支付宝(中国)网络技术有限公司

# 数智时代的支付新安全

吴飞飞 首席网络安全官

2025.9

蚂蚁集团 ANT GROUP | 支付宝

蚂蚁集团 ANT GROUP | 支付宝

# 数智时代的支付新安全

## AI时期的安全也是国家安全的重要支撑

**国家安全工作要贯彻落实党的二十大决策部署，切实做好维护政治安全、提升网络数据人工智能安全治理水平、加快建设国家安全风险监测预警体系**

——2023年5月，习近平总书记主持召开二十届中央国家安全委员会第一次会议

蚂蚁集团 ANT GROUP | 支付宝

# 数智时代支付与安全变化与挑战

## 安全是支付的根基，支付安全始终与技术革新同频共振

### 数字支付

互联网支付、移动支付

- 担保交易
- 快捷支付
- 刷脸支付
- 扫码支付

AI支付市场规模**万亿级**

新交互支付占比**超50%**
智能设备支付**增长10倍**

### AI支付

人工智能&数据要素技术

支小宝

- 碰一下支付（NFC支付）
- 看一下支付（智能眼镜）

**AI新应用形态安全保障**

如何保障AI时代下业务产品的安全性?

**AI赋能风控和安全**

如何利用AI赋能风控和安全的质效?

安全生态联盟体系

蚂蚁集团 ANT GROUP | 支付宝

# AI技术带来的新风险与挑战

## AI是把双刃剑，带来了新的安全风险，也为安全带来了新的可能性

### AI 技术带来的新风险

大模型的极致体验降低了AI应用门槛，引发一系列新风险，如：例如用AI技术挖掘系统漏洞进行攻击，AI换脸带来的核身安全威胁、以及大模型幻觉带来的衍生风险

**利用Agent技术挖掘系统漏洞进行攻击**

**DeepFake深度伪造合成技术威胁核身安全**

**大模型幻觉带来的衍生风险**

蚂蚁集团 ANT GROUP | 支付宝

# AI新应用形态安全保障

## 智能眼镜支付：“看一下”支付，便捷又安全

### 用户自主可控


### 设备安全实时检测

业内首个
基于关联多设备的
眼镜安全可信解决方案

支付安全 | 核身安全
设备风险感知 | 跨端可信互联


### 声纹支付无感核验

业内首个
基于声纹等多因子的
眼镜用户可信解决方案

**四道检测：人-设备-环境可信**

- **声纹伪造检测**
  覆盖AIGC合成主流攻击
- **佩戴检测**
  发声微动异常判断
- **注入检测**
  超声波侧信道
- **声源检测**
  精准定位人声

### 7*24小时智能风控

金融级风控保障
确保每笔
支付的安全

蚂蚁集团 ANT GROUP | 支付宝

# AI新应用形态安全保障

## 支付智能体服务间的协同应用，支付体验进化与安全基础设施

### 支付服务在智能体时代新体验

**更自然的交互**
- 智能体内一句话完成支付

**更智能的服务**
- 跨场景智能体协作：购票->出行->酒店->支付

**随行无感体验**
- 手机、眼镜、车机等AI原生设备无缝协同

### 智能体协同复杂性带来的信任与安全困境

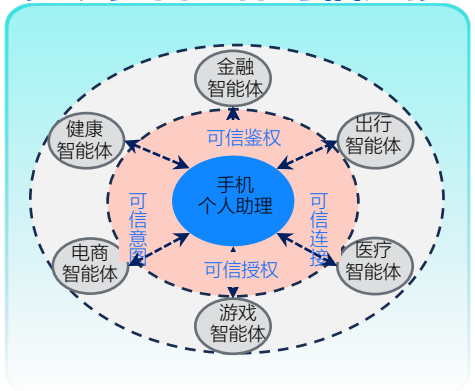
**信任问题**
- 静态防御难以解决动态协同下的信任问题

**安全问题**
- 从设备孤岛到全面连接面临的安全问题

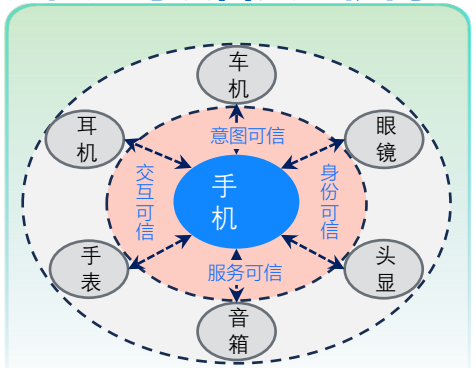
**身份问题**
- 从被动响应到主动决策面临的身份识别问题

### 布局智能体可信互联：建设下一代智能终端可信基座

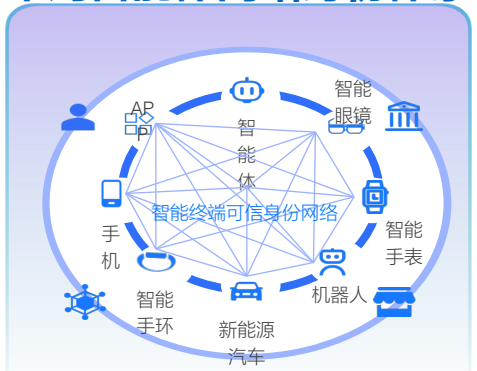
**直面信任难题，实现多智能体可信连接**




**攻克安全难题，构建跨设备安全协同**




**解决身份难题，布局智能体网络身份体系**



蚂蚁集团 ANT GROUP | 支付宝

# AI新应用形态安全保障

## 智能体本身的安全：更智能的服务与安全防护

### 智能决策唤起支付服务

**理解用户意图**

- 从用户一句话拆解服务需要

**规划服务+支付**

- 调用不同服务，满足用户需求

**整合服务结果**

整合支付及场景服务结果，让用户更好理解

### 智能体动态规划带来不可预期的结果

**恶意意图**

- 黑灰产恶意诱导智能体窃取数据、滥用服务

**意图篡改**

- 恶意的智能体和工具被投毒，篡改正常用户意图

**行为偏离基线**

- 用户行为、智能体决策异常，不符合历史基线

蚂蚁集团 ANT GROUP | 支付宝

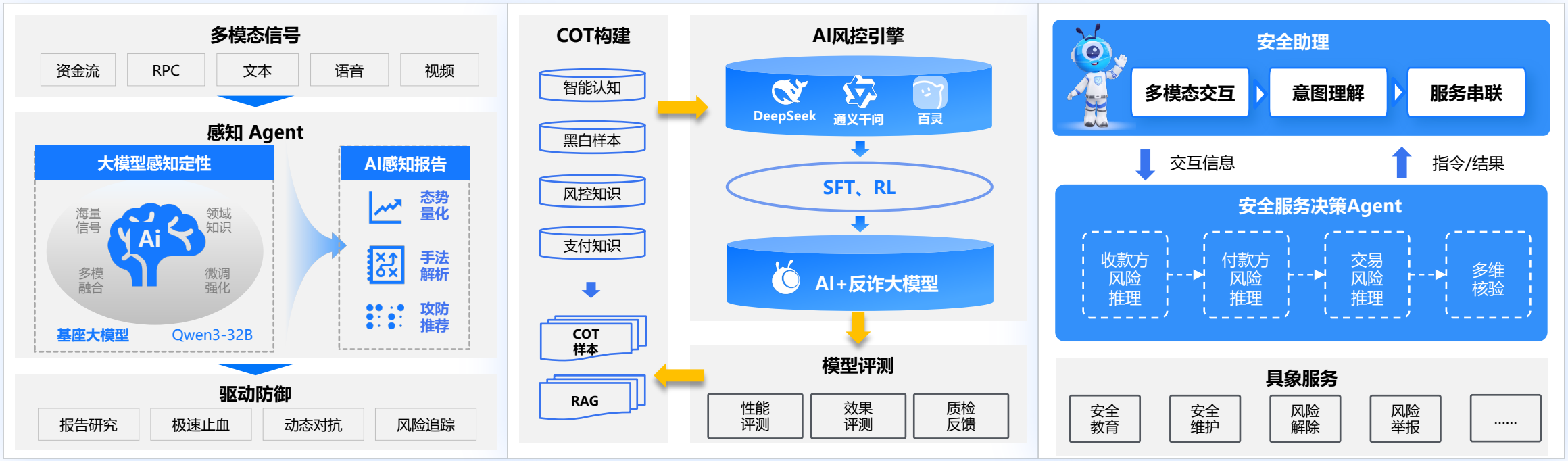
# AI赋能支付风控

## 深度应用大模型技术，注入风控知识，建设多维认知推理AI+风控体系

**感知风险**
快速感知黑产攻击

**识别风险**
通过监督微调、强化学习解决幻觉问题

**安全服务**
为用户提供智能化安全服务




**智能认知**

商家认知 | 用户认知 | 黑产认知 | 业务认知 | 交易认知

蚂蚁集团 ANT GROUP | 支付宝

# AI赋能支付安全

## 深度将AI技术与安全技术结合，实现效率与效果同步提升

### 安全风险发现
基于LLM强化传统安全研发生命周期

### 安全治理与防护
基于LLM，实现对话式安全运营

### 威胁感知与响应
基于图计算引擎，实现海量日志多维融合分析

**基于AI的需求安全分析Agent**

需求池 | 领域知识 | 安全知识 | 历史风险 | 风险评估

**基于智能路径规划的漏洞分析Agent**

VulChecker Agent

智能决策 | MCP | 深度优先 | 污点追踪

VulChecker
INTELLIGENT CODE INSPECTION

多智能体协作

风险运营

- 接口画像
- 漏洞挖掘
- 漏洞修复

**基础安全数据**

- 安全资产
- 安全产品
- 安全报表
- 安全知识

**可信纵深防御智能运营Agent**

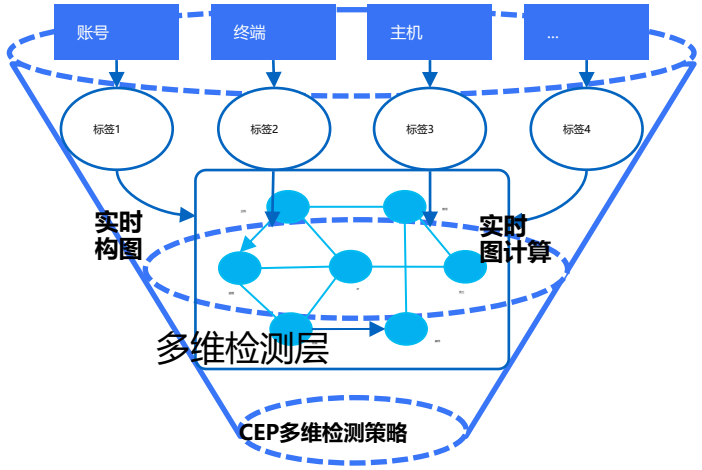
安全告警处置 | 安全防护部署验证

TrustOps
RESILIENT DEFENSE OPERATIONS

安全资产查询 | 安全指标分析

**基础MCP服务**

Code MCP | Trace MCP | Assets MCP




**具象服务**

行为标签 | 风险感知 | 告警研判 | 柔性处置 | ……

蚂蚁集团 ANT GROUP | 支付宝

# 安全生态联盟体系

## 牵头成立国内首个智能体安全生态组织，共建互联新生态

IIFAA 联盟是蚂蚁和行业联合发起的互联网金融级身份认证联盟
未来 IIFAA 将向可信生态联盟升级，在可信认证的基础上，致力于打造互联网金融级可信生态

蚂蚁集团 ANT GROUP | 支付宝

# 感谢聆听！