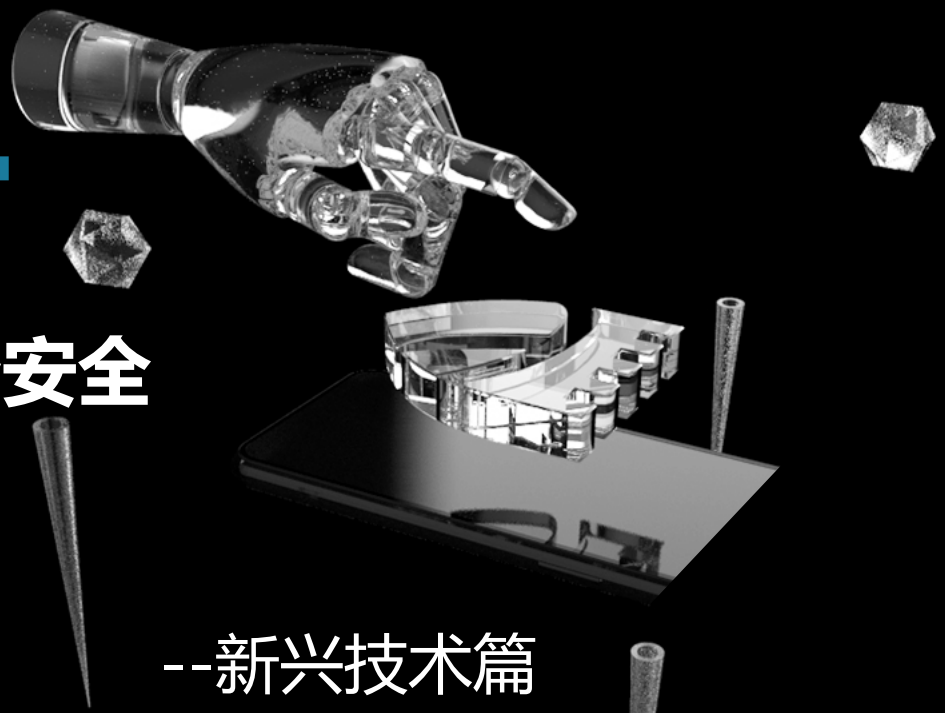
从零信任谈起--
深入剖析以人为核心的业务安全



--新兴技术篇

以人为核心的业务安全

2019.1.18

分类目录

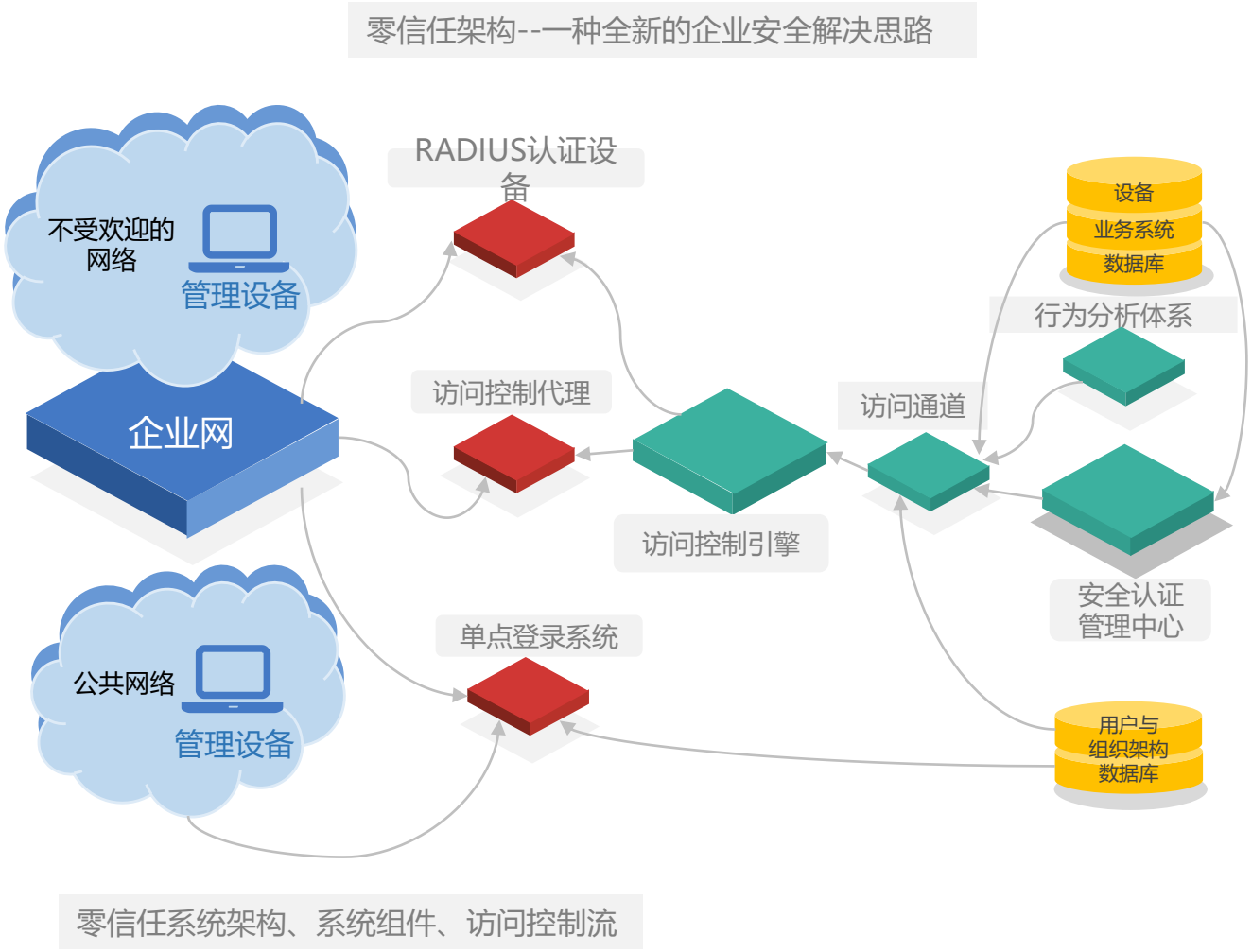
Contents

安全威胁与
零信任架构

芯盾时代
业务安全技术架构

芯盾时代
企业风采

业务安全的最佳实践--零信任安全架构

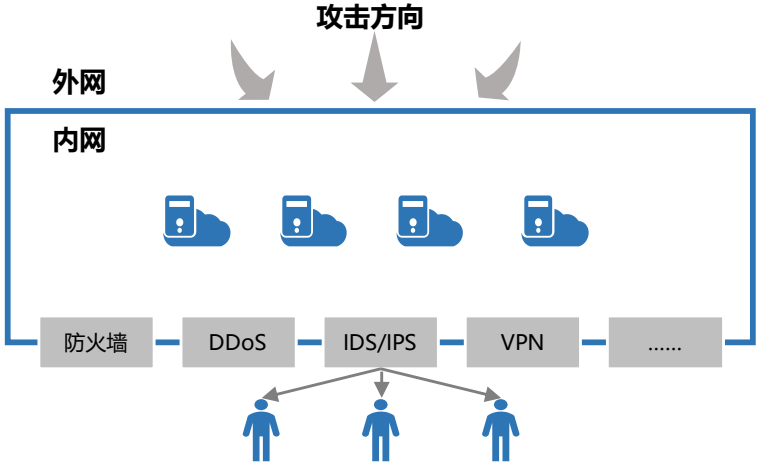


业务安全的初衷是来源于攻防战场的改变

- 统计显示，2017年重大数据泄露事件中**被盗身份是主要突破口，81%**的相关安全事件都源于被盗、默认或弱口令
- 新的安全形势下必须以身份为新的安全边界，**“零信任模型”**将成为最优选择

传统安全

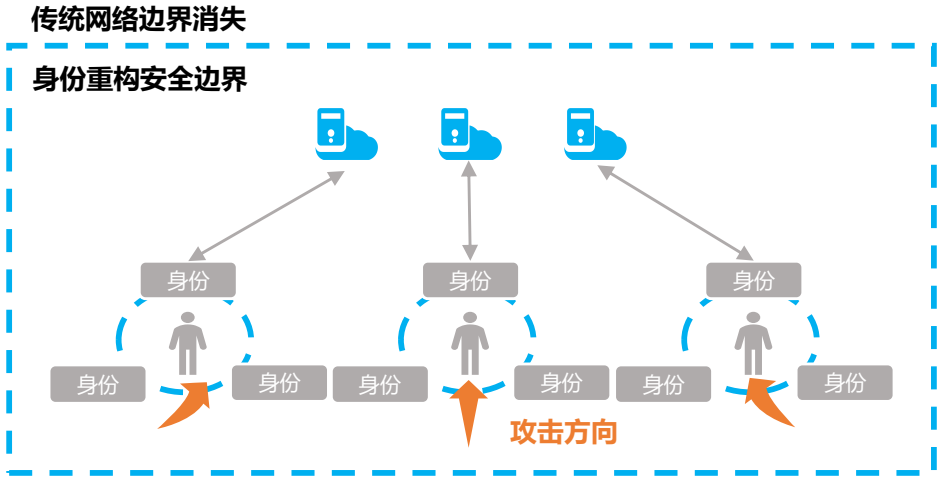
- 背景：信息单向流动，网络核心价值点是设备
- 方式：通过防火墙/DDoS/IDS/IPS等安全设备构建防御边界



传统安全模型认为内网环境是可信任的，内网内部安全防护薄弱；一旦攻破网络边界，整个体系就会处于高度威胁之中

业务安全

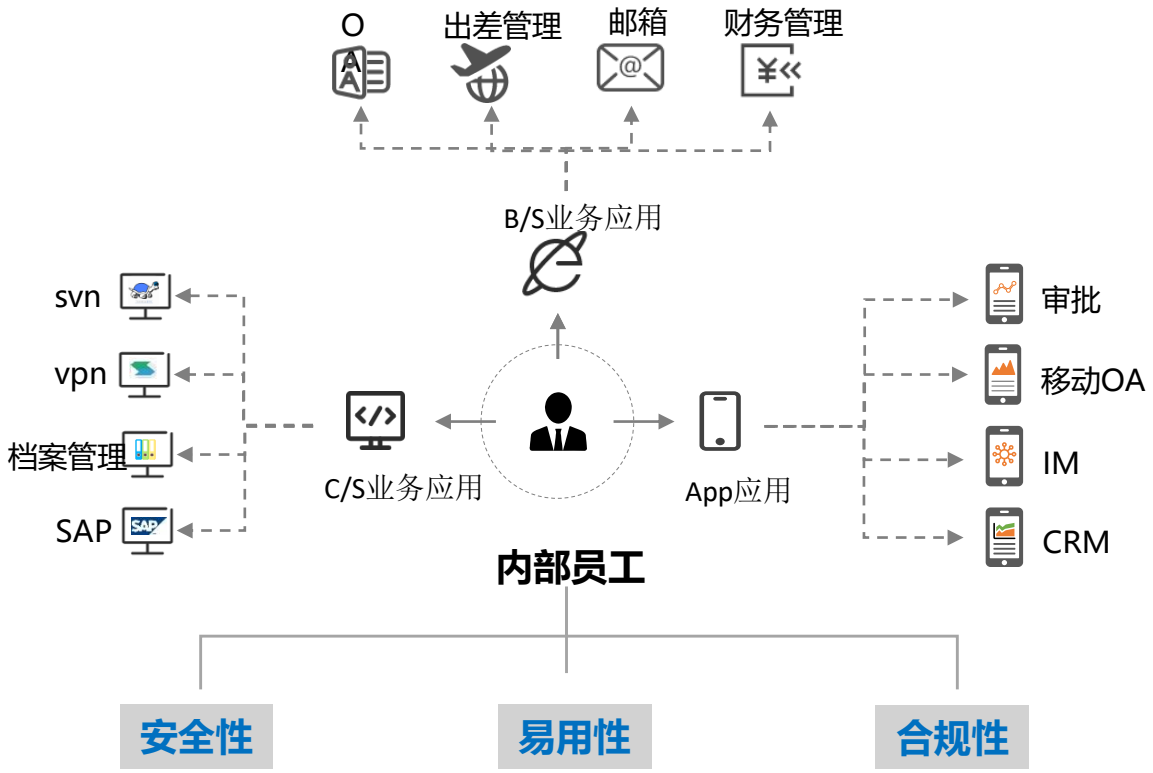
- 背景：移动互联网信息多维流动，“人”是网络核心价值点
- 方式：传统边界消失，以身份为新边界，构建“零信任模型”



只要处于网络中，任何用户都不可被信任。在零信任模型下，任何时刻任何环节，设备、身份及权限都有必要被验证

资料来源： 安全牛

内部泄露往往是信息泄露的最大源头



人民日报四问华住信息疑似泄露 如何避免再次发生？

互联网　人民日报　2018-08-31 06:36　收藏　7 评论　分享

[摘要]目前，一些互联网企业和正处于信息化转型的传统公司，用户信息高度聚集，但安全意识却没能同步升级。

“华住5亿条个人信息疑似泄露”事件引发广泛关注，目前警方已经介入调查。针对公众关注的几个焦点问题，记者采访了业内人士与专家。

项目	金额	用途
手机通话详单	2000~3000	私家侦探、讨债公司、商业间谍；
银行流水单	1000~3000	私家侦探、讨债公司；
身份证/户籍信息	10~40	办理信用卡、网贷、洗钱、重置手机号；
定位、开房记录	150~500	诈骗、私家侦探；
车辆信息	10~40	保险、欺诈；
快递单信息	5~10	电信诈骗、广告、刷单、刷信誉；
银行卡号等信息	0.5~5	电信欺诈等；
已泄露账号信息	0.001	用于撞库；

近3年企业企业信息泄露事件一览

2016年			
1	美国	国家安全局	不详
2	美国	雅虎	5亿
3	美国	MySpace	4.27亿
4	美国	谷歌/微软	2.723亿
5	美国	LinkedIn	1.67亿
6	中国	网易	1亿+
7	美国	Tumblr	6500万+
8	土耳其	政府	5000万
9	英国	反恐资料库	220万
10	美国	Verizon	100万

2017年			
1	中国	京东	50亿
2	美国	yahoo	30亿
3	美国	AWS五角大楼	18亿
4	美国	DRA公司	1.98亿
5	美国	Equifax信用评估	1.455亿
6	南非	Edmodo教育	7800万
7	美国	邓白氏	3380万
8	美国	Uber	5700万
9	美国	Verizon	1400万
10	英国	UK医疗机构	120万

2018上半年			
1	印度	Aadhaar	11亿
2	中国	圆通	10亿
3	中国	华住	5亿
4	美国	Exactis	4亿
5	美国	UnderArmour	1.5亿
6	美国	MyHeritage	9200万
7	美国	Facebook	8700万
8	美国	Panera	3700万
9	美国	Ticketfly	2700万
10	中国	AcFun	800万

地下黑产对政府公信力带来巨大影响

地下产业链

上游：黑客

批量注册软件

刷串号软件

模拟器

中游：卡商

卡商养卡

手机农场

下游：刷客

手机群控系统

批量资料

打码平台

盗转盗刷
电信诈骗
虚假注册
刷交易
刷关注
刷头条
电话推销
伪基站
钓鱼网站
虚拟充值

薅羊毛
社工欺诈
虚假交易
刷评价
刷推广
网络水军
骗补贴
病毒木马
二次打包
信用卡套现

黑灰产业

分类目录

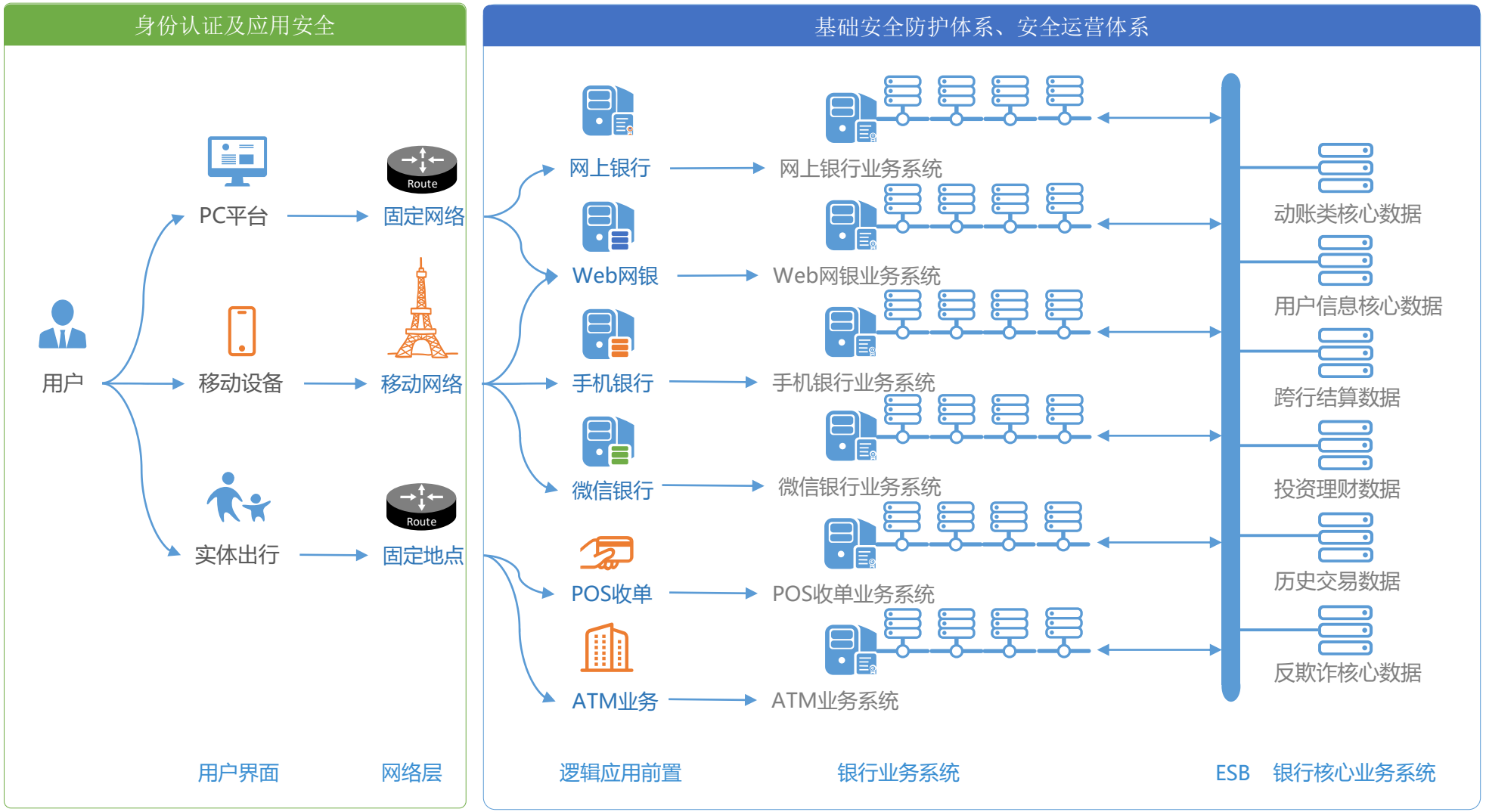
Contents

安全威胁与
零信任架构

芯盾时代
业务安全技术架构

芯盾时代
企业风采

业务安全对身份认证技术变革需求迫切



移动安全：

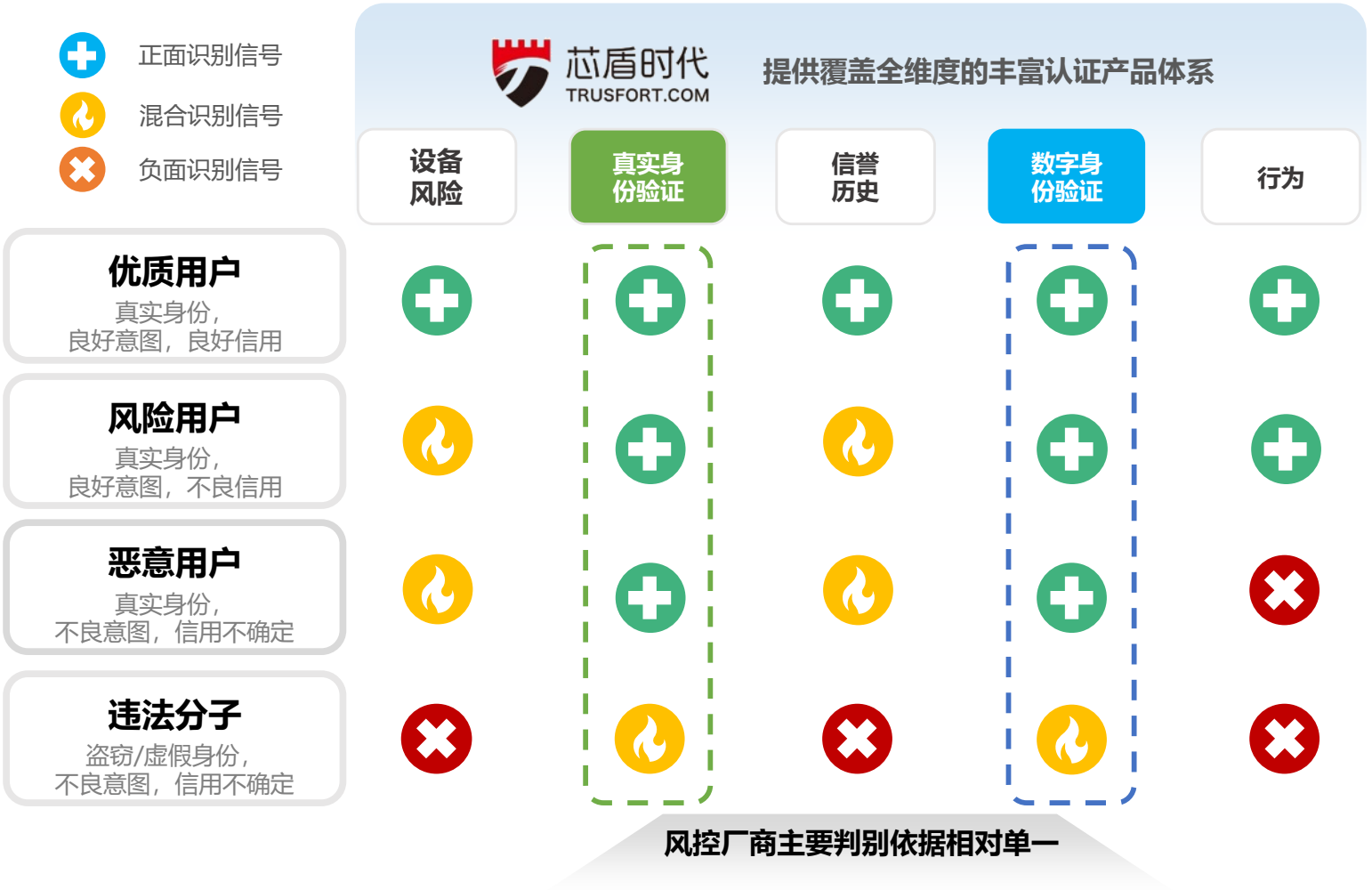
- 身份认证策略；
- 身份反欺诈识别；
- 交易反欺诈识别；
- 移动终端安全；
- 移动连续自适应认证；

传统安全：

- 服务基础安全保障；
- 网络基础安全保障；
- 终端安全保障；
- 运维安全保障；
- 安全态势感知；
- 威胁情报收集处理；
- 安全事件紧急响应；

问题频发的本质是试图使用一种技术手段解决所有安全问题

➢ Gartner认为，在当前伪造身份事件频发的严峻网络环境中，只有通过多维度识别方式才能更好地来判定用户类型（优质/违法）



认证类型	认证方式	认证内容
设备风险	环境监测、设备编码检测等	设备所处环境的风险特征，包含地理位置、IP地址、IMEI码等
真实身份验证	指纹认证、声纹认证等	用户是否是真实用户本人
信誉历史	历史交易分析、征信黑白名单等	用户的过往信用历史，包含贷款历史、信用评分、还款历史等
数字身份验证	扫码验证、动态令牌验证等	用户已有的数字凭证，包括已存储的用户密钥、用户画像等数据
行为	认证行为分析、应用行为分析等	用户在监测时间内的行为特征，包含点击次数、停留时间等

资料来源：Gartner《The Growing Problem of Synthetic Identity and First-Party Fraud Masquerades as Credit Losses》

用户认证是业务安全的基础

以人为核心的业务安全体系

“用户是谁？”

验证对象身份

“用户能做什么？”

管理对象权限

“用户做了什么？”

监测对象行为

多因素认证（MFA）产品体系

通过所知、所持、所有的多因素认证，及设备指纹、终端环境安全、威胁防御等核心EDR技术，实现智能精准识别

- 身份鉴别：设备指纹、生物行为认证
- 端点安全：环境安全、威胁防御
- 通道安全：通道保护、数据保护

终端核心安全（App、H5、IoT）

数据传输安全（互联网、物联网）

统一身份管理（IDaaS）产品体系

企业多角色人员的账户、认证、权限、审计统一管理，通过智能认证技术，实现全流程免密认证

- 账户权限：统一身份权限安全管理
- 持续认证：连续、自适应、免密认证
- 安全管理：移动办公安全、统一身份安全

业务安全管理（账户、权限、认证）

连续自适应架构（分析、阻断，调整）

智能行为认证（IPA）产品体系

以智能安全大脑为核心，通过终端、情报和用户行为数据，使用多模态机器学习和数据分析，实现无感知认证和反欺诈

- 历史行为统计：征信黑白名单、数据服务
- 当前行为分析：交易反欺诈、营销反欺诈
- 未来行为预测：机器学习、深度行为分析

历史行为分析（征信，黑白名单、API）

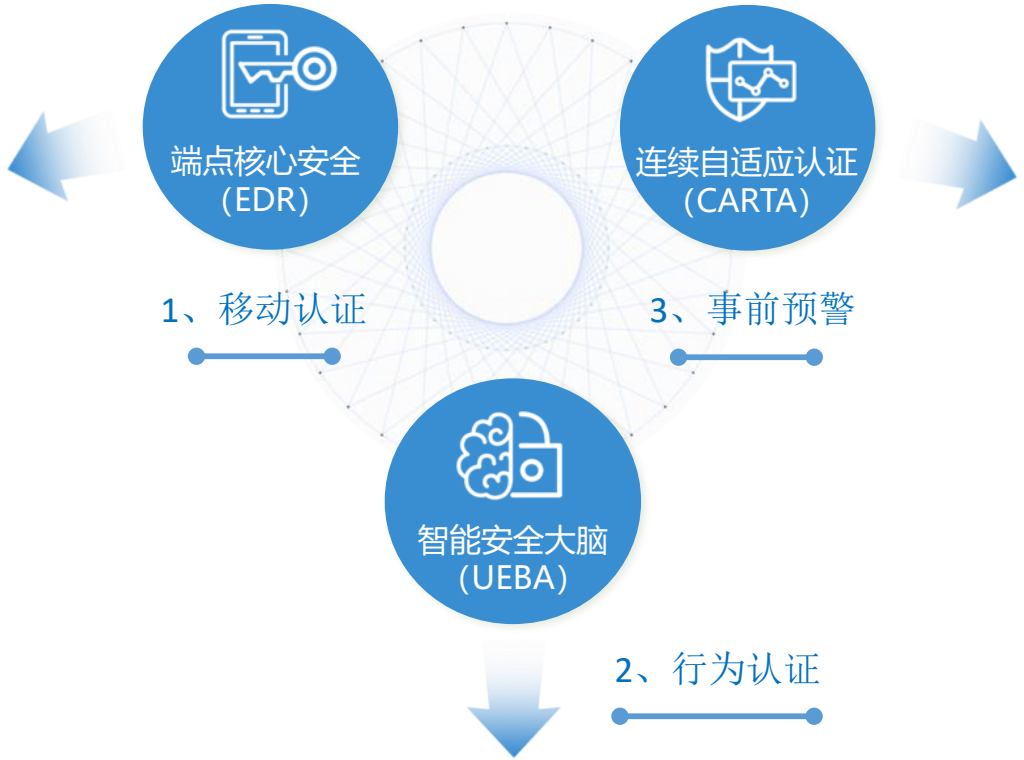
智能识别模型（实施分析，机器学习）

对于用户身份的确认不再是是与否，而是风险与信任关系

- 零信任模型的核心是任何内外部用户都不可信任。在任何授权之前都应对试图接入系统的用户、设备及请求进行验证；通过验证的用户，也只能获得完成特定工作的最小访问权限
- 在零信任模型中，借助多因子身份认证、身份及访问管理、连续自适应认证等技术手段，能够实现用户体验最佳、安全性能最高的解决方案

针对典型特征的阻断	阻断但提示安全问题	允许访问但有限只读	允许访问可读写个人文件	允许访问但记录日志	允许访问但无感知认证	允许访问

把握三点趋势，持续输出行业领先的技术能力



设备指纹（DFS）

主动式指纹2000多特征，被动式指纹上百特征，无需SDK插件，动态设备指纹结合机器学习，准确率已达到99.99%，远超市场平均水平

终端环境安全（SSE）

多种核心专利技术：白盒加密算法，分割密钥算法，应用安全沙箱，虚机源码保护

终端威胁防御（MTD）

模拟器检测270+款，双开程序检测40+，攻击框架、调试状态、高危软件、Root/越狱、代理服务器等独有检测技术

自适应认证（ADA）

国际先进，国内大幅领先，10多种认证方式，20多种自适应策略，上千组模型规则

连续认证（CTA）

连续认证接入技术，多种业务场景决策，10多种认证协议算法，100+应用集成

全微服务架构（MCS）

10大微服务模块，快速零落对接，金融级高性能高QoS

高性能反欺诈平台（OFD）

高性能规则引擎，分布式实时引擎，可视化管理能力，欺诈图谱检测。20渠道2000+规则，单机2000+并发，毫秒级响应

多模态学习引擎（MLE）

图计算、机器学习、深度学习、流式特征等8种多模态引擎支持

多维度机器学习算法（MLA）

超20种有监督、半监督、无监督、迁移学习、增强学习等机器学习算法

准确率：>99.5%，精确率：>98%

召回率：>99%，打扰率：<1%

欺诈团伙识别率>90%

输出行业领先的技战略定位：率先引入零信任理念，提供场景化身份认证和业务安全服务

- **愿景：** 以人为核心，用创新科技赋能安全领域，成为国际领先的“身份认证和业务安全”产品服务提供商
- **定位：** 从零信任模型出发，由端点核心安全、智能安全大脑和连续自适应认证多维技术驱动，提供场景化的业务安全解决方案

场景	金融	政府	运营商	互联网	其他	
方案	账号及交易安全解决方案	设备指纹和终端安全保护解决方案	电子银行全渠道反欺诈解决方案	互联网营销反欺诈解决方案	移动办公安全解决方案	统一身份管理解决方案	企业信息防泄漏解决方案
产品	**多因素认证（MFA）产品体系** (Multi Factor Authentication)	**统一身份管理（IDaaS）产品体系** (Identity as a Service)	**智能行为认证（IPA）产品体系** (Intelligent Portrait Authentication)			
模型	**终端数据安全模型** (App、H5、IoT)	**信息传输安全模型** (互联网、物联网)	**风险识别策略模型** (实时决策、认证、自适应)	**智能分析策略模型** (离线学习、行为分析)		
技术	**端点核心安全** (EDR，Endpoint Detection and Response)	**智能安全大脑** (UEBA，User and Entity Behavior Analysis)	**连续自适应认证** (CARTA，Continuous Adaptive Risk and Trust Assessment)			
理念	**零信任模型：** 网络环境中所有用户都不可信任，需对用户、设备、访问及权限进行连续判断 (IP风险，密码风险，账号风险，设备风险，行为风险，历史信誉风险)					

芯盾时代身份认证体系框架

对外业务 | 对内业务

强 ↑ 用户感知 ↓ 弱

多因素认证（MFA）

通过对用户所知、所持、所有的信息进行分析，进而确定用户身份的唯一性。

一站式移动身份管理（IDaaS）

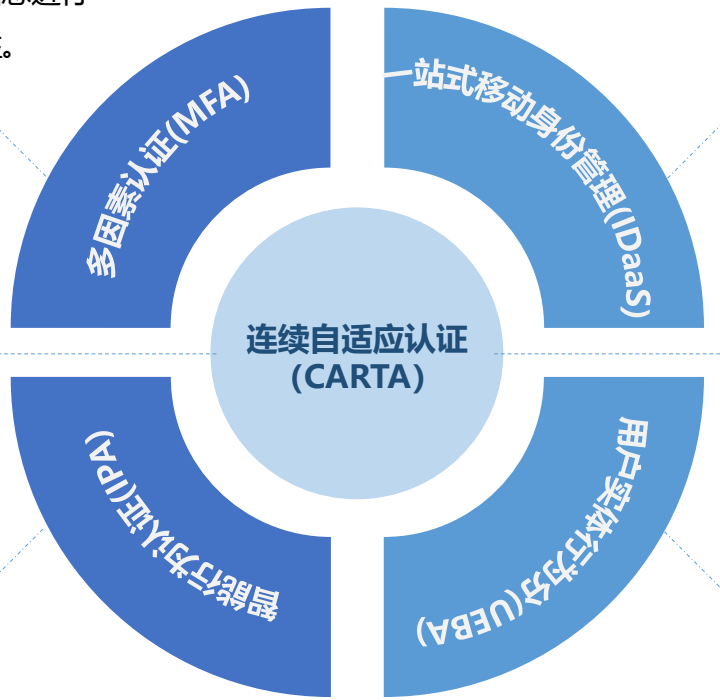
传统4A体系的升级，通过移动认证实现对用户身份的唯一性识别，提升管理效率。

统一认证平台（UAP）

通过提供统一的认证能力接入，为对外业务提供丰富的认证功能及可扩展能力；

连续自适应认证（CARTA）

通过与UEBA的联动，实现对内部用户的智能行为审计，有效防范内部员工泄露企业数据，卖账号的等风险。



用户行为认证（IPA）

通过对用户行为进行分析，采用规则引擎与机器学习引擎判定操作风险。

用户行为认证（UEBA）

通过对用户行为的分析，结合操作系统，安全设备日志，发现可能存在的风险操作。

分类目录

Contents

安全威胁与
零信任架构

芯盾时代
业务安全技术架构

芯盾时代
企业风采

企业概况

独立“身份认证和业务安全”产品服务提供商，率先提出“以人为核心的业务安全”核心理念

- 提供覆盖全流程、全生命周期的“安全、智能、便捷”的身份认证和业务安全解决方案
- 多因素认证（MFA）、智能认证和反欺诈（OFD）、统一身份管理（IAM&IDaaS）、连续自适应认证（CARTA）、用户和实体行为分析（UEBA）产品和技术提供商

拥有来自百度、阿里、360、绿盟、启明、中国移动、握奇、任子行等公司业内最顶尖安全团队

- 超150人的专业身份认证和业务安全团队，70%团队成员是身份认证安全专家及技术工程师
- 密码学、移动安全、认证及访问管理、大数据分析处理、数据建模、实时流计算、人工智能、半监督机器学习等

Redpoint

2015年10月
获得红点
A轮融资

SIG SUSQUEHANNA

2017年3月
获得SIG、红点
B轮融资

YF CAPITAL 云锋基金　昊翔资本 DREAMFLY CAPITAL

2017年12月
获得云锋、昊翔、SIG、
红点B+轮融资

截至2017年12月，2年时间，
芯盾时代完成了3轮融资，
累计融资金额2.2亿元，
进入快速健康发展。

公司及团队技术实力和创新实践受到市场高度认可

2016

首届ISC中国互联网大会安全创客汇第一名

2016年度最具创新性初创安全企业

中关村高新技术企业

中国金融IT服务商评选-优秀创新奖

国家高新技术企业

2016年度最佳新锐人物

2017

2017IT创新中国互联网领军企业奖

中国国际金融展“金鼎奖”优秀解决方案奖

亮相2017Gartner秋季IAM峰会

51CTO中国移动身份认证行业领军企业奖

入选互联网周刊2017年度网络安全服务公司

2018

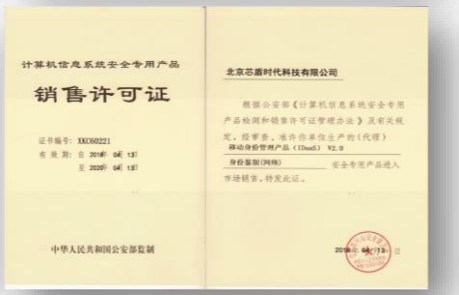
2017年移动支付领域最具影响力企业奖

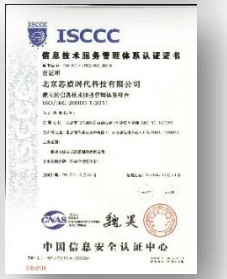
2017中国硬科技独角兽企业

胡润百富50强最具投资价值“独角兽”企业

计算机信息系统安全专用产品销售许可证

中关村科技园高精尖企业 ……





公司产品市占率高、商业化能力强、拥有强大的合作伙伴网络

身份认证产品市占率30%，续费/复购率高，深受市场认可

强大的战略合作伙伴网络

360　蚂蚁金服 ANT FINANCIAL

NSFOCUS　梆梆安全 BANGCLE

知道创宇　AuthenMetric 中科奥森

中国民生银行 CHINA MINSHENG BANK　南京银行 BANK OF NANJING

中共中央网络安全和信息化委员会办公室 Office of the Central Cyberspace Affairs Commission

中华人民共和国水利部 The Ministry of Water Resources of the People's Republic of China

研发两地三中心，六个区域销售办事处，团队成长迅速

北京门头沟科技园
- 创新研发部
- 智能安全联合实验室

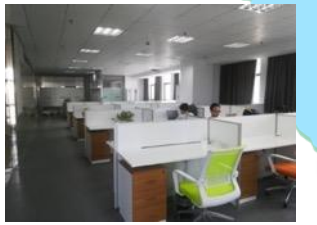
东北区办事处（大连）

华北区办事处（北京）

北京总部
- 解决方案中心
- 平台研发部
- 智能安全研发部
- 产品市场部
- 项目管理部
- 职能部

华西区办事处（西安）

华中区办事处（合肥）



武汉光谷开发区
武汉研发中心

华东区办事处（南京）

华南区办事处（深圳）

- 超**200人**的专业身份认证和业务安全团队，**75%**团队成员是身份认证安全专家及技术工程师。
- 团队中**95%**的员工拥有本科、硕士及博士学历，成员来自清华、中国院、北邮、北航、山大，信息科大等著名高校。
- 拥有来自**百度、阿里、360、绿盟、启明、中国移动、握奇、任子行**等公司业内最顶尖安全团队，平均年龄32岁，安全行业从业经验丰富。
- 芯盾时代的技术支撑体系已遍及全国。

芯盾时代
TRUSFORT.COM

THANKS