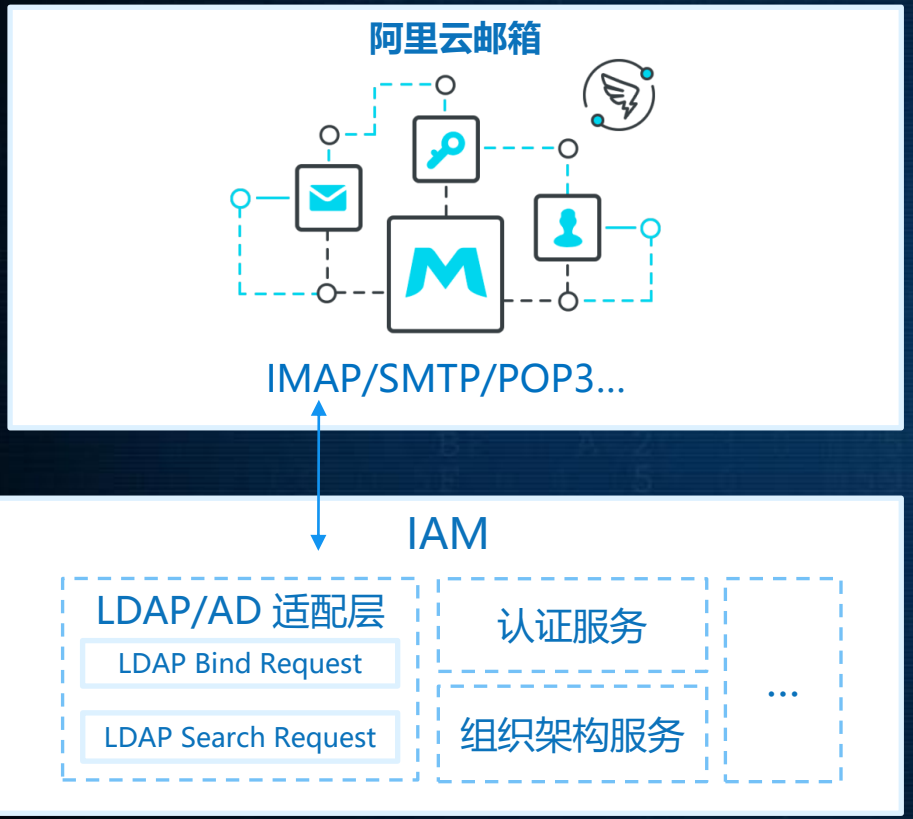
实践总结——IAM与办公网准入网关集成

电脑登录

手机确认

进入办公区自动连Wi-Fi

实践总结——IAM支持联邦认证与阿里云邮箱集成



实践总结——IAM支持认证互操作/移动端APP（与钉钉和菜鸟应用集成）

实践总结——IAM支持跨应用的集中权限管理

实践总结——IAM支持权限矩阵实现SOD

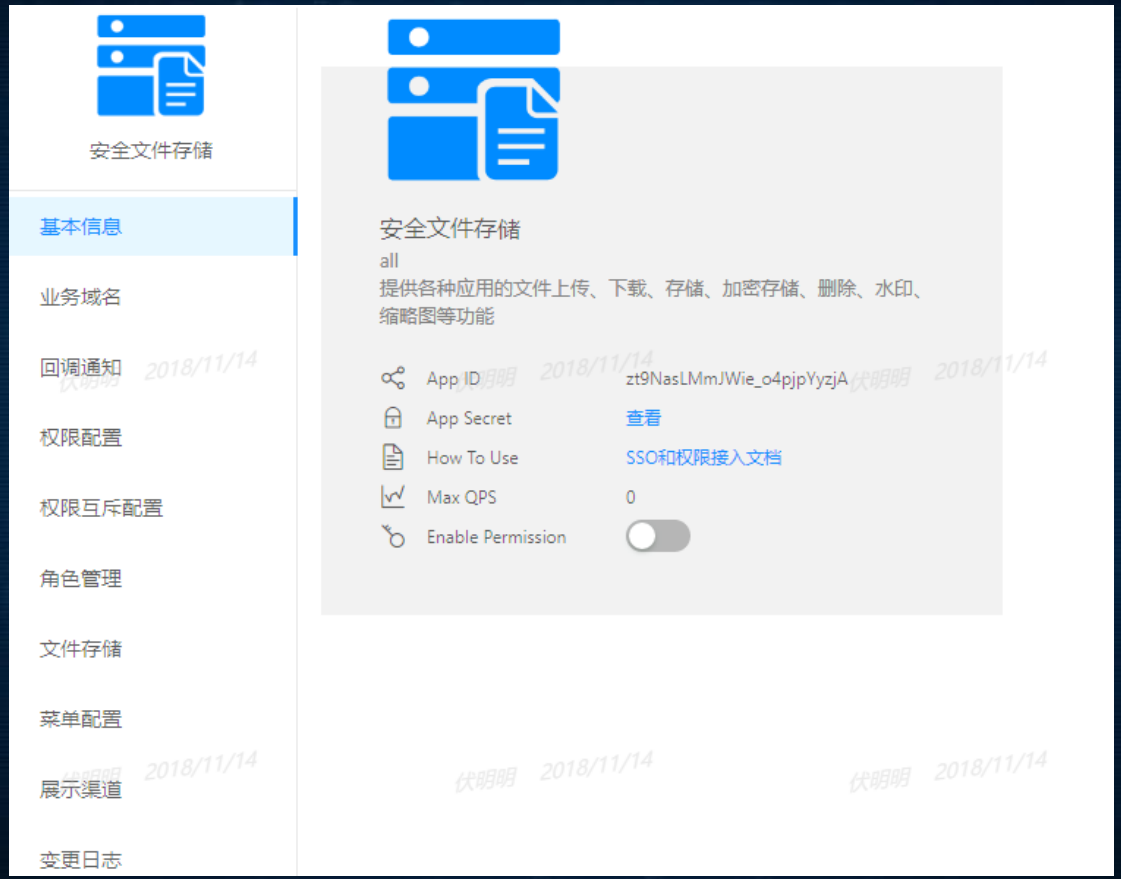
> 互斥配置 <	巴枪功能开关...	机房告警管理...	机房信息管理	机房性能监控...	机房综合监控...
巴枪功能开关...	> 别点我 <				
机房告警管理...					
机房信息管理			> 别点我 <		
机房性能监控...				> 别点我 <	
机房综合监控...					> 别点我 <
告警策略管理...					
告警记录查询...					
设备管理-维...					
基础信息管理...					

机房性能监控管理 <-> 机房告警管理菜单权限

添加互斥

实践总结——IAM支持双向权限审计

实践总结——应用中心支持应用集中统一管理



实践总结——应用中心支持应用集中统一权限配置

实践总结——应用中心支持应用集中统一菜单配置及自动关联权限

目录

未来展望——在IAM基础上集成更多的安全组件

端到端加密组件

零信任安全组件

SDL工具/组件

未来展望——积极拥抱开源技术和开源文化

积极采用开源技术

已采用或即将采用的开源技术: tango、gokit、docker、k8s、istio、hydra、CDH、spark、redis、kafka、es、pg、tidb、openresty、kong、pika、fastdfs、grafana等

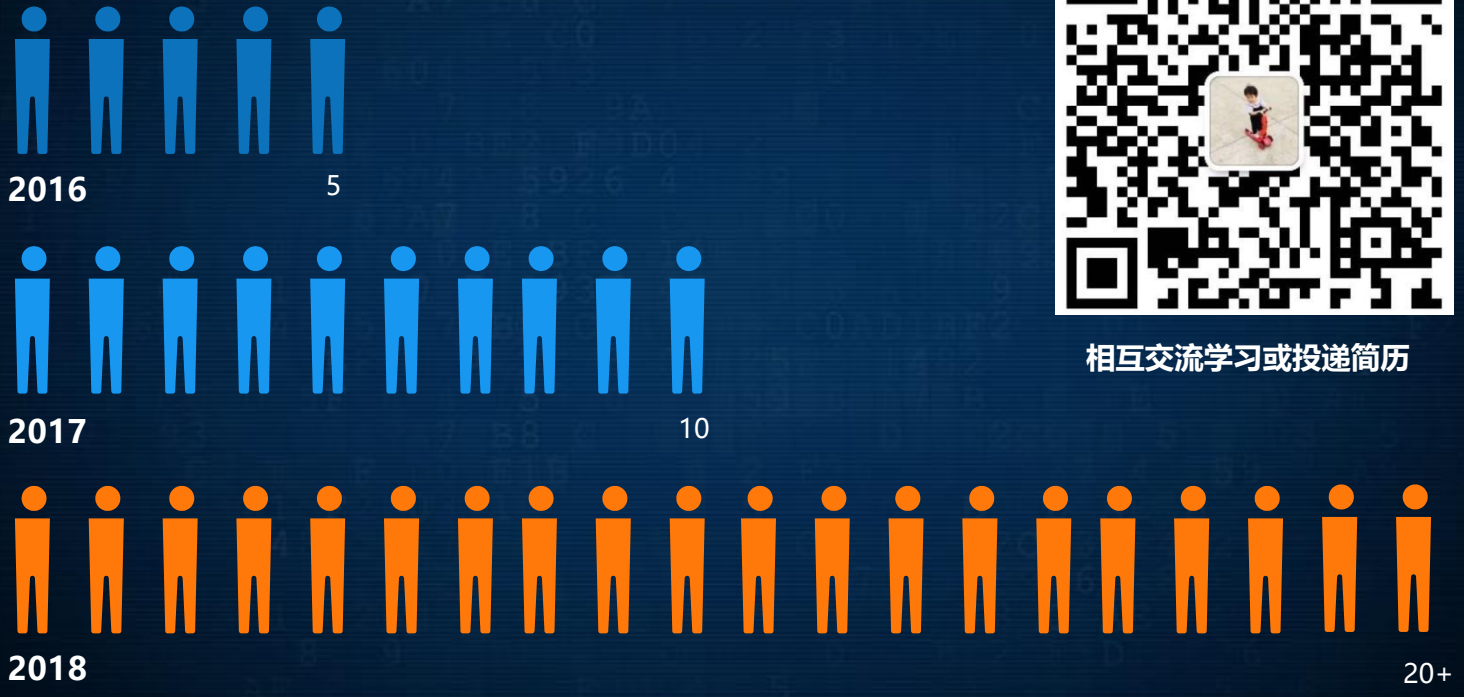
定期与同行技术分享

中通安全应急响应中心（https://sec.zto.com）微信公众号ZTO_SRC每月推送两到三篇技术分享文章以及参加相关会议

制定分步开源计划

计划将IAM平台及其它安全系统组件化后，2019年起逐步开源，希望能帮助到有需要的朋友

未来展望——持续吸纳专业的安全人才



相互交流学习或投递简历

问题讨论

Q&A