



# 吴洪声

洋葱创始人&CEO 前DNSPod创始人



# 云上的身份认证应对趋势

THE TENDENCY OF IDENTITY AUTHORITY ON CLOUD

当云计算不断发展，信任边界不断弱化，身份验证将何以应对？



Gartner 《2016企业安全趋势报告》：

## 今年企业面临安全问题的

### 5 个核心领域

- 物联网安全
- 网络与移动安全
- **身份认证和管理**
- 应用和数据安全
- 威胁与漏洞管理

然而，据《Verizon 2016 数据泄露报告》统计，  
63.5% 的企业安全事故和身份认证凭据被盗用有关。

## 认证方式



密码口令



硬件设备



手机短信

.....

## 认证管理

Windows AD/LDAP

Radius认证服务器

## 认证协议

OAuth

Open ID

LDAP

SAML

.....

## 4A解决方案

认证

Authentication

账号

Account

授权

Authorization

审计

Audit

## IAM

Identity and Access Management

单点登录 SSO

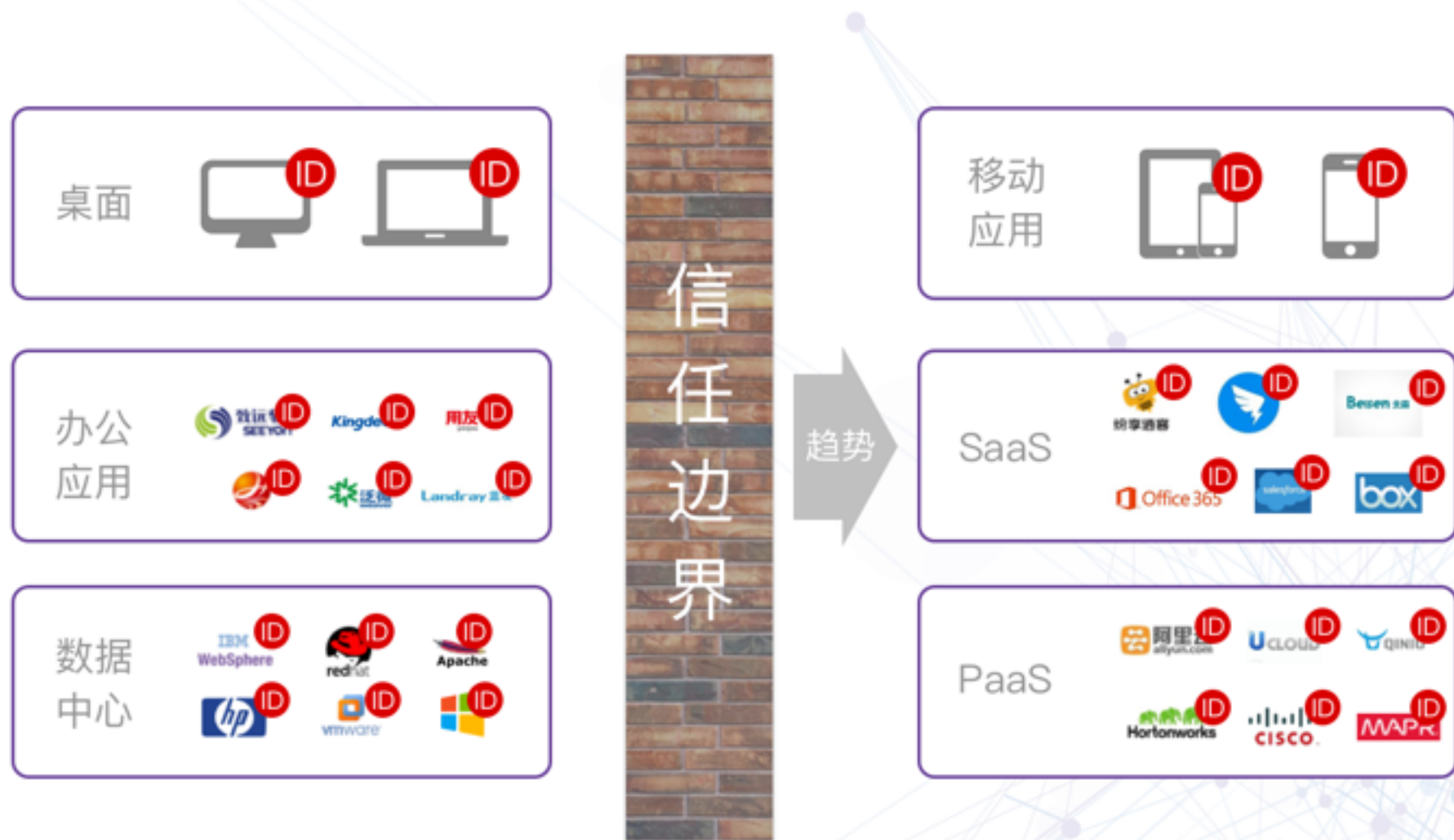
强大的认证管理

基于角色授权

用户行为审计

国内习惯称为4A，而国外更多是IAM，其本质都是**统一认证、统一管理、基于角色的授权和用户行为审计**。  
现在IAM又称之为“**大4A**”。

# 但是，边界正在消失





# 现有的解决方案正在失效



## 边界正在消失

BYOD

云计算

身份变复杂

员工、客户、合作伙伴、子公司、临时授权用户

## 围墙式防御失效

BYOD和云服务让信任边界延伸到你无法控制，看不到的地方

身份验证和有效管理只能作用在防御边界之内的防御

无法有效管理边界之外的身份，无法处理越过边界的威胁。

## 新的诉求产生

身份认证需要同时满足内部应用和云应用

需要在移动设备上实现同样安全便捷的操作

不仅统一管理内部员工，还有合作伙伴、客户等用户

# 于是，“身份”成为一项服务



适应说有用户和设备



以身份供应为中心的服务

强身份验证

单点登录

← 用户行为分析 →

用户目录

生命周期管理

适应云和本地各种场景





# 什么是IDaaS

(Identity as a Service——身份即服务)



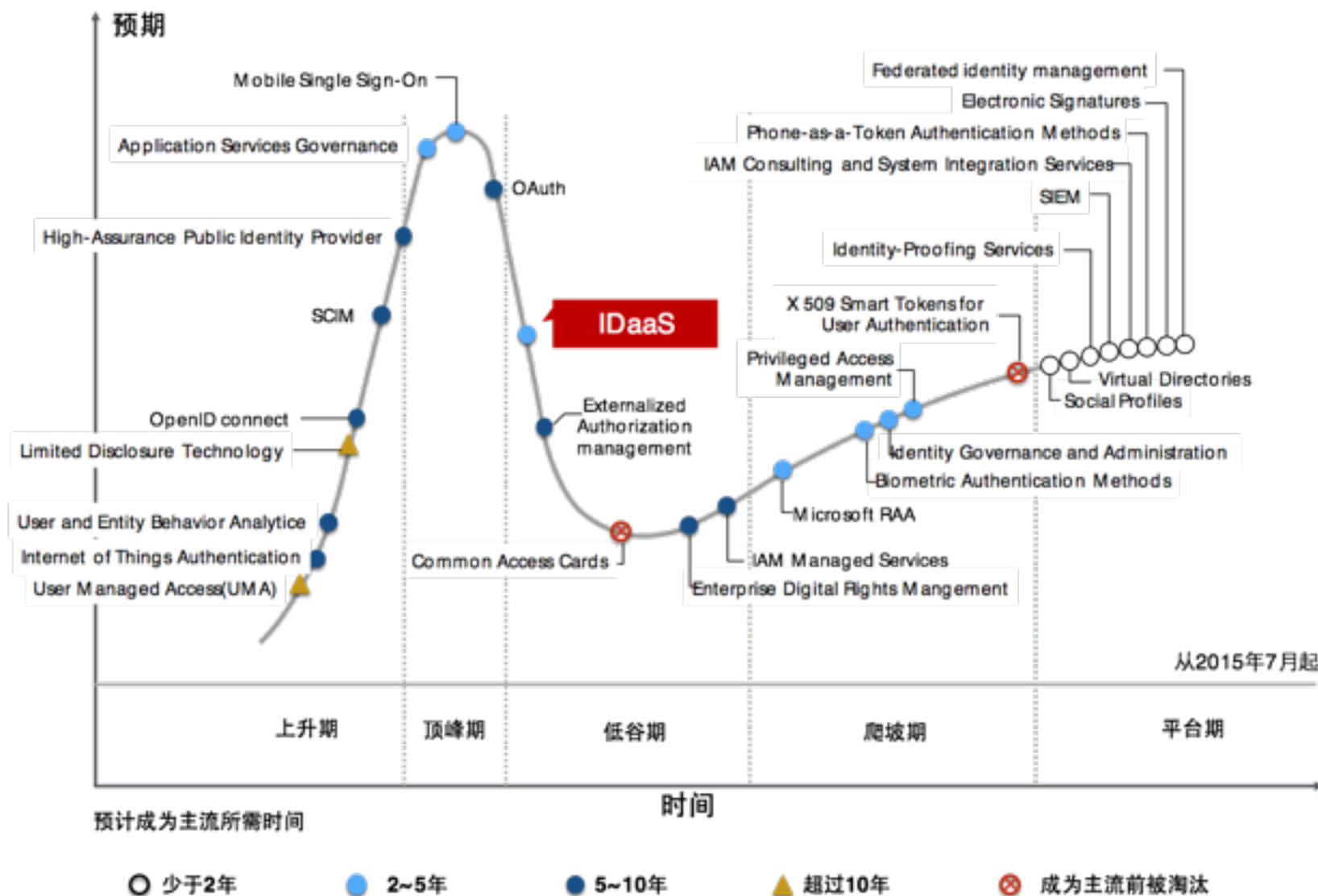
## 定位

- 企业把认证服务委派给云身份提供商
- 云上的SSO单点登录

## 优点

- 同时实现内部和外部的统一认证和管理
- 可以在IAM基础上进行增量投资，部署简单
- 可直接监督身份提供商的安全性和服务水平

# 身份认证行业的各发展阶段及方案



数据来源：《Hype Cycle for Identity and Access Management Technologies,2015》

40% ↑

到 2019年，40%的身份即服务 (IDaaS) 取代内部 IAM 方案，远高于目前的10%

55% ↓

到 2019年，在中等风险场景，密码与令牌使用比例将降低55%，其它新型识别技术将取而代之。

# 身份认证的未来展望



## 挑战

设备接入物联网，认证将成为最大和最频繁的安全挑战

物联网会 形成人与人的交际关系，人与设备之间的访问权限及关系，这些关系都需要管控

## 措施

以人为中心的身份验证体系，数字世界的“身份证”。

基于大数据的用户行为分析，验证变得自动化无感知。

云计算、智能家居、物联网  
让身份认证延伸到衣食住  
行、医疗、工控等等.....

万物互联  
身份无处不在



The background features a light cream color with faint, abstract network-like graphics. These include thin blue lines connecting small dots, some of which are colored in shades of blue and purple. There are also soft, out-of-focus circular shapes in light purple and blue. A solid purple horizontal band spans the width of the image, serving as a backdrop for the text.

THANKS