数据驱动边缘计算安全
Data Driven Edge Computing Security

吴云坤, 总裁, 360企业安全集团
Yunkun, Wu, President, 360 Enterprise Security

2017物联网安全现状
The Status of IoT Security in 2017

- 商业、消费者和工业之间连接的“事物”数量迅速增长
- Number of connected "things “ in commercial, consumer and industries grow rapidly

2015：安装了**49亿**个物联网端点 **4.9B** IoT endpoints
2020：安装基数增长至**204亿** **20.4B** IoT endpoints

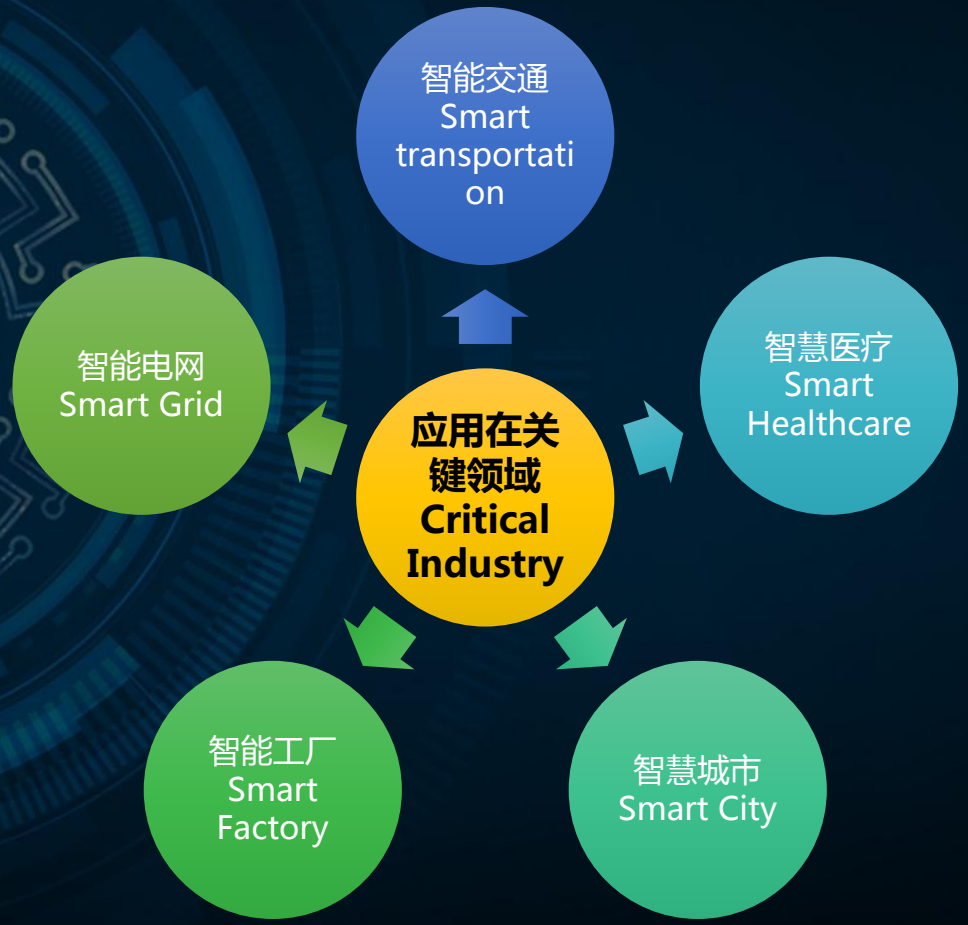
- 物联网安全不是一个“新网络”范式，它需要的是混合方法
- IoT security is not a “new network “ paradigm but requires hybrid approaches.

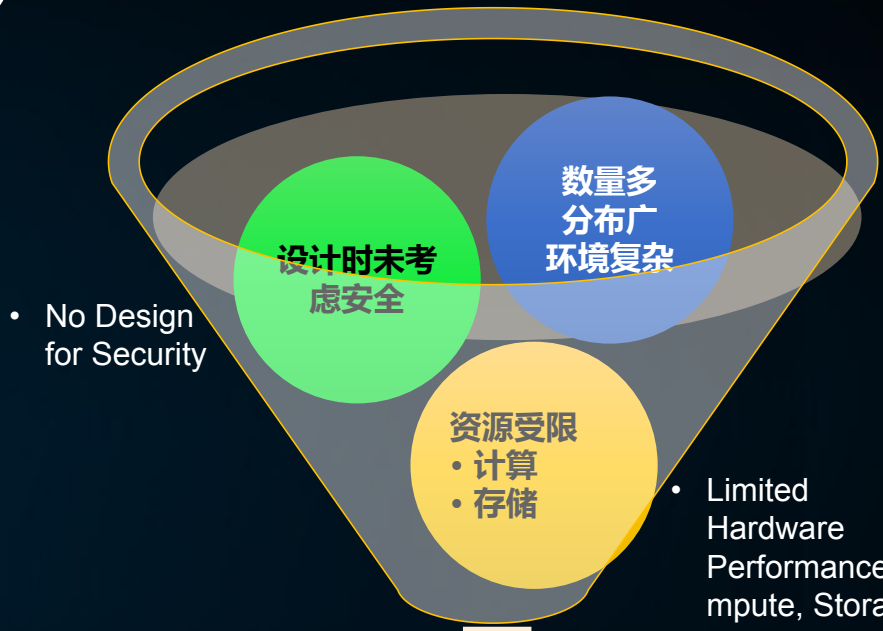
- 工业界和政府活动正在迅速发展和适应
- Industry and government activities are evolving and improving rapidly

- 现实世界的物联网攻击往往击中了主流
- IoT attack hit mainstream

- *未来超过50%的数据需要在网络边缘侧分析、处理与储存！*
- *More than 50% data will be analyzed, processed and storage at the network Edge*

物联网和边缘计算安全现状：关键且脆弱
Status of IoT Edge Computing Security : Critical and Vulnerable





- No Design for Security
- Large Quantity
- Widely Spread
- Complex Environment
- Limited Hardware Performance(Compute, Storage)

传统防护手段不适用
Tradition Protection is no longer appropriate

安全性差
Poor Security Performance

物联网和边缘计算安全现状：安全事件频发

Status of IoT Edge Computing Security : Security incidents occur frequently

- 2015年6月，360安全专家公开展示了利用某汽车厂商云服务漏洞，可以开启汽车的车门、发动汽车、开启后备箱等操作，后续公布了破解特斯拉等车型的演示案例
- 360 Security experts announced that they can open the doors, start the engine through the vulnerabilities of an automobile vendor’ s Cloud Service in June 2015, and soon released the cases of cracking Tesla.

- 2015 年 12 月 23 日，乌克兰电力网络受到攻击，导致伊万诺-弗兰科夫斯克州大停电，成为全世界第一起黑客攻击造成电网大规模停电事件
- Ukraine Ivano-Frankivsk State was power off because of the attack of power grid, which was the 1st massive attack to power utilities in the world

- 2016年10月22日, Mirai病毒将数百万路由器、智能摄像头当做“肉鸡”向美国域名服务器管理机构Dyn发动大规模的DDos (分布式拒绝服务)攻击，致使美国互联网大面积瘫痪。2017年10月，360又发现类似病毒**IoT_Reaper，破坏力更大**
- On Oct. 22, 2016, the Mirai virus put millions of routers and smart cameras as "broilers" on a massive DDoS attack on the U.S. DNS server Dyn, causing widespread disruptions.

网络安全新常态
New Normal of Network Security

四个假设 Four hypotheses

假设① 系统一定有未被发现的漏洞

The system must have undiscovered vulnerabilities

假设② 一定有已发现但未修补的漏洞

There must be discovered but not patched vulnerabilities

假设③ 系统已经被渗透

The system has been infiltrated

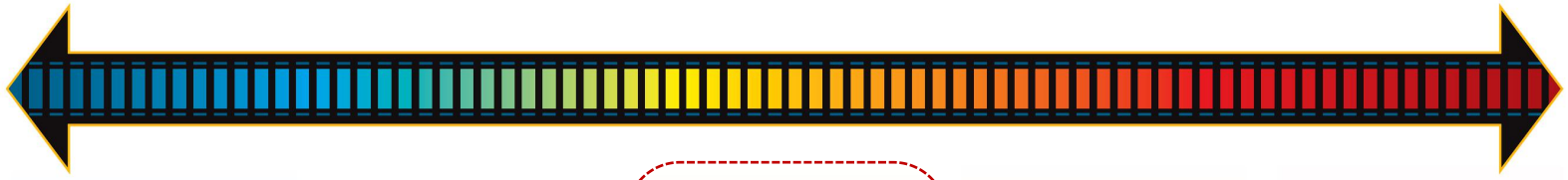
假设④ 内部人员不可靠

Insiders are not reliable

网络安全能力的叠加演进
Overlay Evolution of Network Security Capabilities

边缘计算 Edge Computing CONSORTIUM | 360企业安全

依赖 Dependency



进化 Evolution

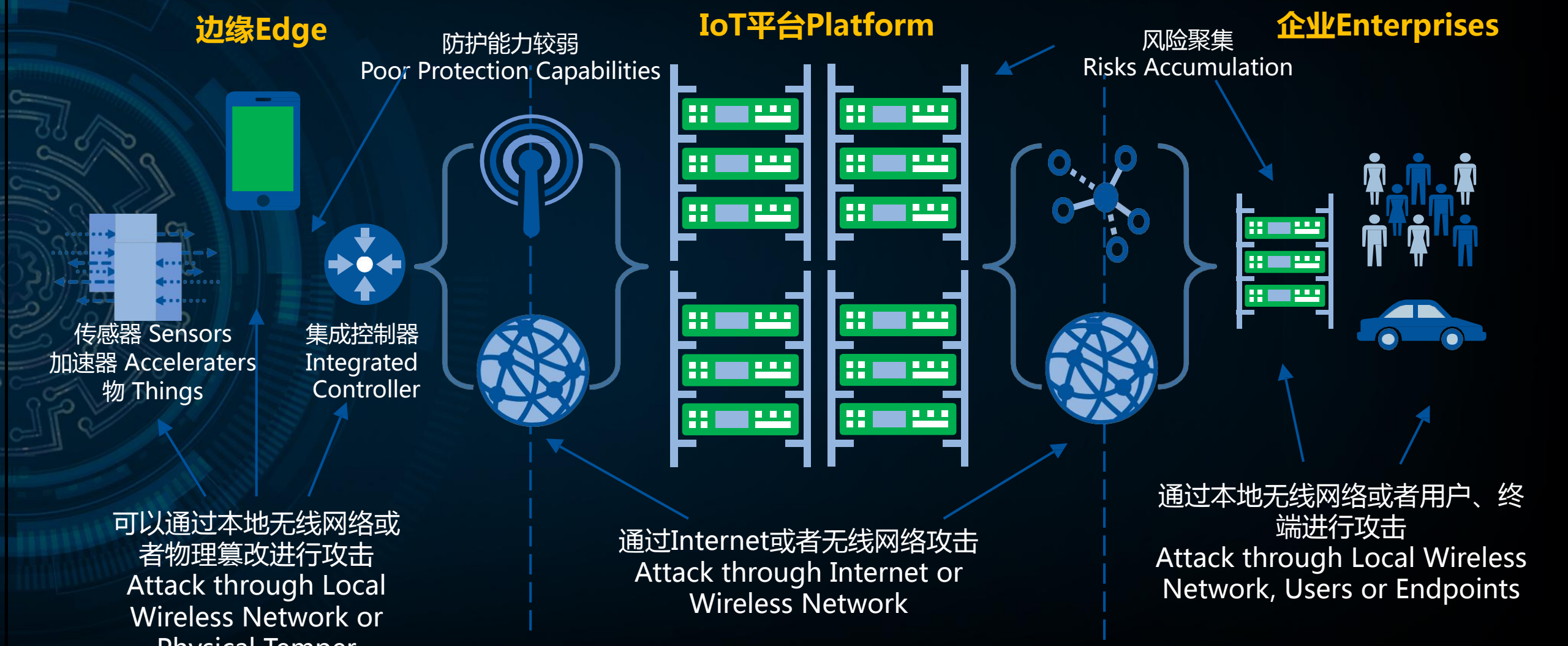
架构安全	被动防御	积极防御	威胁情报	进攻反制
强身健体 Strengthen the Body	纵深防御 Defense in Depth	检测响应 Detection & Response	掌握敌情 Know the Intelligence	先发制人 Preemptive
ARCHITECTURE	PASSIVE DEFENSE	ACTIVE DEFENSE	INTELLIGENCE	OFFENSE
• 安全体系 • 安全域 • 安全加固 • 补丁管理 • 应用内建	• 传统安全 • 收缩攻击面 • 消耗攻击资源 • 迟滞攻击	• 安全分析 • 追踪溯源 • 响应处置 • 人的参与	• 信息收集 • 情报生产 • 分析验证 • 情报猎捕	• 法律手段 • 反制措施 • 自我防卫

降低平均检测时间(**MTTD**)/ 平均响应时间(**MTTR**)

Reduce the Mean Time to Detect(**MTTD**), Reduce the Mean Time to Response(**MTTR**)

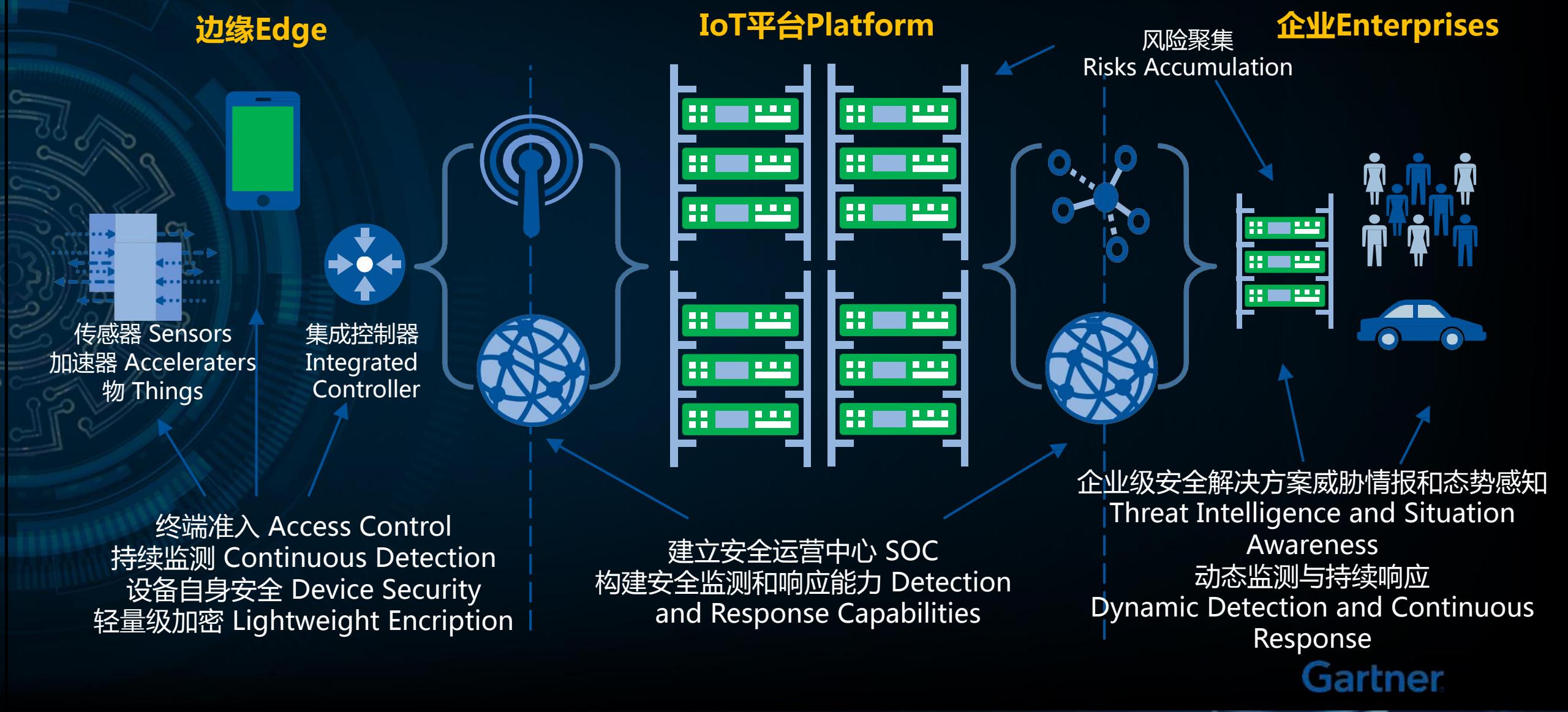
物联网和边缘计算安全现状：攻击路径分析

Status of IoT Edge Computing Security : Attack path Analysis

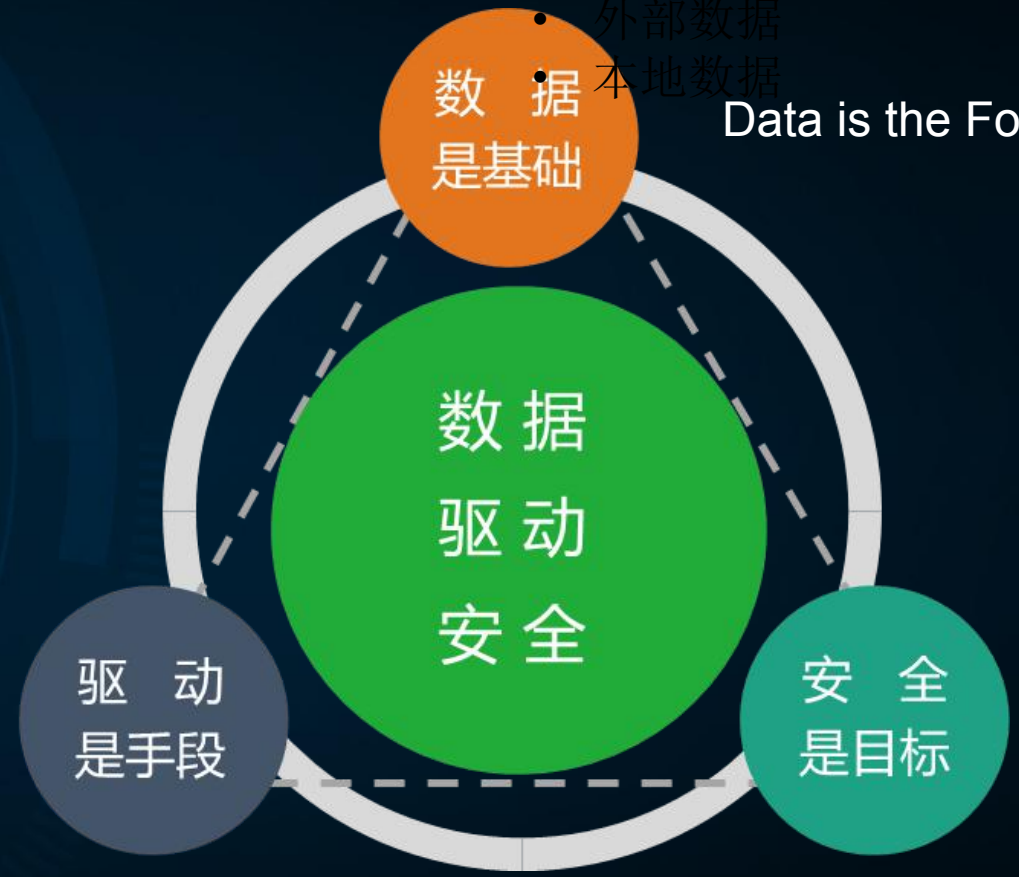


物联网和边缘计算安全现状：防护措施

Status of IoT Edge Computing Security : Protection Methods



数据驱动安全创新理念
Data Driven Security Innovation Concept

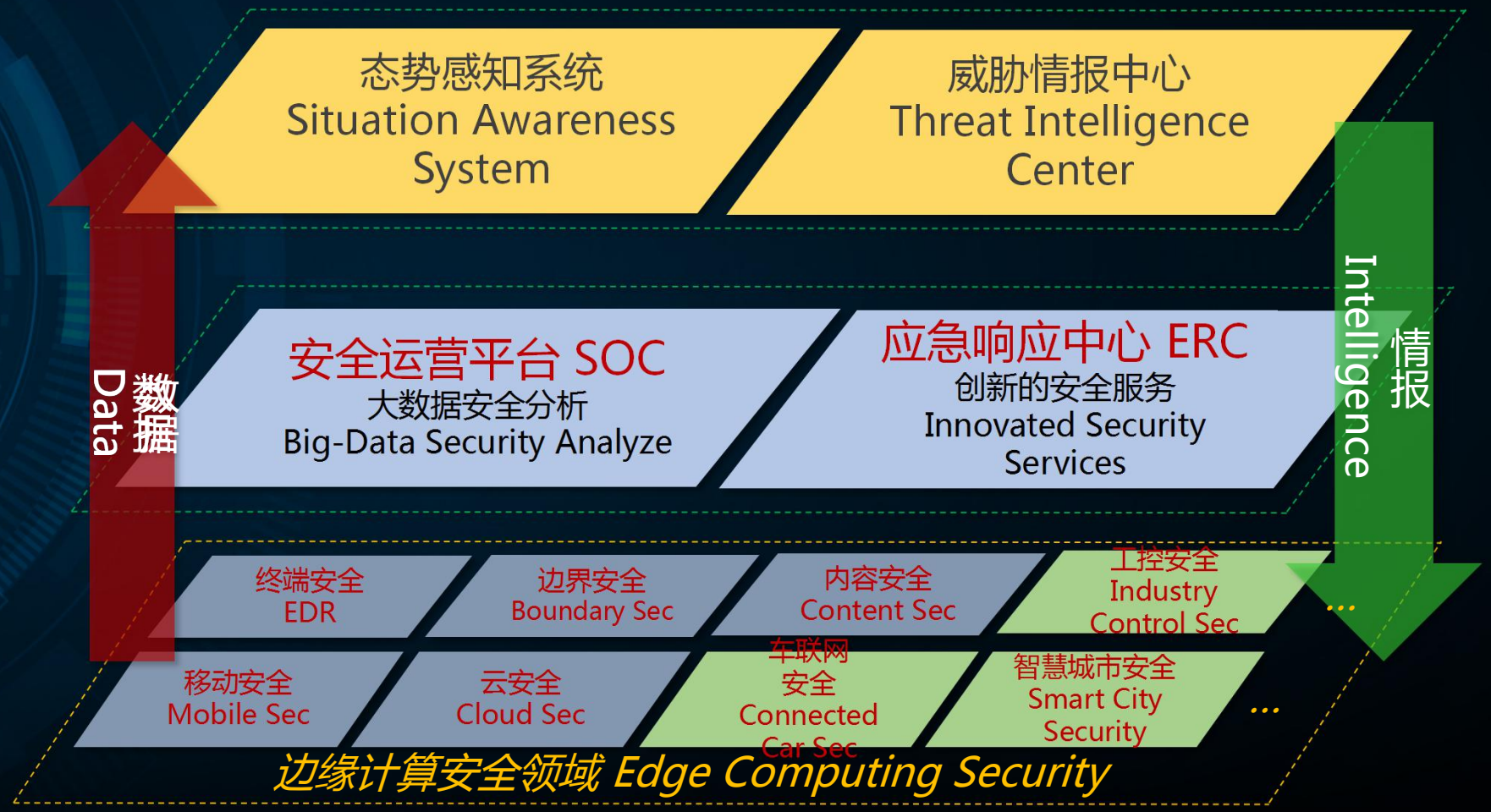


数据驱动安全也适用于边缘计算安全

Data driven security is also applicable to edge computing security

数据驱动的边缘计算协同联动防御体系

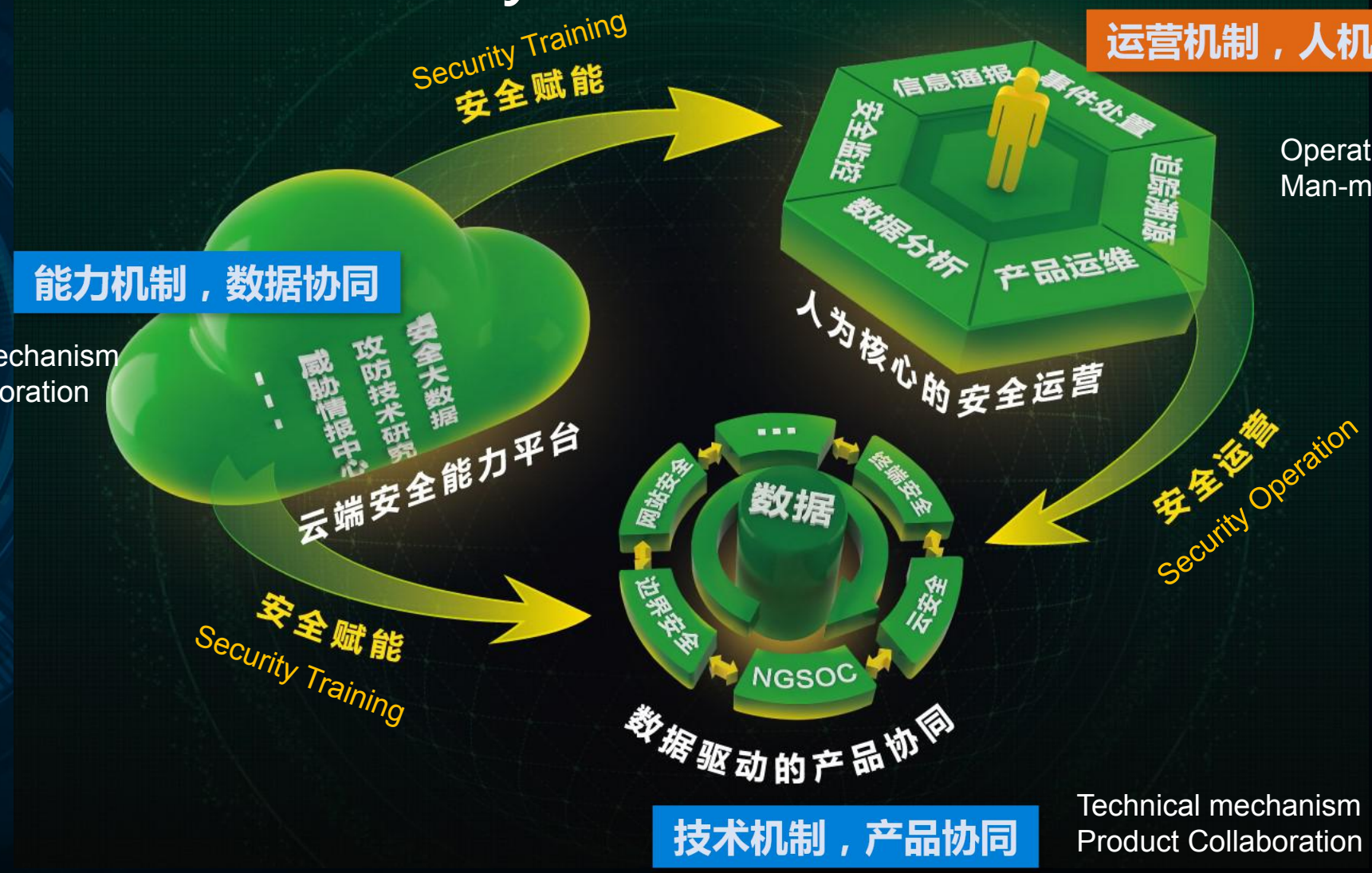
Data driven edge computing collaborative linkage defense system



数据驱动安全2.0
Data Driven Security 2.0

边缘计算 Edge Computing CONSORTIUM

360 企业安全



人是安全问题的根源，也是安全运营的核心

People are the root of Security problems, and are also the core of Security operation

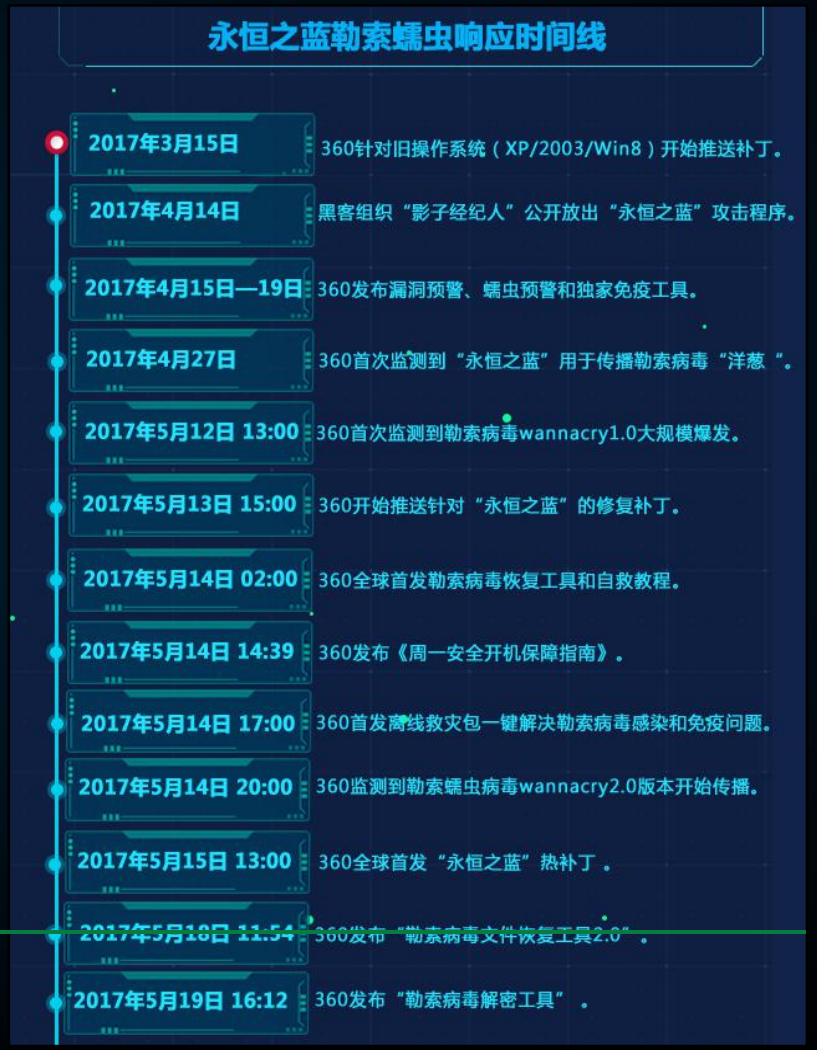
安全本质是人与人的对抗

The essence of security is the confrontation between people

72小时应急响应中人的作用
The role of human in 72 hour emergency response

边缘计算 Edge Computing CONSORTIUM | 360企业安全

- **1500+安全应急响应人员**
  - 安全工程师上门紧急响应
- **1700+客户机构的现场支持**
  - 监管机构、部委、金融机构、大型央企
- **2000+客户机构的电话支持**
- **5000+工具U盘或光盘**
- **9个版本安全预警通告**
- **7个安全修复指南文档**
  - 操作指南、事件百问、开机手册等
- **6个安全软件修补工具**
  - 补丁、扫描、修复、解密多类别工具
- **人均睡眠时间<4小时**



面临的挑战：两个失效定律
The Challenge: two Laws of Failure

- 检测分析手段的缺乏
- Lack of detection and analysis methods
- 响应处置的高效闭环
- Efficient closed loop for response processing

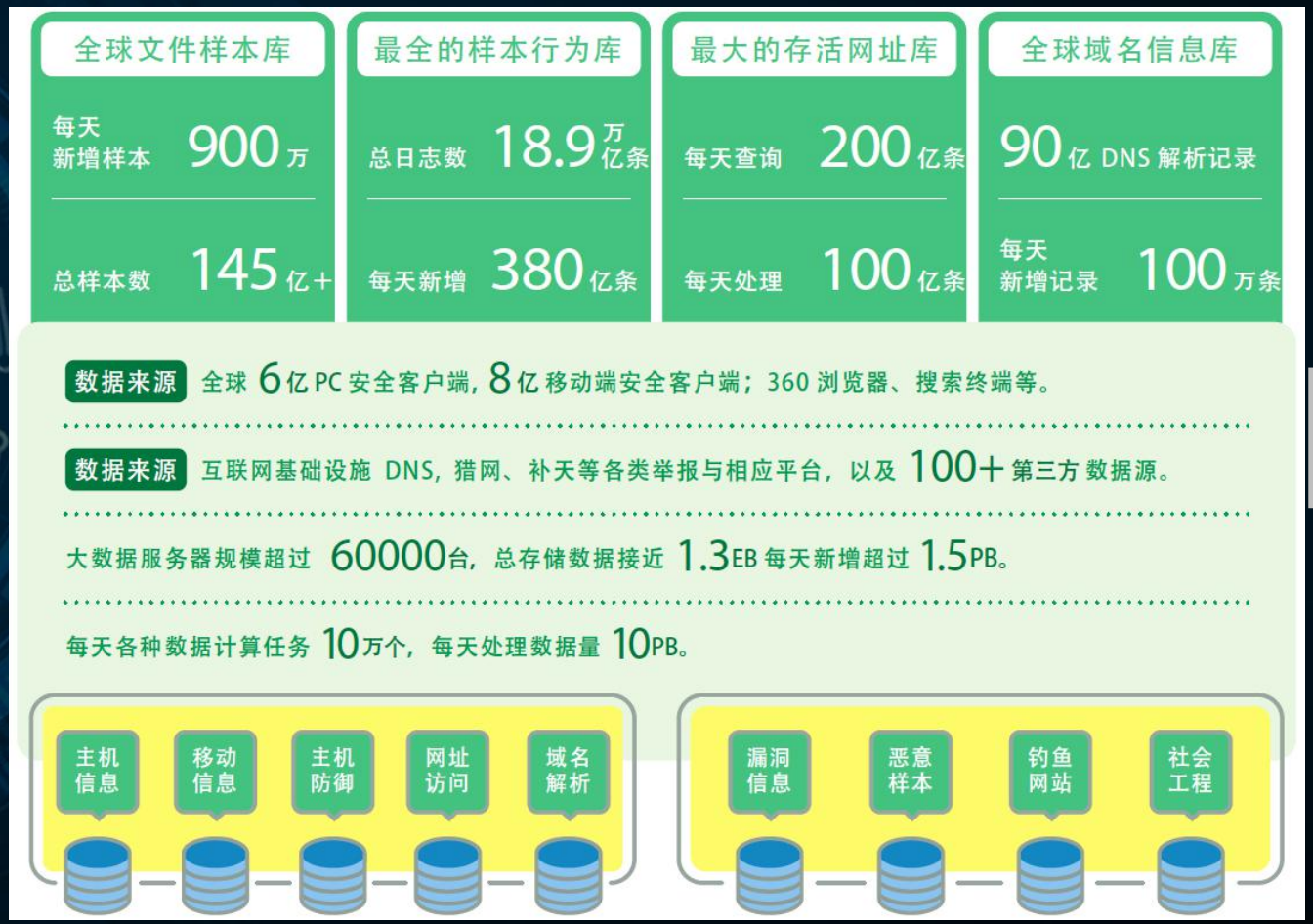
没有技术手段保障的运营机制一定会失效

没有人员参与运营的技术机制一定会失效

- 安全能力的不足
- Deficiency of security capability
- 安全人才的缺乏
- Lack of security personnel

安全大数据是构建安全能力平台的基础

Security Big Data is the Foundation of Building Security Capability Platform



- 威胁情报中心 Threat Intelligence Center
- 应急响应中心 Emergency response center
- 安全运营中心 Safe operation center
- 网站云监测 Website cloud monitoring
- 网站云防御 Website cloud defense
- 云查杀平台 Cloud killing platform

360云端安全能力平台

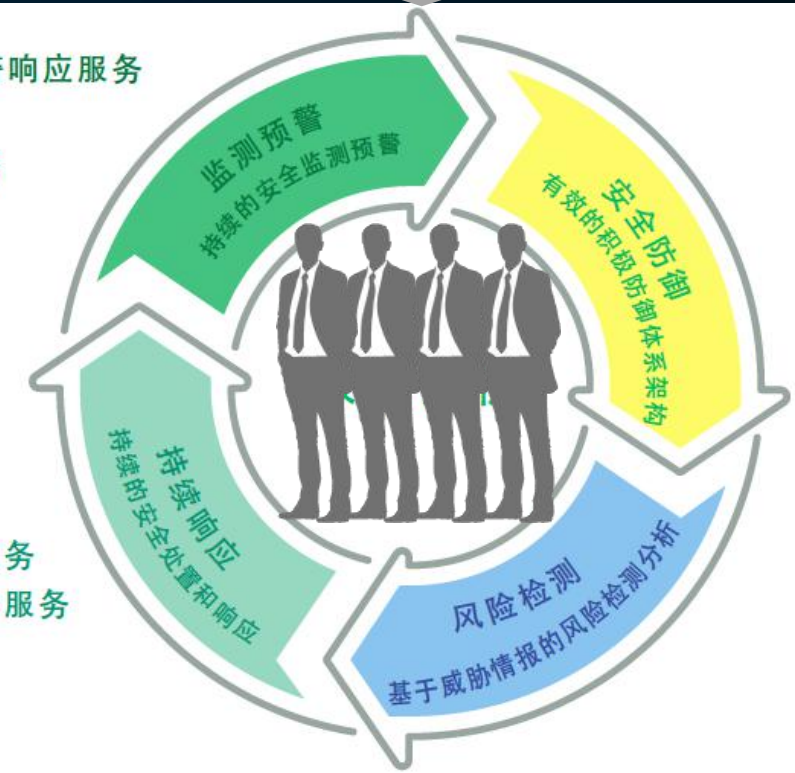
数据驱动的创新安全运营服务
Data Driven Innovative Security Operations Services

边缘计算 Edge Computing CONSORTIUM | 360企业安全

360云端安全能力平台
360 cloud security capability platform

安全赋能

- 基于威胁情报的预警响应服务
- 态势感知服务
- 互联网资产发现服务
- 网站安全监测服务



- 重要时期安全保障服务
- 安全加固服务
- 等级保护合规服务
- 云安全保障服务
- 工控安全服务

- 安全事件应急响应服务
- 可持续安全运营保障服务

- 对抗式演习服务
- 全流量威胁分析服务
- Web 失陷检测服务
- 风险评估服务
- 代码检测服务
- 渗透测试服务

汇聚互联网安全攻防人才的力量

Gather the power of Internet security attack and defense personnel

Solve network security risks and cultivate cyber security talent

网络安全人才培养与实训
Network security personnel training and training

边缘计算 Edge Computing CONSORTIUM | 360企业安全

校企合作 – 360网络空间安全学院
School enterprise cooperation - 360 Network Security Institute

丰富的专业教材	完整的知识架构	专业与实验室建设
先进的安全设备	准确的职业解析	安全师资培训
多维的教学内容	多维的育人体系	多维的合作方式
前沿的安全技术	实用的技能训练	合作科研团队
开放的综合实训	优质的就业推荐	技能认证与竞赛

360安全创新中心
360 Security Innovation Center

大数据协同安全国家工程实验室
National Engineering Laboratory for cooperative safety of big data

★强大的品牌影响
Strong brand influence

★领先的安全能力
Leading security capability

★成熟的安全产品
Mature security products

★完善的认证体系
Perfect certification system

边缘计算 Edge Computing CONSORTIUM

360企业安全

万物智联，  是安全的尺度

Wisdom Alliance, people are safe standards

谢 谢

Thank You