工业互联网产业联盟
Alliance of Industrial Internet

360 安全第一

解决工业互联网安全的“四个新”

360企业安全集团 左英男

创新引领 融通发展

2019 工业互联网峰会
INDUSTRIAL INTERNET SUMMIT 2019

目录
Contents

01 工业互联网规模将比肩消费互联网

02 工业互联网成为首要网络攻击目标

03 四个“新”解决工业互联网安全问题

一、工业互联网规模将比肩消费互联网

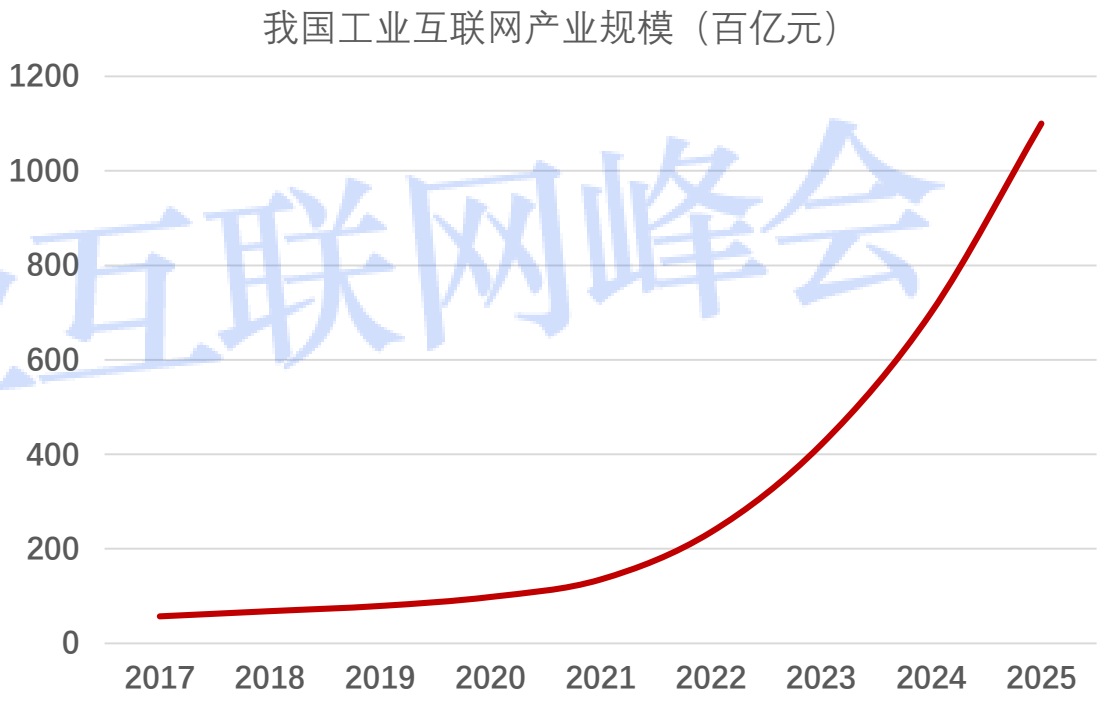
我们正步入工业互联网时代

	消费互联网	→	工业互联网
终端数量	百亿级		万亿级
终端种类	少（PC、手机、服务器、专用设备）		多（难以穷举）
IP地址数量	IPV4（2的32次方，约43亿）		IPV6（2的128次方，约340兆兆兆）
用途	消费、娱乐、社交为主		生产、政务、民生为主
网络复杂度	低		极高
网络依赖度（群众生活）	低		极高
网络依赖度（经济社会）	低		极高
网络依赖度（国家安全）	低		极高

一、工业互联网规模将比肩消费互联网

2025年我国工业互联网将达**10万亿规模**，进入大发展时代

- 2017年我国工业互联网产业规模约为**5700亿元**
- 预计**2020年**工业互联网产业规模将达到**万亿元**
- 预计**2025年**工业互联网产业规模将达到**10万亿**



二、工业互联网成为首要网络攻击目标

“永恒之蓝”勒索蠕虫事件

国内外工业企业成为勒索攻击的重灾区

- **法国雷诺汽车**受勒索病毒入侵，多个工厂被迫停工
- **日产汽车桑德兰工厂**IT系统受到感染，被迫停产
- **西班牙电信公司**大量电脑受到感染，造成业务瘫痪
- **德国汉堡火车站**系统被攻击，陷入瘫痪

……

台积电遭勒索病毒攻击

- **2018年8月**，全球最大的半导体制造商台积电遭到了勒索病毒攻击，**几小时内台湾工厂生产线全数停产**。
- 此次病毒疑似去年全球爆发的“永恒之蓝”勒索病毒变种，在安装新机台时带入，**造成台积电三季度损失1.7亿美元**。

二、工业互联网成为首要网络攻击目标

石油天然气工厂的SIS安全系统被攻击

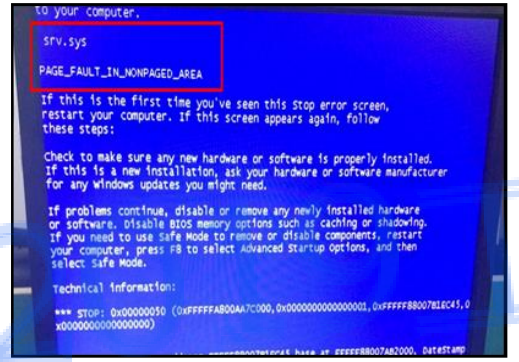
- 2017年12月，黑客利用恶意软件攻击了中东地区一家**石油天然气工厂**的SIS安全仪表系统，可导致不可逆转的关机操作、设备物理损害和工厂运营的中断。
- Triton/TriSYS攻击框架能与施耐德公司的Triconex安全仪表系统控制器（SIS）形成通信交互，并可对SIS控制器重新编程，对工业控制系统有着“改变游戏规则”的影响。

二、工业互联网成为首要网络攻击目标

近几年360企业安全集团处理过的网络攻击事件，涉及汽车生产、智能制造、电子加工、烟草、电力、能源等行业**几十余家企业**，大多数都导致了**工业主机蓝屏，文件加密，生产停工**

某汽车模具厂，停产

2017.05



某冷轧钢板厂，停产

2018.07

某炼钢厂，停产

2018.10

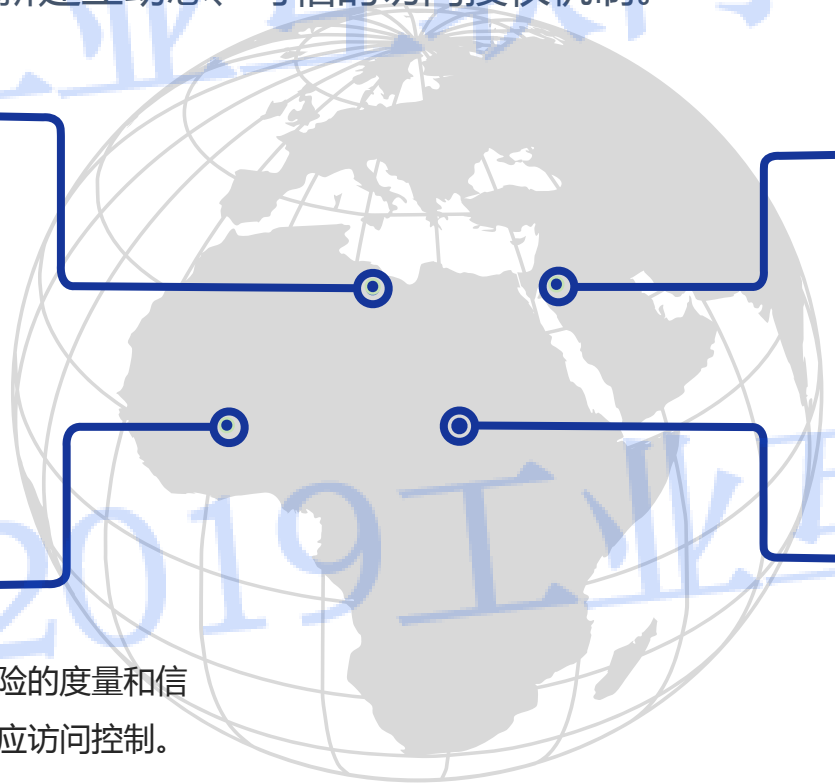
某关键IC厂，停产

2019.01

三、四个“新”解决工业互联网安全问题

① 运用新战术：以“零信任”架构规划工业互联网安全体系和部署网络安全防护设施

- IT/OT技术和应用环境的高度融合，使得传统的安全边界日益模糊。默认情况下不应信任内网、外网中的任何设备、用户和应用，基于零信任架构，重新建立动态、可信的访问授权机制。



1.全面身份化

建设统一身份源，实现全网用户、设备、应用、API接口的统一身份化，实现统一权限梳理。

3.风险度量化

采用大数据分析技术，基于人和设备的环境数据、访问行为数据，进行风险建模，度量潜在的安全风险。

2.授权动态化

访问控制进行细粒度授权，基于风险的度量和信任评估，动态调整授权，实现自适应访问控制。

4.管理自动化

采用机器学习算法，基于高级身份分析技术和工作流引擎，实现身份与访问管理的自动化。

三、四个“新”解决工业互联网安全问题

360 安全第一®

② **提升新战力：数据驱动安全，构建多级工业互联网安全监测平台，建立工业安全态势感知能力。**

- 无损采集数据
- 工业资产发现
- 工业漏洞管理
- 工业威胁检测
- 操作异常监测
- 可视分析大屏
- 协同联动处置

厂级安全监测系统

监测数据

威胁情报

集团级安全监测平台

监测数据

威胁情报

行业/地区级安全监测平台

监测数据

威胁情报

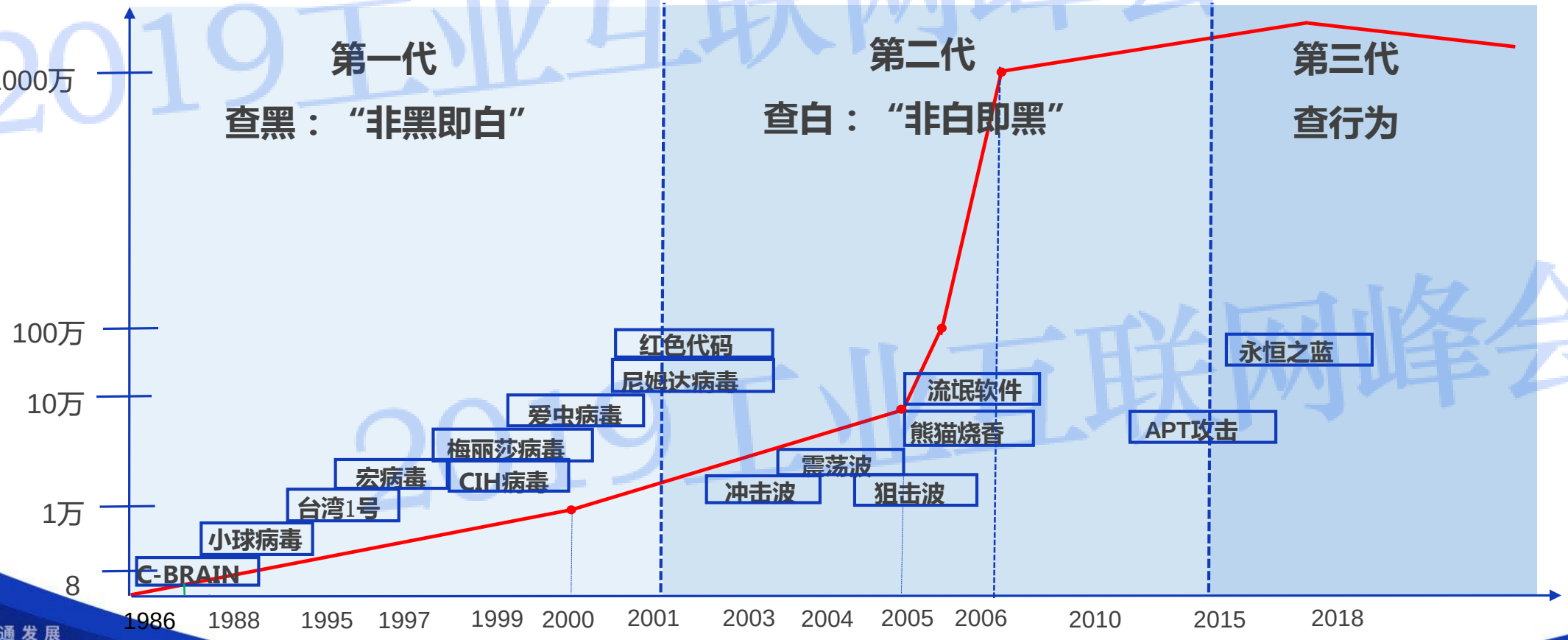
国家级安全监测平台

恐惧源于未知，看见才能安全

三、四个“新”解决工业互联网安全问题

360 安全第一®

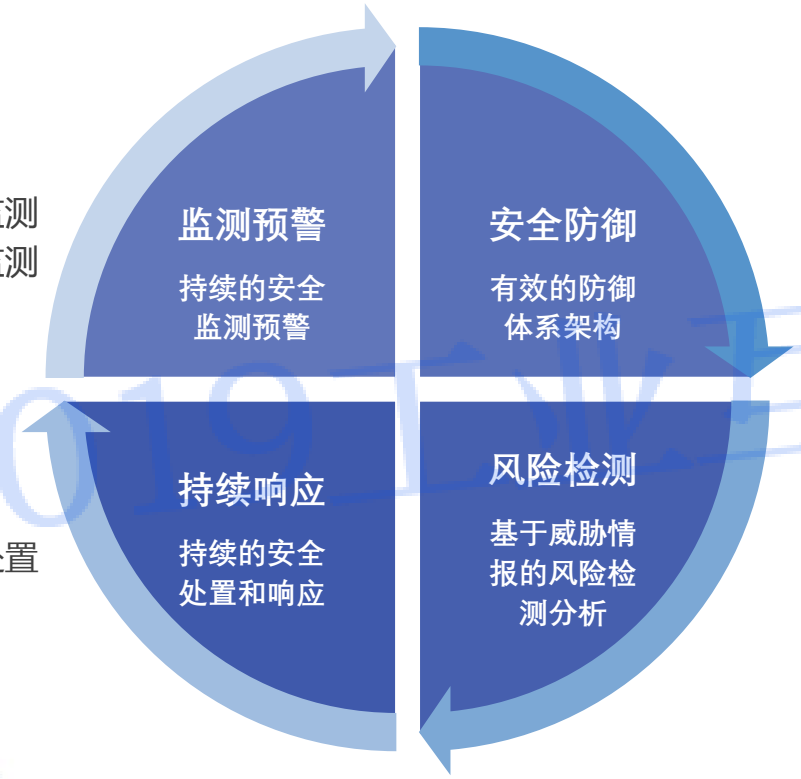
③ **采用新战具：工业主机是信息世界通往物理世界的“大门”，工业互联网安全从工业主机防护开始，发展第三代“查行为”的新技术**



三、四个“新”解决工业互联网安全问题

④ 锤炼**新战法**：形成“人+机器”协同作战的新方法，建立工业互联网安全应急响应和持续运营能力

- 安全的本质是人与人的对抗。新形式下的网络安全，不仅仅是安全能力建设，更是**动态安全运营的过程**；
- 建立一支“人+机器”协同作战的安全团队，是动态化安全体系的关键。



- 态势感知
- 资产告警
- 工业应用站点监测
- 工业威胁情报监测

- 终端安全
- 边界安全
- 安全域
- 服务器安全
- 工业互联网平台安全
- 工控安全
- 重要时期安全保障

- 安全事件响应处置
- 追踪溯源
- 运营保障

- 风险评估
- 代码检测
- 渗透测试
- 工业应用失陷检测
- 全工业流量威胁分析
- 对抗式演习

实践1：BYD集团17,000台工业主机安全防护案例

360 安全第一

该项目入选工信部工业互联网安全优秀应用案例

背景需求

- BYD生产制造产线遭受**“永恒之蓝”勒索病毒**侵袭
- **场景复杂**：电池、手机、笔记本、汽车电子、配件、整车组装等各类车间，涉及电子制造、汽车制造场景，工业软件众多。
- **适配复杂**：工业主机多样，硬件配置多样，操作系统有WinXP、Win7、Win8、Win10等，各种汽车的测试板卡、数据采集卡适配

方案效果

- **应用规模巨大，国内领先**

37个工业园区，**17000台**工业主机

- **实施复杂度高**

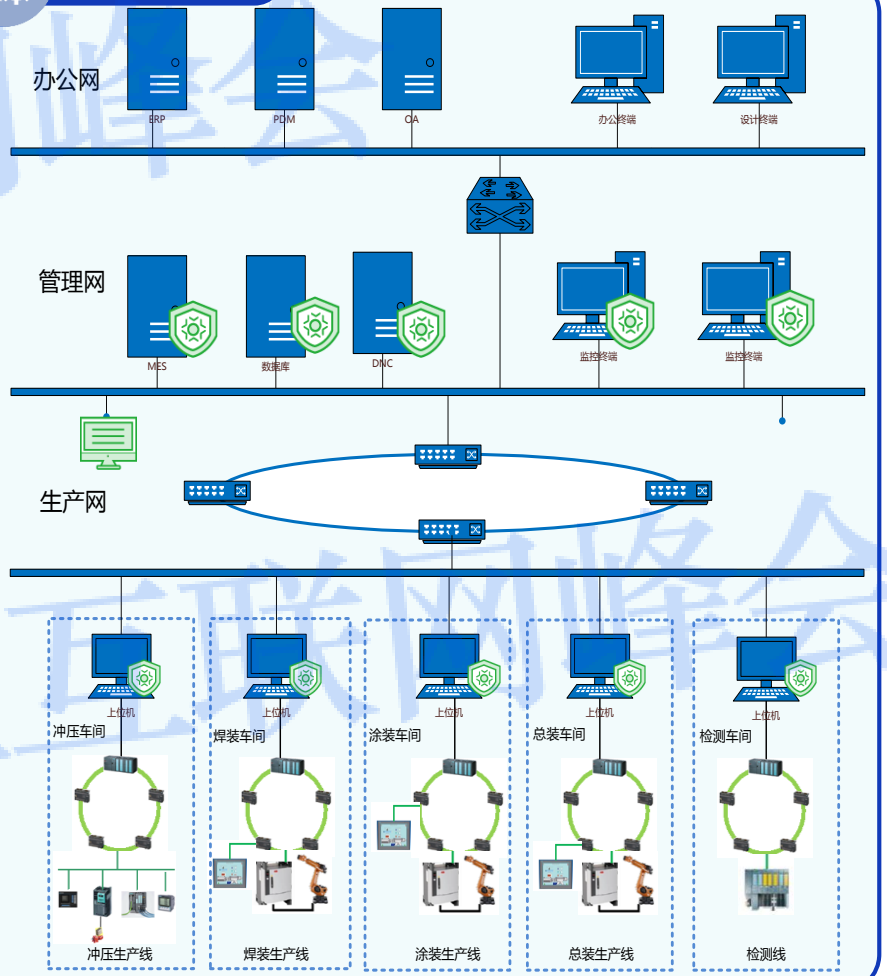
场景复杂：**10+种**工业制造场景

操作系统：**15种**

应用复杂：**100+**工业软件适配

实施复杂：**非停产实施**

部署方案



实践2：海尔集团智能工厂工业安全监测系统案例

360 安全第一

背景需求

- 海尔集团是智能制造行业的龙头企业，为加强**COMSO生态体系**安全防护，发现潜在的生产安全隐患，及时处置，保障生产连续性。
- **厂区监测**：涉及到**5座**城市的**8家**智能工厂，覆盖空调、洗衣机、电冰箱三大产线。
- **全网感知**：掌握各厂区的工业资产家底和生产安全整体状况。

方案效果

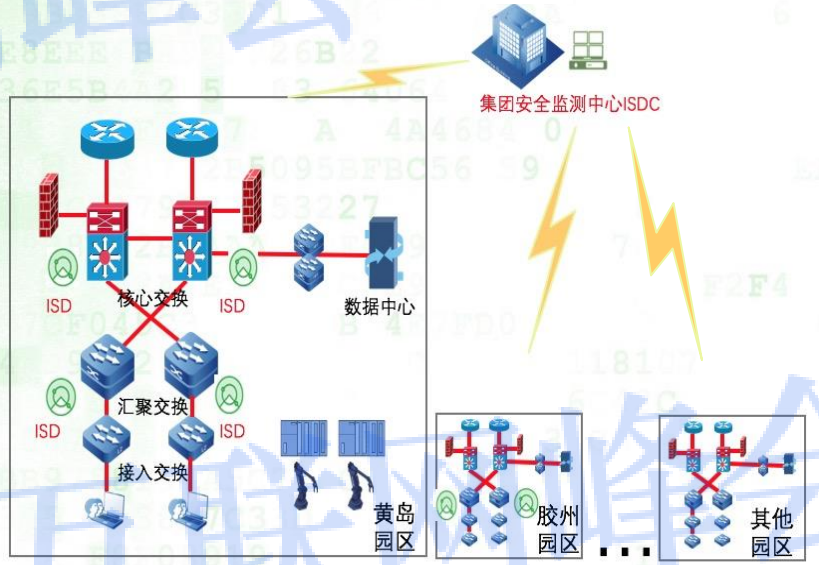
在8个厂区部署工业安全监测系统ISD

- 获取完整资产清单
- 发现生产安全漏洞
- 监测工控系统异常

集团总部工业安全监测系统控制台

- 汇总分析各厂区数据
- 大屏集中展示全网安全态势

部署方案



- **集团和厂区采用级联部署的方式**
- **分布式采集，集中存储，分析，展现**

该案例是海尔COSMOPlat生态体系安全防护的重要部分

工业互联网产业联盟
Alliance of Industrial Internet

360 安全第一

Thanks

2019工业互联网峰会

创新引领 融通发展

2019工业互联网峰会
INDUSTRIAL INTERNET SUMMIT 2019