万物互联下的边缘计算安全挑战与应对

Data driven edge computing security

陶耀东
ECC安全组 主席
工业控制系统安全国家联合实验室 主任
360 工业安全业务线 总经理

2017物联网安全现状

The State of IoT Security in 2017

边缘计算 Edge Computing CONSORTIUM | 360企业安全

- 商业、消费者和工业之间连接的“事物”数量迅速增长

  Rapid growth in the number of connected "things“ across commercial, consumer and industrial

  - 2015：安装了49亿个物联网端点 49B IoT endpoints
  - 2020：安装基数增长至204亿 204B 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“net new” paradigm but requires hybrid approaches.

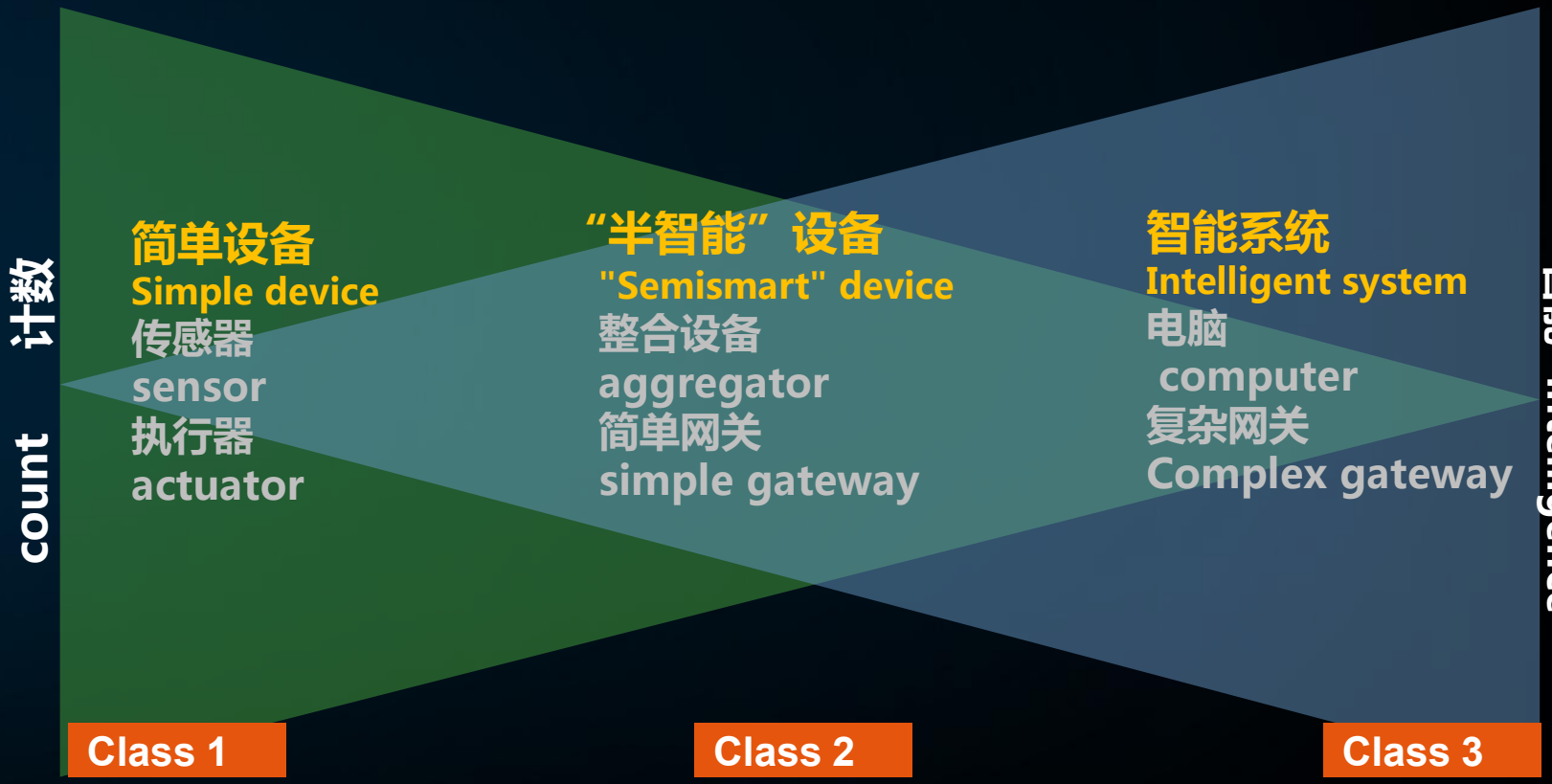
- 工业界和政府活动正在迅速发展和适应

  Industry and government activity is evolving and adapting rapidly

- 现实世界的物联网攻击往往攻击中了主流 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！

边缘物联设备分类
IoT Device Classes



物联网和边缘计算安全现状：安全事件频发

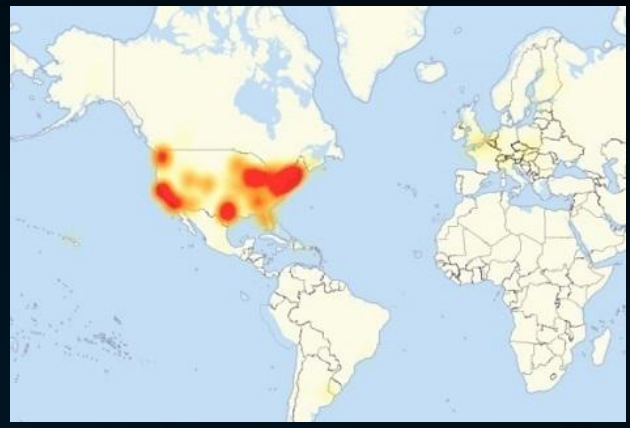
IoT and Edge Computing Security Status : Security incidents occur frequently

2015年6月，我公司安全专家公开展示了利用比亚迪云服务漏洞，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

Announce the demonstration case of cracking Tesla and other models

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。

Large scale blackout in Ukraine power grid



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。

the United States was attacked by the Mirai virus.

2017年10月，360又发现类似的病毒**IoT_reaper，破坏力更大**

The virus IoT_reaper was discovered by 360.

表面上，物联网（IOT）安全与IT安全相似...

IoT security is seemingly similar to IT security ...

边缘计算 Edge Computing CONSORTIUM | 360企业安全

设备管理
Device Management

- 密码 Cryptography
- 设备标识、访问和关系管理 device ID, access, relationship
- 设备配置和系统管理 device config , system

端点和数据安全
Endpoint and data security

- 设备的保护 device protection
- 防篡改 Anti-tampering
- 个人数据隐私权 Personal data privacy

资产管理
Assets Management

- 资产发现和数据库 asset discovery and database
- 实时可见性和控制 real-time visibility and control

应用于：Applied to:

应用程序, 数据, 网络, 端点 apps, data, network , endpoint

跨越：Across

端点、边缘、企业和平台中心
endpoint, edge, enterprise, platform center

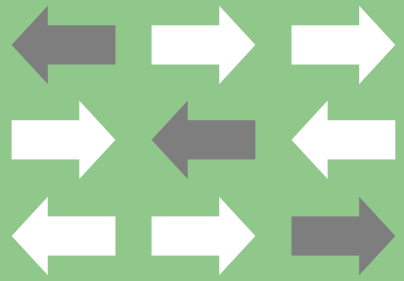
…但是ECC/物联网安全有什么不同呢？

…characteristics of IoT security

边缘计算 Edge Computing CONSORTIUM | 360 企业安全

规模scale

- 数以百万计的设备
  Millions of device
- 多个网络
  Multiple network
- 大数据，更大数据
  Big data
- 较长的供应链
  Long supply chain

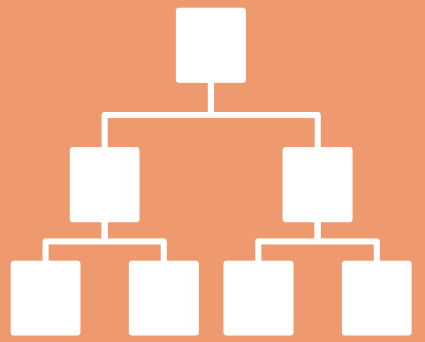


多样性diversity

- 无数的平台
  Myriad platforms
- 年份
  Age
- 协议类型
  Protocol types
- 不同的供应商
  Vatied Vendors

功能function

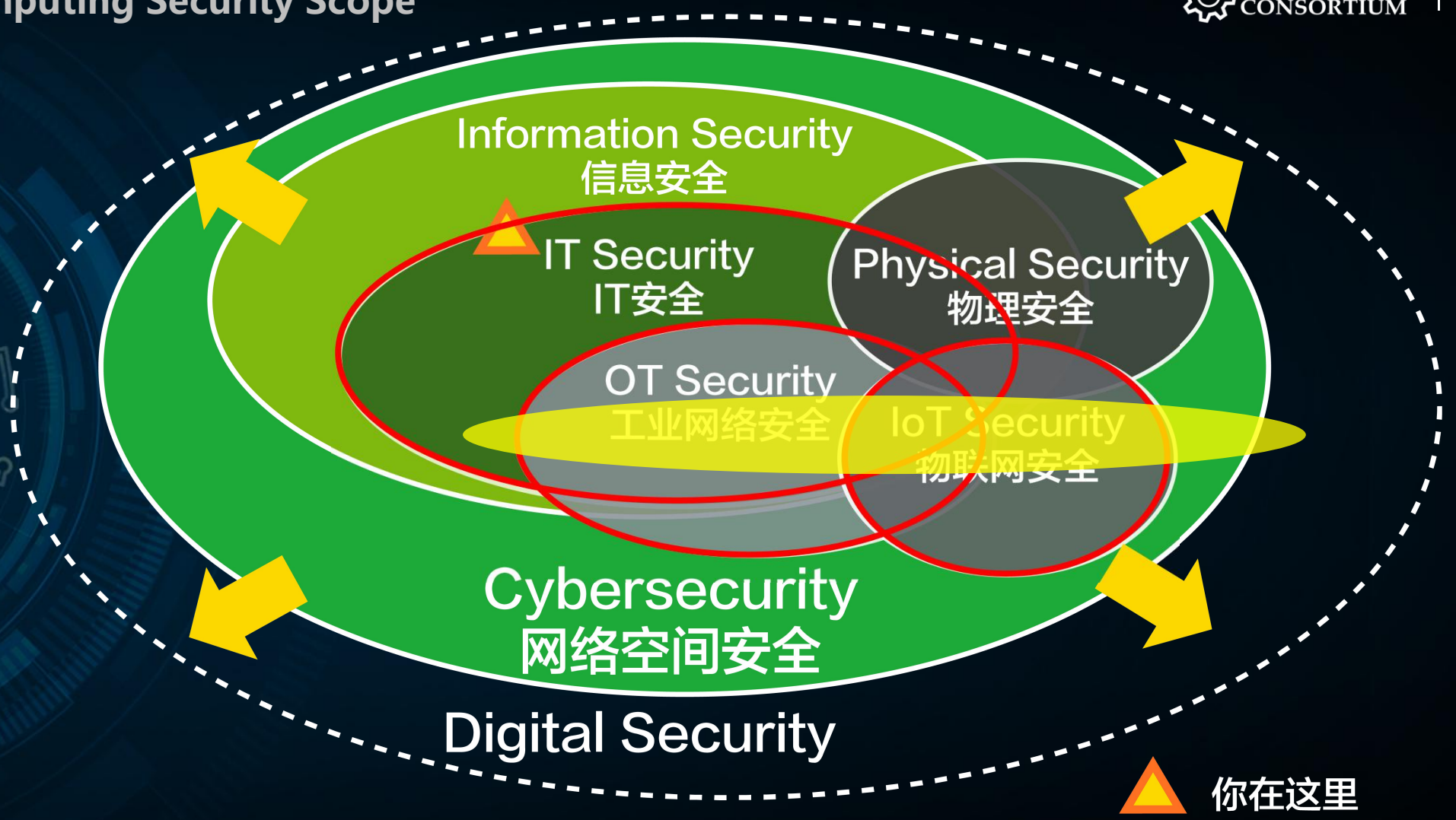
- 适合用途
  Fit-for-Purpose
- 嵌入的
  Embedded
- 物理的
  Physical
- 安全的
  Safety



数据流data flow

- 类型 Type
- 速度 Velocity
- 目的 Destination
- 背景 Context

边缘计算安全的范畴
Edge Computing Security Scope



ECC安全工作范围=IOT安全 + OT安全 + 部分IT安全 + 部分物理安全

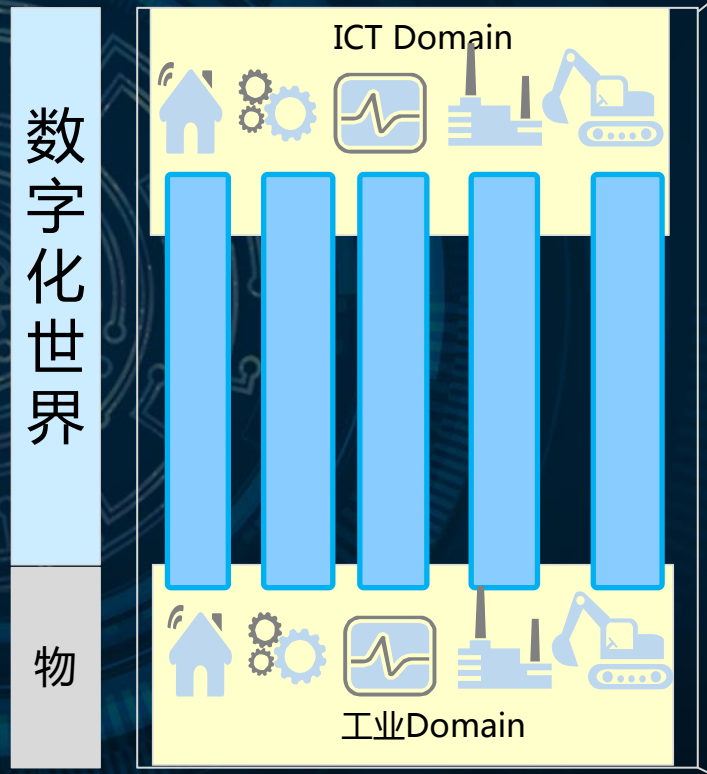
ECC security scope = IoT security + OT security + partial IT security + partial physical security

从行业数字化转型看边缘侧五大挑战

CROSS ： 5 challenges

边缘计算 Edge Computing CONSORTIUM | 360企业安全

垂直行业烟囱式格局

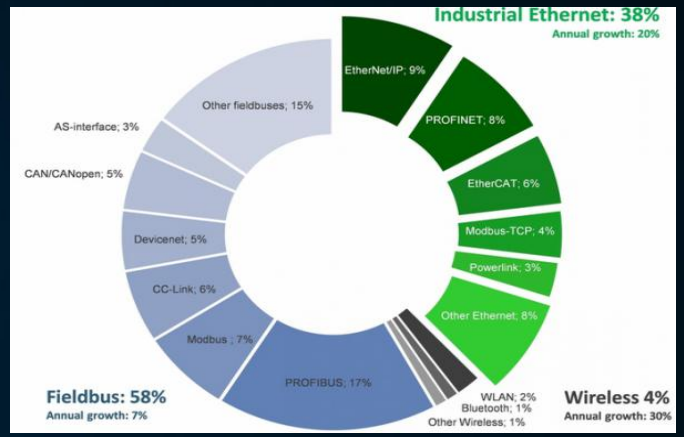


定制化生产，产品即服务等驱动行业数字化转型，建立广泛的开放联接

网络边缘侧面临五大挑战

1 联接海量与异构

海量：500亿联接
异构：40+总线标准，8+以太联接



2 业务实时性，时间确定性

工业检测，控制和执行环节要求信息与指令传输的实时与确定性

生产线：10ms –1ms
包装机械： 5ms-80us
机器人：8ms– 70us

3 数据优化

多种异构信息模型

PackML MtConnect DevNet FDT BACnet PLCopen ControlNet

统一信息模型

OPC-UA

4 应用智能性

业务创新离不开工业现场的实时数据采集与分析

预测维护　智慧节能
良品识别

5 安全与隐私保护

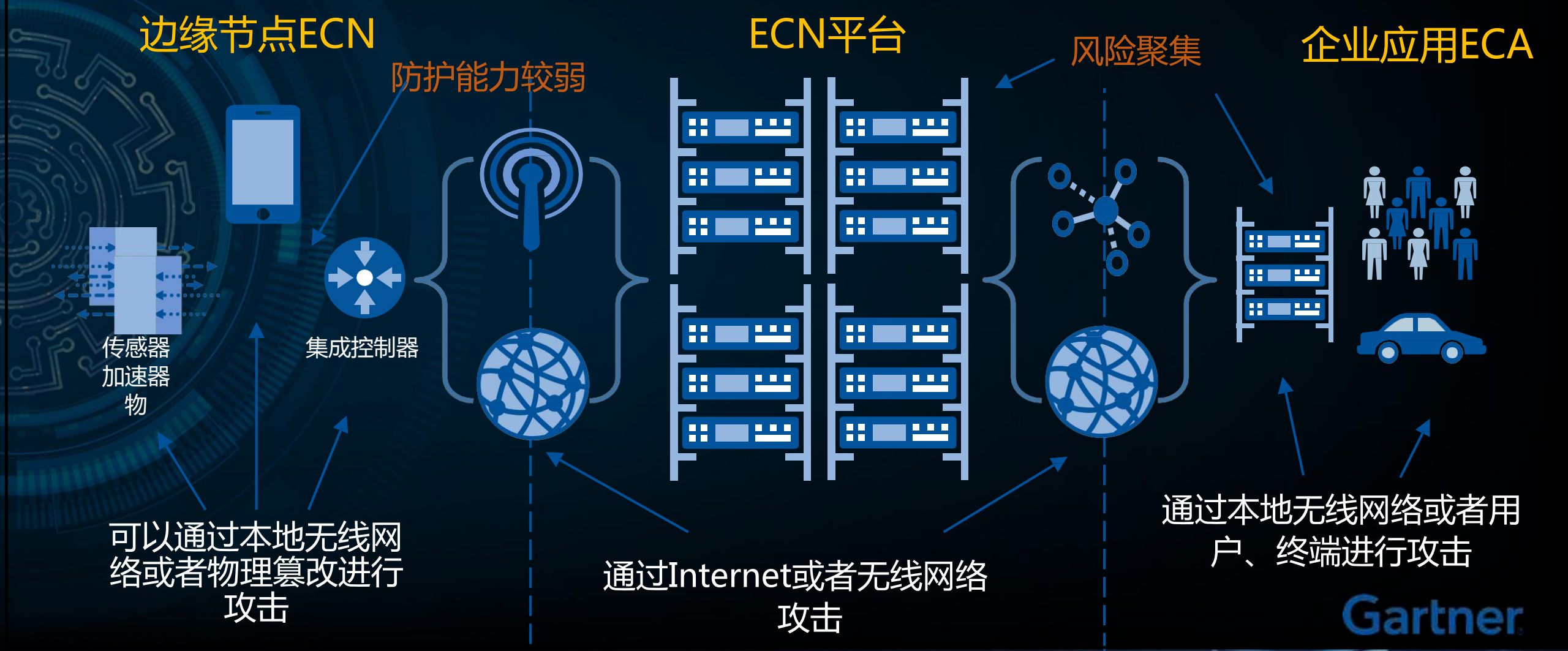
需要端到端防御安全威胁，同时保护数据隐私

设备	网络	数据	应用

CROSS：Connection Real-time Data optimization Smart Security

物联网/边缘计算安全现状：攻击路径分析

IoT and Edge Computing Security Status : Attack path analysis



保护普遍的数字场景

Securing the Pervasive Digital Presence

风险 Risk

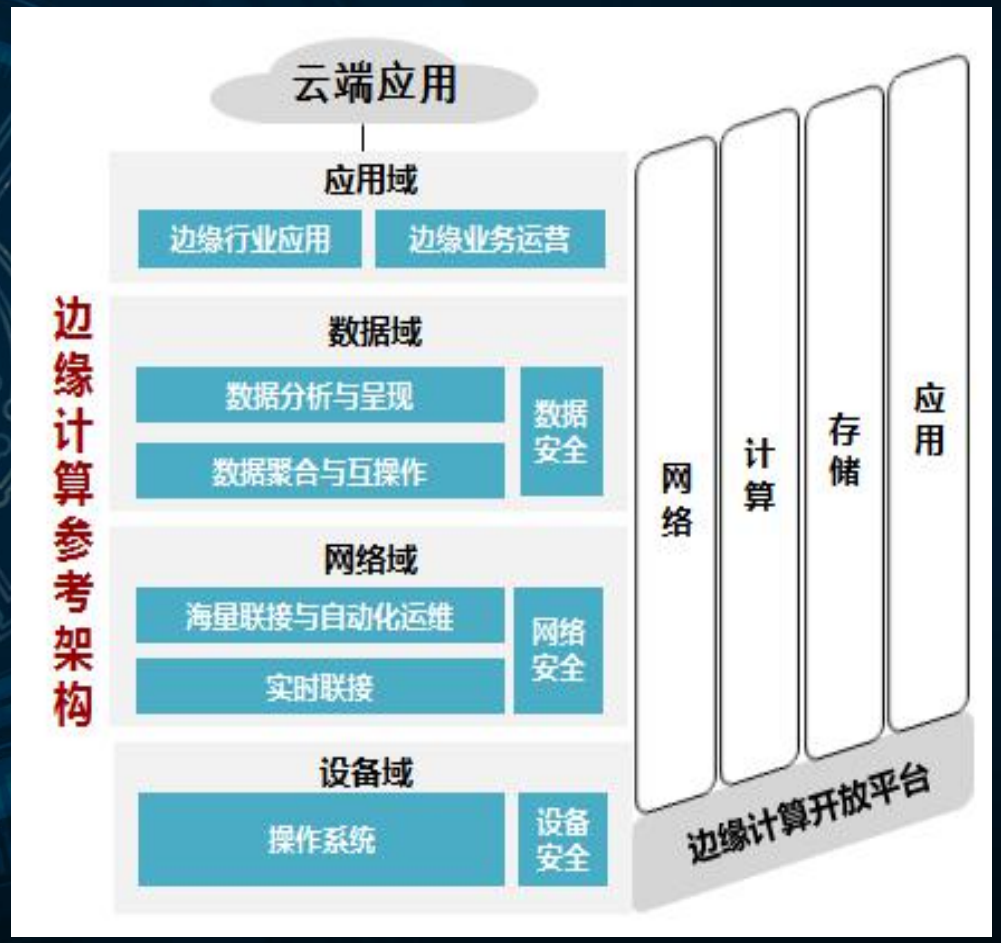
- 业务中断 Business Disruption
- 间谍和欺诈 Espionage and Fraud
- 财务上的浪费 Financial Waste

- 网络黑客 Platform Hacking
- 数据窥探与篡改 Data Snooping and Tampering
- 破坏自动化设备 Sabotaging Automationand Devices

- 设备模拟 Device Impersonation
- 设备窃听 Device Hacking
- 设备的伪造 Device Counterfeiting
- 窥探、篡改、破坏、损害 Snooping, Tampering, Disruption, Damage

边缘计算安全防护思路：分层安全需求

Security ideas for edge computing: layered security requirements



应用域安全

Application domain security

- 轻量化应用
- 专用化应用
- 生命周期管理

数据域安全

Data domain security

- 容错
- 实时
- 流式数据

边缘计算安全需求

Edge computing security requirements

网络域安全

Network domain security

- 实时性与可靠性
- 多种标准兼容
- 缺乏原生加密
- 边缘易受DDoS

设备域安全

Device domain security

- 多样化
- 海量
- 资源受限

边缘计算安全：分层安全应对

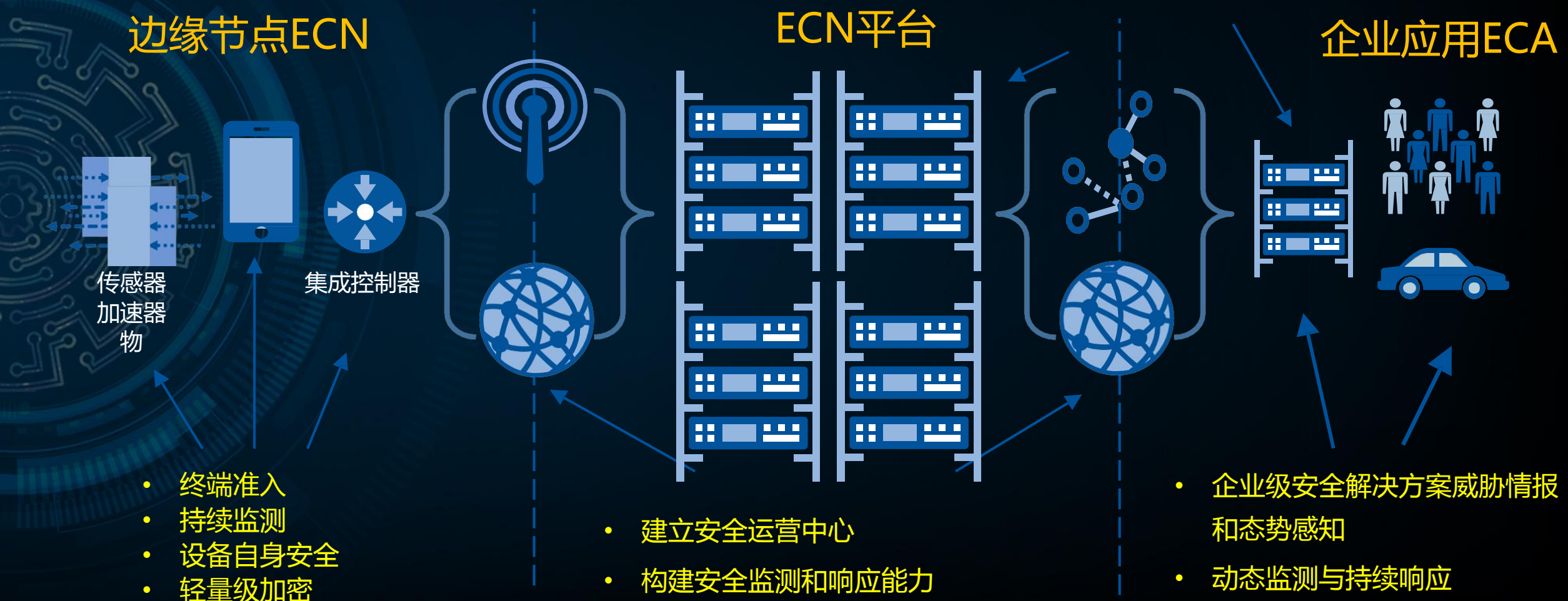
ECC Security：Layered security protection

逻辑分层（layer）	需求和特点	主要应对方法（Layered security protection）
安全配置与管理	海量、异构、跨行业	
用户认证	海量、低功耗、低性能	分布IAM式身份认证
应用域 App	1、轻量级应用 2、专有化应用 3、生命周期管理	1、应用的安全审计　2、软件加固 3、补丁　4、安全配置管理 5、沙箱　6、白名单库 7、恶意代码防范　8、WAF 9、检测和响应
数据域 Data	1、容错 2、实时 3、流式数据	1、加密（使用中、存储中、传输中）　2、隐私保护（脱敏） 3、数据访问控制　4、数据防泄漏
网络域 Net	1、实时性要求高 2、可靠性、可信 3、兼容多种标准，多样性 4、并非所有平台软件都有原生加密协议 5、网络边缘易于收到DDoS攻击	1、抗DDoS，在设计中考虑带宽的变化 2、FW/IPS/IDS 3、TLS/VPN，轻量级加密和连接 4、使用已有的协议并重用其安全性（例如REST）
设备域 Device	1、多样化 2、海量 3、资源受限	1、端点安全（包括虚拟化端点）　2、ECN安全 3、软件加固和安全配置　4、基于硬件的Safety（硬件开关） 5、安全的远程软件升级和更新　6、增加安全功能和监测功能 7、ECN需要包含检测和响应能力

物联网和边缘计算安全现状：防护措施

IoT and Edge Computing Security Status : Protective measures

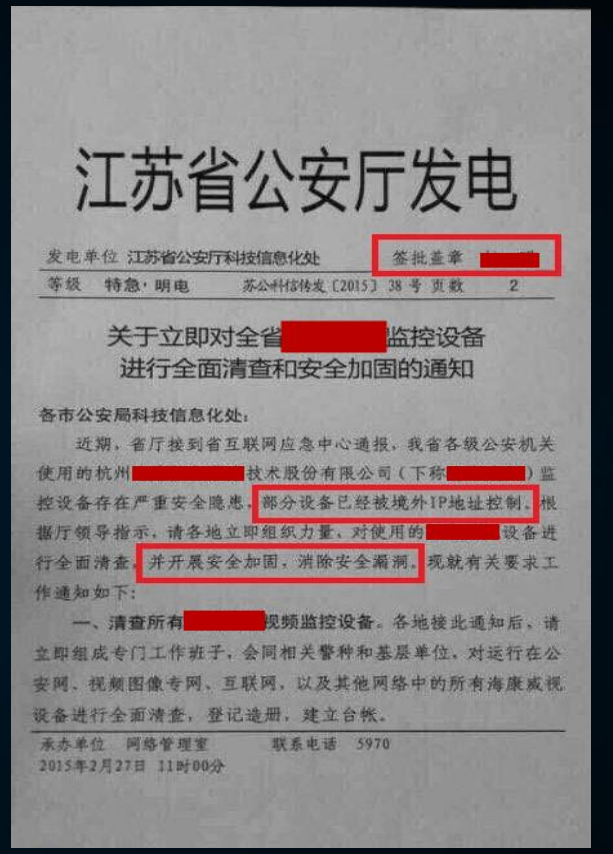
边缘计算 Edge Computing CONSORTIUM | 360企业安全



案例：边缘计算-视频监控安全问题

Case : EC-video monitoring security issues

监控录像机被黑，监控画面网络流传



公安厅发电，监控设备全面清查加固

黑客可通过控制边缘设备，进而控制核心服务器，如：控制边缘-视频监控设备

Hackers can control the servers by controlling the edge devices

视频监控网络常见问题

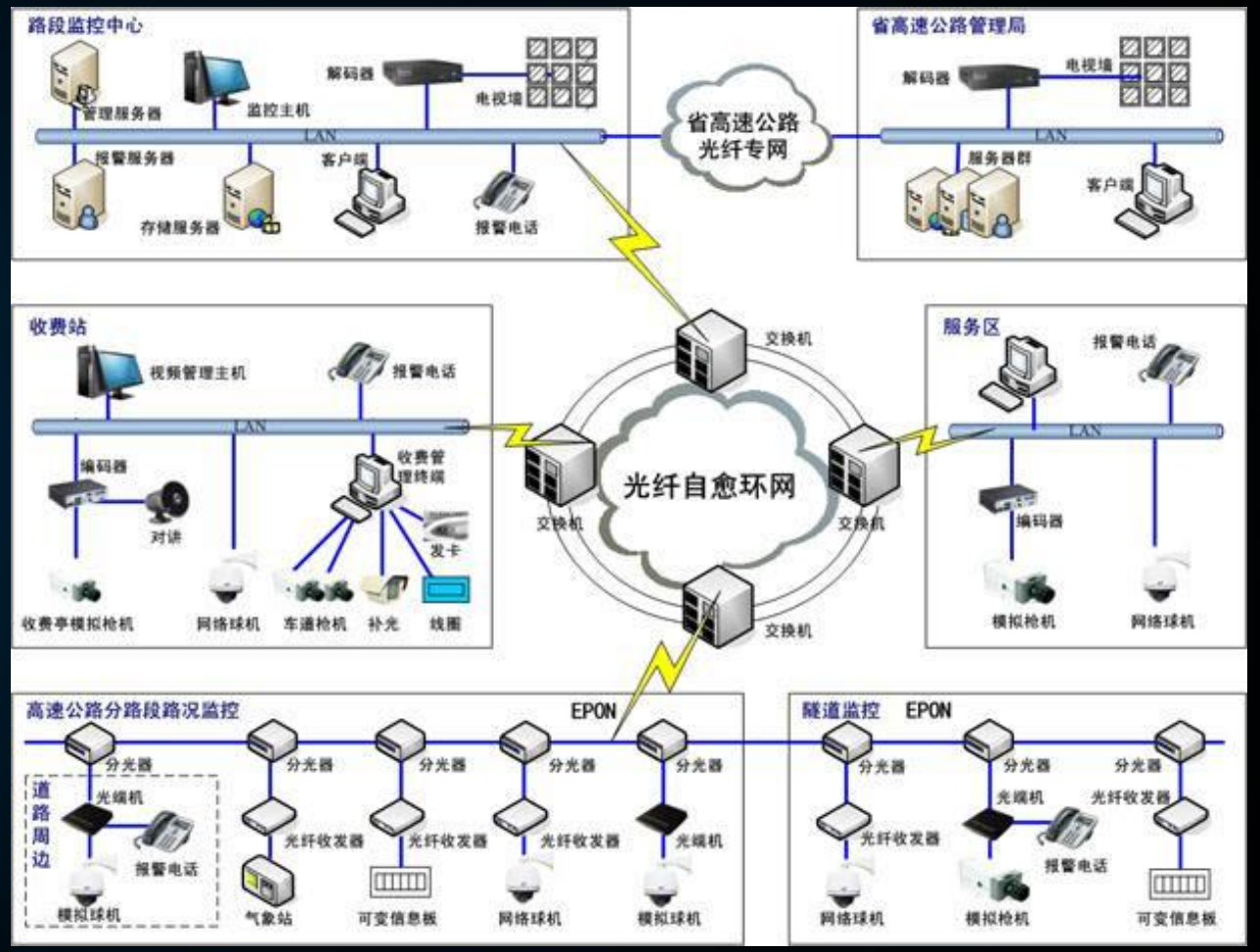
Security issues of video monitoring network

面临的问题（RISK）

1. 终端设备非法接入(PC、扫描仪等带有入侵功能的终端) Device Hacking
2. 伪造终端设备接入(伪造MAC/IP逃避安全策略) Device Counterfeiting
3. 终端设备识别(终端类型、位置、入网感知) Device Impersonation

解决方案（Solution）

1. 网络准入策略(MAC地址认证，IP白名单)
2. 合法终端识别(建立私有终端特征库Q4)
3. 终端类型识别(公共协议库、终端指纹)



典型高速公路视频网络

Video monitoring network for highway

安全实践：基于流量分析的安全解决方案

Security practice: a security solution based on traffic data analysis

边缘计算 Edge Computing CONSORTIUM | 360企业安全

- 入网感知-看得见

  Perception of access to the Internet

- 流量基线感知-看得清

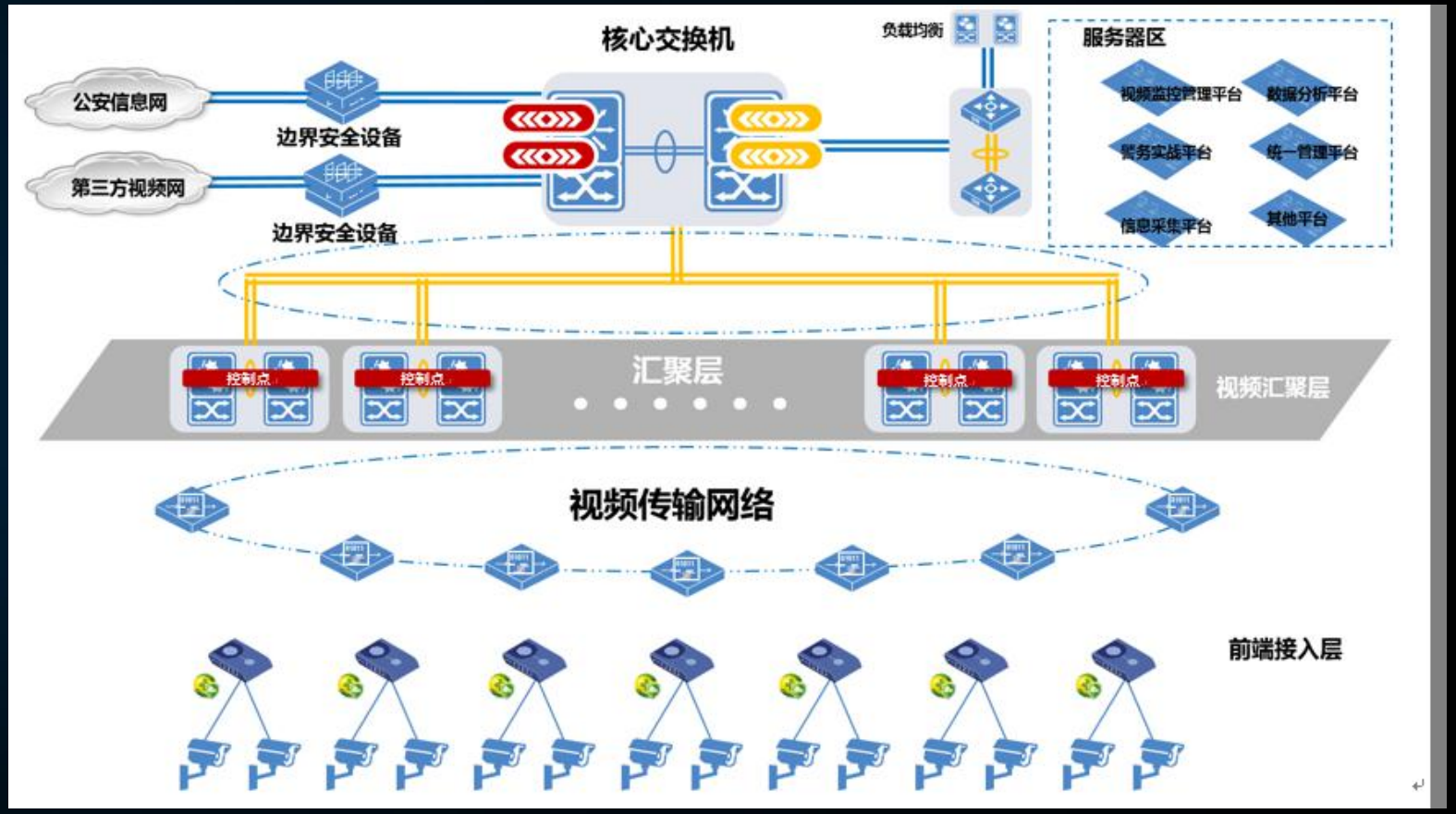
  Traffic baseline perception

- 行为基线感知-看得明

  Behavioral baseline perception

- 终端探针-看的远

  Terminal probe



360在物联网安全防护方面的工作

360 security work in the Internet of things

边缘计算 Edge Computing CONSORTIUM

360 企业安全

一个联盟 consortium

边缘计算产业联盟（ECC）

五个方向 Application

- 消费物联网安全 IOT
- 产业物联网安全 IIOT
- 车联网安全 Vehicle networking
- 工业控制系统安全 ICS
- 无线电和硬件安全 Wireless

两个参考 Framework

- 360物联网安全参考框架
- 360智能硬件安全参考技术规范

五个产品 Products

- 物联网终端安全
- 物联网安全网关
- 物联网云平台安全
- 物联网业务安全
- 移动端安全

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

边缘计算 Edge Computing CONSORTIUM | 360 企业安全

数据驱动边缘计算安全Data driven EC Security

谢 谢

thank you