Microsoft

IoT in Action

#IoTinActionMS

Microsoft

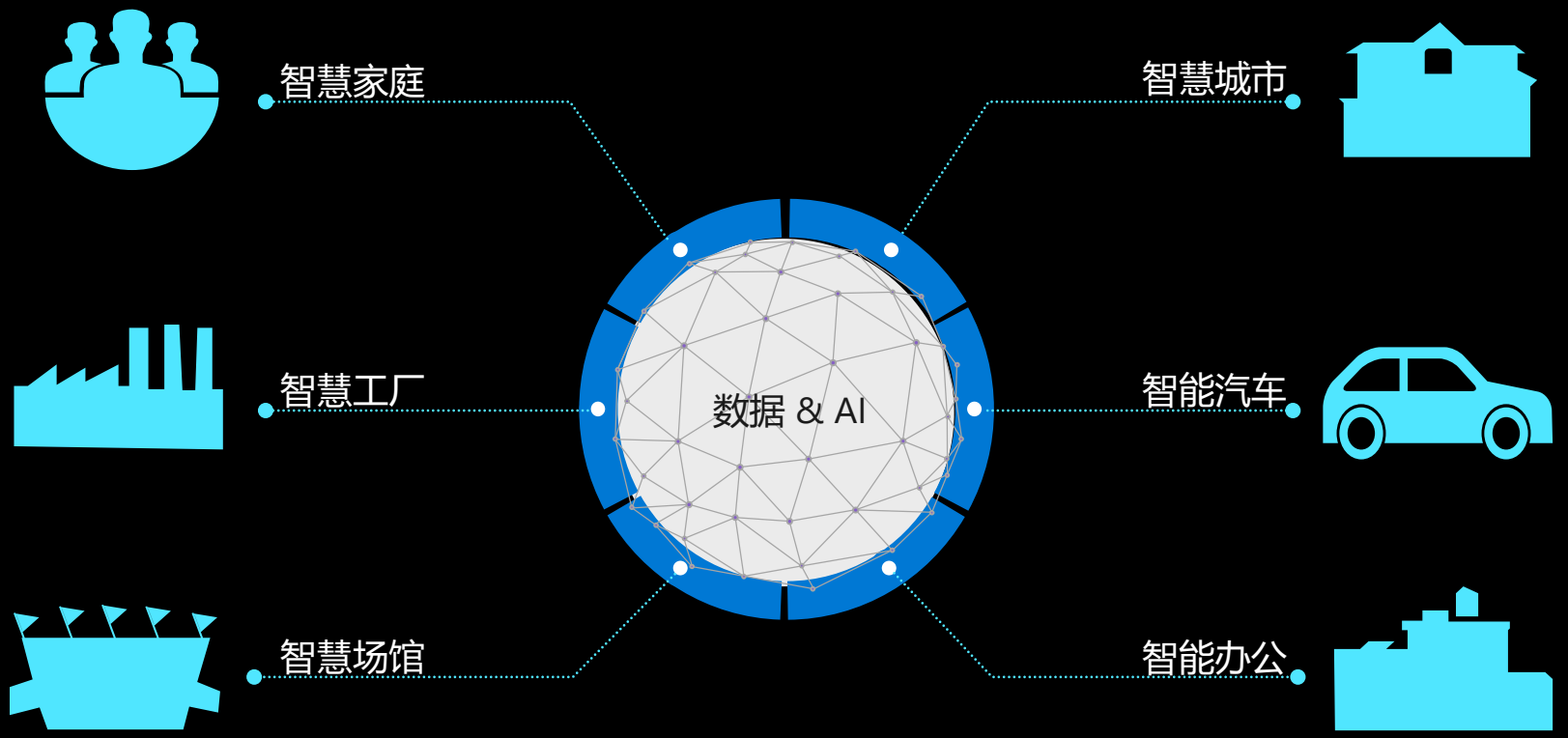
开展
物联网 (IoT) 安全实践
打造长效创新机制

Neo Xiong
微软IoT技术专家

Vincent Zhao
微软安全项目经理

IoT in Action

物联网 (IoT) 助力数字化转型



2020 年完成连接的设备数量将达到 200 亿

—Gartner

416 亿

2025 年实现“物物”相连，产生 180ZB 数据

$1,300 亿美元

物联网 (IoT) 相关服务拓展的新盈利渠道

80%

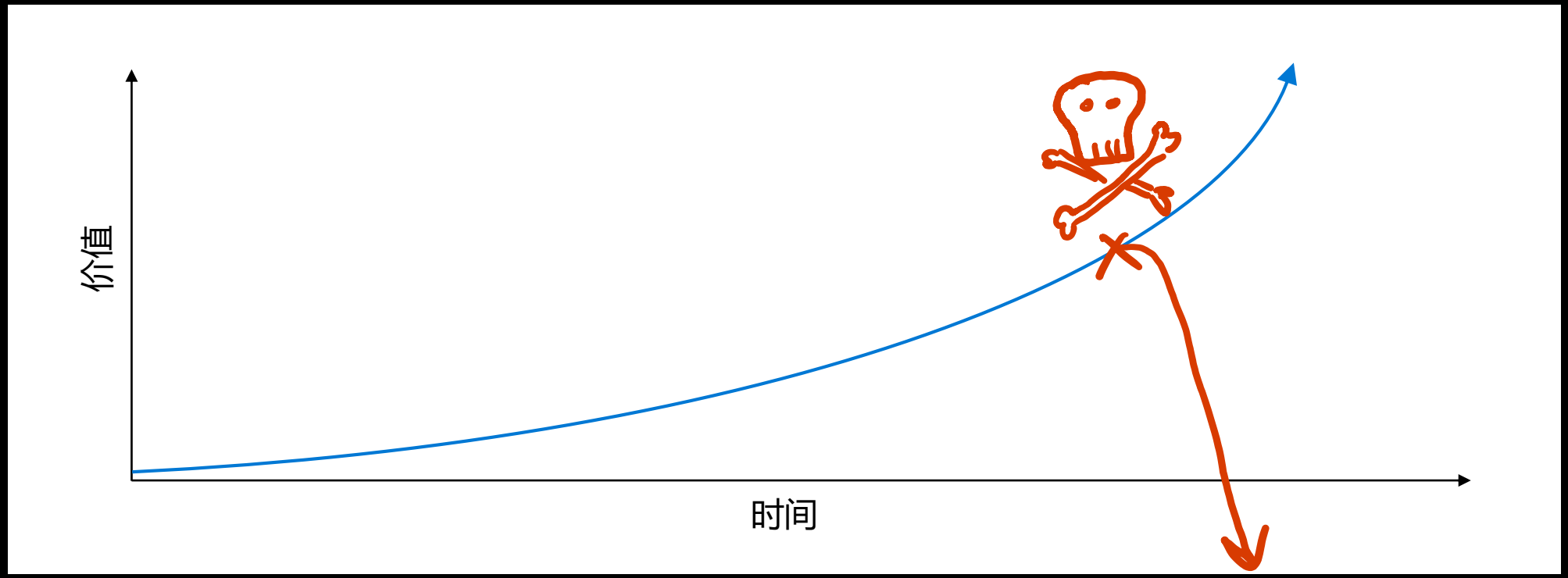
因推行物联网 (IoT) 而提升盈利的公司

$1,000 万美元

完成数字化转型的企业营业收益平均增长量（平均 8%）

- 成本缩减
- 客户受益
- 运营合理化
- 商业模式创新

IoT 带来的价值逐步攀升，而有人对你虎视眈眈...



概念验证
价值小幅攀升

量产部署
交付真正商业价值

重复循环
数字化正反馈加速
价值提升

74%

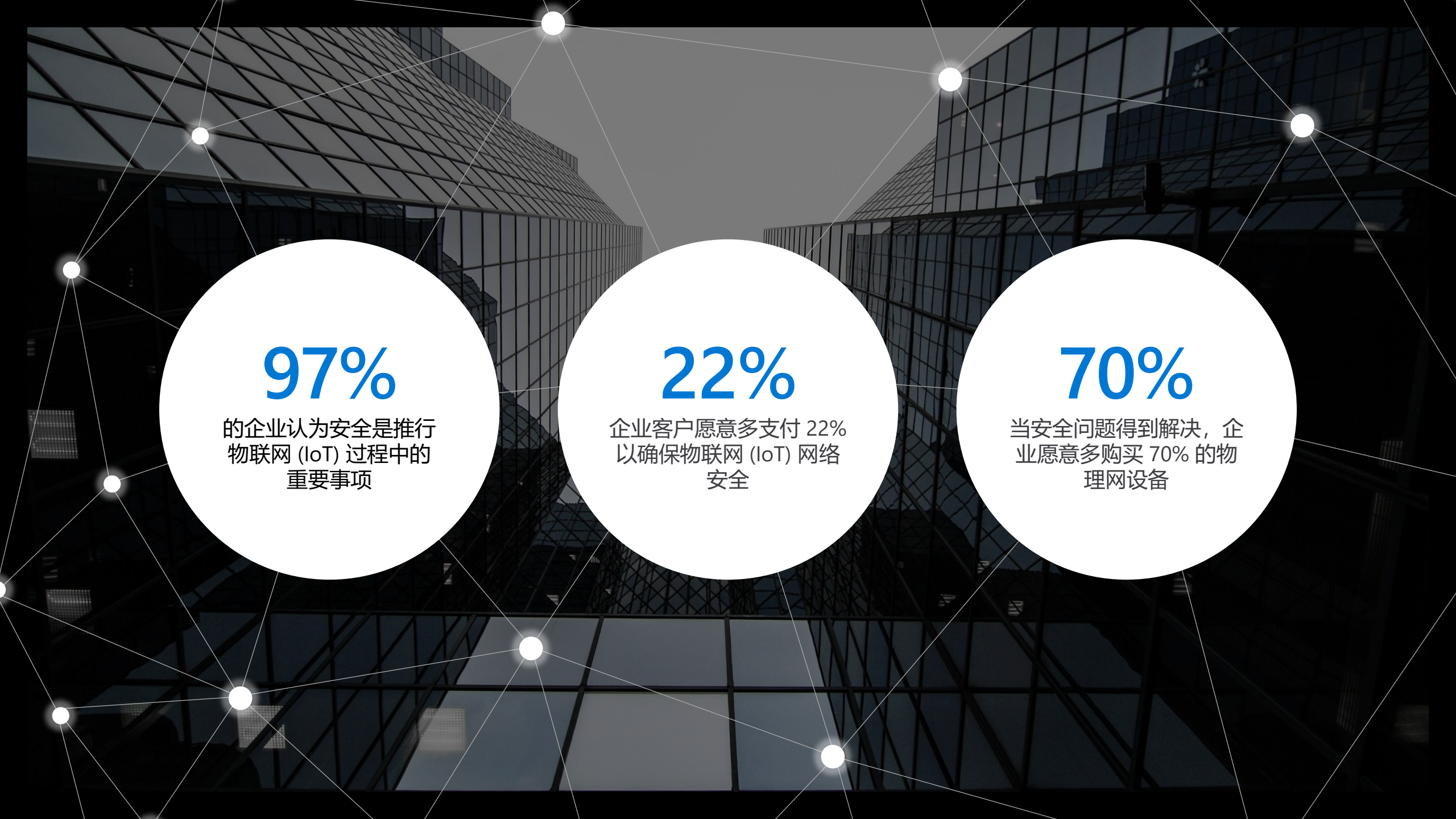
的消费者愿意
花高价购买安全性能
更好的智能设备

65%

的消费者不会购买出现过
安全漏洞的智能设备品牌

93%

的消费者认为制造商需要
进一步提升智能设备的
安全性



97%

的企业认为安全是推行物联网 (IoT) 过程中的重要事项

22%

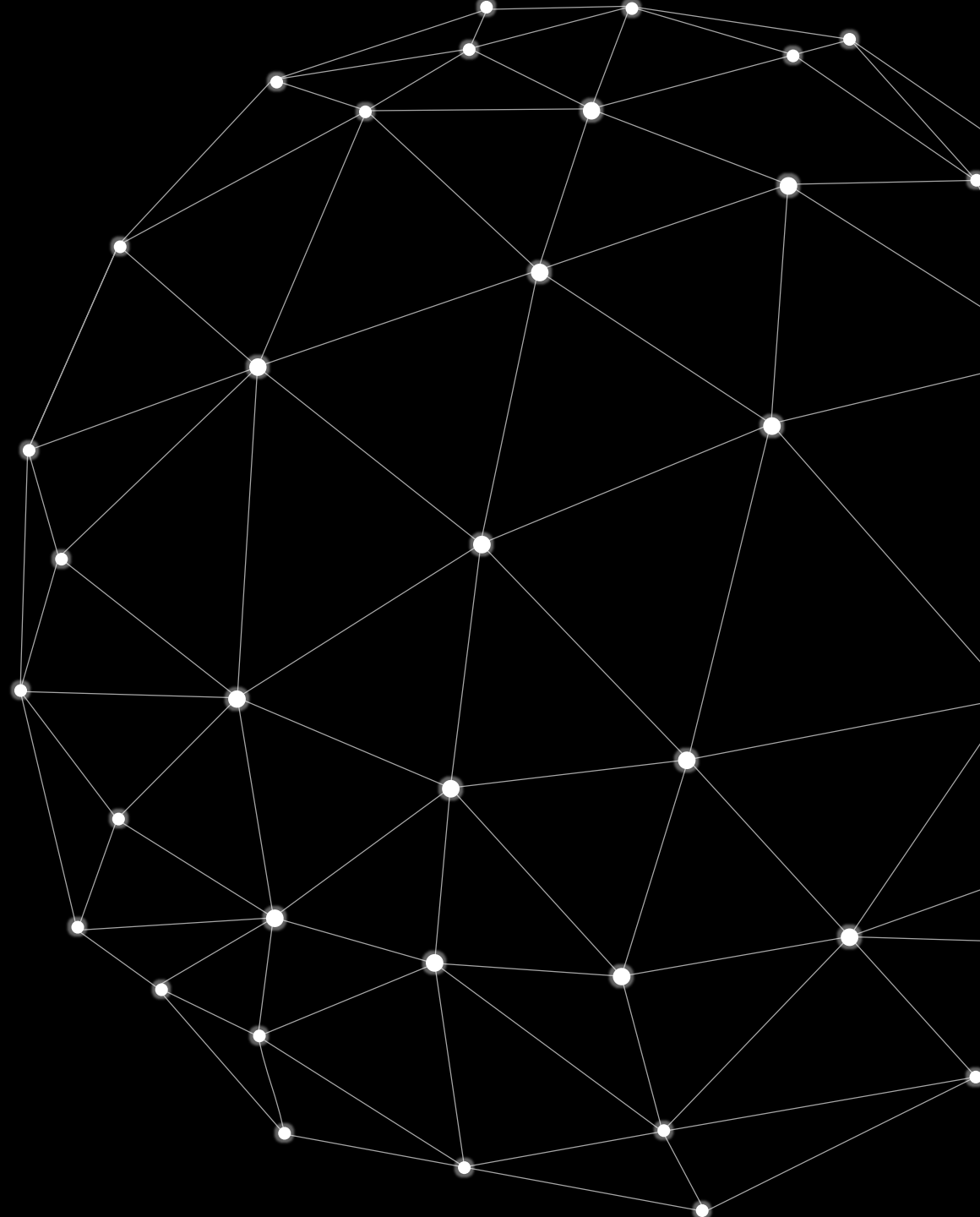
企业客户愿意多支付 22% 以确保物联网 (IoT) 网络安全

70%

当安全问题得到解决，企业愿意多购买 70% 的物理网设备

网络犯罪无处不在

- 民族国家
- 有组织的犯罪团伙
- 竞争对手
- 机会主义者
- 黑客爱好者
- 企业内鬼



IoT设备的攻击面

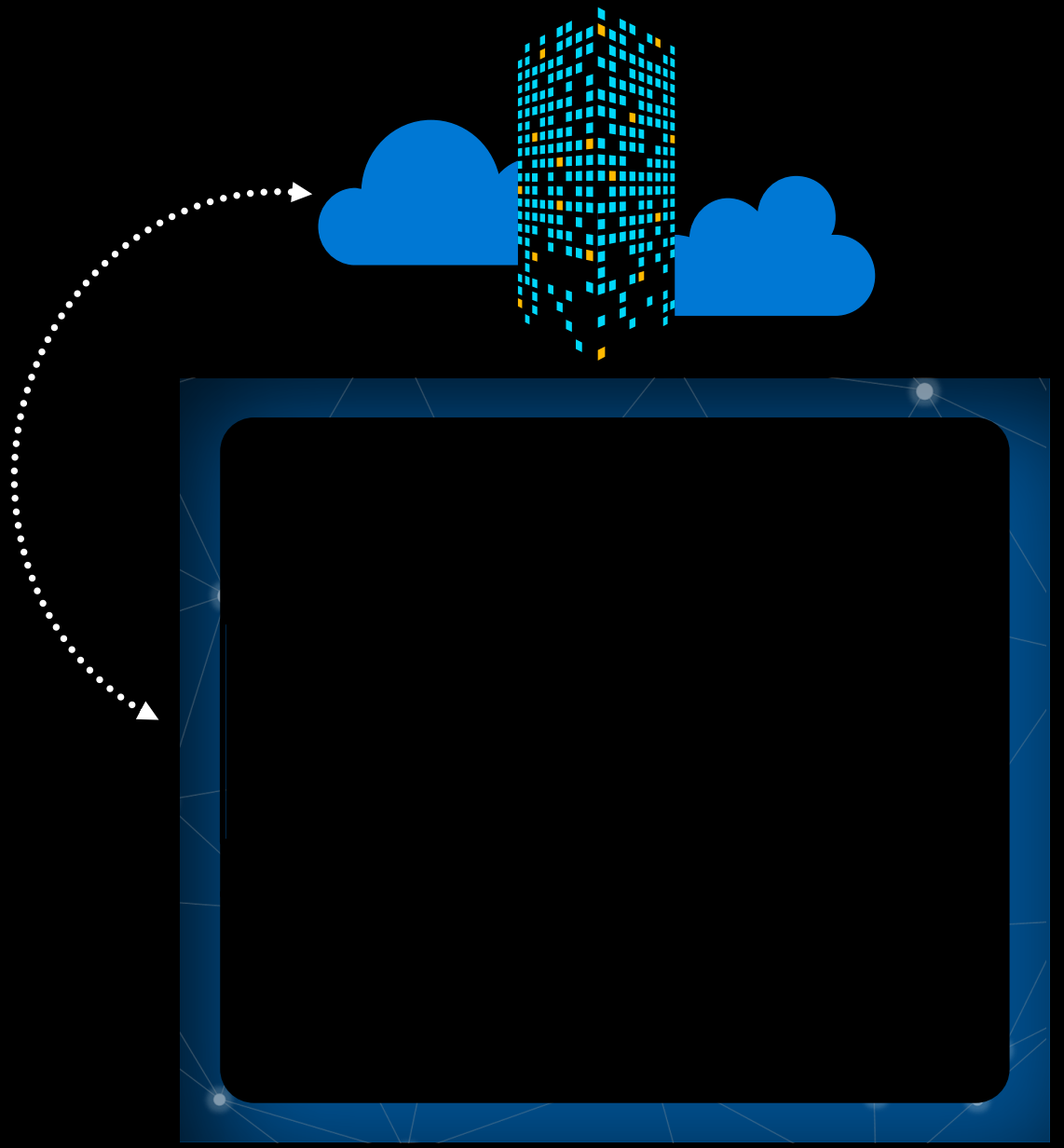
Applications 应用程序

Network 网络通讯

Network stack 网络协议栈

OS 操作系统

Hardware 硬件



对物联网 (IoT) 的攻击威胁企业发展

设备变砖或
被敲诈勒索

设备用于
恶意目的

数据与 IP
被盗

数据被污
染泄露

设备用于
攻击网络

对物联网 (IoT) 的攻击威胁企业发展

设备变砖或
被敲诈勒索

设备用于
恶意目的

数据与 IP
被盗

数据被污
染泄露

设备用于
攻击网络

物联网 (IoT) 攻击造成的损失

IP 或其他重要数据被盗

违反监管或认证

品牌冲击（信誉下降）

恢复产生的成本

经济与法律责任

停工

设备变砖或被敲诈勒索

设备或关键任务装备无法实现功能。只能通过技术人员现场作业或向攻击者支付赎金，方可恢复。

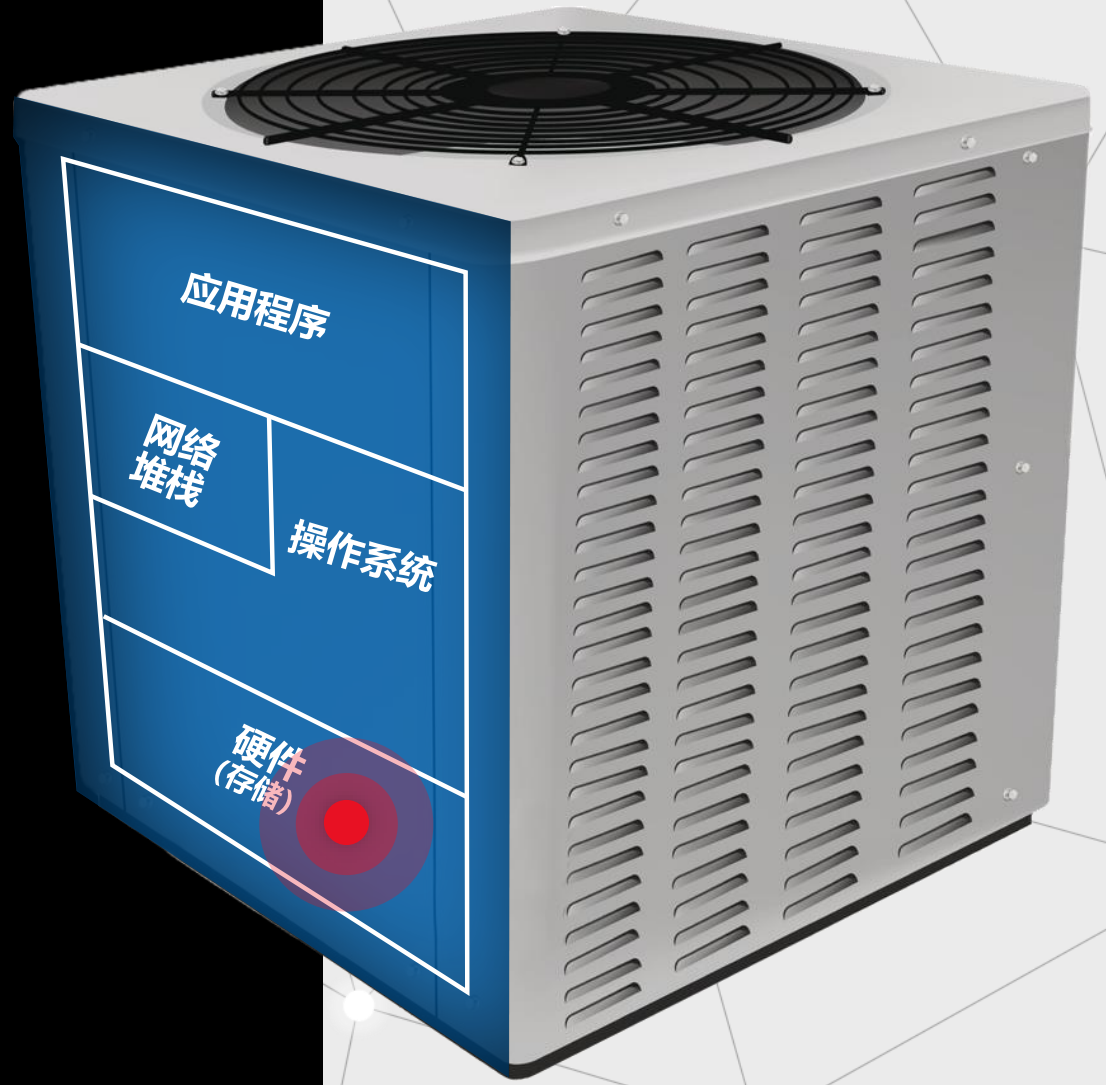
风险评估：

- 设备/装备停工是否会影响收益？
- 停工是否会产生额外成本？
- 相关设备/装备异常否影响人员的健康安全？

设备变砖或被敲诈勒索

此类攻击的目的在于获取硬件和存储信息的访问权

攻击手段包括恶意的未授权执行代码，升级权限以便访问平台最内部信息，进而更改数据和行为。



设备变砖或被敲诈勒索

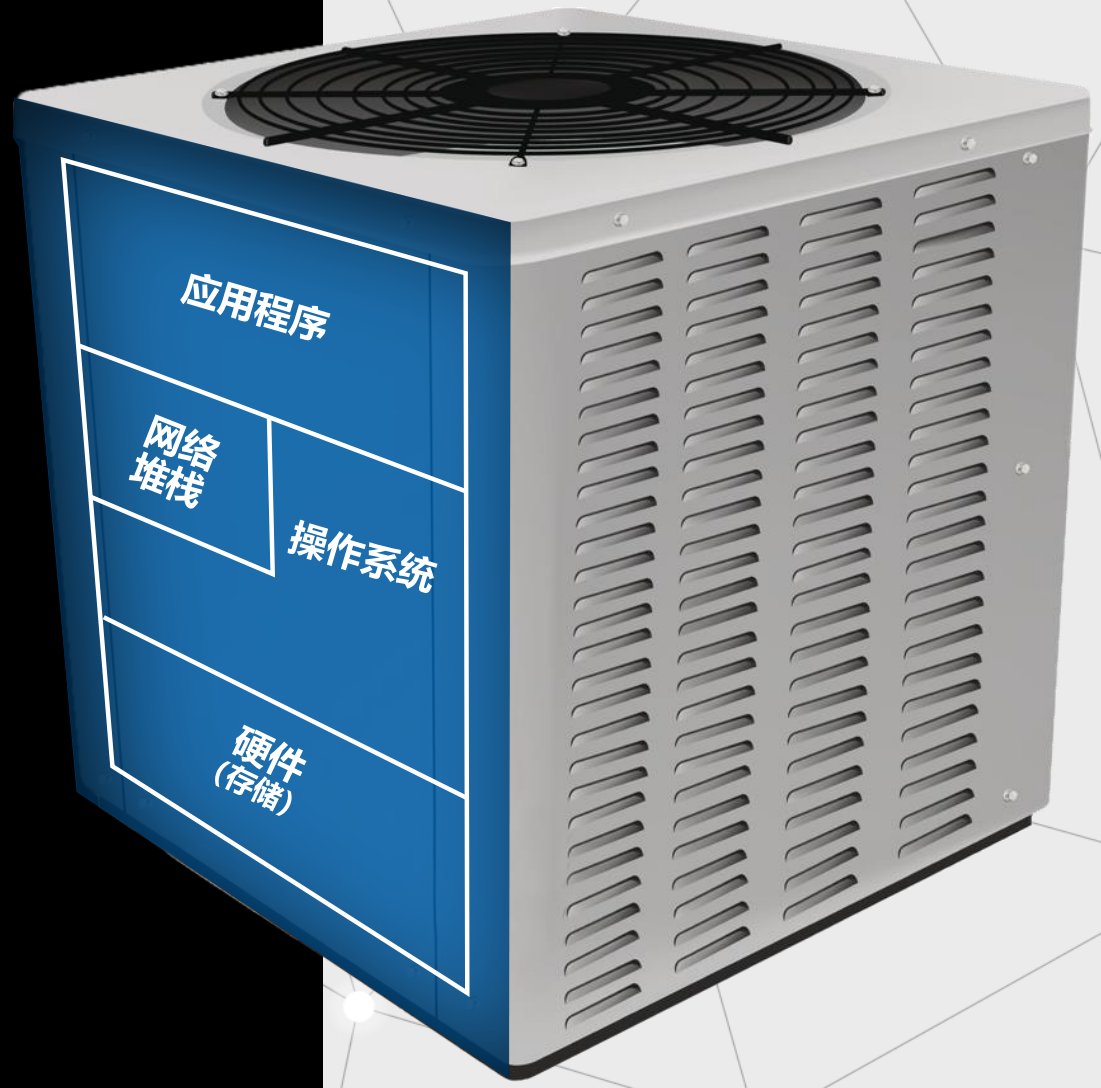
防护策略与能力

深度防御：多层防御，保护控制硬件和存储

划分区域：限制对操作系统不同区域的访问权

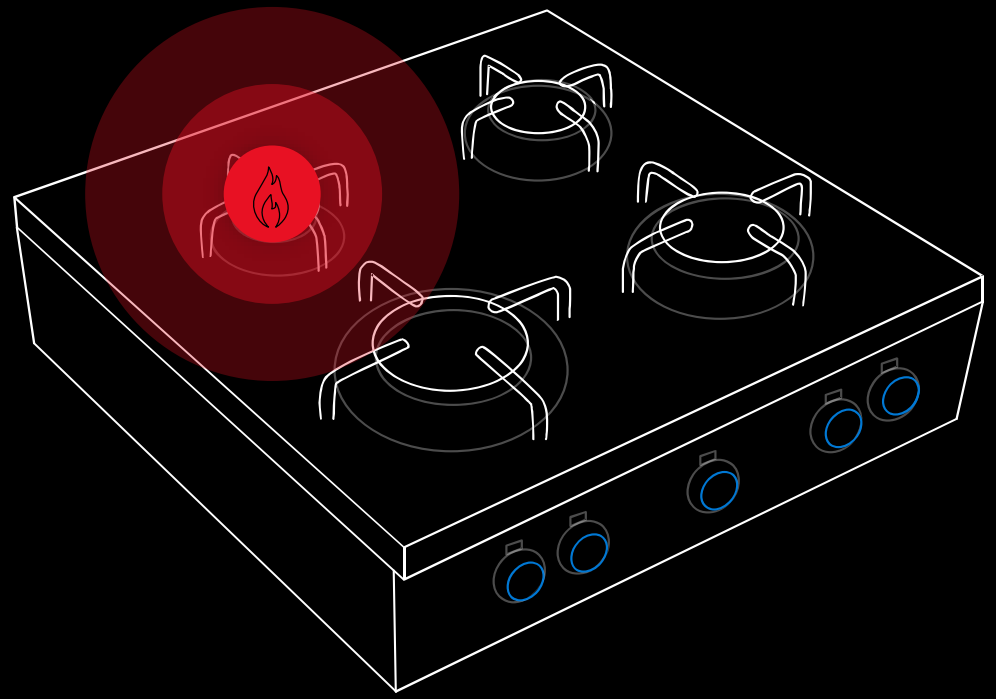
硬件壁垒：例如利用内存管理单元 (MMU) 管理进程间通讯流程

空中 (OTA) 更新：更新设备安全，限制成功机会



设备用于恶意攻击

设备会危害其所处的操作环境，导致设备损毁、人员受伤、以及法律责任



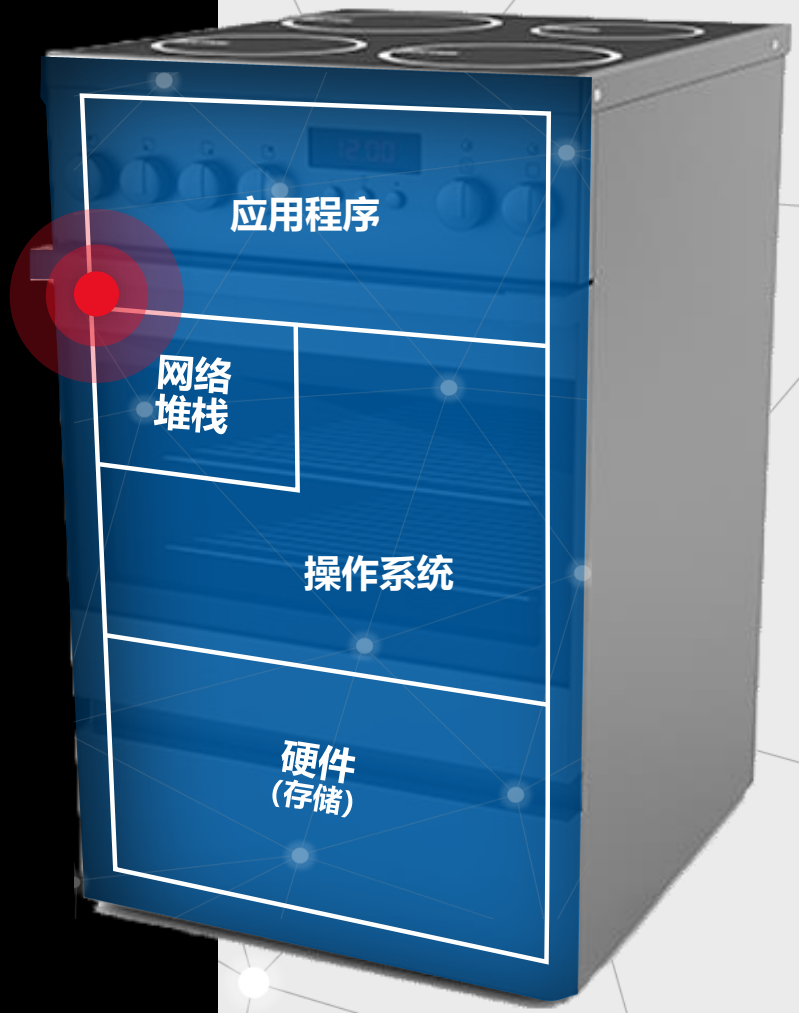
风险评估：

- 设备是否访问加热组件、燃气或用水管线？
- 操作环境是否存在潜在危险？
- 设备是否会给操作员带来伤害？

设备用于恶意攻击

攻击者会让设备产生定义行为以外的操作

攻击手段包括通过网络篡改来模仿您的指令和控制。攻击者也可能让设备运行恶意代码，以便获取对设备的控制。



设备用于恶意攻击

防护策略与能力

使用公私钥对：以确保通讯协议的加密和协议；确保可信通讯

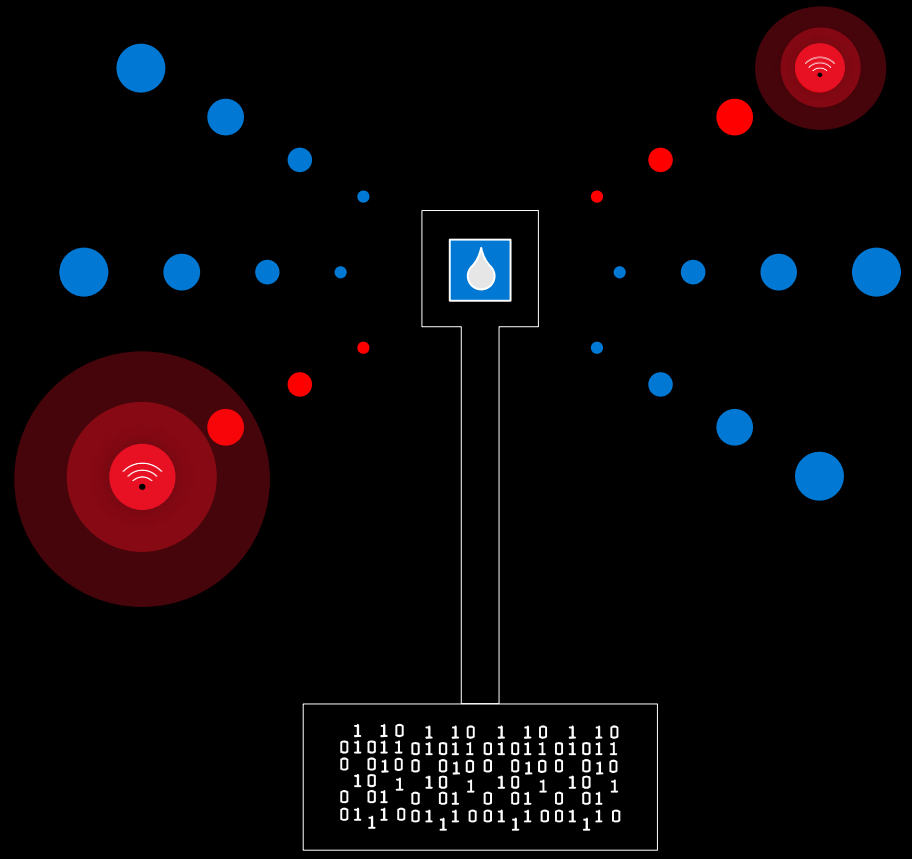
安全启动：确保设备仅运行正版和最新版软件

应用容器和权限限制：限制对物理控制的访问

系统层面应用描述文件：定义和管理应用行为范围

数据污染与商业泄密

无法信任源自设备的数据与产生的结果。直到出错之后才能发现问题所在。



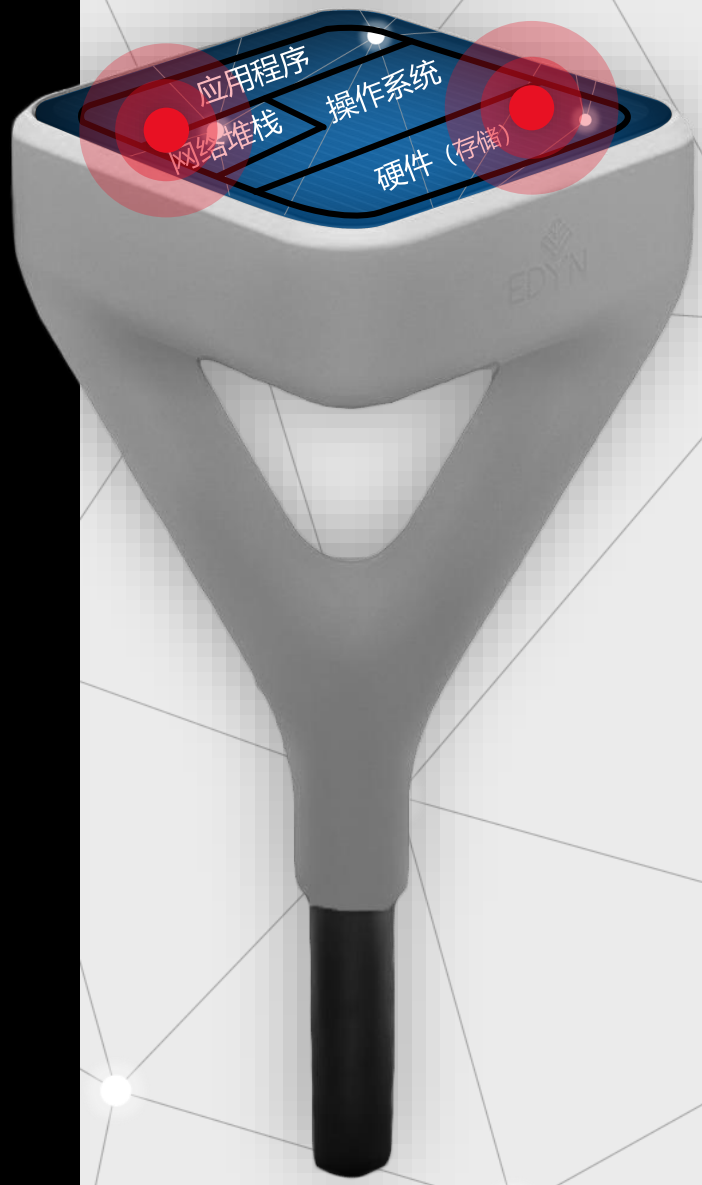
风险评估：

- 是否依赖于数据制定重要业务决策？
- 设备的数据是否用于机器学习 (ML) 或人工智能 (AI) 建模？
- 是否基于设备数据实现创收或向客户收费？

数据污染与商业泄密

攻击者使用伪造/窃取的身份篡改数据或模仿设备

攻击手段包括中间人攻击，篡改输出数据/数据包。还可利用伪造身份来（如保护不得当的密码和密钥证书）模拟设备。



数据污染与商业泄密

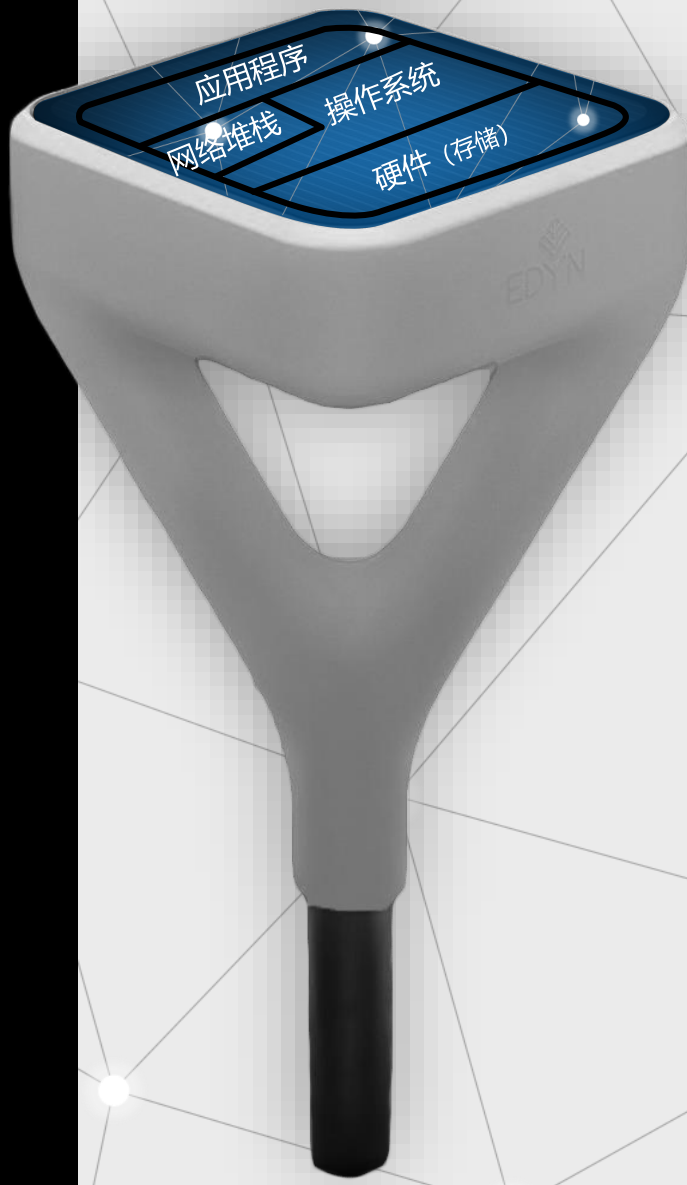
防护策略与能力

硬件可信根创：建独一无二不可复制的身份

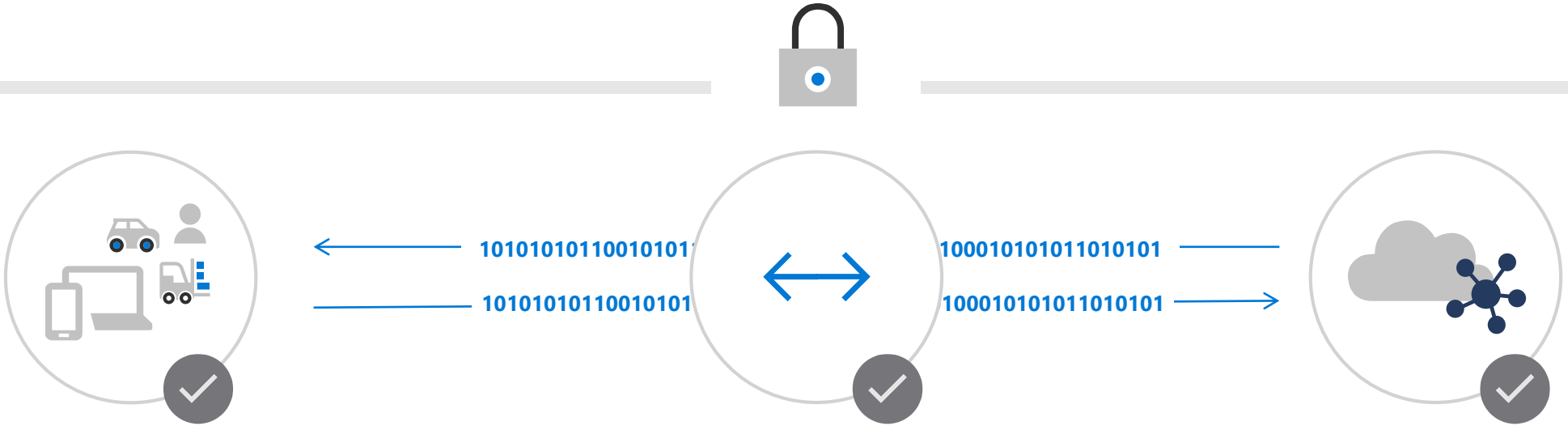
双向验证：确保服务器和客户端均被验证。

认证：确保仅限运行信任软件的正版设备连接到您的服务

加密的通讯：确保数据和数据包不被泄露



微软物联网 (IoT) 安全：从端到云：



设备

对任何设备实现安全支持

跨设备实现威胁监控与防护

连接

可靠的协议与技术

基于标准的双向验证

物联网 (IoT) 服务

IoT Hub 和 Central 充分考虑安全设计

基于政策的可扩展访问控制

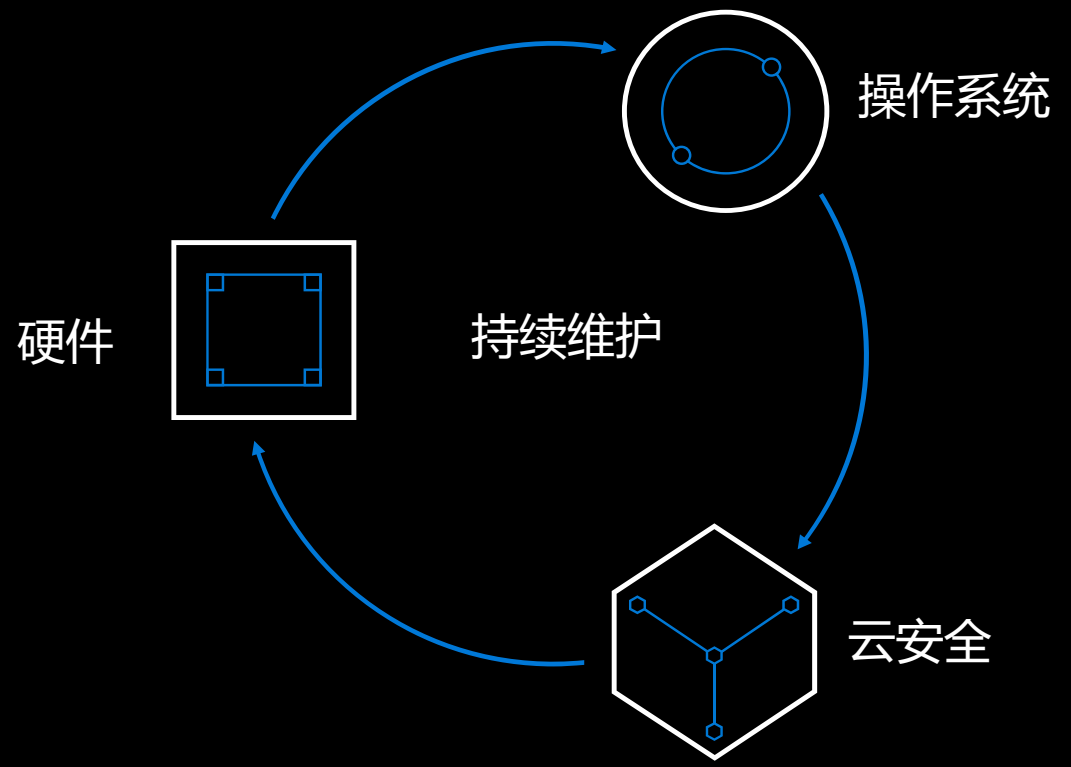
行业领先的可靠性与适应性

安全监控、警告与响应

Azure Sphere

高度安全的物联网端到端解决方案，从芯片，操作系统，云服务三个维度协同来提供极高的安全机制，从而打造全新物联网 (IoT) 设备。

- Azure Sphere 认证芯片
- Azure Sphere 操作系统
- Azure Sphere 安全服务
- Azure Sphere 持续维护



微软直接向各设备提供 10 年以上的安全与操作系统更新服务

Windows for IoT

Windows for IoT 具备与 Windows 10 相似的功能和管理能力

内置 Windows 10 安全机制，时时保持更新，安全补丁支持长达 10 年

利用 Windows 10 最新的安全技术，保护从设备到云端的物联网 (IoT) 解决方案

致力于平台安全与隐私的专家团队服务

Windows 10 IoT Core & Services

针对小型智能设备
低成本设备也可以使用Windows IoT

Windows 10 IoT Enterprise

针对功能固定的智能设备
已锁定的完整版 Windows 10

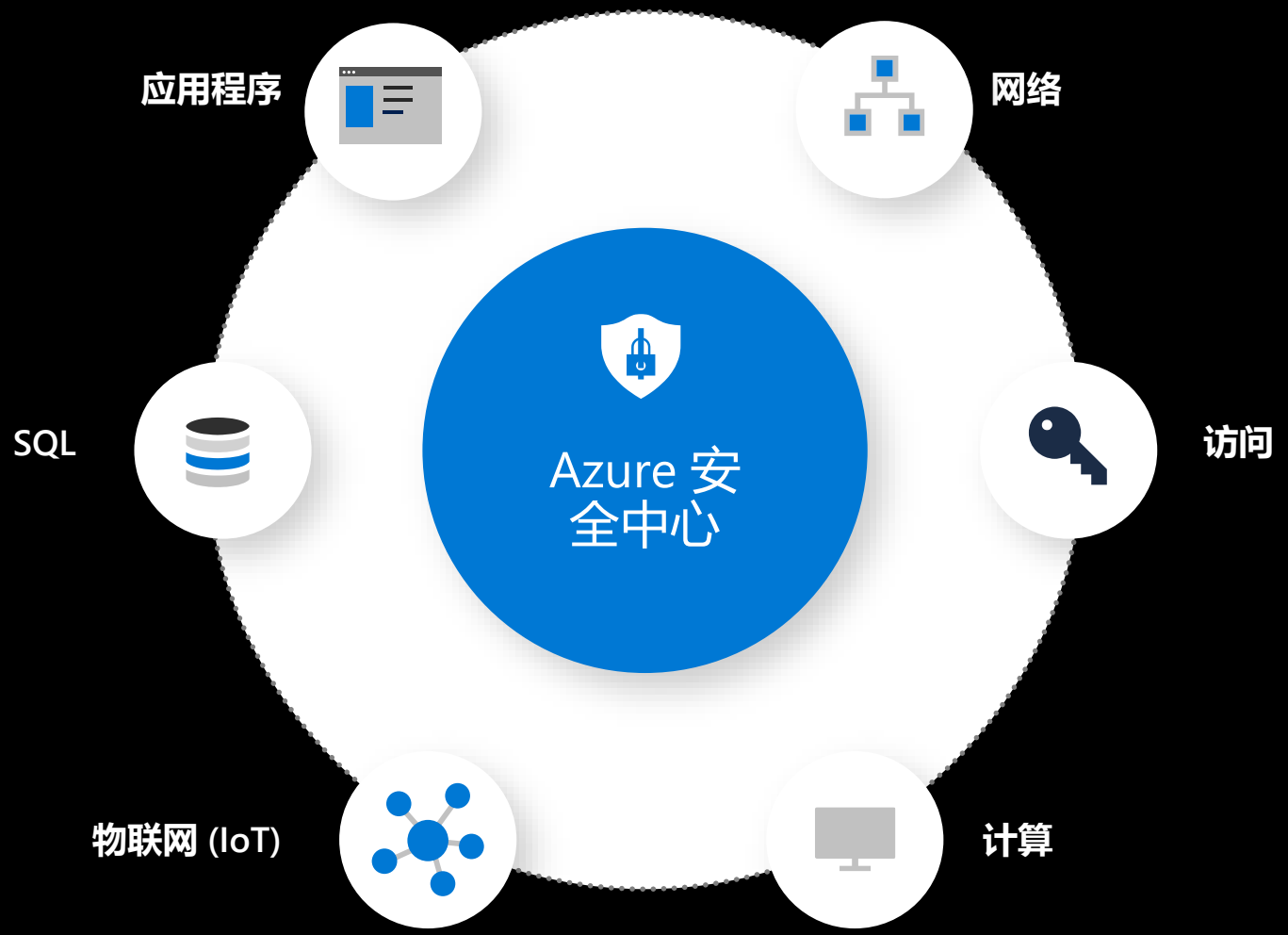
Windows Server IoT 2019

针对要求最严苛的边缘
计算工作

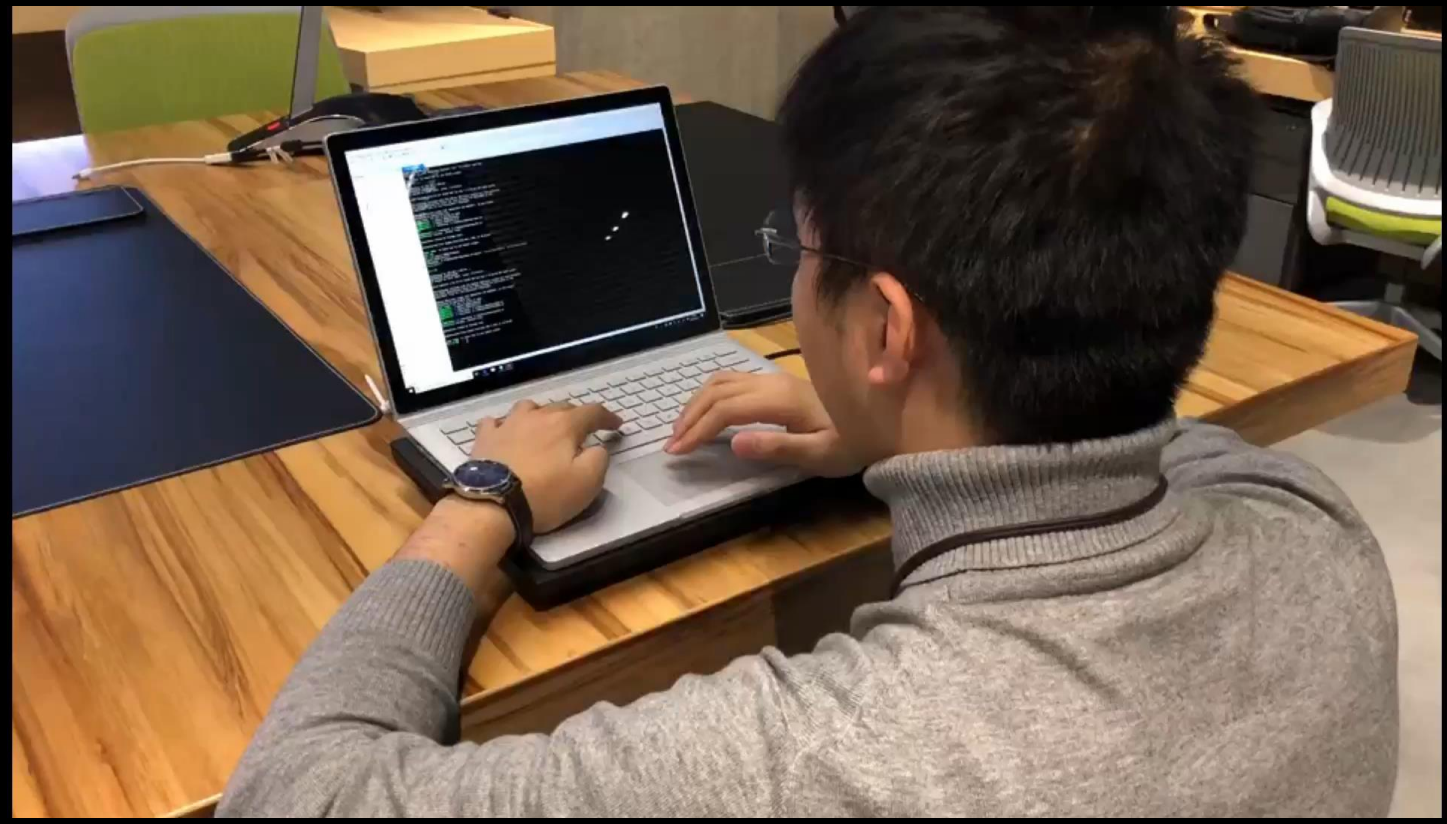
以 9 亿台活动的 Windows 10 设备为基础构建

Azure 安全中心

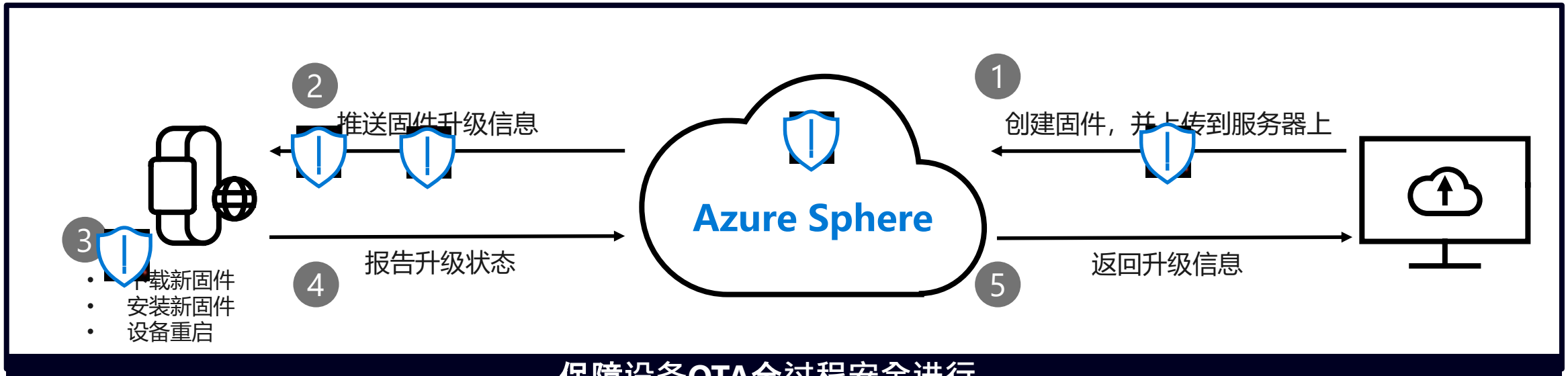
Azure 安全中心可帮助用户抵御威胁，管理安全风险，保护云端和物联网 (IoT) 资源，包括微软和第三方设备。Azure 物联网安全中心 是首个端到端物联网 (IoT) 安全服务，助力各类机构预防、探测和修复潜在攻击，覆盖物联网 (IoT) 实施过程中的所有组件。



发生了什么？



IoT设备空中升级（OTA）过程中的安全风险及应对



保障设备OTA全过程安全进行

- 固件开发时存在漏洞/后门
- 服务器/云遭受恶意攻击
- 设备冒充
- 中间人攻击
- 设备安装了存在后门的固件，将遭受黑客的进一步攻击

- AS3提供撤销、回滚和删除机制，以减小错误更新带来的影响
- 微软Azure基础设施具备成熟的安全能力，支持全球IoT设备升级的同时，提供强大的安全保障
- Azure Sphere MCU从硬件层面进行身份认证，防止设备冒充
- AS3通过高强度加密算法实现传输加密（TLS v1.2）及签名（ECC），防止中间人攻击
- Azure Sphere MCU提供硬件防火墙，结合AS3的回滚机制，实现对威胁的抵御和应对

中国网络安全现状 - 2018

8.28亿
中国网民

10.6万
网络安全事件

- 77,373 个控制端
- 27,890 个位于中国境内
- 49,483 个位于境外
- 655万 台中国境内主机被控制

木马和僵尸网络

- 4,451万起恶意嗅探事件
- 6,020 个联网工业设备暴露

工业互联网安全

- 1,700 个高危漏洞
- 46%为XSS跨站脚本漏洞
- 28% 为SQL注入漏洞
- 5.1% 为Spring遍历漏洞

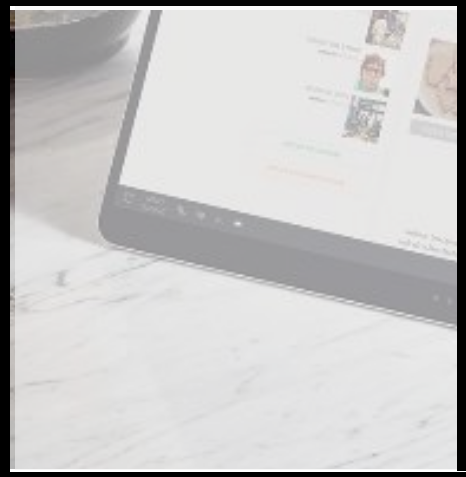
互联网金融安全

- 2,108 个控制端
- 144万 个总肉鸡数量
- 4,000 起攻击/每月
- 1G Bit/s 以上的攻击峰值

拒绝服务攻击

- 14,201 个安全漏洞
- 4,898 个高危漏洞
- 11% 较2017年下降

安全漏洞



主要的针对云端的攻击类型包括：

DDoS攻击

后门攻击

网页篡改

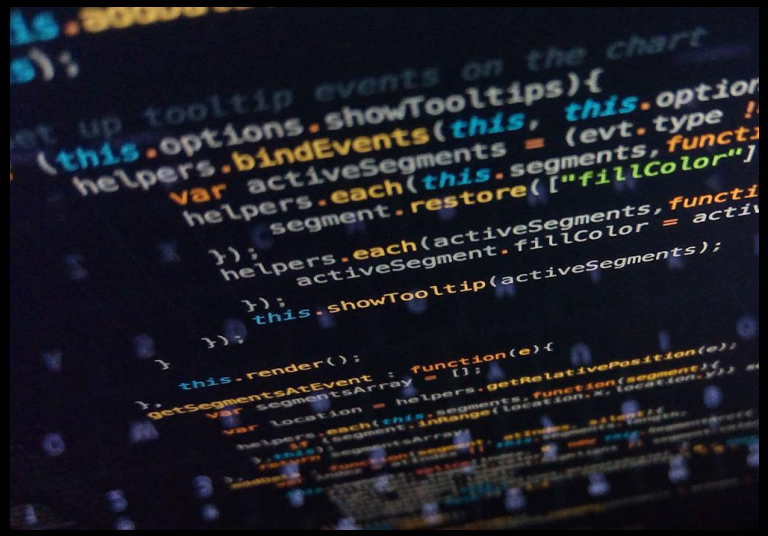
云端安全

- 超过 15 种恶意代码家族
- 2,194 个通用型IoT设备漏洞
- 446.9万 个受控智能设备IP地址

智能设备安全

数据来源: CNCERT/CC《2018年中国互联网网络安全报告》

通量和转型的时代

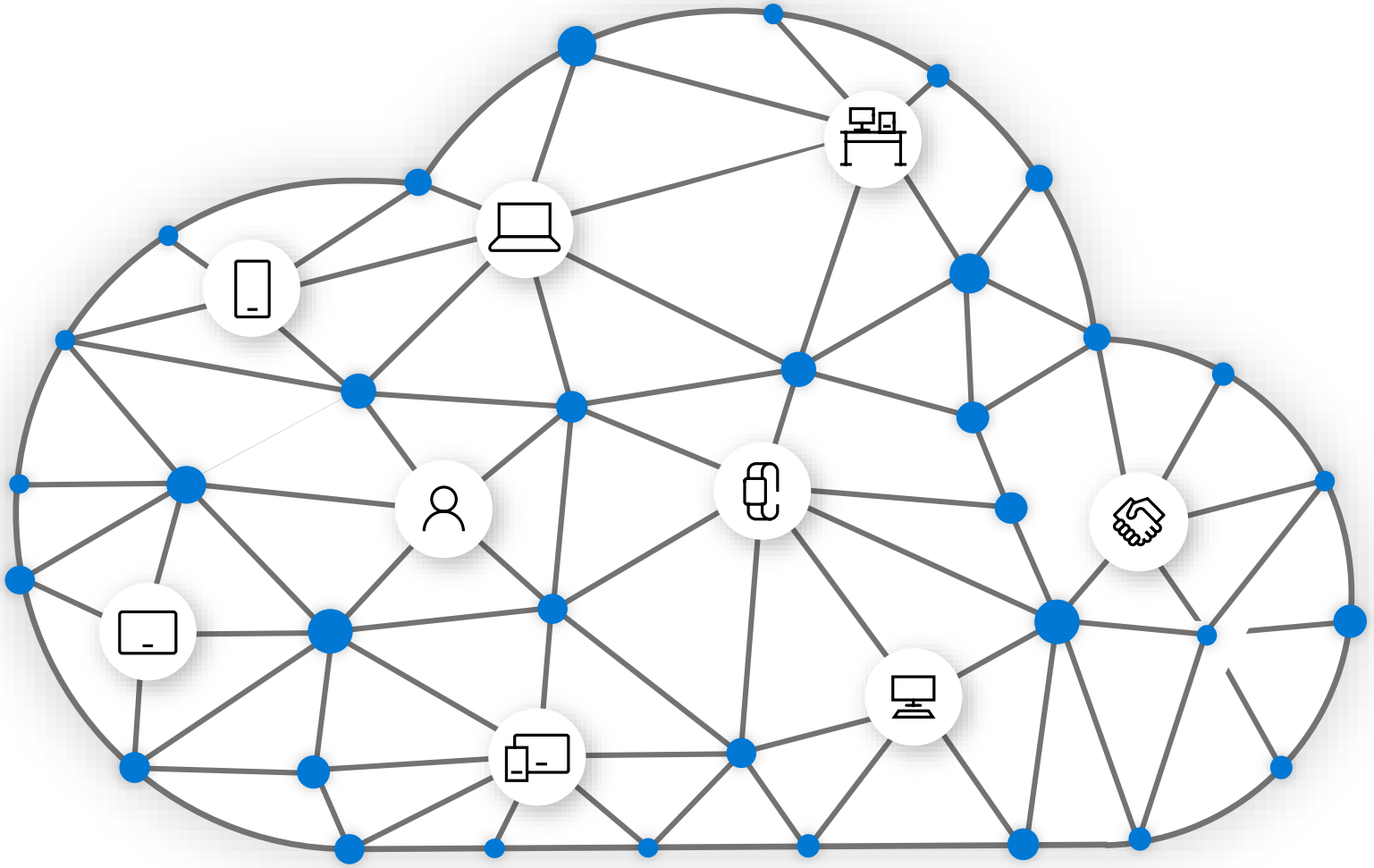


现在每个人都在从事
技术业务

传统的安全工具
没有跟上步伐

只依靠安全专业人员
无法填补安全防护的空白


个人电脑
家庭办公室
个人可穿戴设备
个人设备
客户可穿戴设备
公司设备
合作伙伴
客户
合作伙伴设备
客户设备
内部部署
移动设备
移动设备



FORRESTER®

“Cybersecurity的未来...在云。 ”

运营

为您服务的安全运营

技术

企业级技术

政策、合作伙伴

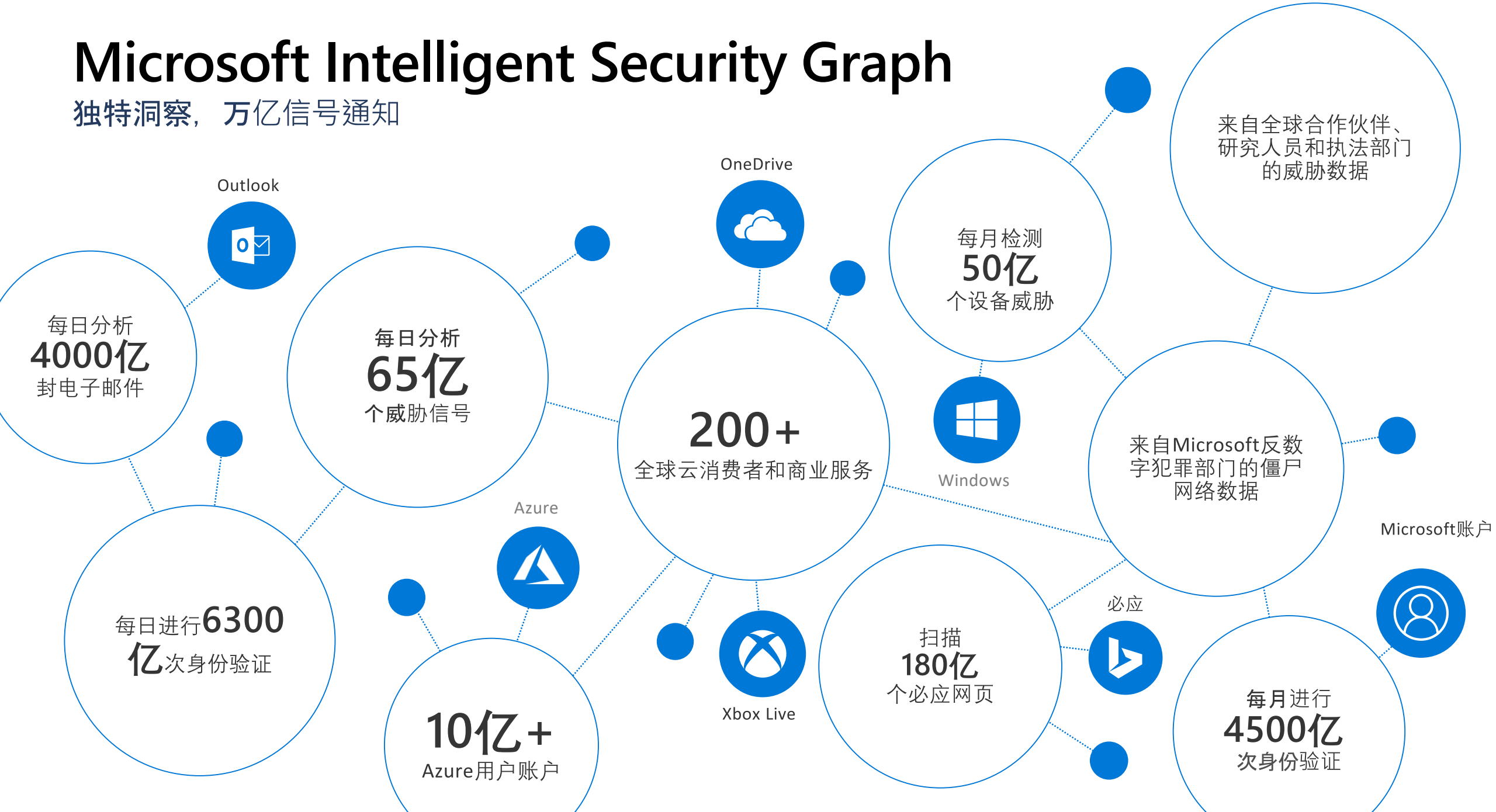
达成合作关系建立多元化世界


运营
为你服务的安全运营
微软安全
技术
企业级技术
政策、合作伙伴
达成合作关系建立多元化世界

这是您的安全团队

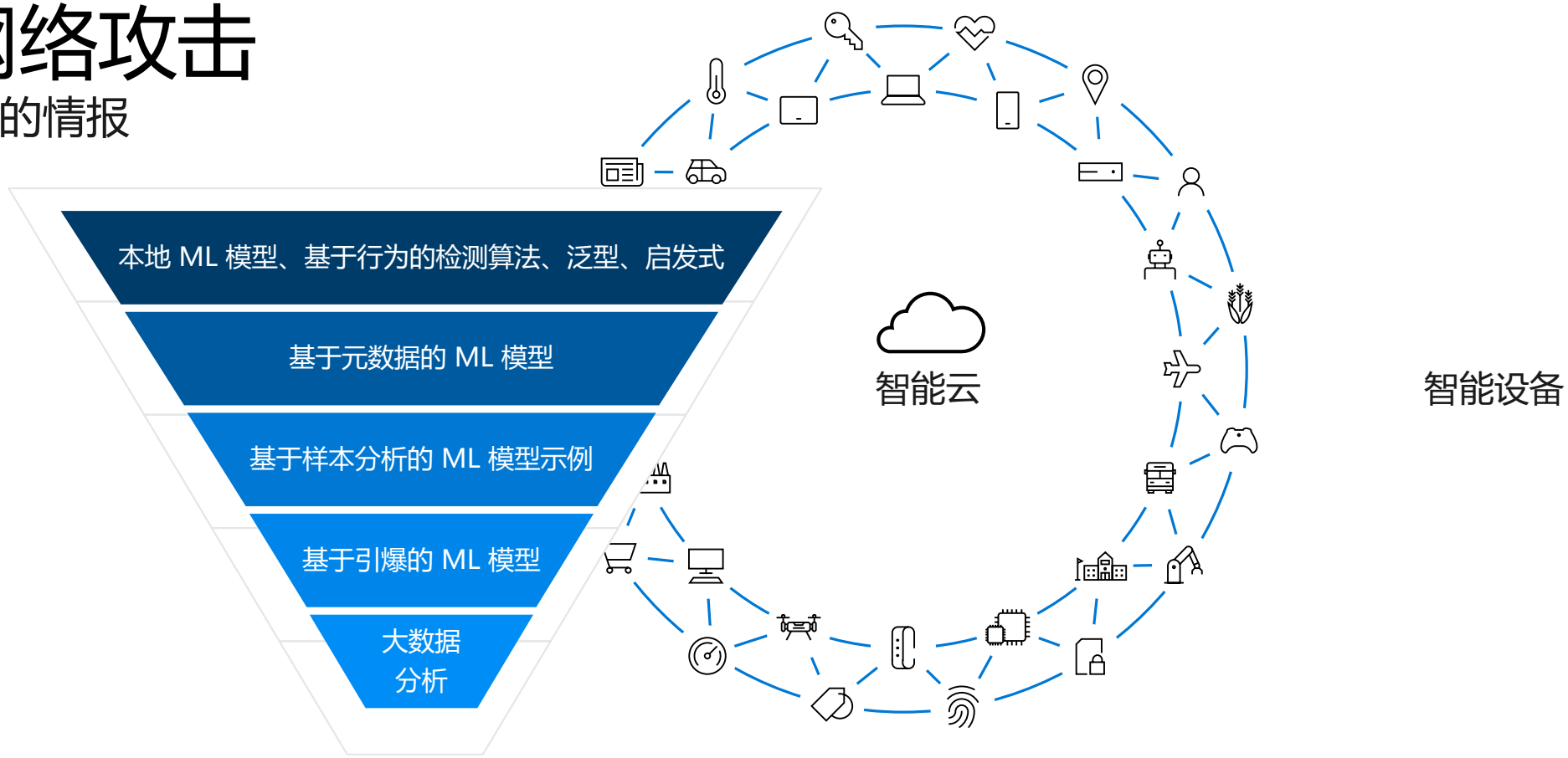
Microsoft Intelligent Security Graph

独特洞察， 万亿信号通知



阻止网络攻击

真实场景中的情报



2017

2017年10月 –基于云的启发式 ML 模型识别出 Bad Rabbit，在第一次遭遇14 分钟后保护用户。

2018

2018年3月 –基于行为的检测算法阻断了超过40万个Dofoil 木马的攻击实体

2018年11月 – 基于行为的保护措施阻断了针对非盈利组织和政府机构的 spear-phishing 行动

2019

2019年6月 –下一代保护措施披露并阻止了复杂的、无文件的Astaroth行动，而传统基于文件的解决方案无法检测到这一活动。


运营
为你服务的安全运营
微软安全
技术
企业级技术
政策、合作伙伴
达成合作关系建立多元化世界

企业级技术

全球范围
响应紧急安全挑战

- 95% 的财富 500 强企业都依靠我们。
- 无可比拟的多样化威胁遥测数据 – 每天 6.5T 信号。
- 每年 10 亿美元的网络安全投资。
- 保护未来：物联网、分散式数字标识、量子计算。

AI + 自动化
让您的团队专注于他们最擅长的事情

- 3,500 位安全专家和AI基于微软全球威胁数据抵御威胁。
- 通过抑制误报，将警报疲劳降低 90%。
- 97% 的所有攻击都在终端上自动修复。

跨您的产品组合
集成高级能力

- 跨您的解决方案的共享情报、自动化和编配。
- 跨标识、终端、应用程序、数据、基础设施的端到端覆盖。
- 由解决方案提供商和 ISV 组成的广泛生态系统。

企业级技术

身份和访问管理

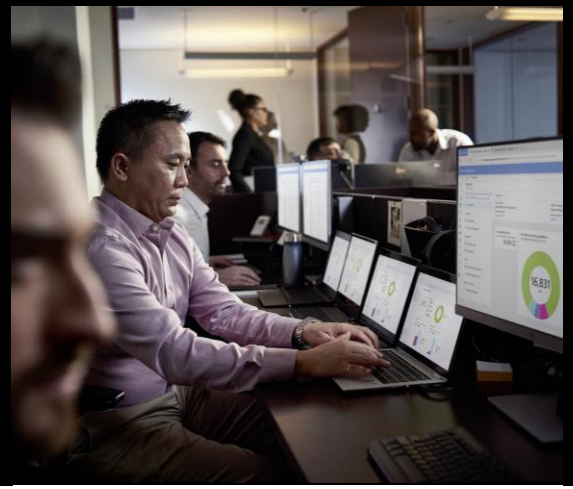
安全标识，
实现“零信任”。

威胁防护

通过集成和自动化的安全
阻止攻击。

信息保护

保护您的敏感数据
— 无论它是静态或被传输中。



安全管理

通过洞察力和指导
来强化您的安全态势。

运营

为你服务的安全运营

微软安全

技术

企业级技术

政策、合作伙伴

达成合作关系建立多元化世界

运营 技术 **政策、合作伙伴**

网络安全技术协议

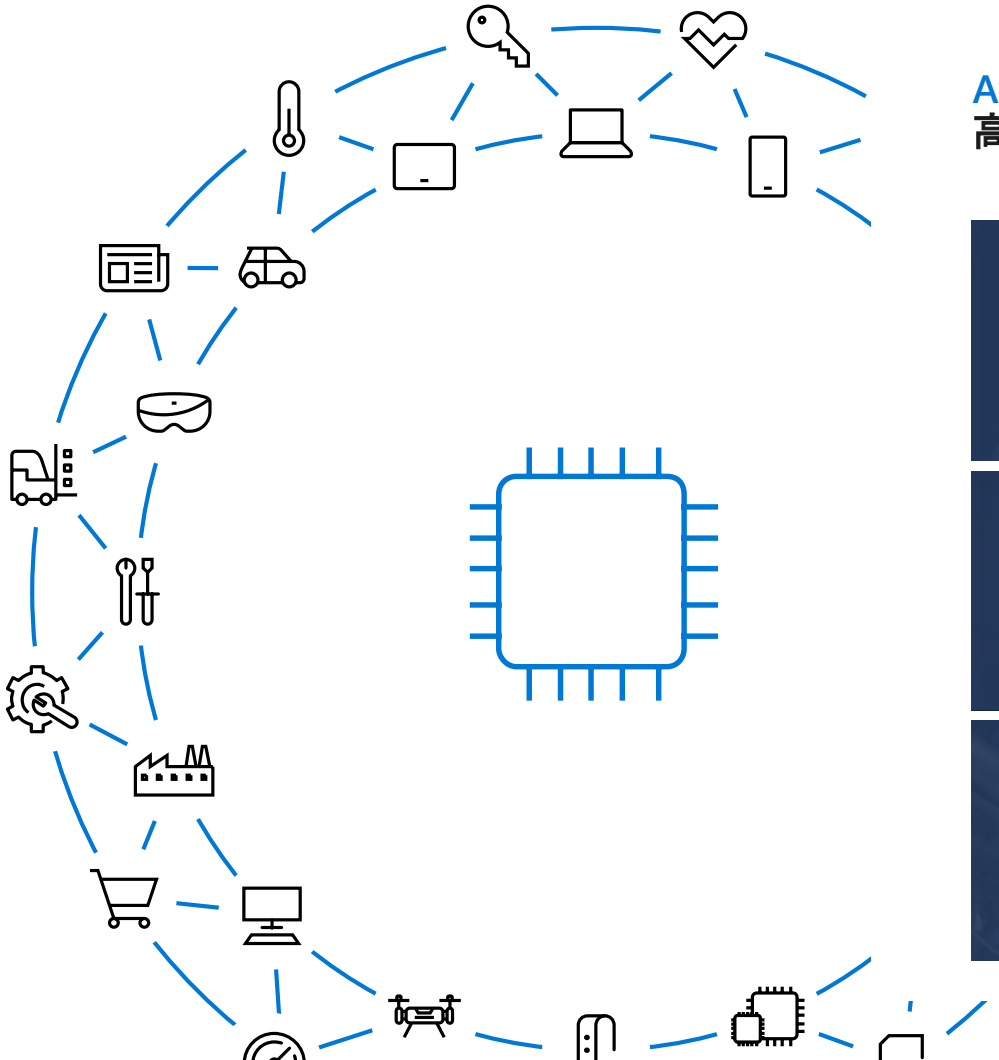
100 多家全球公司正在共同努力，提高网络空间的安全性、稳定性和弹性。

“

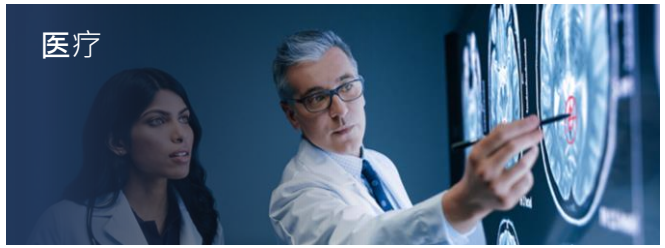
创造更安全的互联网的第一步必须来自我们自己**的行**业，即创造和运营世界在线技术和基础设施**的企**业。”

Brad Smith
总裁兼首席法务官，微软公司

合作实现跨行业的安全物联网



Azure Sphere **将硬件、操作系**统和云安全性结合在一起，以帮助客户构建**高度安全的、相互**连接的智能设备。



微软智能安全联盟

合作以加强保护

与我们的安全合作伙伴合作，构建智能安全解决方案生态系统，更好地抵御世界上不断增加威胁。

Microsoft 安全

我们承担起我们的责任，创造一个更安全的世界，使组织能够实现数字化转型。

Microsoft

谢谢！