

智能生活全连接趋势下的智能安全

——从硬件安全到智能安全



物联网时代，人人拥有未来之屋

比尔盖茨的豪宅：未来之屋



Artificial Intelligence



Big data



Cloud



Internet of things

政策红利 — 地产进入精装修时代

北京、郑州、浙江、上海、山东、海南.....

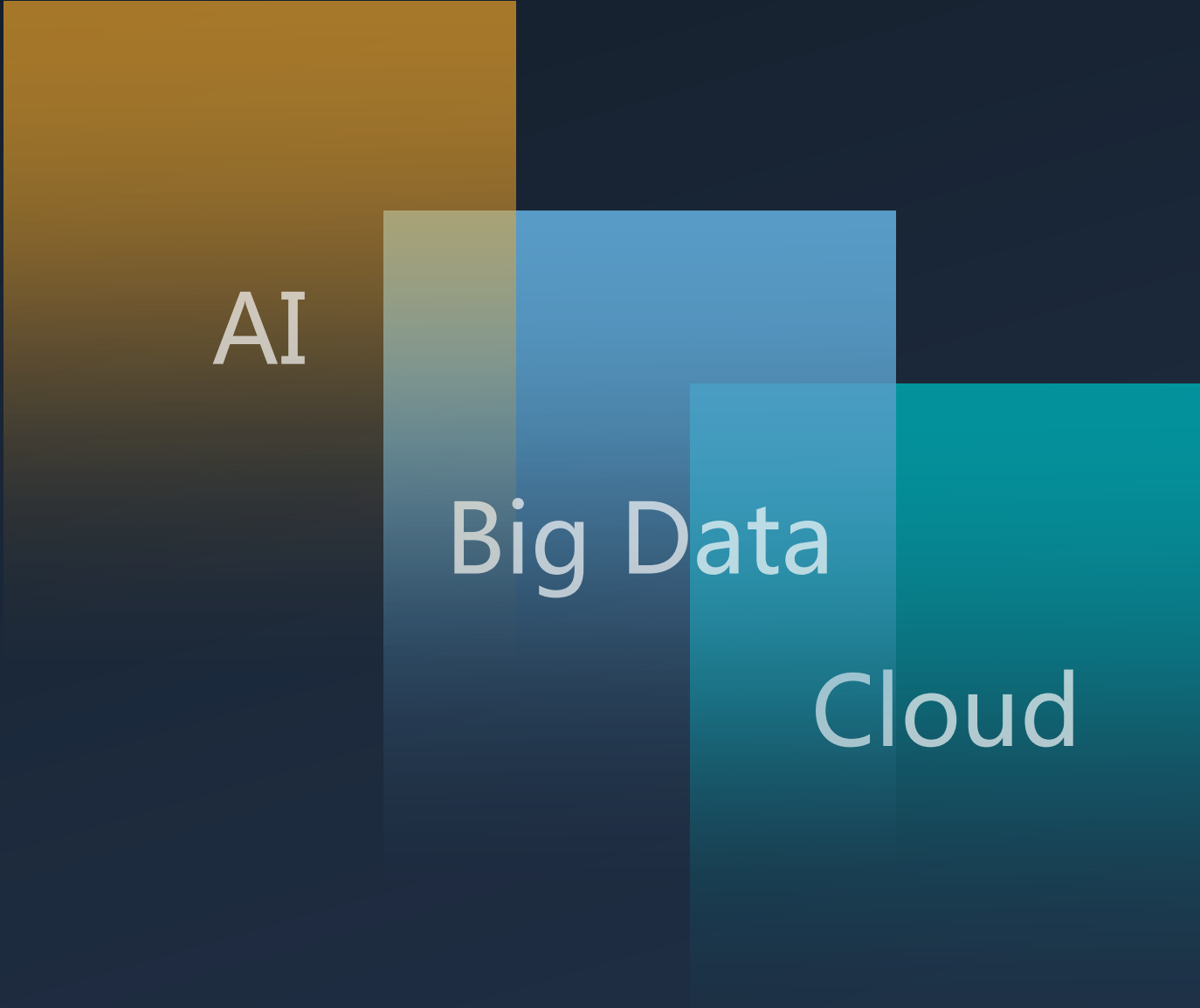


智能家居成为地产业新概念

打造美好生活，提升社区管理效率

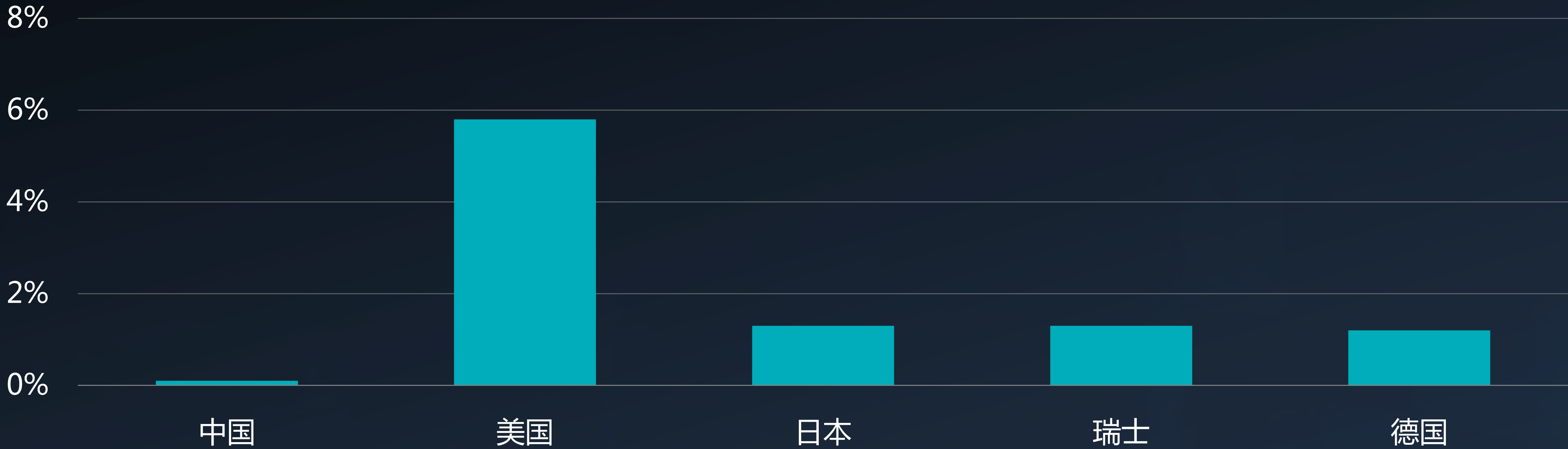
AI、大数据、云计算

更智能 更人性 更低廉 更普及



市场增长迅猛

智能家居渗透率(%)



中国 (2017-2021)年均复合增长率约为48.12%，2021年市场规模将达到4369亿元

(资料来源：中投顾问)

2020年——1.12万亿元

- ✓ 存量家电升级
- ✓ 新型智能家居市场
- ✓ 硬件耗材与增值服务

家庭物联网：从全屋智能到数据服务

历史上的两次连接

01 第一次连接：人+电脑



02 第二次连接：人+移动设备



第三次连接：家庭+边缘网络+下一代移动互联(5G)



从物联网到家庭物联网

From the Internet of things to the Internet of home Things

统一数字属性、物理属性

2020

年

340

亿设备

安全边界已被打破



目前主流全屋智能方案



安全挑战：

- 各硬件品牌产品对接到自己的云端，绝少统一的安全保护
- 各节点存在被攻击的可能性，如何防止固件被篡改，木马病毒等
- 如何有效保障云端通信的数据安全

新安全：从端到系统



无边界安全

— 智能家居时代的安全新命题

家庭 —— 下一个安全战场

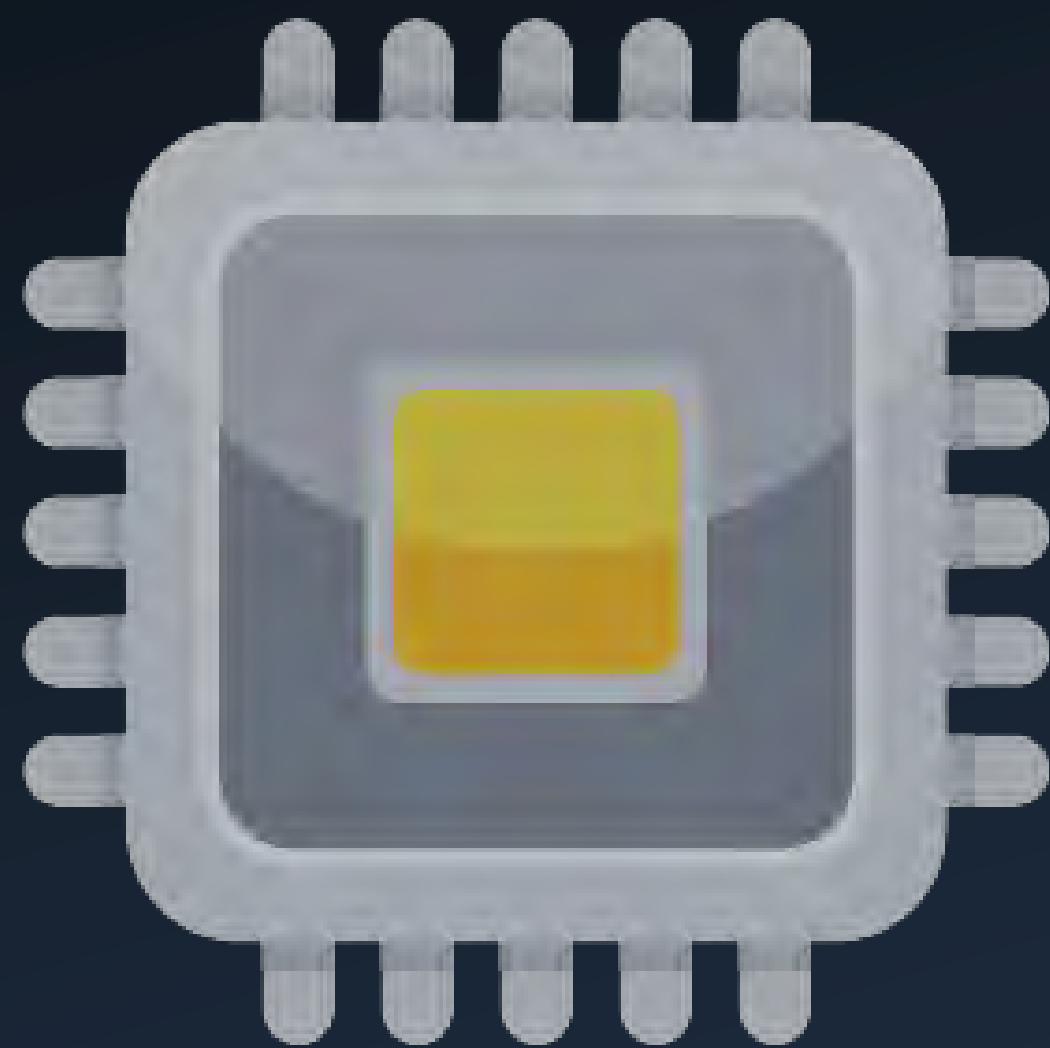
雅观全屋智能方案



安全保障：

- 以Home Server作为跟云服务对接，统一设备的安全保障机制
- 充份利用芯片的安全特性，大大提高全屋智能方案的安全性
- Home Server运行SeLinux，严格控制应用程序对系统资源的访问权限
- 第三方软件在Home Server运行必须通过签名校验
- 个节点接入到Home Server必须通过身份认证和数据加密
- Home Server和云端通信必须通过签名校验和数据加密

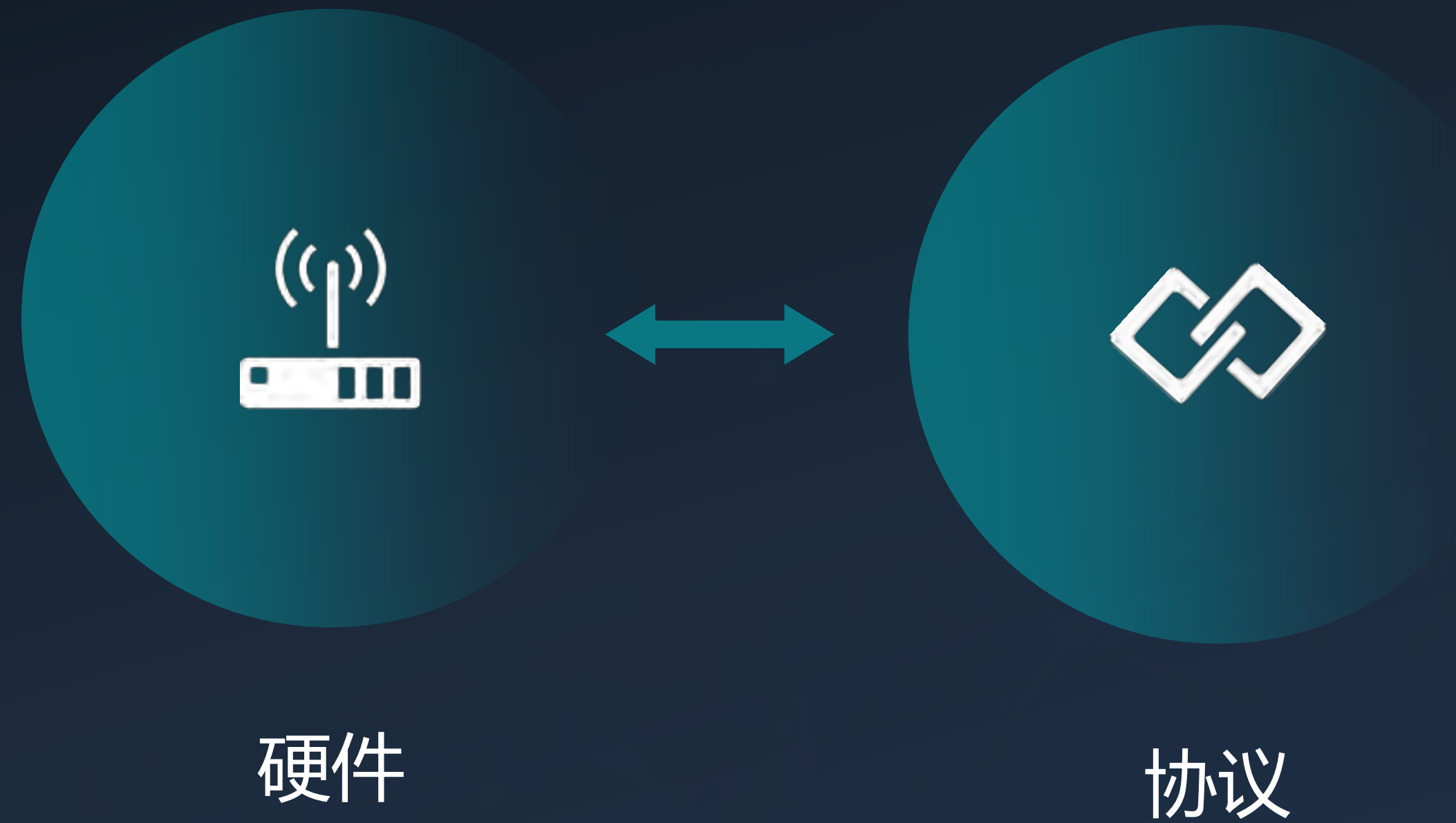
充分利用芯片能力保障系统安全



- 市场上已有部份支持Secure boot，雅观Home Server采用支持Secure boot的SoC（System On Chip），镜像必须通过合法的签名才能启动，有效避免固件被非法篡改
- 数据加密可以通过软件实现，但单纯通过软件对数据进行加解密会增加CPU的负担，从而引起功耗提高，和降低数据传输速度，为了保障数据安全的同时不影响到系统的性能，雅观Home Server利用了SoC内置的安全模块进行数据加解密。
- Home Server使用支持TrustZone技术的SoC，使可信应用程序和主OS分开，防止恶意软件攻击

为设备商赋能：从“硬件”到“硬件+服务”

打破障壁，多协议、多设备互联互通



联通多种协议，兼容多类型设备



面板

热水器

电视

扫地机器人

冰箱

插座

空调

地暖

灯泡

门锁

支持市面上 1000+ 款智能设备

音箱

开关

洗衣机

烤箱

体重秤

空气净化器

传感器

路由器

雅观科技·智能家居场景运营平台

边缘计算，系统运行更稳定

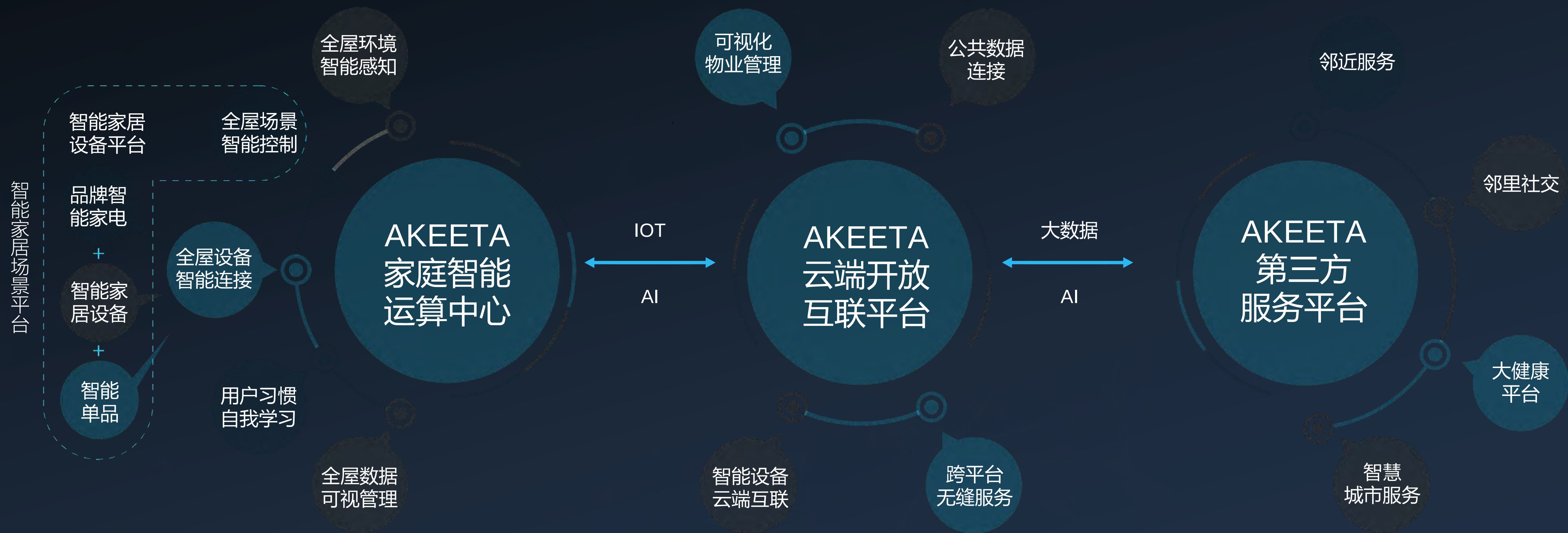


深度学习，无感操控

AI、大数据深度学习用户习惯

雅观目标：打造智能家庭场景 提供更多服务

雅观全屋智能方案逻辑



Argrace

雅观科技·智能家居场景运营平台

Home Sweet Home