

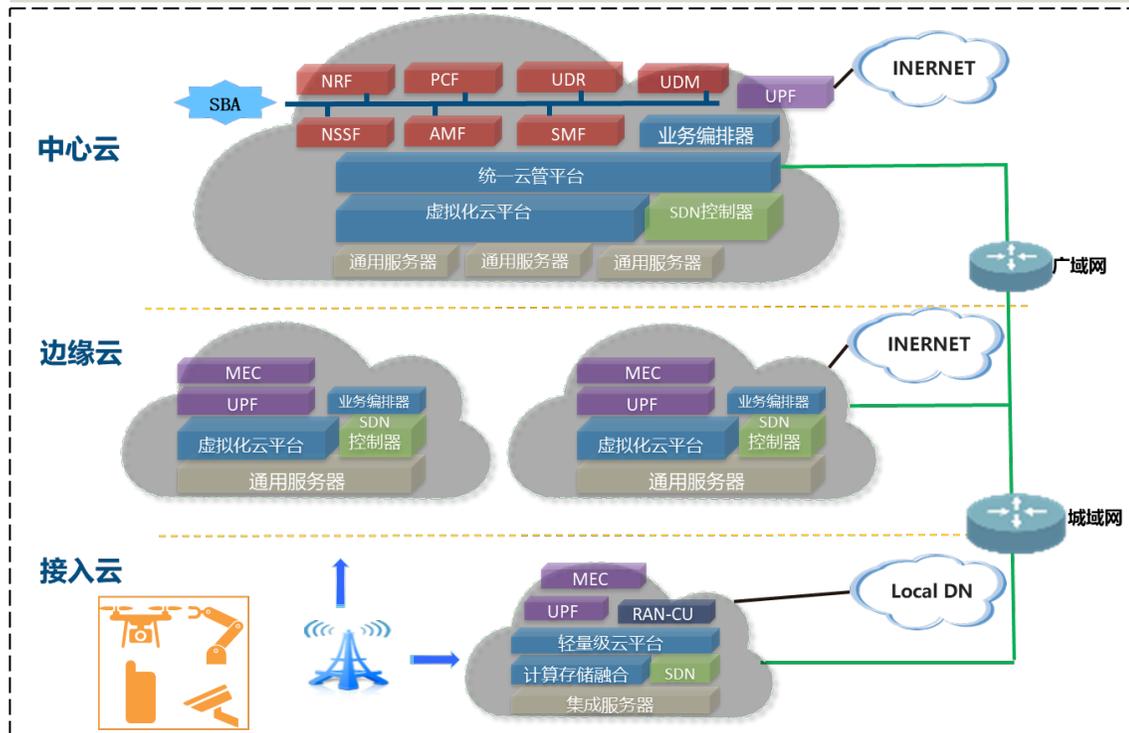
云网协同助力5G安全

---5G融入“千行百业”安全思考与实践

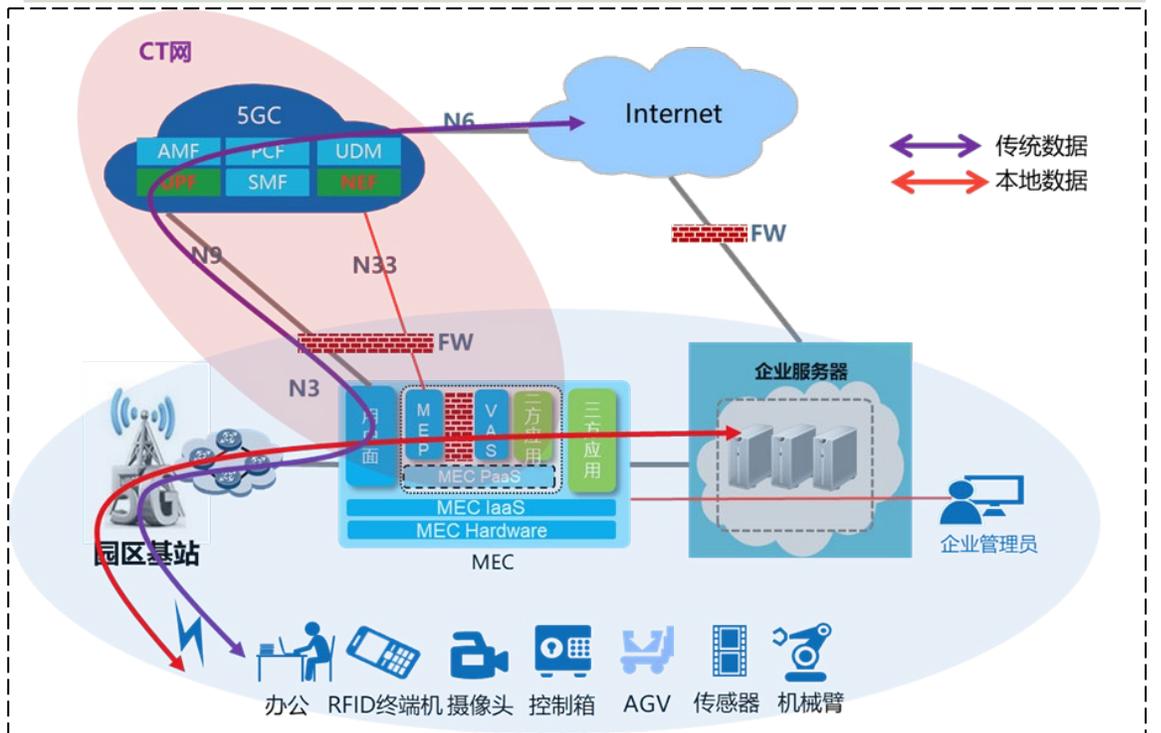
恒安嘉新（北京）科技股份有限公司

从安全的角度看5G的变化

从封闭的通信网（CT）变成了开放的IT网；从专用硬件设备变成了通用服务器和云。



通信网（CT）深入到各垂直行业，原来封闭或半封闭的网络变得更加开放。



◆ 5G网络安全总的需求是，假设系统处于一个开放、非信任的环境中，如何搭建出一个可信赖的通信网络，并提供安全服务与保障的能力。

从网络演进的角度看安全

“5G+云+AI” 将作为智能世界的基石，面向行业提供云网一体化的新型服务体系，以网带云，以云促网，将网络的价值不断提升，赋能到各行各业。

云网一体化

概念：基于业务需求和技术创新并行驱动带来的网络架构深刻变革，使得云和网高度协同，互为支撑，互为借鉴的一种概念模式。

以网络为核心：SDN/NFV等技术将网络云化，打通云到端的连接管道，实现以云服务方式提供网络产品，按需提供可定制、高可用网络服务。

以云为核心：云计算业务的开展带动网络资源升级，匹配企业对云和网络高效互联的市场需求，满足新的云场景下的用户需求，创造更大的商业价值。



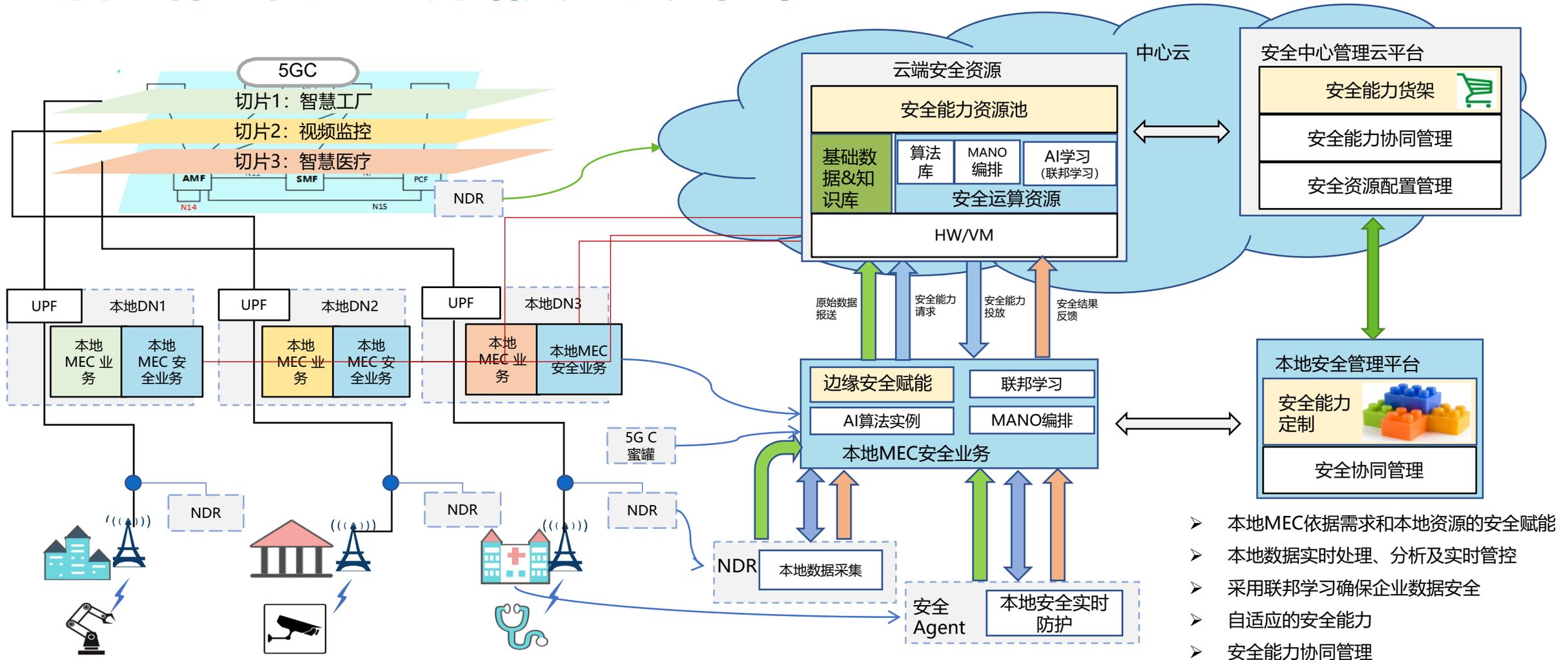
SDN/NFV驱动5G时代网络重构



5G三大应用场景驱动云计算新业务升级

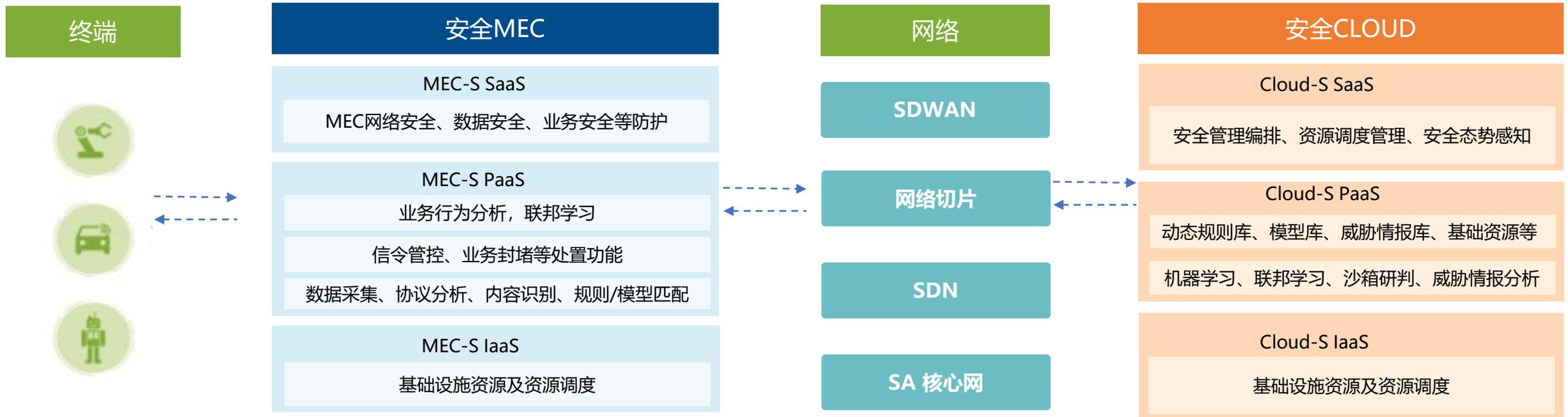
- ◆ 云网一体化为**安全即服务**提供了基础。云网一体化推动网络互联向“云+网+业务”演进，提供更加敏捷、开放、定制的服务能力。
- ◆ 云网一体化为**可定义、可编排、可管理**的安全框架提供了基础，为**安全自适应、运维自动化、分析智能化**提供了基础。
- ◆ 云网一体化为“云网边端”**协同联动**提供了基础，特别借助**云边协同，投放安全算子和接受边缘反馈实时优化，实现全网的安全动态可控。**

以云网一体化构建5G网络安全能力框架



基于云网一体化构建“云-网-边-端”协同联动安全平台

云是**安全业务聚能平台**，网是**安全业务赋能平台**，边和端是**安全业务使能平台**。



- ◆ 通过云边协同，打通业务与安全的根本性联系，打造**安全可感知业务、业务可定制安全**的螺旋式迭代体系；
- ◆ 采用AI学习尤其是**联邦学习**，推动平台向智能化、精细化、柔性化、协同化发展；
- ◆ 面向**业务提供安全即服务**。

云网一体化赋能智慧工厂安全感知

业务健康运营

终端设备安全

IT网络安全

OT网络安全

业务视图

态势感知

工业资产管理

安全事件监测

威胁情报分析

资产漏洞管理

联动处置

多维纵深防御

从主机到边界，从OT到IT，从被动监测到主动诱捕，建立纵深防御体系。

能力视图

业务感知保障

安全数字化感知

信令监测

接入失败定位

设备运行管理

信令风暴监测

性能趋势跟踪

业务质量

柔性生产感知

业务健康运营

OT设备
IT主机

主机IP/端口

操作系统

应用软件

身份信息

网络拓扑

资产管理

漏洞名称

漏洞等级

漏洞数量

漏洞分布

影响评估

漏洞管理

入侵检测

恶意代码程序

样本研判

攻击流量分析

攻击链分析

隔离审计

敏感数据泄露

API接口滥用

追踪取证

智能基线

安全监测

威胁流量分析

威胁文件分析

终端恶意接入

异常流量审计

工业安全审计

基于AI的业务基线

采用AI面向工业企业IT、OT域建立全方位的资产管理、威胁感知、安全审计等能力。

数据存储

数据关联

UEBA

机器学习

情报知识库

多源数据接入能力

支持通过分光、镜像、OVS镜像方式获取南北向、东西向的信令流量和业务流量，支持主被动方式采集资产数据及入侵事件，支持在边界通过拟态诱捕。

采集能力

信令流量NTA

业务流量NTA

主机检测引擎

主动探测引擎

攻击流量牵引

日志采集引擎

配置信息

OVS镜像/镜像/分光

Agent

资产探测

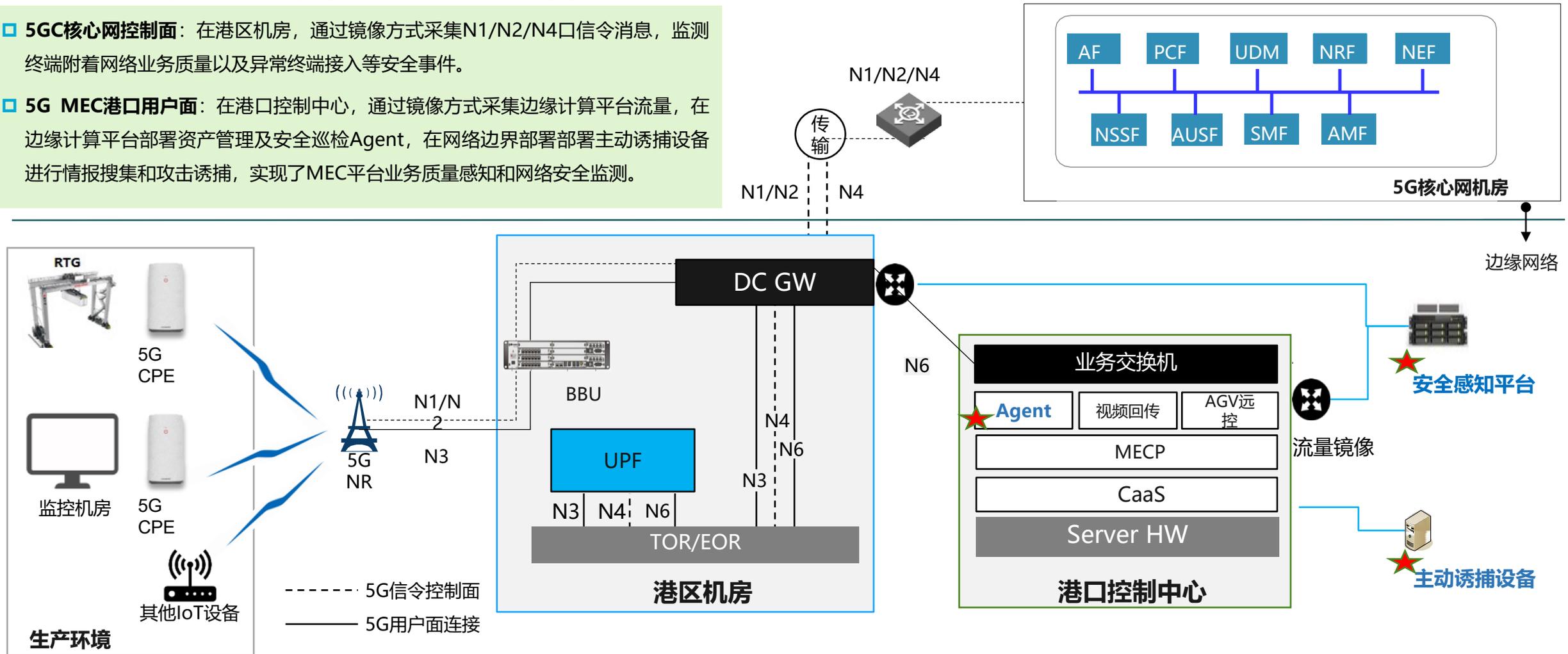
漏洞扫描

拟态诱捕

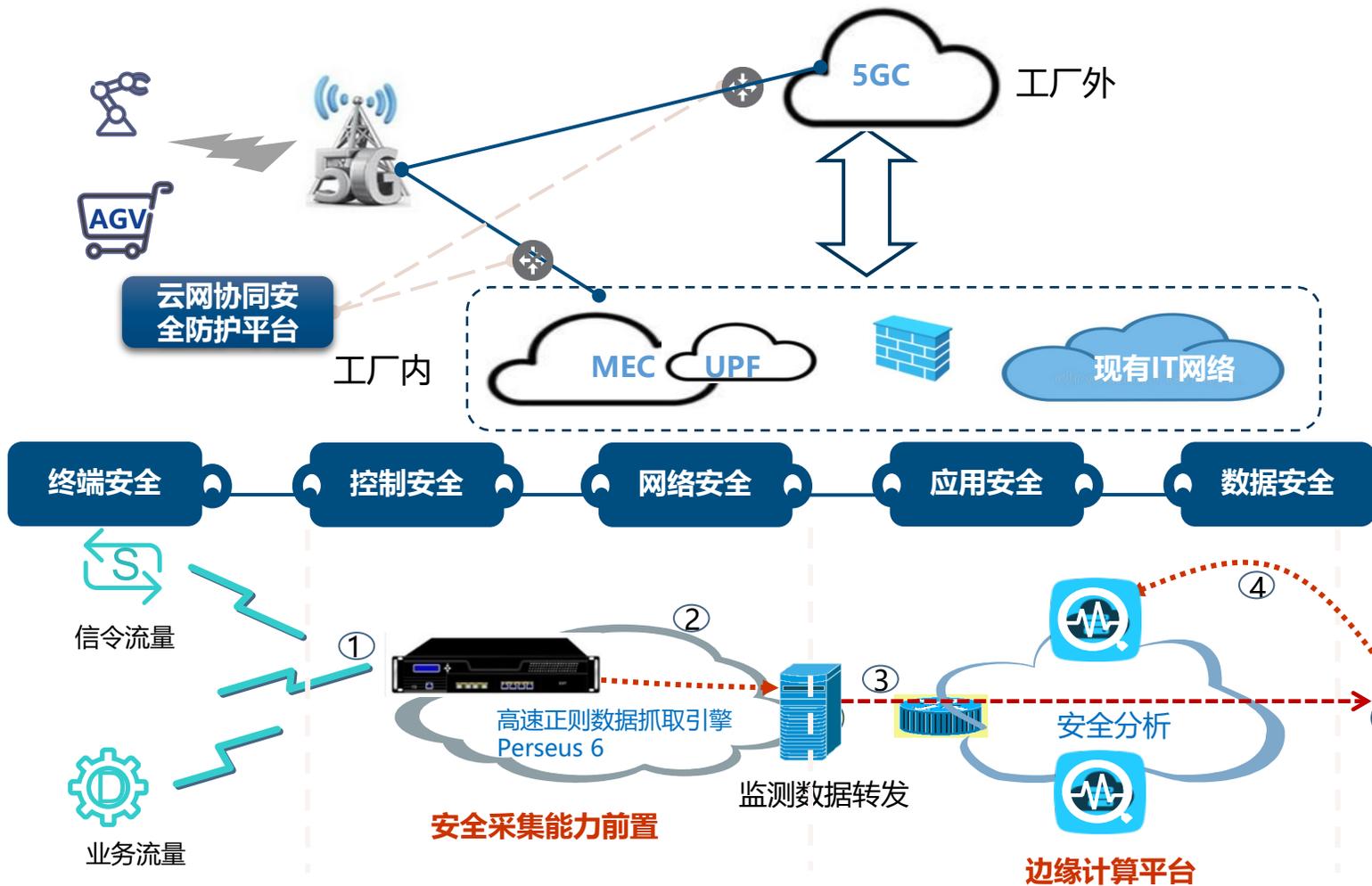
安全设备

安全实践：5G智慧港口网络安全态势感知系统

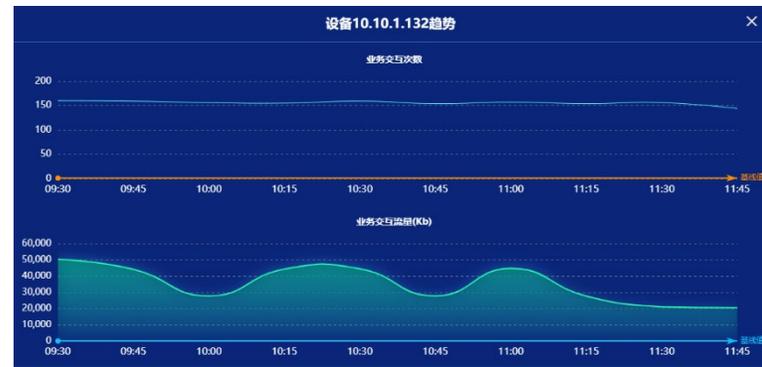
- 5G核心网控制面：**在港区机房，通过镜像方式采集N1/N2/N4口信令消息，监测终端附着网络业务质量以及异常终端接入等安全事件。
- 5G MEC港口用户面：**在港口控制中心，通过镜像方式采集边缘计算平台流量，在边缘计算平台部署资产管理及安全巡检Agent，在网络边界部署部署主动诱捕设备进行情报搜集和攻击诱捕，实现了MEC平台业务质量感知和网络安全监测。



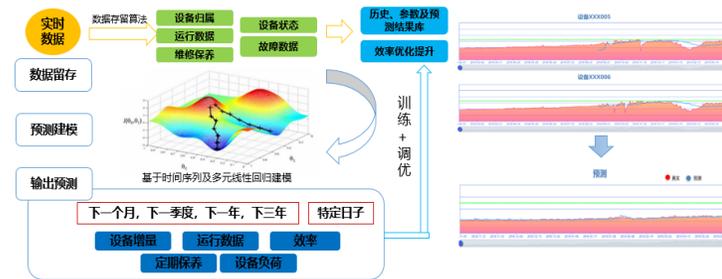
安全实践：工业企业5G安全防护



安全基线分析



运行效率分析



THANKS

谢谢!