

智能家居（小家电）产品的发展现状 与未来信息安全需求



哈士奇机器人CEO、千家智客创始人 向忠宏

当我们在说智能家居的时候：



20年前

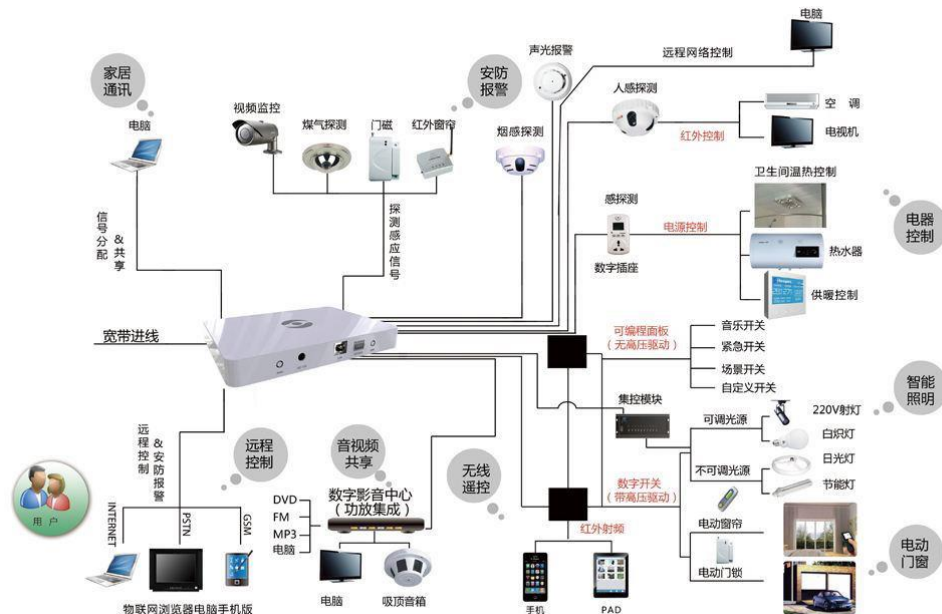


4年前



现在

当我们在说智能家居的时候：



20年前/少数人的享受/窄众市场

当我们在说智能家居的时候：



20年前/少数人的享受/窄众市场



当我们在说智能家居的时候：



4年前/年轻人的玩具/快消市场

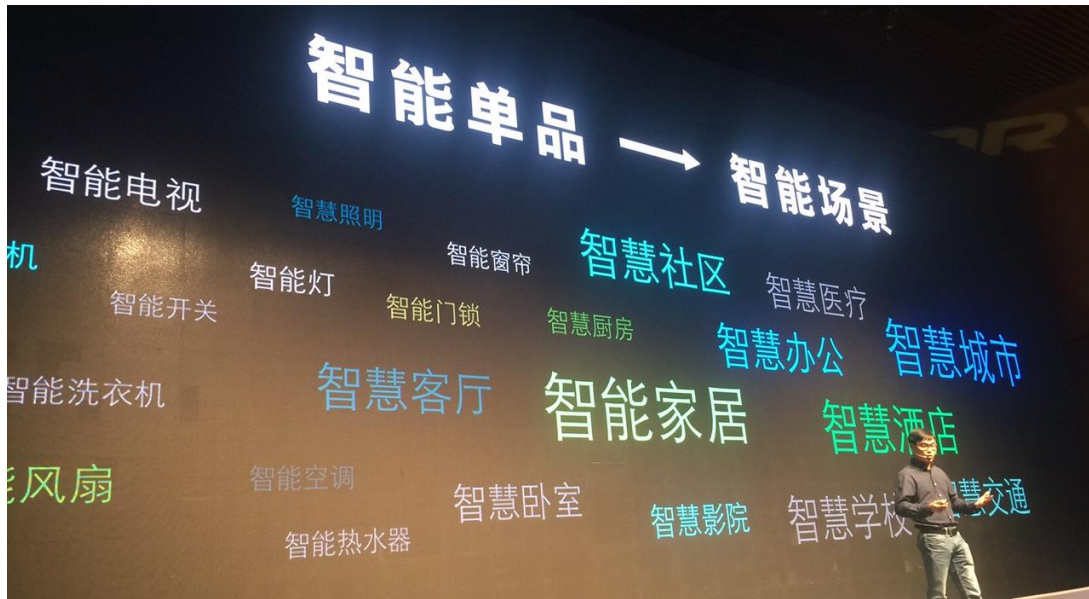
当我们在说智能家居的时候：



4年前/年轻人的玩具/快消市场



当我们在说智能家居的时候：



现在/无所不在的智能场景表达

当我们在说智能家居的时候：

场景

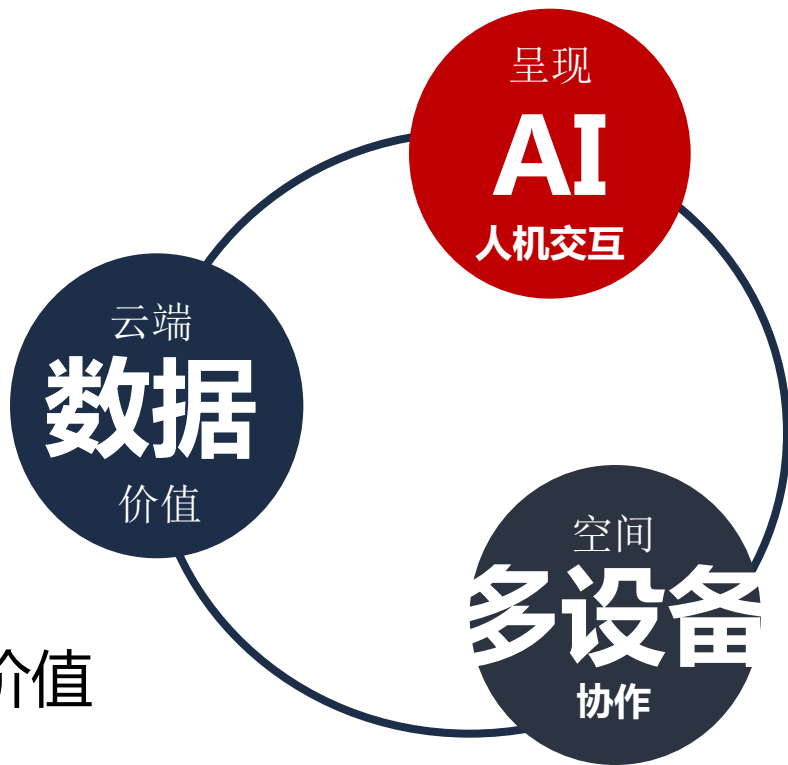
现在/真实的虚拟世界



当我们在说智能家居的时候：



现在/ 人与设备交互、数据的价值





智能家居的解读

构建高效的住宅设施与家庭日程事务的管理系统，提升家居**安全性**、便利性、舒适性、艺术性，并实现环保节能的居住环境。

智能家居要素

舒适性

便利性

社交

健康

安全性

艺术性

个性

智能家居的健康、安全

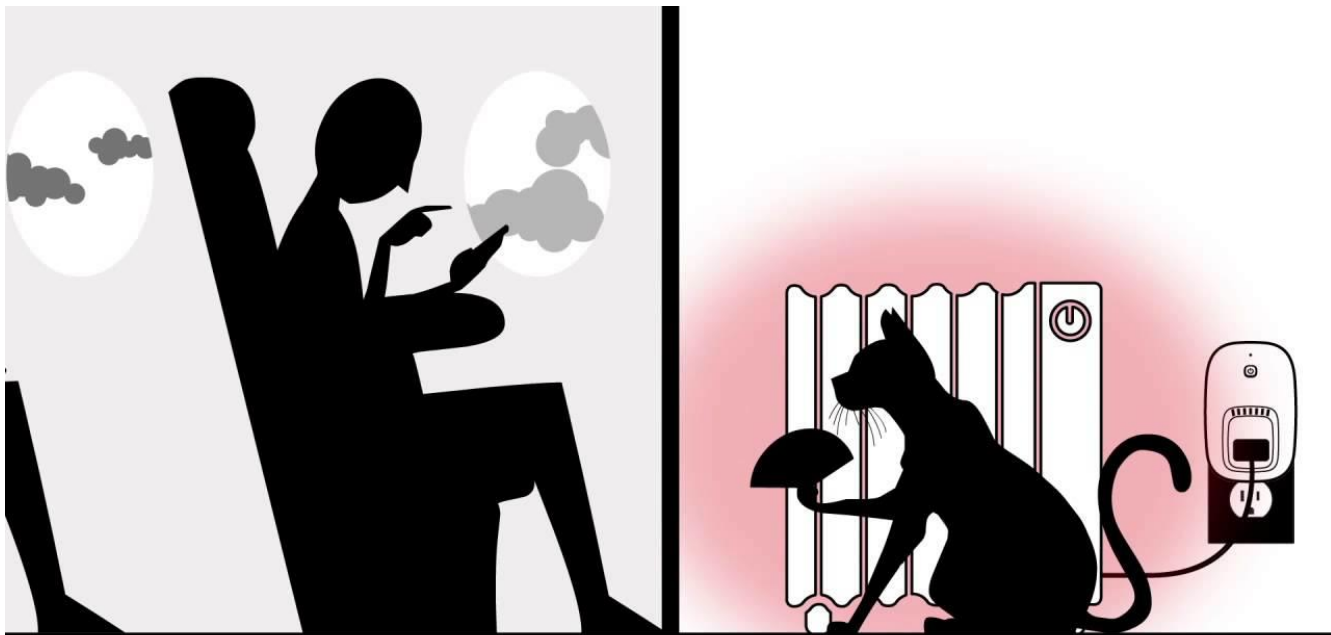
健康

环境健康、人的健康（生理、心理）

安全

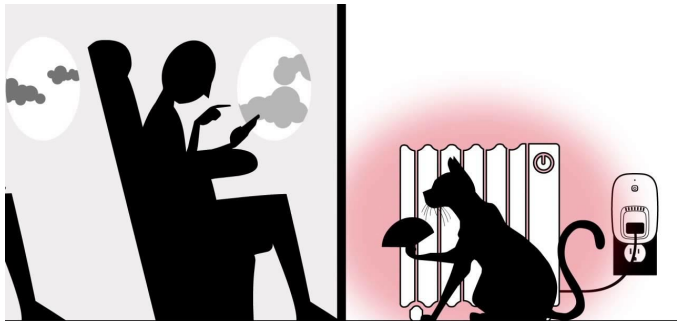
财产安全、生命安全、安全感

智能家居系统与产品自身的安全



你也许会担心，有不怀好意的人远程启动你家的WeMo智能家居系统

智能家居系统与产品自身的安全



你也许会担心，有不怀好意的人远程启动你家的WeMo智能家居系统

位于Seattle的安保公司IOActive2014年2月18号宣布了一项Belkin WeMo安全漏洞分析研究结果。IOActive的声明中指出，WeMo设备的软件漏洞可能让攻击者远程控制设备，安装恶意固件，监测目标设备的运行状况甚至进入目标设备的计算机网络。

这种脆弱性存在于WeMo的固件升级过程中，这个过程完全依赖于连接到WeMo设备的智能手机应用。值得赞扬的是，Belkin的每次新的固件更新都加密了，但是，每次新更新的密钥已经在系统现存的固件内了。实际上，这就让黑客在固件发布前就能够瘫痪它了。

尽管WeMo的产品线现在是安全的，但却透露出了智能家居技术最隐秘的秘密：总的来说，智能家居安保协议很搞笑。ZigBee和Z-Wave是两项最普遍的智能家居协议，几个月前就被黑过，但很少的公司有兴趣修复这些问题。

智能家居什么数据最敏感、最可能出问题？



基于场景的智能家居比以往更脆弱



云端
数据
价值

呈现
AI
人机交互



空间
多设备
协作



多模态人机交互情况下，安全保障受到更大的挑战



💧 为正确的人、以正确的方式提供了正确的服务？

切实考虑智能家居
信息安全

让其成为产品交付必不可少的部分

创造前所未有 实现前所未能

智能家居行业奠基人向忠宏的财经视角新作

第2版加入场景智能、人工智能新内容

智能家居 下一场巨头的游戏 (第2版)

◆ 向忠宏 著



- 专业解读苹果、谷歌、亚马逊智能家居平台
- 全面分析智能家居概念股
- 展望智能家居与室内装饰融合趋势
- 分享人工智能领域创新创业经验



中国工信出版集团



电子工业出版社
http://www.ghei.com.cn

谢谢！



向忠宏 xiangmiles@gmail.com

“未来对我而言...像深夜中的一条看不见的公路，而人类在未加分隔的领域中，在前进的旅程上不断创造历史。” 《终结者2》