



深信服统一身份安全管理系统主打PPT

全网身份治理

深信服 智安全

目录

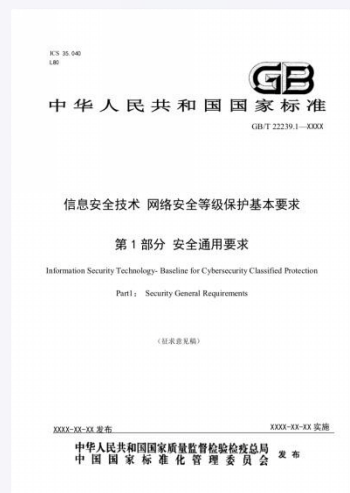
- 一. 挑战和背景
- 二. 深信服解决之道
- 三. 成功案例

国家把网络可信身份作为核心战略

— 《网络安全法》

身份鉴别和双因素认证成为合规要求

— 《等级保护2.0：基本要求》



Facebook负面新闻事件

安全事件原因:权限泛滥

2018年5月, Facebook的一位安全工程师利用自身权限在线跟踪并骚扰女性, 同时, 他还在社交平台吹嘘自己可以看到任何一个Facebook用户的个人资料



SunTrust银行150万数据泄漏

安全事件原因: 账号未回收

2018年4月, 美国银行SunTrust Bank宣布, 发现一名离职员工盗取了超过150万名客户的数据, 包括姓名、住址、电话号码和账户余额等重要信息, 并将其售卖

81%的数据泄漏与身份安全有关 - 《2017年数据泄露调查报告》

账号管理繁重

标准企事业单位的应用数量超过15+



ERP系统



CRM系统



OA系统



WIKI系统



邮件系统



HR系统



VPN系统

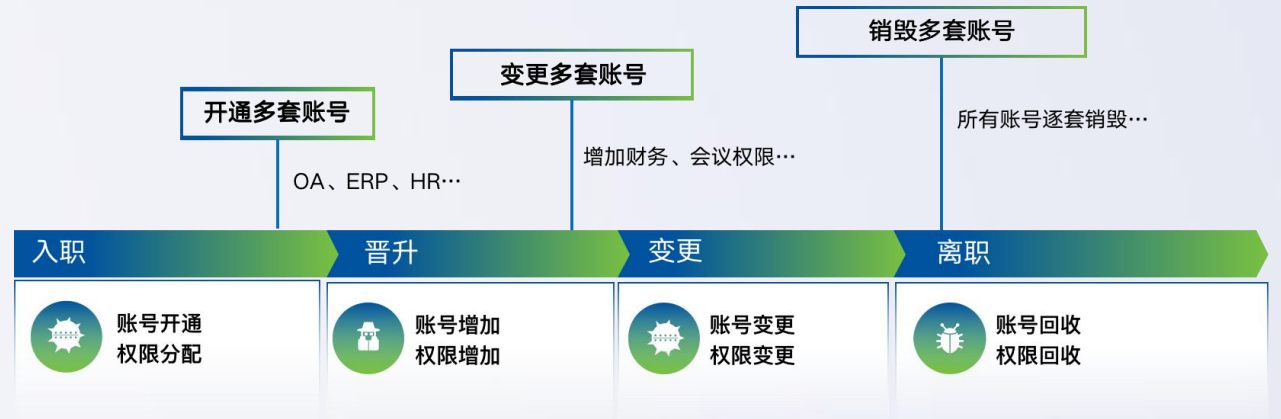


上网行为管理



桌面云

需要管理多套账号/密码体系



账号注册/密码找回/信息修改均需要管理员操作



用户认证繁琐



员工



多套账号，体验差/效率低

OA系统



ERP系统



邮件系统



- 应用系统多，用户需要记住多套账号/密码，易忘记
- 应用系统多，入口繁多，用户记不住URL地址
- 应用系统多，切换访问需要多次认证，工作效率低

1 账号安全性差



- ❑ 密码复杂度不够，缺乏定期改密机制
- ❑ 账号密码认证方式，易出现账号共享、暴力破解等安全问题

2 权限管理不规范



- ❑ 员工具备超级权限，能访问所有应用系统，应用风险不可控

3 安全审计缺失



- ❑ 基于账号密码的认证方式，无法确定到“人”
- ❑ 出现异常行为，无法告警，例如异地登陆、异常时间段登录

目录

- 一. 挑战和背景
- 二. 深信服解决之道
- 三. 成功案例

国际相关标准框架

NIST



管理、技术、运营三管齐下

- 管理策略：策略流程管理，人员意识培训
- 组织可以通过访问控制策略和访问执行机制控制对PII的访问
- 实现基于角色的访问控制并配置它，以便每个用户都可以访问只有用户角色所需的数据片段

ENISA



更加注重云计算中的身份安全

- 在NIST基础上，ENISA在2009年推出了云计算风险评估
- 2015年推出了中小企业云安全指南

NCSC



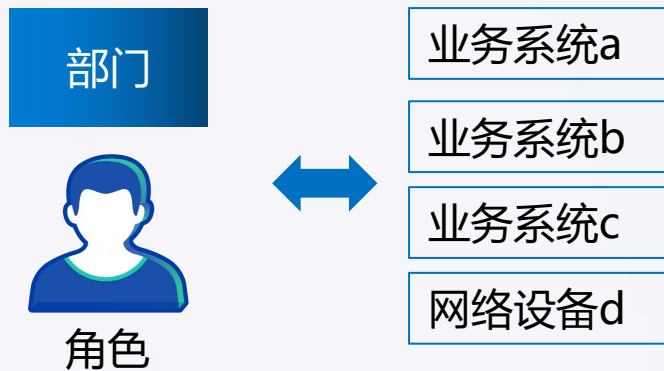
访问程序接口的需要身份验证

- 管理接口和程序是安全屏障的重要组成部分，可以防止未经授权的访问和更改您的资源、应用程序和数据
- 身份和身份验证所有对服务接口的访问都应限于经过身份验证和授权的个人

NIST作为国际上著名的标准提供者，具有更高的权威及更适合落地的标准

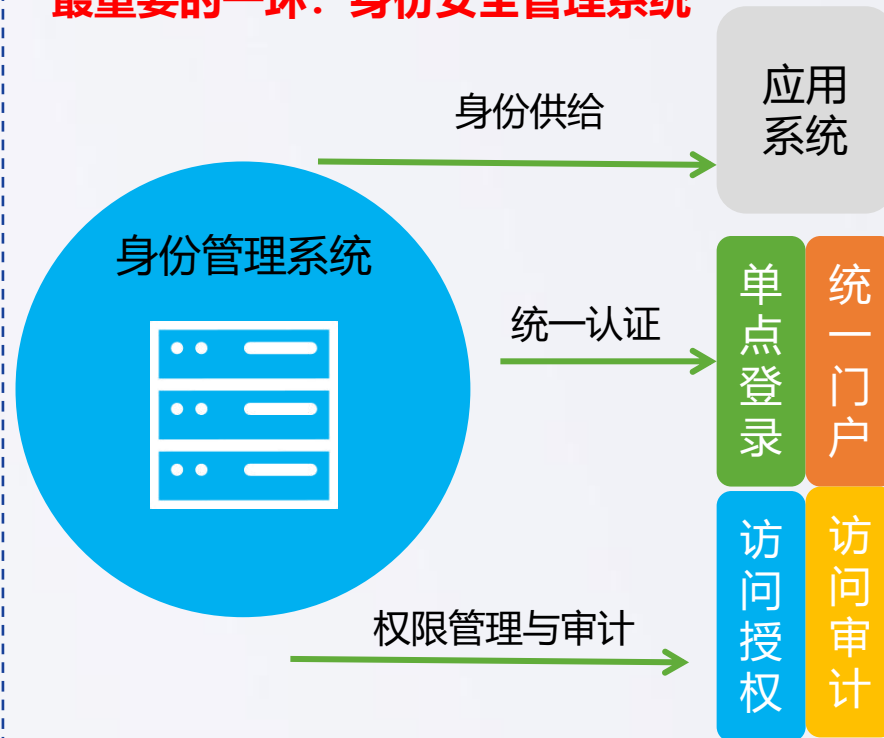
“三步走” 路线

组织架构及权限清单



最小权限原则

最重要的一环：身份安全管理系统



优化清单/反哺落地

员工	部门	岗位角色	权限
张三	财务部	员工	OA: 普通员工 ERP: 普通员工
李四	信息部	经理	OA: 管理员、普通员工 ERP: 普通员工
王五	业务部	经理	OA: 普通员工 ERP: 普通员工 业务系统: 普通用户
....			

梳理业务及网络权限

借助工具实现自动化身份管理

持续运营

深信服统一身份安全管理系统 (IDTrust) 简介



身份管理 Account



账号同步



OA系统资源



.....

账号自注册/密码自找回/信息自修改

认证管理 Authenticatio



n



OA系统资源



.....

无密认证/统一门户/单点登录



IDTrust

权限管理 Authorizatio

n



OA系统资源



ERP系统

行为审计 Audit



应用访问审计
异常行为分析

员工	部门	岗位角色	时间	IP	访问应用	异常行为
张三	财务部	员工	2020.5.21 14:42	113.110.229.125	OA系统	异地登录

1 简化身份管理

- 账号生命周期管理
账号新增删改自动同步至全网应用，避免频繁操作，提高自动化水平
- 员工自服务中心
提供员工自注册，密码找回以及信息修改，减轻运维管理工作

2 便捷身份认证

- 统一认证门户
提供统一认证门户，员工只需要记住门户登录地址，即可访问相应权限业务应用
- 单点登录
只需认证一次，即可单点登录具备权限的业务应用，使办公更高效，体验更良好

3 增强身份安全

- 增强认证安全
可设置密码复杂度与定期改密，提供生物认证及“无密认证”，并可自由组合成双因素认证，解决账号共享、密码被爆破等问题
- 加强权限管控
设置员工可访问应用权限，防止越权访问
- 异常行为分析
异地登录、异常时间段登录告警





简化身份管理



自动化身份同步



SANGFOR
深信服科技



深信服智安全
SANGFOR SECURITY

上游

中游

下游



HR系统



AD域



数据系统



其它系统

拉取身份信息



IDTrust

身份信息供给



网络设备



ERP系统资源



CRM系统资源



邮件系统资源



OA系统资源

业务应用

- 支持LDAP、数据库、API同步
- 每30分钟自动同步一次
- 可作为用户源取代上游能力
- 用户新增删改在一个系统操作
- 身份生命周期管理

□ 减少“简单且繁琐”的运维管理工作



员工账号自注册



密码自助找回



员工自助信息修改



管理员审批中心

账号注册

* 用户名:

* 密码:

* 确认密码:

* 邮箱:

* 邮箱码:

部门:

注册

已有账号, 请登录

找回密码

请使用手机/邮箱验证码找回密码

[用户登录](#)

个人中心

个人信息

姓名: idtrust 用户组: /体验管理员和用户/idtrust

角色: --

基本属性

手机号: 15361026466 工号: 372245

邮箱: user@qq-qidian.cn

[返回首页](#)

审批中心

审批通过 驳回申请

<input type="checkbox"/>	序号	申请单号	申请...	用户名	用户组
<input type="checkbox"/>	1	202003110...	自注册	wx_test	/



便捷身份认证

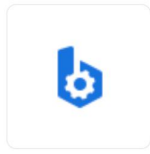


您的账号将于2019-12-01过期，过期账号将无法正常使用，如需要延长账号过期时间，请点击延期申请！ 账号延期申请

常用应用 | 编辑常用应用



OA系统



BPM平台



SAAS测试申请



OA系统



知识库



SANGFOR认证中心

我的待办

待办事项	时间	操作
【账号延期】您的账号xiaoyao将于2020.1.10过期，请及时在个人中心申请延期	2019-12-01 15:32:32	立即处理
【年假审批】您有 2 条请假申请待审批	2019-12-01 15:32:32	立即处理
【报销审批】您有 1 条出差报销申请待审批	2019-12-01 15:32:32	立即处理
【账号延期】您的账号xiaoyao将于2020.1.10过期，请及时在个人中心申请延期	2019-12-01 15:32:32	立即处理
【账号延期】您的账号xiaoyao将于2020.1.10过期，请及时在个人中心申请延期	2019-12-01 15:32:32	立即处理
【账号延期】您的账号xiaoyao将于2020.1.10过期，请及时在个人中心申请延期	2019-12-01 15:32:32	立即处理
【账号延期】您的账号xiaoyao将于2020.1.10过期，请及时在个人中心申请延期	2019-12-01 15:32:32	立即处理
【账号延期】您的账号xiaoyao将于2020.1.10过期，请及时在个人中心申请延期	2019-12-01 15:32:32	立即处理
【账号延期】您的账号xiaoyao将于2020.1.10过期，请及时在个人中心申请延期	2019-12-01 15:32:32	立即处理
【账号延期】您的账号xiaoyao将于2020.1.10过期，请及时在个人中心申请延期	2019-12-01 15:32:32	立即处理

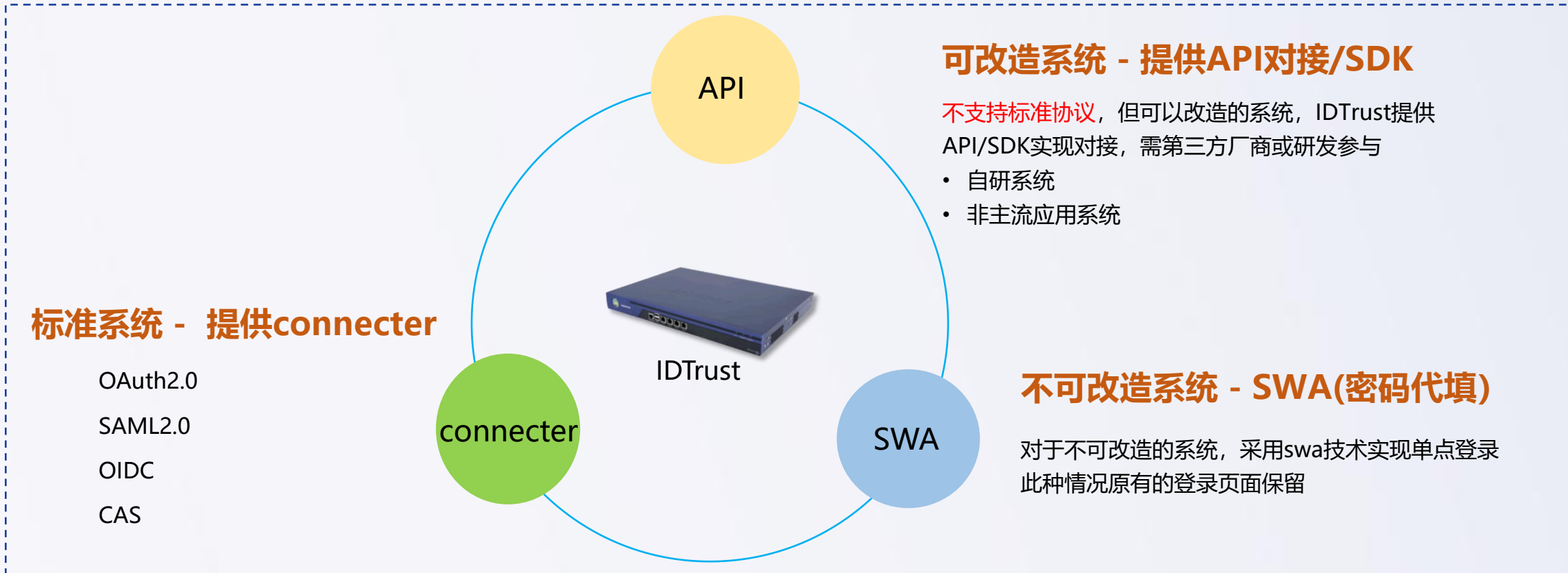
共 240 项 < 1 2 3 4 5 ... 24 > 每页 10

公告中心

- 放假通知 | 2019.12.01
2020年春节放假及全年假期的安排及通知请各位同事悉...
- 应用更新 | 2019.11.31
上班时间吸烟制度强调及处罚通知公示，请各位同事悉...
- 系统通知 | 2019.11.31
从网络运行和管理者角度说，希望对本地网络信息访问...
- 系统通知 | 2019.11.31
从网络运行和管理者角度说，希望对本地网络信息访问...
- 系统通知 | 2019.11.31
从网络运行和管理者角度说，希望对本地网络信息访问...

- 应用模块：已经实现
- 消息模块：需要接口
- 待办模块：需要接口

- 消息和待办模块设计逻辑：
 - 通过接口获取消息或待办流程
 - 点击链接回到应用处理





增强身份安全



增强认证安全



密码认证



短信认证



UKEY证书认证



指纹认证



动态码认证



扫码认证

统一身份安全管理系统 v2.0.0
Unified Identity Security Management

监控中心 用户管理 认证管理 应用管理 系统设置 日志中心

认证管理

- 认证策略
- 服务器配置
- 多因子认证
- 联动配置
- 认证高级选项

认证策略

序号	名称	操作
1	zzj 测试	新增 删除 启用 禁用 更多操作
2	扫码	默认认证方式编辑 认证页面编辑
3	sms_test	
4	旭辉测试	
5	ios开发	
6	SDP测试	
7	测试用户	
8	sms	
9	默认策略	

认证策略配置窗口

指定的URL: <HTTP>://<PORTAL>

多因子认证

多因子认证方式:

- 短信认证
- APP扫码
- 动态码认证
- APP指纹
- 证书认证
- USB-Key认证

认证优先级: 请选择

认证有效期

时间选择: 2 小时

提交 取消

Sketch 9:41 AM 100%

Sangfor Auth

扫码认证 动态码 指纹认证

授权终端

WEB端已登录

登录时间: 2019.10.24 14:36

统一身份安全管理系统 V2.0.6 | 监控中心 | 用户管理 | 认证管理 | 应用管理 | 系统设置 | 日志中心

用户管理

- 组/用户
- 用户列表**
- 用户属性管理
- 角色授权
- 用户源导入
- 用户供给
- 用户自服务

用户列表

搜索关键字

- /
- EDR
- 信息系统部
- default
- debug
- debug1
- 深信服科技
 - mi
 - 新单位
 - 新产品培训
 - 测试用户**
- SSL

测试用户 | 编辑

组路径: /测试用户
描述信息:
组信息: 子组个数: 0, 直属用户个数: 7, 总用户个数(包含子组): 7

成员列表 | 授权应用

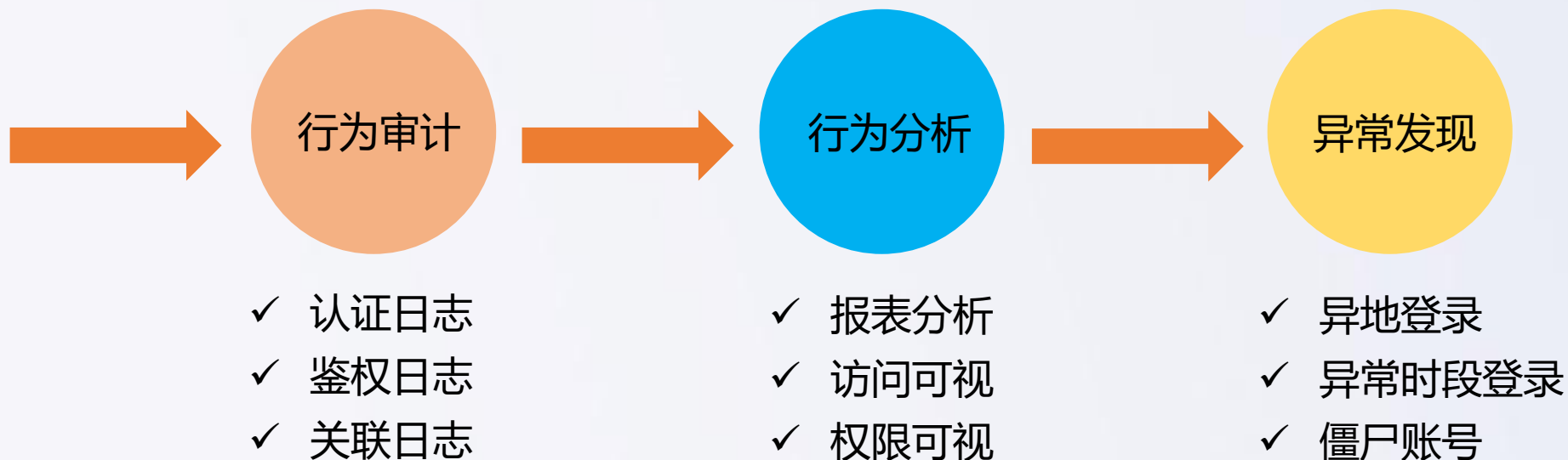
授权 | 删除 | 批量设置有效期 | 授权应用数: 33 | 请输入关键字

<input type="checkbox"/>	应用	授权有效期	分类	操作
<input type="checkbox"/>	来源于角色 (3)			
<input type="checkbox"/>	自定义应用 (33)			
<input type="checkbox"/>	51	永不过期	其他应用	删除 有效期
<input type="checkbox"/>	liaoxuda	永不过期	测试	删除 有效期
<input type="checkbox"/>	深信服社区	永不过期	测试	删除 有效期
<input type="checkbox"/>	VDC	永不过期	测试	删除 有效期
<input type="checkbox"/>	渠道scp	永不过期	测试	删除 有效期
<input type="checkbox"/>	会议系统生产环境	永不过期	办公应用	删除 有效期
<input type="checkbox"/>	sdp133	永不过期	其他应用	删除 有效期
<input type="checkbox"/>	zex_sdp	永不过期	测试	删除 有效期
<input type="checkbox"/>	EDR安全赋能平台	永不过期	测试	删除 有效期

□ 基于组授权: 部门

□ 基于用户授权: 个人

□ 基于角色授权: 岗位





联动网络设备



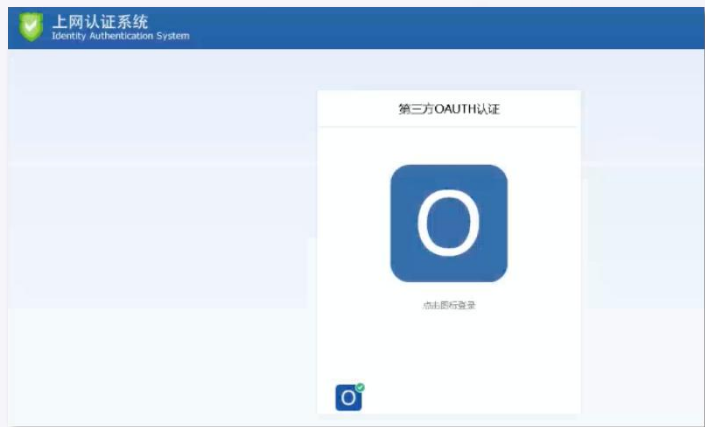


- 同时对接网络设备和业务系统
- 支持对接AC、VPN、EMM等
- IDTrust保持开放支持对接不同厂家产品
- 联动效果：身份同步/统一认证/单点登录

全网联动效果演示



□ AC联动效果展示



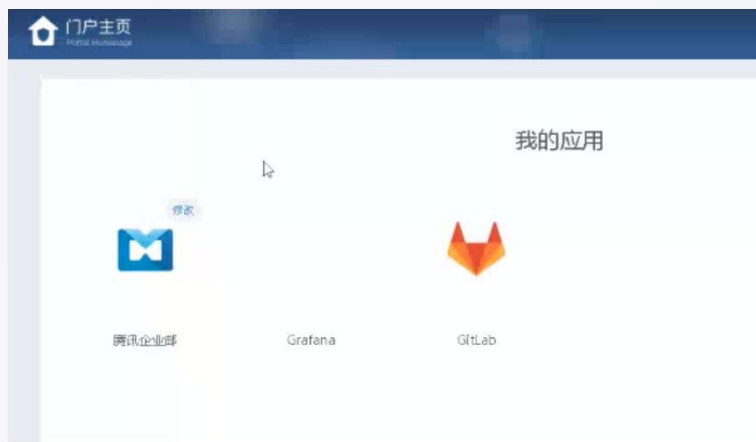
1、用户上网认证，提示跳转IDTrust



2、IDTrust指纹认证



3、认证通过，具有上网权限



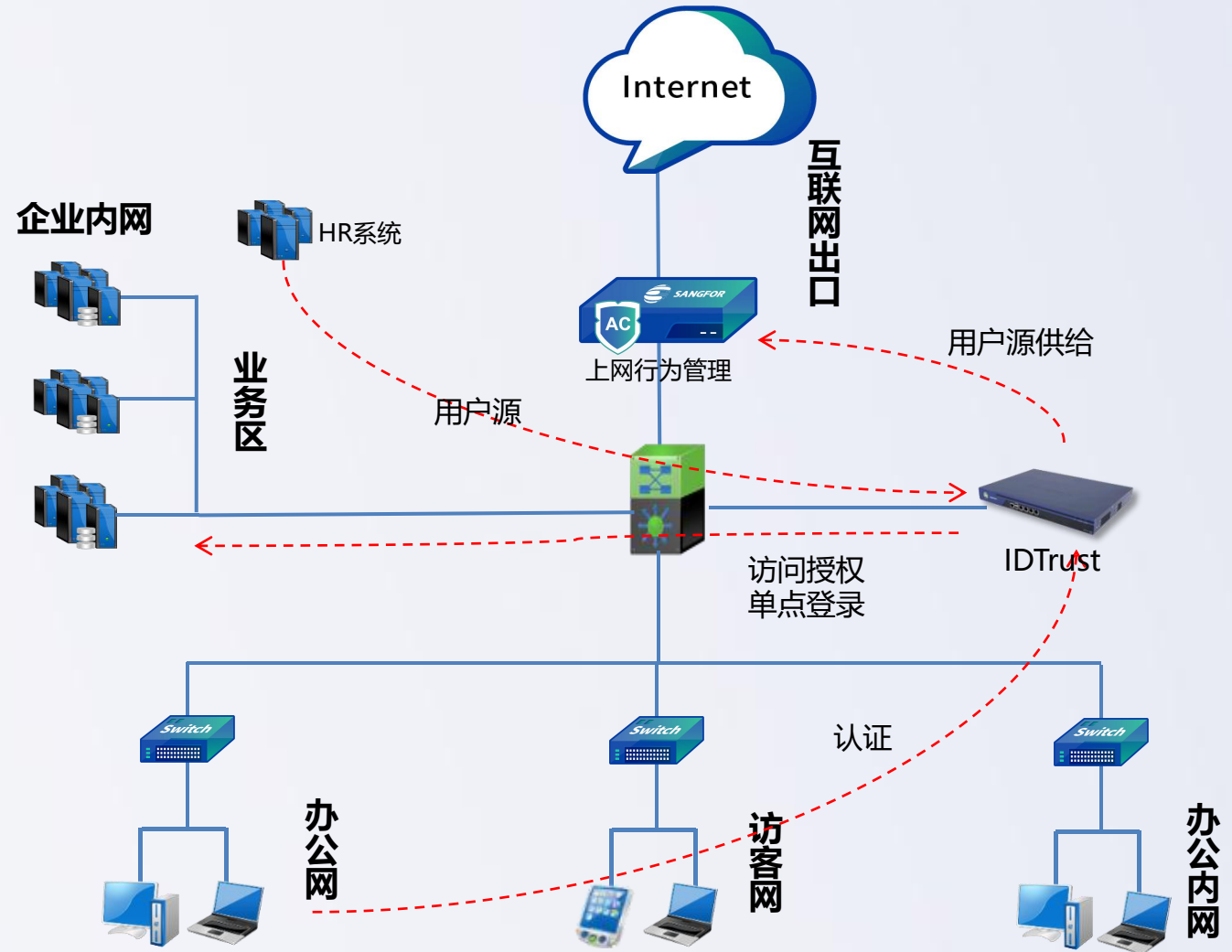
4、无需认证，直接打开IDTrust门户



5、点击邮件，无需认证实现SSO

产品形态及部署方式

- IDTrust产品形态有两种：工控机/OVA镜像
- IDTrust设计架构建议：主主/主备



我的应用

淘宝网	新浪微博	36kr	goole	知乎	优酷
Bilibili	Producthunt	QQ空间	搜狗	Dribbble	京东
Iconfont	8613Free Svg	大众点评	新浪网	Tripadvisor	站酷

搜索用户名 | 请输入关键字

因子认证	状态	操作
	✓	上移 下移 删除
	⊘	上移 下移 删除
	✓	上移 下移 删除
	✓	-
	✓	上移 下移 删除
	✓	-
	⊘	上移 下移 删除
	✓	上移 下移 删除
	✓	上移 下移 删除
	✓	上移 下移 删除

3 4 5 ... 24 > 每页 10 前往 10 页

目录

- 一. 挑战和背景
- 二. 深信服解决之道
- 三. 成功案例

成功案例



项目背景

某政府单位目前有10万员工，4000+应用，现有4A系统对接了部分应用，认证方式采用账号密码加CA Key。随着员工和应用的逐年增加，现有架构问题越来越多，急需一套开放、高效、安全的身份认证系统支撑现有业务。

客户需求

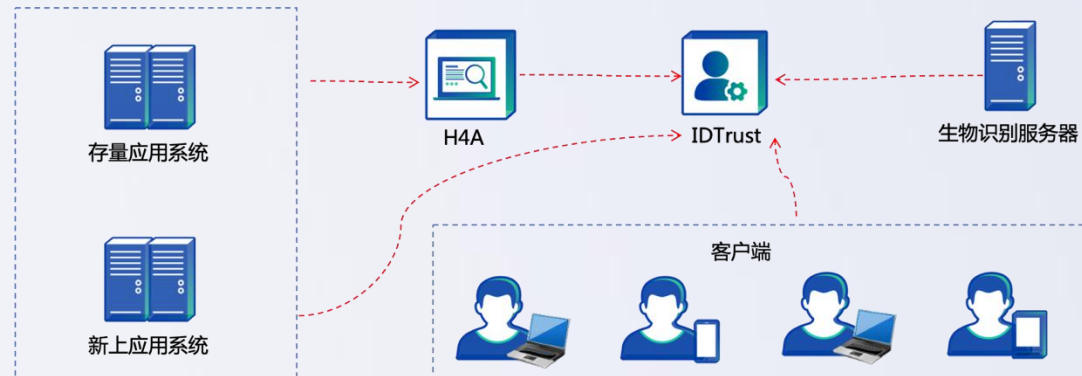
- 1、使用指纹、人脸方式替换原有账号密码认证，二次认证需使用原有CA证书；
- 2、身份认证系统必须保持高度开放，提供标准协议、接口，对接新上业务系统，老旧系统对接逐步替换原有4A系统；
- 3、所有传输必须加密，数据必须保证安全性；

解决方案

部署IDTrust对接CA服务器，新上业务系统，同时提供基于FIDO协议的指纹、人脸认证方式。

方案价值

- ✓ 在保障安全与合规的基础上，实现了便捷认证，使业务办理更高效；
- ✓ 高度开放的身份中心，更具包容性和扩展性，后续应用和系统对接更简单；
- ✓ 在客户需求基础上提供用户自助服务（找回密码、查看修改信息），降低海量用户管理工作；



成功案例



项目背景

某企业客户的业务系统有17个，同时购买了VPN、AC、aDesk、门禁等网络系统，如何打通网络、业务实现全网统一用户管理、统一认证和授权，成为了亟待解决的问题。

客户需求

- 1、建设权威用户中心，自动同步身份信息至网络和业务系统；
- 2、打通网络和业务，建设统一认证和授权审计中心，基于组织架构进行业务应用授权；
- 3、提供统一门户及全网单点登录，任意系统认证即可全网SSO；

解决方案

部署IDTrust实现统一身份管理、统一认证、集中授权和审计（4A）。

方案价值

- ✓ 建立权威用户中心，实现全网身份生命周期管理；
- ✓ 统一认证和授权审计，加强身份管理提高安全性；
- ✓ 提供统一门户和全网单点登录，提升办公效率；



成功案例



项目背景

某医院目前在申报等级保护三级测评，其中关于业务系统多因子认证的测试项无法满足，另外VPN接入以及堡垒机也面临着双因素认证的要求。

客户需求

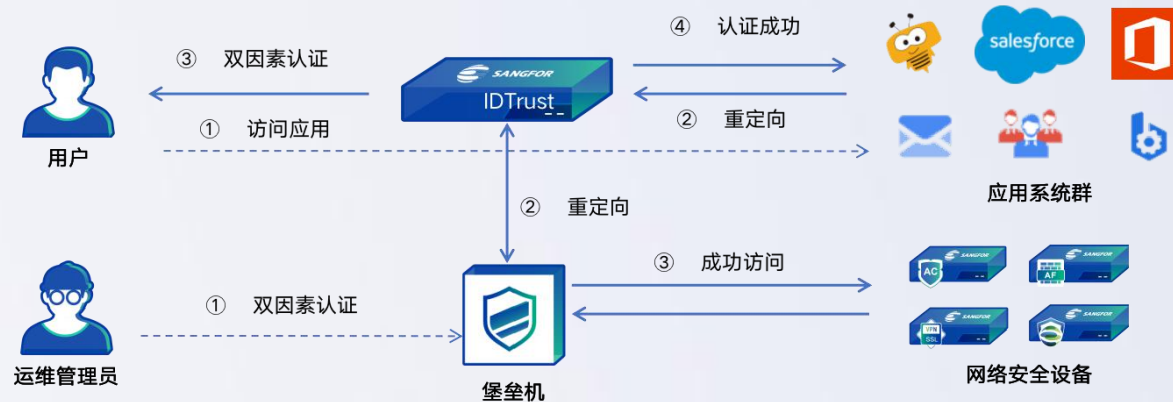
- 1、拉取HR系统的用户信息，同步至VPN、EMM，后续只需操作HR系统即可实现全网同步；
- 2、实现VPN、EMM登录，堡垒机运维以及后续的业务系统双因子认证，满足等保合规要求；

解决方案

部署IDTrust联动VPN、堡垒机，提供身份信息同步以及多因子认证能力，满足合规要求。

方案价值

- ✓ 全网统一身份体系，实现自动化身份信息同步；
- ✓ 多因子认证提高认证强度，保障业务安全；
- ✓ 满足等保高风险项要求，促进通过等保三级测评；





THANK YOU

深信服 智安全

一、确定身份源

- 1、IDTrust是否需要对接现有的身份源系统（HR系统、AD域等）？还是IDTrust就是用户源？
- 2、如果需要对接，那请问身份源支持哪些方式对接？（IDTrust提供：ldap、数据库同步、api）

二、确定对接的应用

- 1、业务系统需不需要从IDTrust同步用户？
- 2、业务系统是否需要实现单点登录？

说明：请收集客户期望的应用对接情况，收集模版《应用系统信息收集表.xls》

三、认证方式

- 1、认证方式想采用账号密码，还是考虑指纹、扫码、动态码等，或是双因素认证，具体是哪些认证方式？

四、统一门户

- 1、客户需不需要统一门户？
- 2、如果需要，统一门户是由IDTrust提供，还有客户已经有现成的门户了（已有门户则需要集成工作）？

主从账号解决老旧系统存量账号无法同步的问题

- ❑ 老旧系统存量账号第一次需要手动导入至IDTrust作为从账号，后续账号状态自动同步
- ❑ 新员工身份同步，IDTrust会按照主账号名称同步至业务应用
- ❑ 员工只需要记住IDTrust主账号，员工在点击业务应用图标时，IDTrust会拉起对应业务应用账号，全程无感知
- ❑ 身份同步不会同步密码信息，标准协议及API接口认证流程不需要密码，仅密码代填需要



附录-菜单级权限自动化分配


- 业务应用第一次需要配置好组与功能模块的策略，后续身份同步自动获取菜单级权限

□ OA系统:



IDTrust

部门/岗位

A screenshot of an OA system's 'Department Management' (部门管理) interface. The interface is divided into several sections. On the left is a navigation menu with '部门管理', '用户管理', and '岗位角色'. The main area is titled '新建部门' (New Department) and contains a '部门列表' (Department List) on the left and a form on the right. The '部门列表' includes a tree view with '深圳' (Shenzhen) as the parent, and sub-items like '运营中心', '客服部', '行政人事部' (highlighted with a red box), '财务部', '市场部', and '设计部'. The form on the right has fields for '企业全称', '企业简称', '电话', '传真', '邮编', and '管理员邮箱'. Below this is a '岗位管理' (Position Management) section with a table showing '排序序号' (3), '岗位名称' (职员, highlighted with a red box), and '岗位分类' (默认分类). Below the table are buttons for '权限设置' (highlighted with a red box), '岗位说明书', and '岗位成员'. At the bottom, there's a '人力资源' (HR) section with a '组织架构' (Organizational Structure) checkbox checked, and buttons for '用户管理' (View/Manage), '岗位管理' (checked), and '部门管理' (checked).