派拉软件
PARAVIEW SOFTWARE

替换AD&国产化架构方案

——数字身份安全专家——

背景

安全性差

- 大量使用非加密通道
- 密码策略单一大量存在简单密码和重复密码
- 特权账号密码无强认证
- 管理员需要登录域控本机操作
- 不支持国密算法（密码存储、数据通道）

平台局限

- 限制在Windows平台
- 微软系应用服务绑死
- Mac系统无法兼容
- 国产化系统无法兼容
- 商业化、自开发应用对接困难
- 被互联网应用抛弃

管理复杂

- 管理平台繁琐，无法支持Web化管理
- 备份恢复操作困难
- 批量操作缺乏，运维人员工作量巨大
- 与IIS、ADFS等联合配置非常复杂繁琐

认证方式单一

- 只能支持简单的用户名密码登录
- 无法进行多因素认证
- 无法支持认证协议，进行单点登录

网络架构限制

- 只能部署企业内网
- 外部用户必须拨入VPN后才能使用
- 离线情况基本不可控
- 跨组织无法互信、同步

替换AD步骤

1.建设IAM

建设统一身份管理
建立权威数据源
单点登录
网络设备认证更改
非微软系服务认证更改

2.域下线

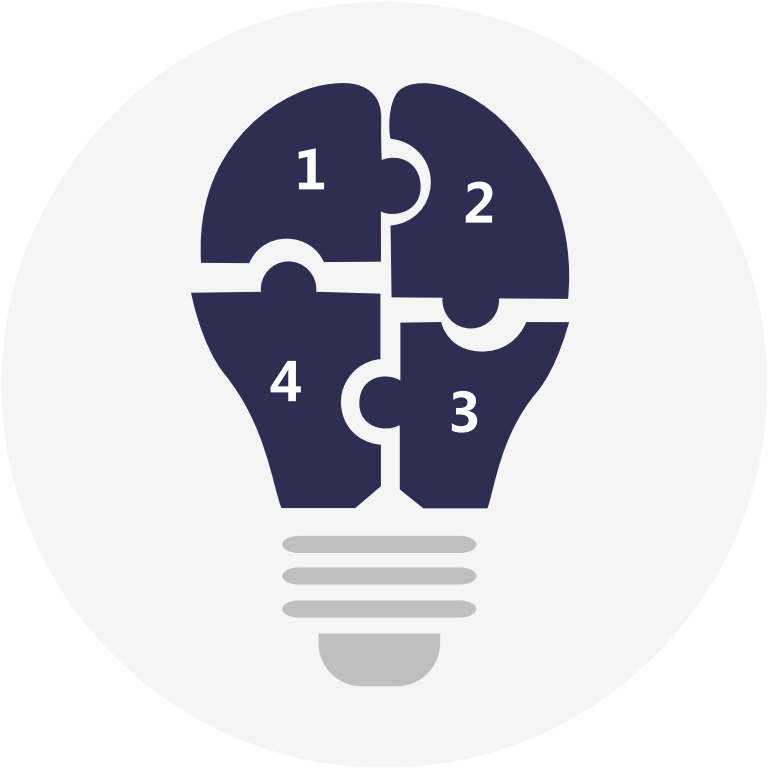
Windows操作系统退域
Mac接入统一认证
Linux接入统一认证
系统本地用户&策略接管
统一多因素强认证接入

3.AD下线

AD停止服务
域功能接管
微软系应用服务替换
风险识别
终端管控、安全基线

4.全面国产化

国产操作系统
国产中间件
国产PKI体系
通讯&数据国密化
零信任架构



分段规划，逐步实施

1. 建设IAM

统一身份管理

身份&角色&权限同步
身份全生命周期管理

权威数据源

企业员工身份唯一主数据源
认证凭据组织内唯一

单点登录

CAS、OAuth2、OIDC、SAML、ADFS
安全保障、多认证中心互信、域单点

网络基础设施认证

准入、F5、VPN、防火墙、备份设备
派拉EDS、Radius中转权威身份数据

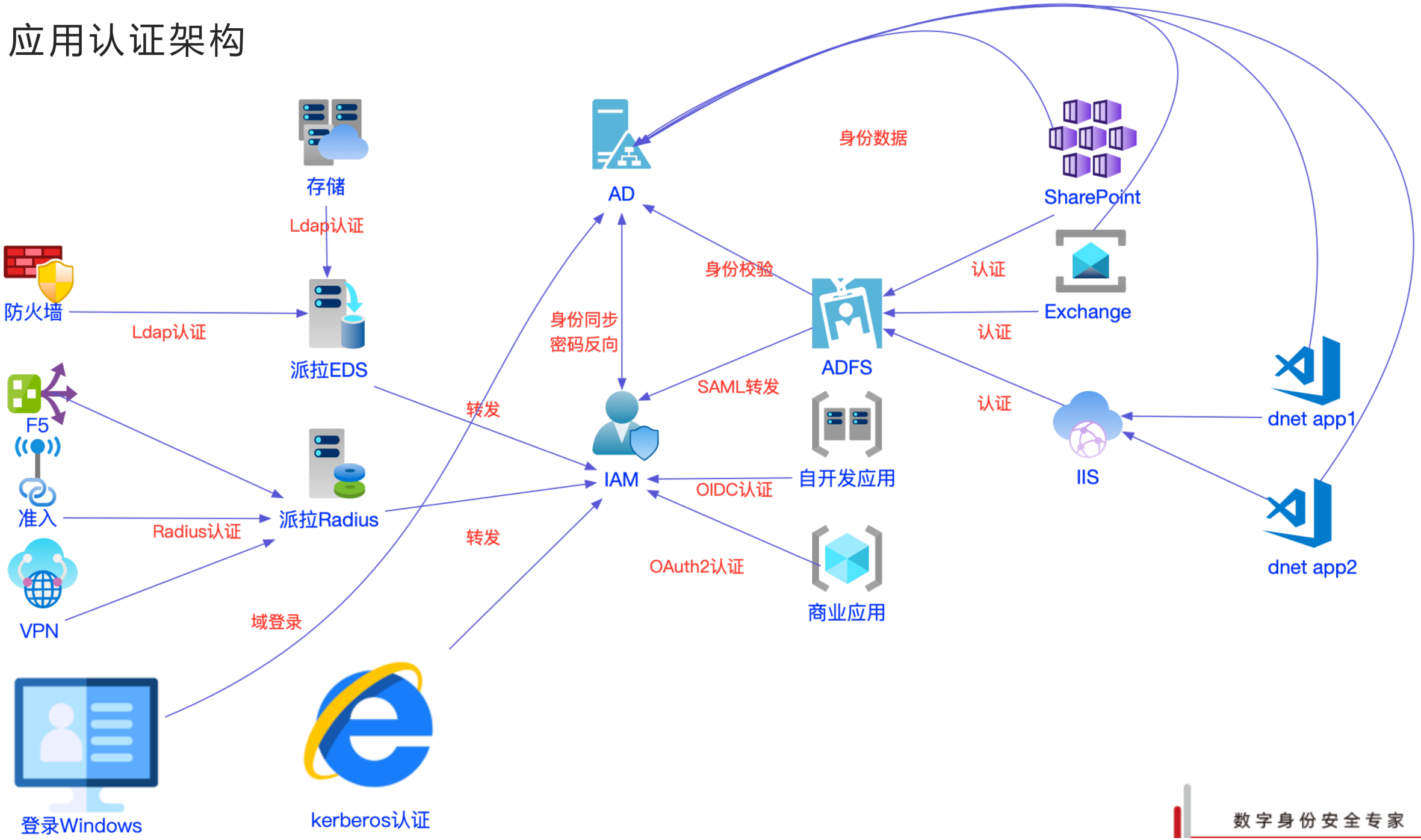
应用认证

自开发应用、商业应用、微软系应用
协议认证、LDAP认证、Radius认证中转

AD统一管理

AD用户、组织、组转交IAM管理
AD密码反向同步保证密码一致

应用认证架构


存储
Ldap认证
AD
身份数据
SharePoint
防火墙
Ldap认证
派拉EDS
身份校验
身份同步
密码反向
ADFS
认证
Exchange
认证
F5
转发
SAML转发
认证
dnet app1
IAM
自开发应用
IIS
准入
Radius认证
派拉Radius
OIDC认证
转发
VPN
OAuth2认证
商业应用
dnet app2
域登录
登录Windows
kerberos认证

AD域密码问题解决方案

密码策略不统一

问题：AD自带的密码策略与IAM或其他应用的密码策略不一致，导致一个点修改密码其他地方自动修改密码失败；

解决：自定义AD密码策略检查插件，用户在本地修改改密码或管理员修改密码，必须通过插件检查密码强度，策略检查插件规则由IAM统一管理；

邮箱客户端锁定账户

问题：AD密码被外部修改或离线修改后，本地邮箱客户端使用旧密码不停重试导致账户被锁定；

解决：邮件协议代理服务器，截获用户认证，在少于规定锁定账户前锁定邮件客户端登录行为，防止整体锁定AD账户

系统本地凭据不更新

问题：操作系统本地记住的凭据密码，在密码被修改后未同步更新，如打印机、共享目录、FTP等；

解决：通过安装客户端策略工具 ，自动与IAM联动，密码修改后自动更新本地登录凭据；

密码重置方法单一

问题：用户只能使用Ctrl+Atl+Del方式修改密码；

解决：IAM与AD联动，使用IAM丰富的修改密码方式进行修改密码，包含密码找回，忘记密码等；并可以提供密码到期提醒服务 ，大幅减少IT管理工作量；

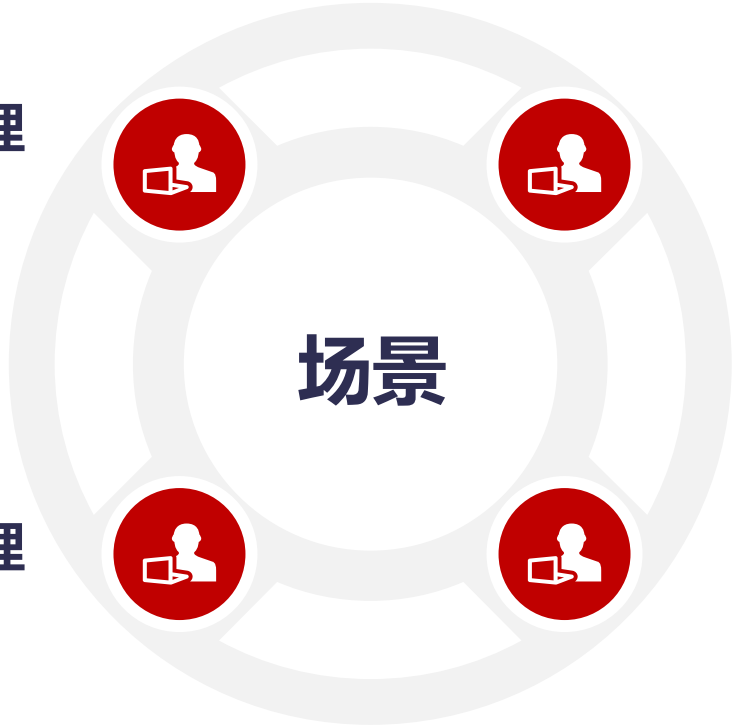
应用场景

AD用户、组、安全组管理

IAM作为权威数据源，管理用户生命周期，并自动同步到AD，解放AD管理员操作；
AD的密码策略，过期通知、自动修改、自助找回，通过IAM统一管理

Exchange邮箱管理

通过Exchange同步器，管理员从IAM中自动管理Exchange账号的邮箱创建、禁用、删除、迁移



单点登录&身份管理

自开发应用、商业应用使用认证协议与IAM集成；
微软系应用或部署IIS应用，通过ADFS月IAM互信进行单点登录；
与AD域集成，通过kerbose认证与操作系统单点；

网络设备统一认证

派拉提供标准的LDAP和Radius服务，用于网络设备的认证接口集成，LDAP和Radius服务接收认证请求后统一转发到IAM认证，提供统一认证能力

2. 域下线

Windows登录接管

登录页面接管，桌面单点
Outlook登录页面接管

Mac登录接管

登录页面接管，桌面单点
SSH登录接管

Linux登录接管

登录页面接管，桌面单点
SSH、Telnet登录接管

本地用户管理

本地用户、组创建、修改、删除
密码自动管理

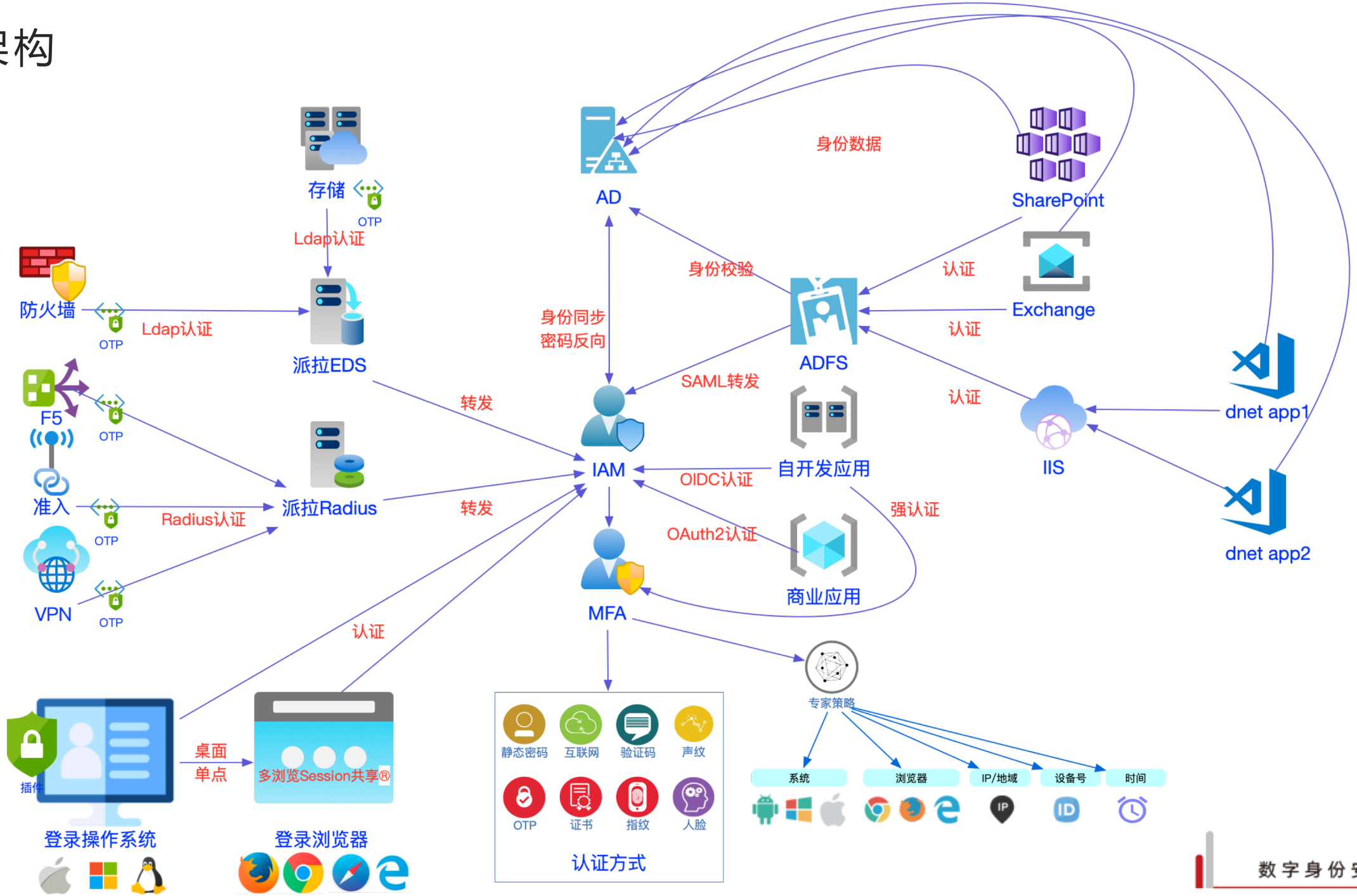
本地策略管理

组策略管理配置
系统策略管理配置

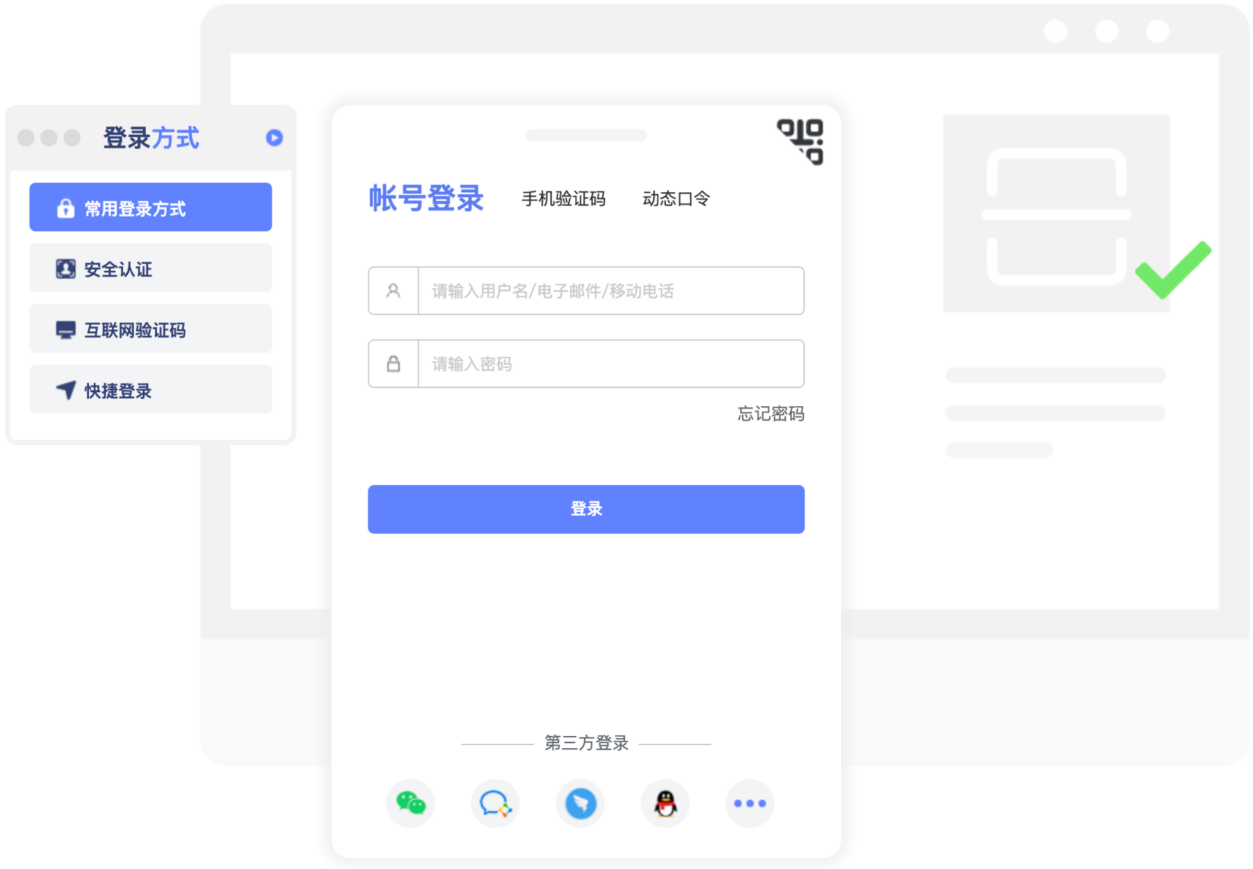
多因素强认证

20+强认证方式、互联网融合
专家策略风险规避

架构

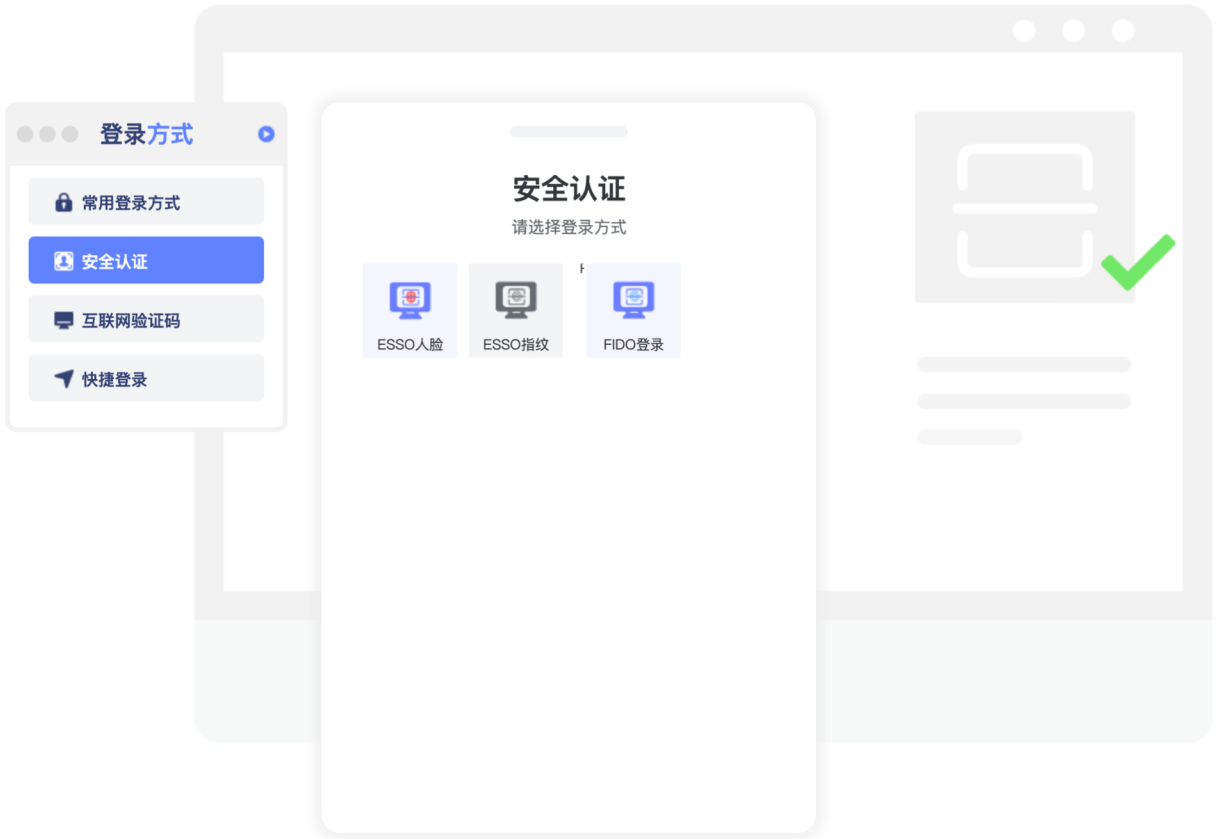

存储
OTP
Ldap认证
AD
身份数据
SharePoint
防火墙
OTP
Ldap认证
派拉EDS
身份校验
认证
Exchange
身份同步
密码反向
ADFS
认证
F5
OTP
转发
SAML转发
认证
dnet app1
IAM
自开发应用
IIS
准入
OTP
Radius认证
派拉Radius
转发
OIDC认证
强认证
dnet app2
VPN
OTP
OAuth2认证
商业应用
MFA
认证
专家策略
插件
桌面
单点
多浏览Session共享®
静态密码
互联网
验证码
声纹
系统
浏览器
IP/地域
设备号
时间
OTP
证书
指纹
人脸
认证方式
登录操作系统
登录浏览器

强认证方式



常用登录方式

- 账号密码登录
- 手机短信验证码登录
- OTP动态口令登录
- 二维码扫码登录
- 社交第三方登录



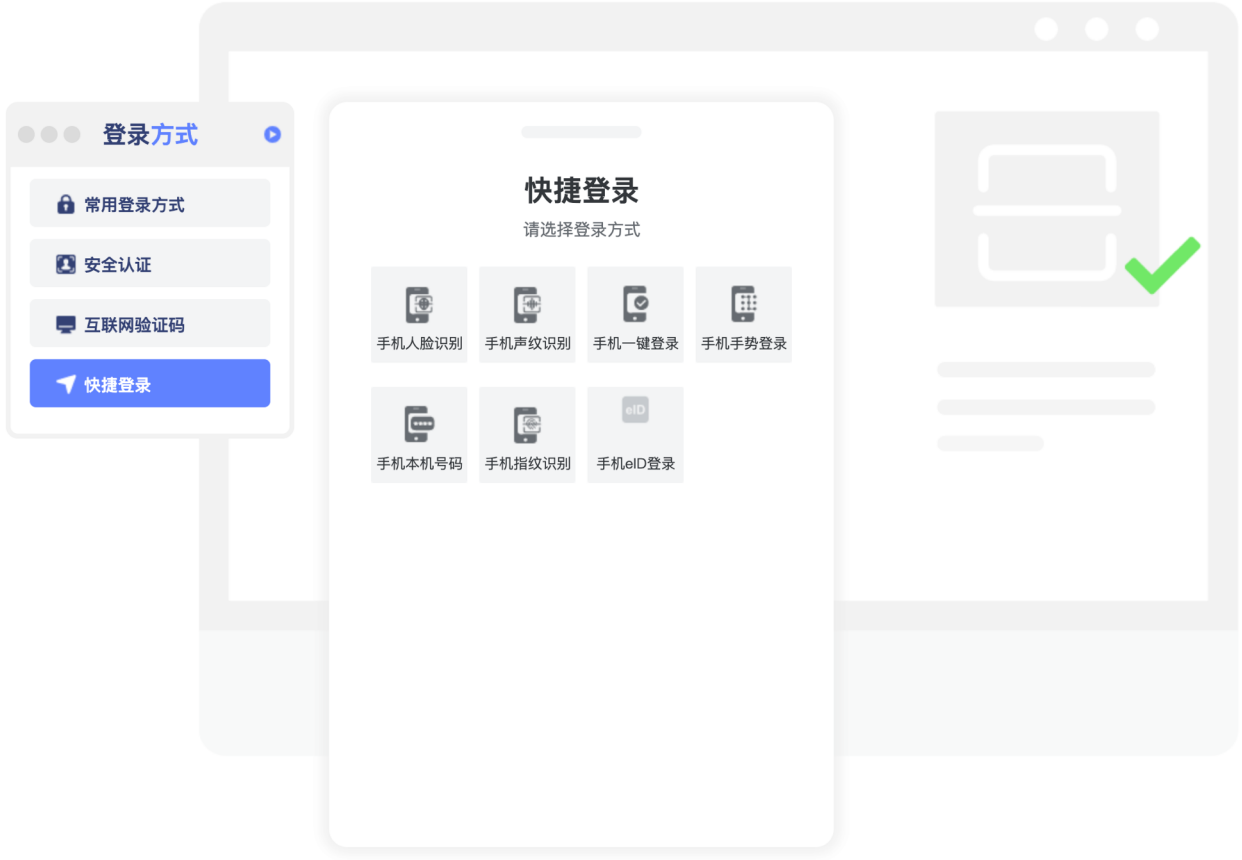
安全认证

- 人脸识别认证
- 指纹，掌纹识别认证
- UKey/PKI认证
- FIDO认证

强认证方式

互联网验证码

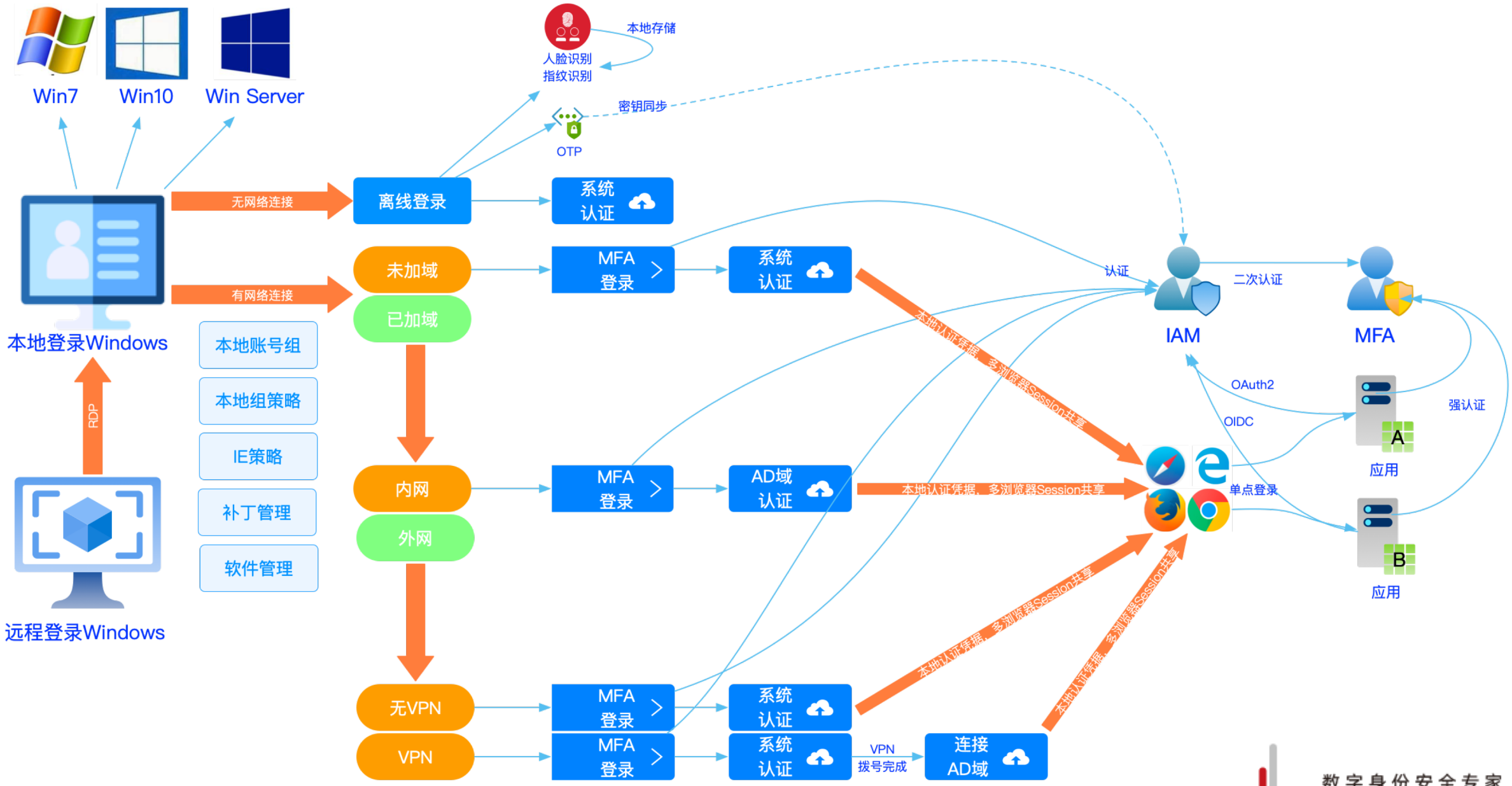
- 钉钉验证码登录
- 微信公众验证码登录
- 企业微信验证码登录



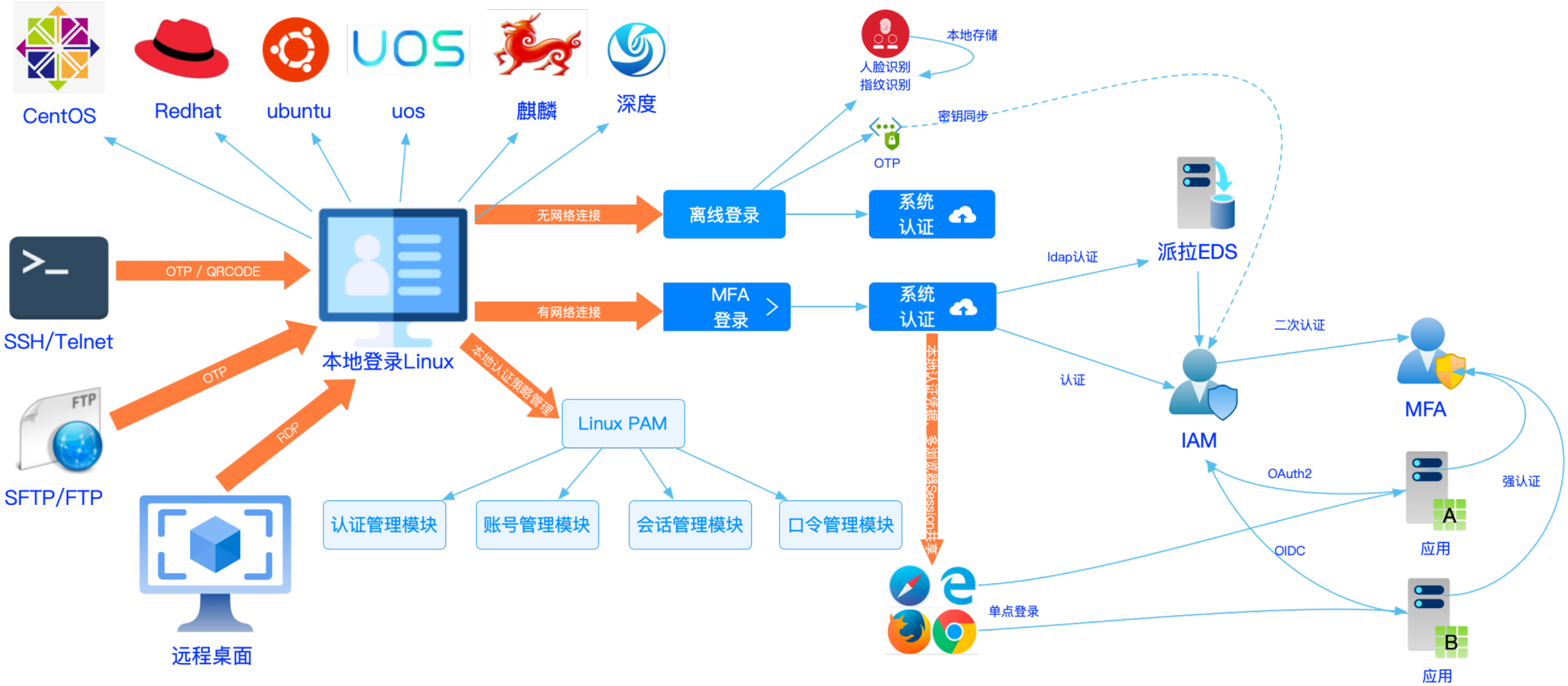
快捷登录

- 手机人脸、指纹、声纹
- 手机一键登录、手势登录
- 手机本机号码登录
- 手机eID登录

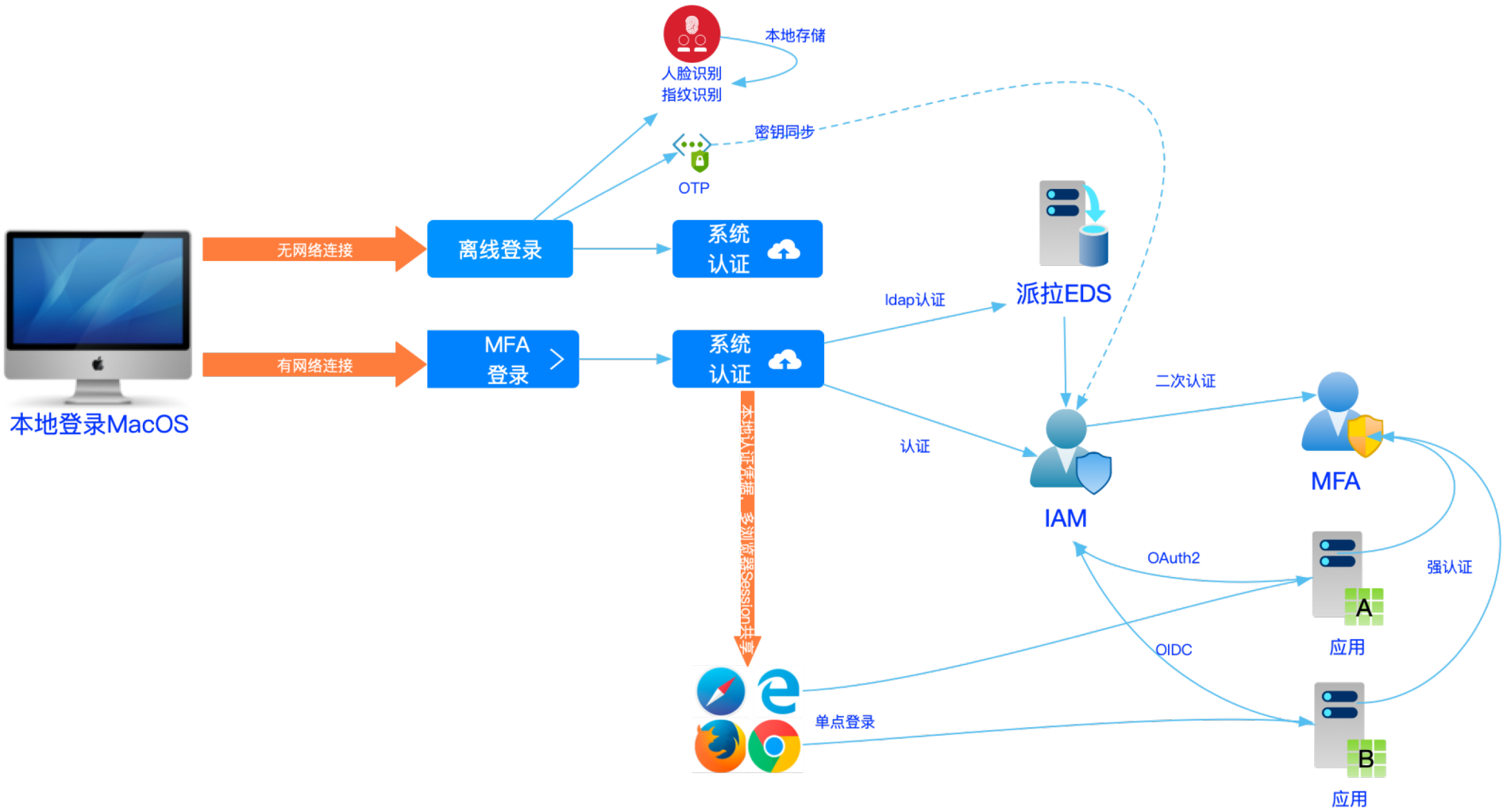
Windows系统登录



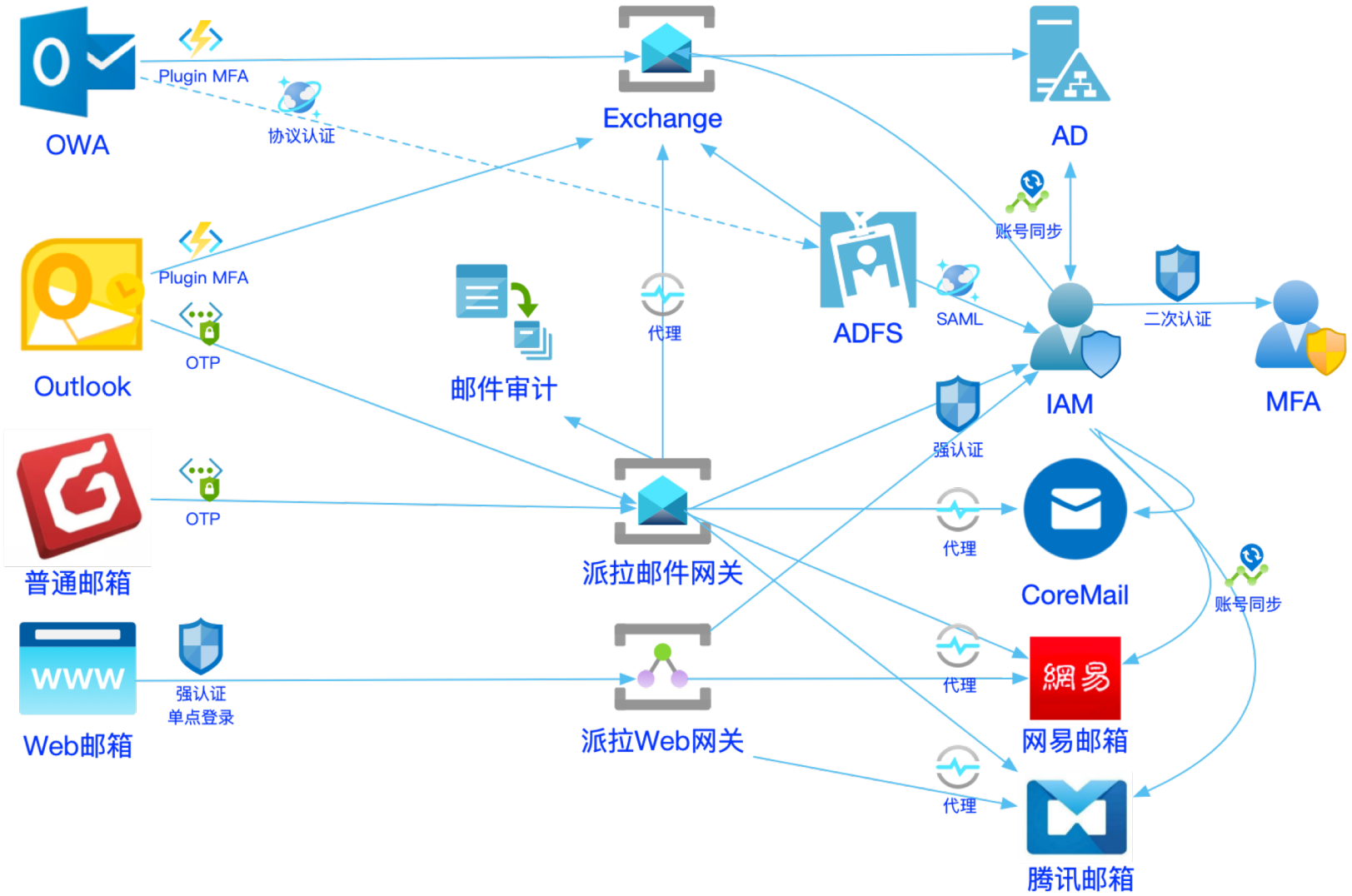
Linux登录


CentOS
Redhat
ubuntu
uos
麒麟
深度
本地存储
人脸识别
指纹识别
密钥同步
OTP
无网络连接
离线登录
系统认证
派拉EDS
ldap认证
OTP / QRCODE
SSH/Telnet
有网络连接
MFA登录
系统认证
二次认证
MFA
本地登录Linux
本地认证策略管理
Linux PAM
认证
IAM
OTP
FTP
SFTP/FTP
RDP
本地认证凭据，多浏览器Session共享
OAuth2
强认证
OIDC
A
应用
认证管理模块
账号管理模块
会话管理模块
口令管理模块
单点登录
B
应用
远程桌面

MacOS登录


本地存储
人脸识别
指纹识别
密钥同步
OTP
无网络连接
离线登录
系统
认证
本地登录MacOS
有网络连接
MFA
登录
系统
认证
ldap认证
派拉EDS
二次认证
认证
IAM
MFA
本地认证凭据，多浏览器Session共享
OAuth2
强认证
OIDC
A
应用
单点登录
B
应用

邮件单点和强认证


OWA
Plugin MFA
协议认证
Exchange
AD
Outlook
Plugin MFA
OTP
邮件审计
代理
ADFS
SAML
账号同步
IAM
二次认证
MFA
普通邮箱
OTP
强认证
派拉邮件网关
代理
CoreMail
账号同步
Web邮箱
强认证
单点登录
派拉Web网关
代理
网易邮箱
代理
腾讯邮箱

AD域下线问题解决方案

系统离线修改用户

问题：无域管理，用户登录系统后在本地修改系统的用户信息、密码、策略、组策略等，怎么检测；

解决：通安装客户端Agent，通过windows标准接口接管了windows用户、组、组策略、密码等操作并定时与iam同步；
Linux/MacOS通过标准PAM Agnet管理本地用户；

操作系统无法强认证

问题：大部分操作系统还在使用用户名密码方式登录；除个别高配笔记本内置指纹仪进行强认证；并且没有统一管理能力；

解决：通过安装客户端Agnet，接管操作系统登录界面，并能实时或离线方式与IAM+MFA进行认证登录，提供20+种认证方式；

kerberos域单点替换

问题：AD域下线后，由于原有旧系统使用kerberos认证方式，只有登录域就可以直接认证访问；

解决：操作系统登录Agnet在经过强认证后会缓存IAM颁发的认证Token，通过派拉多浏览器Session共享技术（专利），实现用户访问集成iam的应用可以直接单点访问，无需再次认证；

邮箱系统无法强认证

问题：市场上大部分邮箱系统还在使用用户名密码方式登录；除个别SaaS邮箱提供了简单的二次认证能力；

解决：通过使用Plugin和邮件协议代理组件，在登录邮箱时进行OTP二次认证能力；

应用场景

本地用户、组、安全组管理

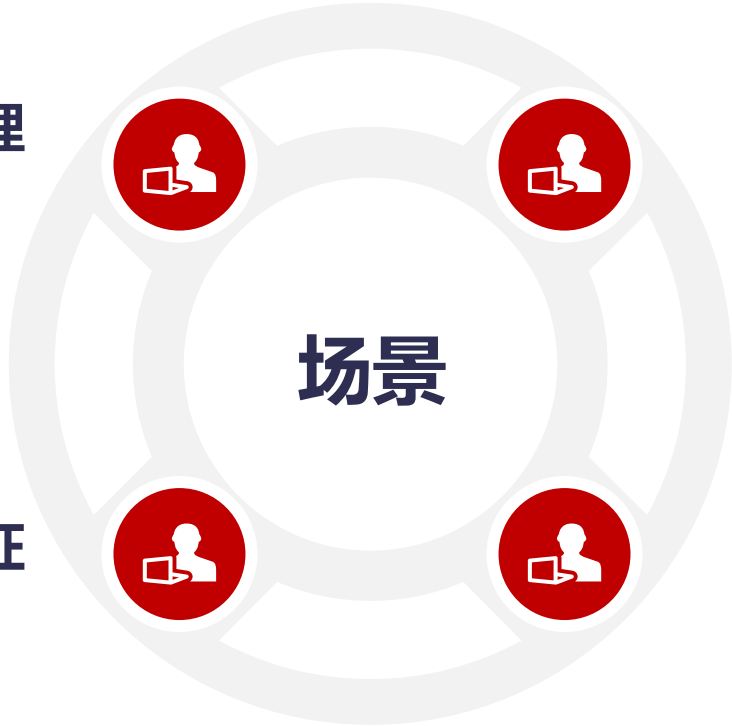
替换AD域功能，包括操作系统本地用户、组、组策略等能力

通过IAM统一管理用户本地系统的用户相关功能

全面的无密码强认证

通过标准认证协议、网关、插件、接口 、SDK与所有需要认证的系统进行连接，用户可以抛弃静态的密码，通过派拉提供的快捷无密码登录方式进入系统；

快捷登录包括：二维码扫描、社交平台集成（微信、支付宝等）、生物认证、硬件卡认证、FIDO认证



与VPN或准入系统联动

提供派拉自研的LDAP和Radius服务，与VPN和准入系统集成，并且提供OTP强认证能力；

通过VPN或准入提供的硬件信息或定制Token，实现网络接入后续操作自动单点登录

全操作系统平台支持

Windows、Linux、MacOS三大平台完全支持

国产系统UOS、麒麟加入生态合作

3. AD下线

AD停止服务

AD历史密码抓取
去除AD环境依赖

域功能接管

DNS、PKI、文件共享功能接管
本地用户、策略、补丁、基线

去微软应用

微软商业应用第三方替代
IIS自开发应用接入IAM

风险识别

监测用户、设备、行为风险
机器学习、AI算法

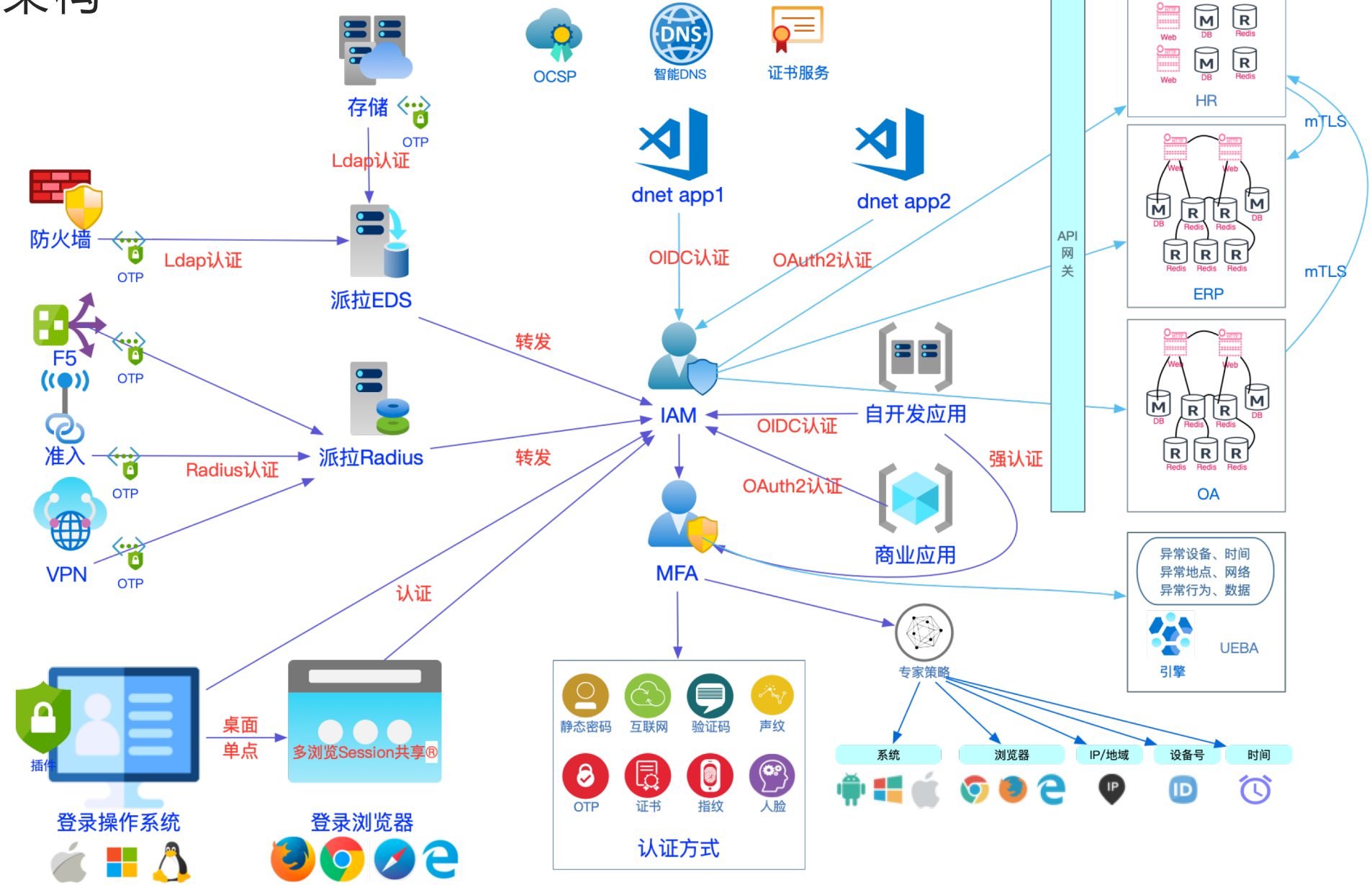
终端设备管控

终端检测、安全基线
补丁软件更新、自动运维、MDM

远程运维

服务器远程访问，单点登录
运维自动化、审计、特权管理

架构



本地账号组 | 本地组策略 | IE策略 | 补丁管理 | 软件管理 | 终端检测 | 安全基线 | 远程运维 | 特权账号

域下线问题处理

AD历史数据怎么处理

AD中存在的用户、组织、组同步到IAM
AD中存在的用户密文密码，通过工具抓取密文存储到IAM，用户登录直接校验

AD域提供的DNS和PKI服务怎么替换

派拉提供智能DNS服务，通策略定义dns解析能力
派拉提供PKI服务，颁发服务端和客户端证书，支持国密，支持mTLS双向认证

微软系应用怎么处理

强依赖AD无法替换LDAP的应用可以使用第三方替换应用

AD域策略怎么处理

派拉提供客户端Agnet，全部管理本地的用户、组、密码、组策略、补丁、软件更新等功能

个人系统怎么运维

派拉提供客户端Agnet，提供MDM功能，远程直接执行远程命令

依赖AD认证的应用系统怎么处理

派拉提供标准LDAP服务，并可以进行OTP登录验证
派拉提供标准Radius服务
LDAP和Radius访问策略通过IAM统一管理

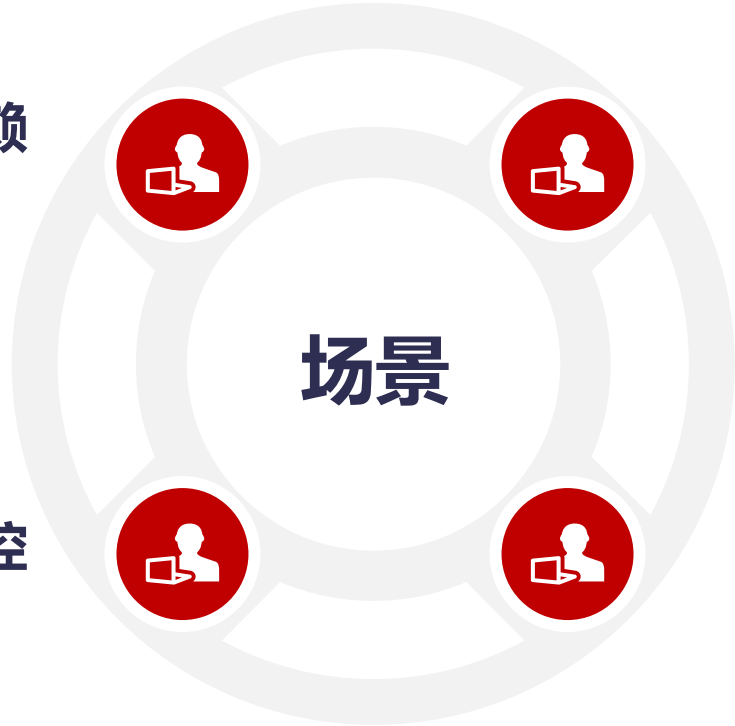
应用场景

组织内去除AD依赖

完全替换了AD所有功能
大量减少IT对AD运维工作量

增强风险管控

通过终端的安全检测、安全基线
用户登录、访问的行为风险识别
对全过程进行风险检测，并进行处置



特权账号管控

无论是操作系统特权账号或应用系统特权账号，
使用人员无需获取明文密码，通过流程审批动态
的下发特权访问权限，并进行全程监控和审计；
在操作敏感信息或命令时通过风险引擎进行判断，
经过强认证后才能继续执行

基于PKI体系的服务访问隔离

所有后台提供的应用服务接口必须同mTLS进行
双向认证，即使黑客进入内部服务器也无法探测
应用接口
提供国密认证和智能DNS能力，进一步加强应用
间访问安全

4. 全面国产化

国产操作系统

国产操作系统平滑迁移
国产操作系统域管理

国产中间件

国产网关、容器、数据库支持

国产PKI

国产PKI体系（算法、证书）
国产mTLS支持，OCSP支持

服务隔离

服务间调用基于mTLS
服务间网络调用隔离

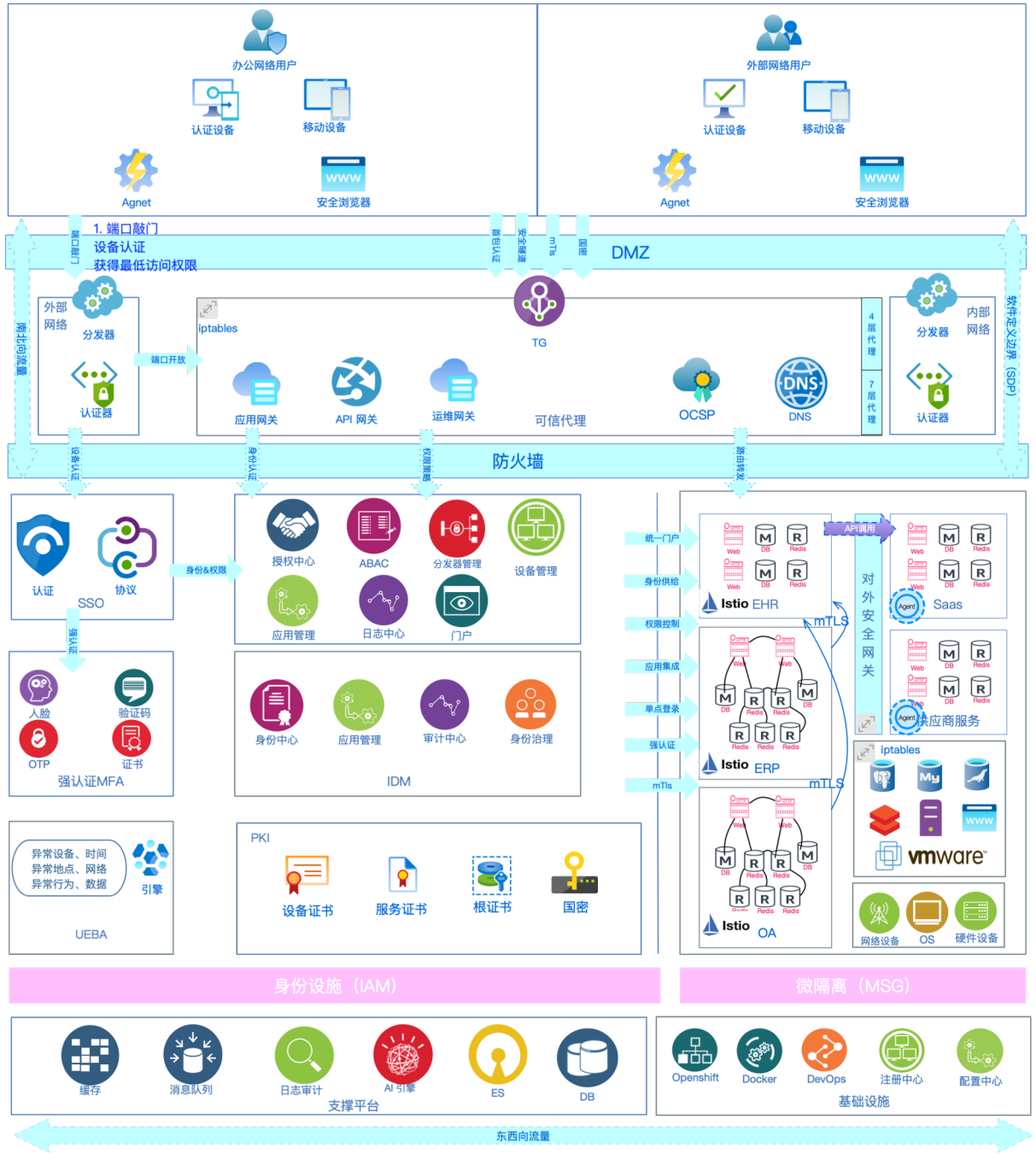
多云管理

多云系统/应用账号统一(SCIM)
多云直接网络数据调用mTLS

零信任架构

SDP、IAM、MSG

零信任架构


办公网络用户
认证设备
移动设备
Agnet
安全浏览器
外部网络用户
认证设备
移动设备
Agnet
安全浏览器
1. 端口敲门
设备认证
获得最低访问权限
端口敲门
单包认证
安全隧道
mTls
隧道
DMZ
南北向流量
外部网络
分发器
认证器
端口开放
iptables
TG
应用网关
API 网关
运维网关
可信代理
OCSP
DNS
4层代理
7层代理
分发器
内部网络
认证器
软件定义边界（SDP）
防火墙
设备认证
身份认证
权限策略
路由转发
认证
协议
SSO
强认证
身份&权限
授权中心
ABAC
分发器管理
设备管理
应用管理
日志中心
门户
人脸
验证码
OTP
证书
强认证MFA
身份中心
应用管理
审计中心
身份治理
IDM
异常设备、时间
异常地点、网络
异常行为、数据
引擎
UEBA
PKI
设备证书
服务证书
根证书
国密
统一门户
身份供给
权限控制
应用集成
单点登录
强认证
mTls
Istio EHR
Istio ERP
Istio OA
mTLS
mTLS
API调用
对外安全网关
Saas
供应商服务
iptables
vmware
网络设备
OS
硬件设备
身份设施（IAM）
微隔离（MSG）
缓存
消息队列
日志审计
AI 引擎
ES
DB
支撑平台
Openshift
Docker
DevOps
注册中心
配置中心
基础设施
东西向流量

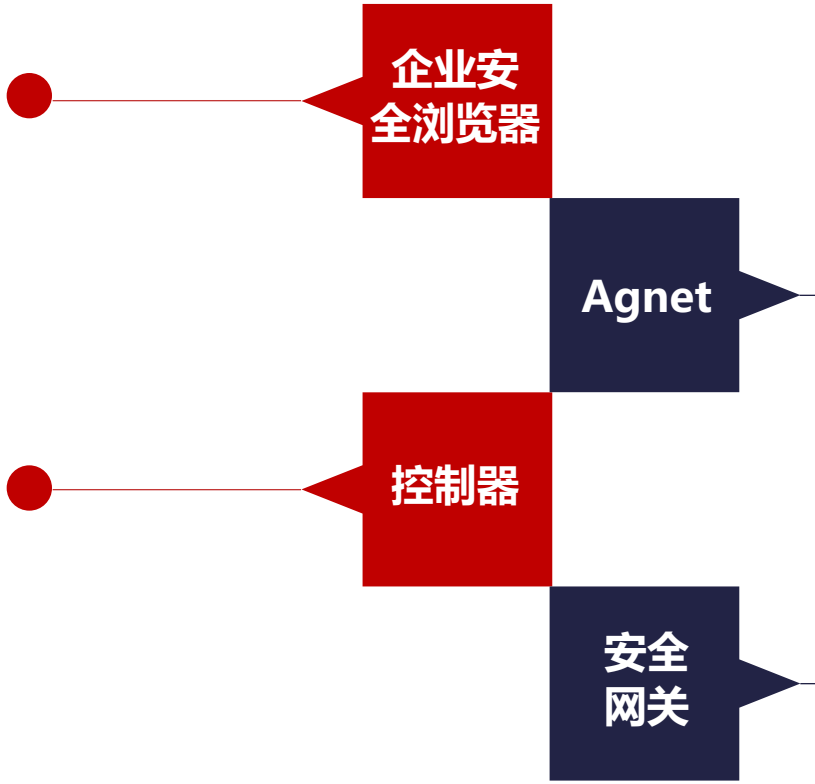
SDP

企业安全浏览器

支持chorme和IE双内核的浏览器，作为Web应用的沙箱，可以有效方式终端环境本身不安全问题；安全浏览器自动与网关建立加密的安全隧道，保障通讯数据的安全性，发布的后端应用只能在安全浏览器中访问，并能支持国密化方案；

控制器

SDP控制器提供一个单向端口，接受终端的认证请求，对终端的设备状态、身份凭据、行为上下文进行判断；只有认证通过的认证的访问请求，控制器才会通知安全网关临时开放访问端口，接受终端的访问请求，并在访问过程中持续监控终端状态，发生访问或设备风险时进行实施阻断网关端口的关闭操作；



Agnet

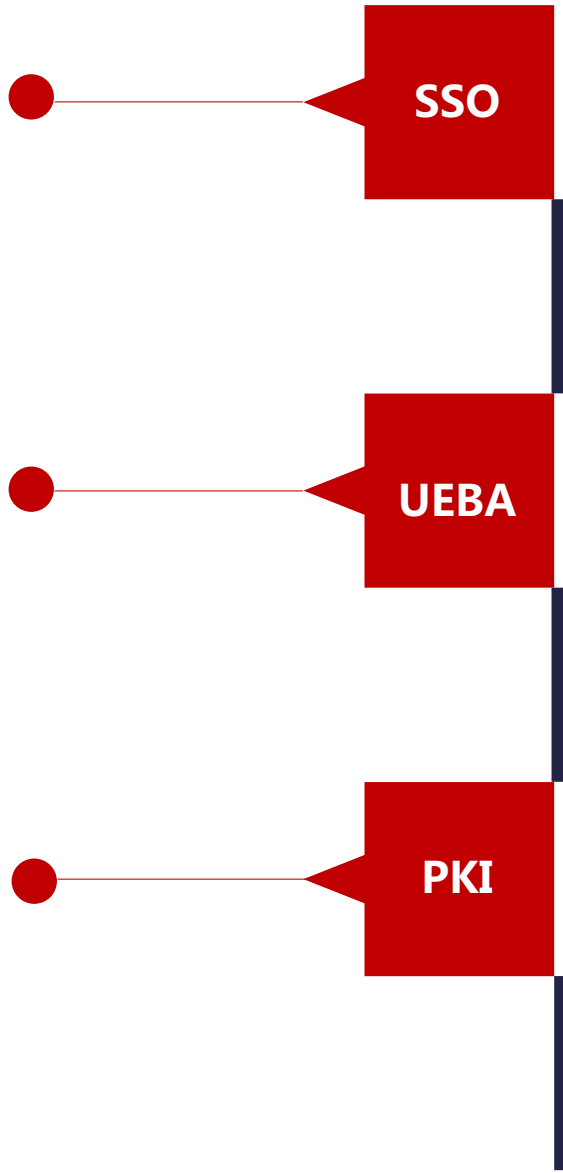
在无安全浏览器或CS应用的TCP通讯场景下，需要一个独立的客户端服务来建立可信的mTLS安全隧道，同时还要负责终端的安全评估、设备的上下文获取、终端的安全基线建立；保证在发起认证前的终端环境的安全；

安全网关

提供一可信的mTLS安全隧道服务，隧道联通后分发到应用网关、API网关、应用网关，满足不同场景下不同应用的代理访问能力，对于终端只能与安全网关进行连接，不与实际资源直接交互，所有流量都通过3个业务网关进行转发，在转发过程中进行实施的细粒度权限控制；

SDP的作用是定义访问的边界，保护南北向流量安全；

IAM



SSO

单点登录组件，提供身份验证、授权；用于零信任架构中所有组件的认证功能；作为一个IDP支持Oauth2、OIDC、SAML等认证中心；

MFA

多因素认证中心，结合SSO和UEBA在用户认证阶段提供强认证能力，标准的OTP、短信认证、二维码扫描、生物认证、第三方互联网认证能力；

UEBA

持续用户行为风险分析能力，在零信任架构中解决持续认证的有效架构，实施的根据终端状态 、访问行为、数据流量、资源状态综合分析，可以通过学习算法和模型进行风险判断，并通过MFA能力进行风险缓解的操作；

IDM

身份控制和管理，统一身份源的建立、角色身份的供给、权限的细粒度控制、资源应用的身份同步能力；有效的整合企业内部所有应用的统一管身份治理能力；

PKI

公钥基础设施，具有数字证书、认证中心（CA）、证书资料库、证书吊销系统、密钥备份及恢复系统等构成部分；为数据通道mTLS的底层安全提供能力，为设备认证和数据发送提供不可抵赖性保障；

控制中心

零信任架构能控制大脑和配置中心，所有组件安装部署配置、策略制定下发、终端网关资源的控制；

1

微隔离提供东西向数据安全保护，即应用程序之间不是人为发起的数据通信的安全保护；

2

Istio对部署在容器的应用集群进行分类保护，以业务系统为单位统一数据出口和入口；逻辑上将数据中心划分为不同的安全段，一直到各个工作负载级别，然后为每个独特的段定义安全控制和所提供的服务。多采用软件方式，而不是安装多个物理防火墙，微隔离可以在数据中心深处部署灵活的安全策略。

3

所有应用程序间交互基于PKI系统提供的证书服务，提供mTLS的双向认证，资源调用者和提供者必须基于证书体现才能进行访问 ；

联系派拉

官 方 网 址：www.paraview.cn
企 业 邮 箱：marketing@paraview.cn
全国服务热线：400-6655-745
企 业 微 信：派拉软件

上海：上海市浦东新区张东路1388号27-02幢
北京：北京市海淀区农大南路1号院硅谷亮成2号楼B座520室
广州：广州市天河区大观中路科汇园A座312室
武汉：武汉市江汉区泛海国际SOHO城6栋3206室
成都：四川省成都市高新区天府大道北段28号茂业中心B座1508室长
春：吉林省长春市高新区飞跃路东北亚文化创意科技园A栋212室