运营商边缘计安全技术研究报告

（2020年）

SDN/NFV/AI 标准与产业推进委员会

2020 年 8 月

版权声明

前　言

本报告在分析运营商边缘计算场景、架构以及安全威胁的基础上，提出了运营商边缘计算安全技术要求、边云协同安全要求，并提供了安全关键技术、安全解决方案、等保对标建议。本报告为运营商规划和部署边缘计算网络、业务提供了安全参考。

本报告的编制得到了中国移动、中国信息通信研究院、中国联通、华为、中兴、爱立信、绿盟、山石网科、天融信、亿阳信通等企业的大力支持和配合，在此一并表示感谢。

目 录

一、 概述

为了有效满足垂直行业对网络高带宽、低时延、高可靠要求，承载大规模 MTC/IoT 终端连接等要求，学术界和产业界提出了边缘计算的概念。2014 年 9 月，欧洲电信标准化协会（European Telecommunications Standards Institute, ETSI）成立了 MEC 工作组（Mobile Edge Computing Industry Specification Group）；2016 年，考虑到移动通信网络与固定宽带网络架构融合的趋势，将 MEC 概念扩展为多接入边缘计算（Multi-Access Edge Computing）。根据 ETSI 定义，MEC 技术是指在靠近用户的位置（如：无线接入侧、核心网的边缘）部署通用服务器，提供云计算能力。

随着 5G 标准的成熟和大规模部署，边缘计算成为 5G 的关键技术特征。5G 网络通过将用户面功能（User Plane Function，UPF）下沉到边缘，实现对边缘计算的支持，以满足垂直行业的低时延、高带宽、安全等要求。边缘计算把存储、计算和网络能力从云数据中心带到边缘，可助力运营商快速建立起与应用提供者或应用开发商合作的桥梁。运营商不仅可以将 MEC 平台的存储、计算能力开放给应用开发商和内容提供商，为它们提供全新的业务开发环境及用户体验；也可以将运营商网络特有的能力封装成各种服务（例如：RNIS、位置服务、带宽管理服务等）在边缘计算平台上开放给企业和垂直行业应用，从而提供更有竞争力的增值服务，实现网络价值的最大化。边缘计算将推动运营商网络和业务的重构，形成面向多种行业、满足泛在计算、低时延通信、智能协同需求的新网络架构、新业务生态。

边缘计算具有靠近用户、第三方应用托管、能力开放等特点，因此，相比传统的通信网络，其开放性和攻击面均增大，包括：核心网网元 UPF 下沉到边缘，运营商的控制能力减弱，可能遭受物理接触攻击；边缘计算第三方应用可托管在运营商边缘计算平台以及运营商网络能力可向边缘计算应用开放，引入来自第三方应用对边缘计算平台以及核心网的安全攻击等。所以，自提出以来，安全就成为边缘计算研究、规划、建设、业务上线等必须要考虑的关键问题之一。

本研究报告旨在对运营商边缘计算架构、平台、应用的安全进行全面分析，为边缘计算的规划、建设和运营提供安全参考，在保障边缘计算不降低运营商网络的安全性的前提下，为垂直行业用户提供安全运行环境和安全能力。本研究报告首先分析运营商边缘计算场景和标准架构，并在此基础上全面分析运营商边缘计算的安全威胁、安全要求、边云协同安全要求以及边缘计算安全关键技术，提出了针对具体的边缘计算场景，安全解决方案；此外，还提出了参考性的等级保护对标建议。

二、 运营商边缘计算场景

2.1 概述

边缘计算的需求主要来自用户业务对超低时延、高带宽、通信和数据安全的需求，如：实时处理实时内容、在更靠近用户的位置处理海量数据、避免敏感数据在公众网络上传输等。根据最新发布的《5G 时代的边缘计算：中国的技术和市场发展》[1]，智慧工厂、智能驾驶、智慧城市、超高清视频是未来五年（2021 年至 2025 年）最具商业规模、排名靠前且极具典型性的边缘计算需求场景，并且运营商也在智慧工厂、智能驾驶、智慧城市以及超高清视频领域与行业客户紧密合作，共同推动边缘计算的发展，为客户提供安全可靠的边缘计算业务。

本节分析上述几个典型的应用场景的业务需求、技术特点和实施方案进行分析，作为安

全威胁问题、安全方案制定的基础。

2.2 场景1：智慧工厂

边缘计算低延迟、低负载和近边缘服务的特点在智慧工厂中获得较好的应用，可以提高工业生产效率、降低重要生产数据泄露的安全风险。

如下图 2-1 所示，工业设备通过基站（gNodeB 或 eNodeB）连接边缘计算节点；工业设备中的数据通过基站传输到边缘计算节点的数据面网关（如 5G 数据面功能 UPF），由数据面网关转发给边缘计算节点上部署的应用进行处理。另外，工业设备上传的数据也可以通过边缘计算节点传输到外部企业应用进行处理。上述场景不仅可以减轻核心网络中的存储和计算资源，同时还可以降低响应延迟和带宽消耗。

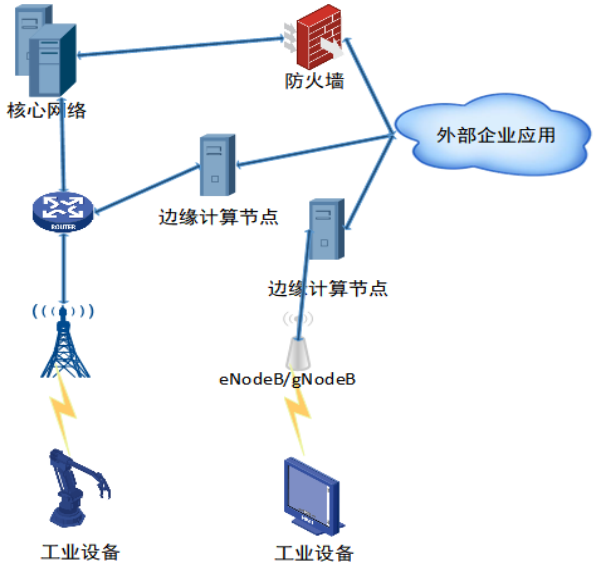

图 2-1 智慧工厂场景

2.3 场景2：智能驾驶

如下图 2-2 所示，智能驾驶系统的组网中，设备分别部署在智慧车辆设备边缘设备层、连接层和核心服务层，边缘计算节点通常位于连接层，其中：

（1）智能车辆边缘设备层可实现共享智能车辆资源，行驶中或驻停状态中的智能车辆间互为分享者和受享者。该层中的智能车辆均已配备车载单元（On Board Unit，OBU），OBU 具有计算、存储以及网络功能。同时，OBU 包含检测传感器（距离和光检测）、全球定位系统（GPS）、视频和相机等电子设备/功能。

（2）连接层中的路侧单元（Road Side Unit，RSU）或蜂窝基站（Base Station，BS）连接到边缘计算节点以提供高计算性能和存储能力。边缘计算节点可以部署在同一地点的 BS 或 RSU。由于 RSU 比 BS 更靠近车辆，所以可优先选择 RSU 为车辆提供边缘计算服务。在没有 RSU 覆盖的情况下，BS 可以为智能车辆提供边缘计算服务。

（3）核心服务层由大量高性能专用服务器组成，具有强大的计算、存储能力以及稳定的连接。

上述利用边缘计算的智能驾驶场景中，智能车辆边缘设备层的流量或部分流量卸载在边缘计算节点，并将核心服务层的部分能力下沉至边缘计算节点，有效实现了边缘分流和核心能力下沉，为车辆提供了低时延和高品质体验的边缘计算服务。

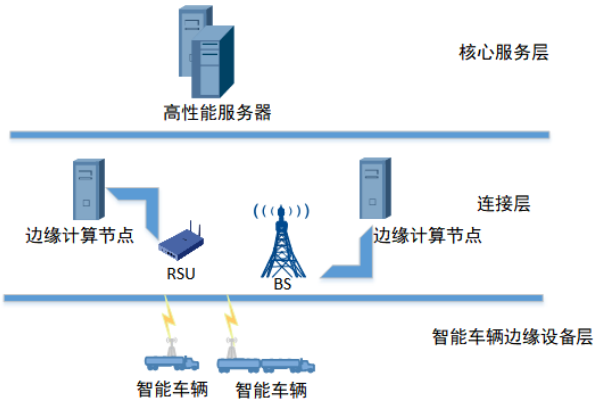

图 2-2 智能驾驶场景

2.4 场景3：智慧城市

智慧城市系统中包括安防监控、基于位置信息的服务等业务功能。智慧城市中需要实现对海量联网智能设备的数据的处理。比如安防监控系统由许多个摄像头组成，传统的部署方式一般采用有线网络或 WiFi 为摄像头提供回传，有线网络布线成本高、效率低且占用大量资源，而 WiFi 稳定性较差、覆盖范围较小、需要补充大量路由节点以保证覆盖和稳定性。并且，传统方式下需要将监控视频通过承载网和核心网传输至云端或服务器进行存储和处理，不仅加重了网络的负载，也难以保证业务的端到端时延。同时，大量的摄像采集工作使得监控器需要具备较强的数据采集能力，这就对摄像头的整体架构提出了较高的要求。

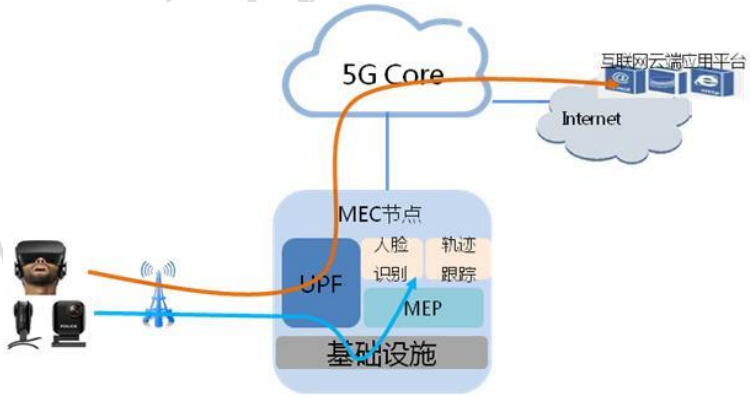

图 2-3 智慧城市场景

如上图 2-3 所示，引入 MEC 后，可将监控数据分流到边缘计算节点，有效降低网络传输压力和业务端到端时延。此外，安防监控还可以和人工智能相结合，在边缘计算节点上搭载人工智能（Artificial Intelligence，AI）视频分析模块，面向智能安防、视频监控、人脸识别等业务场景，以低时延、高带宽、快速响应等特性弥补当前 AI 视频分析中时延大、用户体验差的缺陷，实现本地分析、快速处理、实时响应。云端执行 AI 的训练任务，边缘计算节点执行 AI 的推理，二者协同可实现本地决策、实时响应，可实现表情识别、行为检测、轨迹跟踪、热点管理、体态属性识别等多种本地 AI 典型应用。

2.5 场景4：超高清视频

超高清视频业务（如 AR、VR、4K/8K 视频）要求网络和平台具备大带宽、低时延、实时计算能力。传统通过中心视频云提供超高清视频的方式，不能满足低时延、实时计算的需求，并且，对传输网络带宽也提出了较高的要求。随着 5G 以及边缘计算的发展，中心视频云平台可通过边缘计算，将视频能力下沉到运营商边缘计算节点的边缘计算平台，在时延、带宽、算力方面，为视频发展提供更好的支撑。

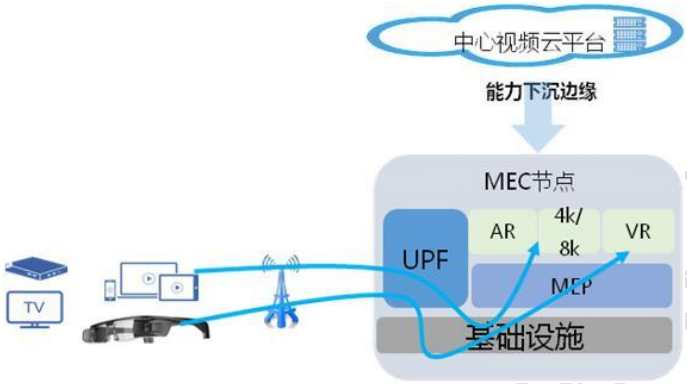

图 2-4 超高清视频场景

如上图 2-4 所示，通过下沉到边缘的 AR 边缘能力，可提供 3D 模型渲染、位置注册、目标识别，目标追踪等能力；VR 边缘能力可提供 VR 点播、VR 直播、VR 内容快速分发、FOV 带宽节省等能力；超高清 4K/8K 边缘能力可提供 4K/8K 点播、4K/8K 直播、4K/8K 互动直播、内容快速分发等能力。

三、 边缘计算架构

ETSI 在 2016 年 3 月发布了 ETSI GS MEC 003[2],定义了移动边缘计算的框架和参考架构标准，如下图 3-1 所示。该架构规划了 MEC 平台组件以及接口功能，与 ETSI 提出的 NFV 架构比较类似。ETSI 在 2018 年 2 月发布了 ETSI GR MEC 017[3]，对于 NFV 环境中如何部署 MEC 提出了分析和技术建议。该参考架构（如下图 3-2 所示）也被纳入 2019 年 1 月更新的 ETSI GS MEC 003 中，作为 NFV 中 MEC 的参考架构。在此架构中，MEC app 和 MEP 均作为一个 VNF 部署在边缘基础设施上，MEPM 分别与 MEC app 和 MEP 的 VNFM 协同实现对 MEC app 和 MEP 的生命周期管理。

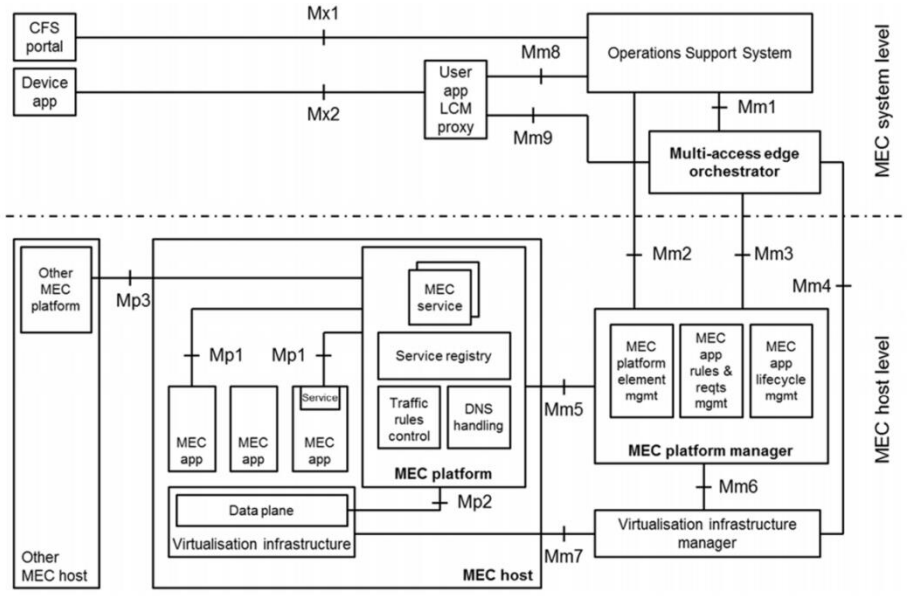

图 3-1 ETSI MEC 参考架构

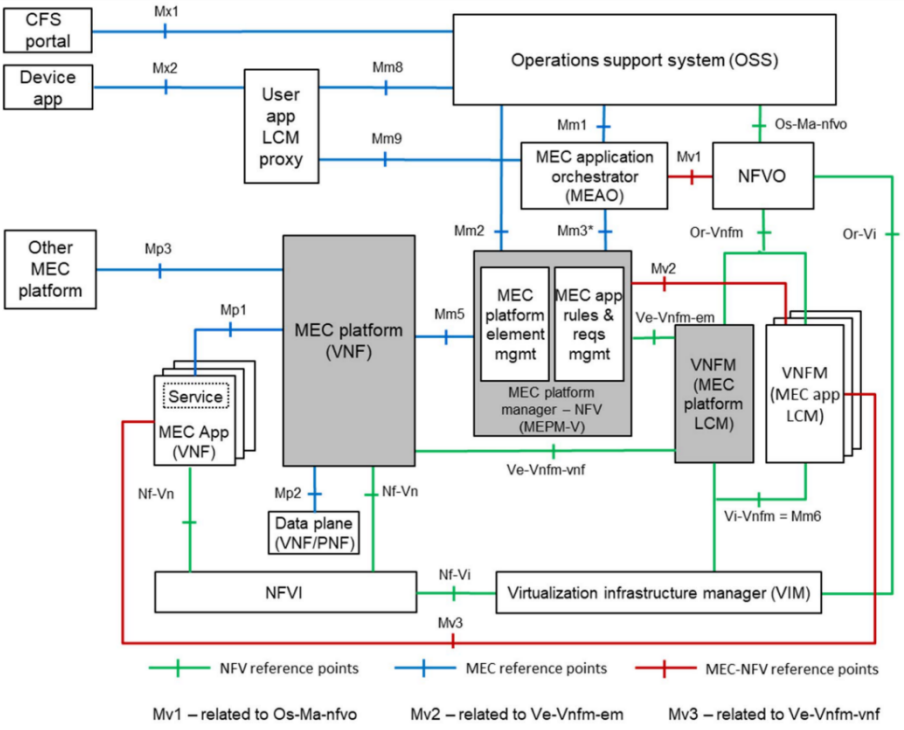

图 3-2 ETSI NFV 环境中部署 MEC 的参考架构

CCSA 在《5G 核心网边缘计算总体技术要求》[4]中也提出了 5G 边缘计算系统架构，如下图 3-3 所示。

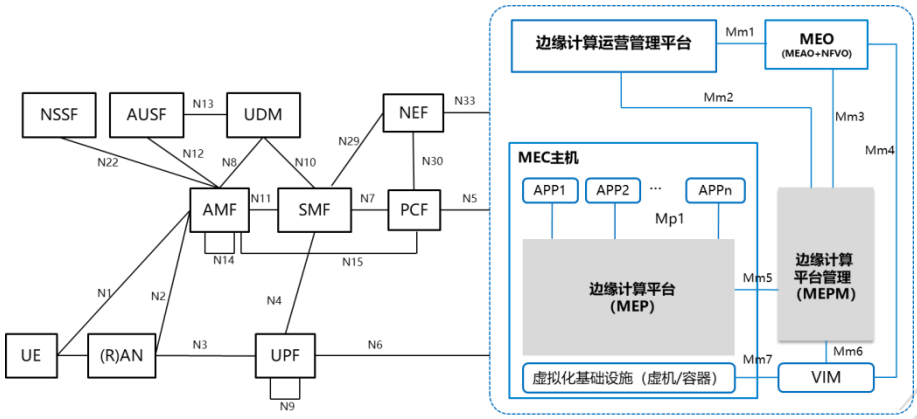

图 3-3 CCSA 5G 边缘计算系统逻辑架构

CCSA 5G 边缘计算系统逻辑架构将 5G 的 UPF 作为边缘计算的数据面，边缘计算平台系统为边缘应用提供运行环境并实现对边缘应用的管理。5G 边缘计算平台系统相对于 5G 核心网络是 AF+DN 的角色，与 UPF 之间为标准的 N6 接口连接。相比于 ETSI 的 MEC 架构，该架构是对 5G 网络中部署 MEC 提供了更具体的参考架构。

四、 边缘计算安全威胁

如前所述，边缘计算系统作为运营商网络的一部分，首先会继承传统安全威胁；同时，由于其技术特点、组网方式、业务承载方式的不同，也会面临传统安全威胁的变化、新的安全威胁。

4.1 传统安全威胁

边缘计算作为云计算能力下沉的一种新型计算模式，继承了部分传统安全威胁，主要包括：

（1）基础设施安全：攻击者可非法访问物理服务器的 I/O 接口，获得敏感信息；容器或虚拟机部署 APP 时，攻击者可篡改容器或虚拟机镜像，如置入恶意代码等；可利用容器逃逸/虚拟机逃逸攻击主机或其它容器/虚拟机。Host OS/虚拟化软件的漏洞也可被攻击者利用发起针对容器或虚拟机的 DoS 攻击、非法访问等。

（2）网络安全：包括恶意代码入侵、窃取、篡改、删除、伪造数据等威胁。

（3）数据安全：包括数据丢失或泄露、数据库破解、备份失效、隐私泄露等威胁。

（4）应用安全：包括拒绝服务攻击、越权访问、软件漏洞利用、权限滥用、身份假冒等威胁。

（5）管理安全：恶意内部人员非法访问、使用弱口令等。

4.2 新引入的安全威胁

边缘计算节点之间具有一定的异构性，并且网络规模相对核心云较小，所以网络攻击的影响范围小于核心云。但是，边缘计算节点会承载垂直行业应用，一旦攻击者成功控制了边缘节点，整个边缘节点的应用均受到影响，可能影响多个行业。同时边缘计算节点靠近用户，引入第三方 APP，暴露面增加，边缘计算会引入新的安全威胁，并且部分传统安全威胁会在边缘计算场景和网络架构下更易被利用或影响范围更广。发生变化的传统安全威胁和新引入的安全威胁主要包括：

（1）基础设施安全：相比核心网，边缘计算节点可能部署在无人值守机房或者第三方机房，更易遭受物理接触攻击，如攻击者近距离接触硬件基础设施，篡改设备配置等；同时，由于边缘计算节点分布式部署，依赖远程运维，升级和补丁修复不及时，会导致攻击者利用漏洞进行攻击。

（2）网络安全：边缘计算架构下，接入设备数量庞大，类型众多，更容易实施分布式拒绝服务攻击。并且，新引入的 MEP 以及边缘计算编排系统成为攻击者的重要攻击对象，如果未与第三方 APP、互联网等进行安全隔离导致被攻击者控制，攻击者可对所有 APP 进行非法的访问、编排等，后果非常严重。

（3）数据安全：边缘设备可能包含多种 APP，存在 APP 之间的非法访问的安全威胁。由于边缘计算节点的资源受限，更容易因为缺乏有效的数据备份、恢复、以及审计措施，导致攻击者修改或删除用户在边缘节点上的数据来销毁某些证据。

（4）应用安全：边缘计算节点连接海量的异构终端，承载多种行业的应用，终端和应用之间采用的通信协议具有多样化特点，多数以连接、可靠为主，并未像传统通信协议一样考虑安全性，所以攻击者可利用通信协议漏洞进行攻击。同时，如果 APP 的应用数据未全部终结在 APP，可造成数据泄露；非授权 APP 调用边缘计算平台 API，可造成非法访问或 DoS 攻击等。

五、 边缘计算安全要求

5.1 概述

由于垂直行业的需求差异，UPF、边缘计算平台存在不同的部署方式。比如：对于智慧工厂，客户数据的敏感程度高，客户会要求将运营商的 UPF 和边缘计算平台均部署在客户可控的园区，实现敏感数据不出园区。对于超清视频，客户无额外的边缘计算节点的部署位置需求，UPF 和边缘计算平台可部署在运营商汇聚机房，为客户提供服务。不同的部署方式，导致运营商网络的暴露面不同，所以，应针对不同的部署方式及业务需求考虑边缘计算的安全要求，设计相应的安全解决方案，在保证运营商网络安全的同时，为客户提供安全的运行环境以及安全服务。

5.2 组网安全

边缘计算的组网安全与 UPF 的位置、MEP 的位置以及 APP 的部署紧密相关，需要根据不同的部署方式进行分析。

5.2.1 组网方式1：UPF和MEP均部署在运营商机房

在运营商边缘云中部署 UPF 和 MEP，垂直行业的 APP 托管到运营商的边缘 MEP，其组网安全要求如下：

（1）三平面隔离：服务器、交换机，应支持管理、业务和存储三平面物理/逻辑隔离。对于业务安全要求级别高并且资源充足的场景，应支持三平面物理隔离；对于业务安全要求不高的场景，可支持三平面逻辑隔离。

（2）安全域划分：UPF 与通过 MP2 接口通信的 MEP 应部署在可信域内，和自有 APP、第三方 APP 处于不同安全域，根据业务需求实施物理/逻辑隔离。APP 之间应进行

逻辑隔离。

（3）Internet 安全访问:对于有 Internet 访问需求的场景,应根据业务访问需求设置 DMZ 区（如 IP 地址暴露在 Internet 的 portal 等部署在 DMZ 区），并在边界部署抗 D、IPS/IDS、防火墙、WAF 等安全设备，实现边界安全防护。

（4）UPF 流量隔离:UPF 应支持设置白名单,针对 N4、N6、N9 接口分别设置专门的 VRF;UPF 的 N6 接口流量应有防火墙进行安全控制。

5.2.2 组网方式2：UPF部署在运营商机房，MEP部署在客户机房

MEP 部署在客户机房，其组网安全要求相比方式 1 的不同点体现在安全域划分方面，UPF 和客户数据中心之间应进行安全隔离。部署在客户机房的 MEP 和 APP 之间应进行安全隔离，APP 与 APP 之间应进行隔离（如划分 VLAN）。

5.2.3 组网方式3：UPF和MEP均部署在客户机房

UPF 和 MEP 均部署在园区,其组网安全要求相比方式 1 的不同点包括 UPF 流量隔离方面，除了方式 1 的要求，还应针对 UPF 的 N4 口设置安全访问控制措施，对 UPF 和 SMF 的流量进行安全控制。

5.2.4 组网方式4：仅做转发，UPF部署在运营商机房

UPF 部署在运营商机房中做流量转发，运营商不提供 MEP；其组网安全要求相比方式 1 的不同点包括安全域划分方面边缘 UPF 与客户私网、APP 之间应进行安全隔离。Internet 访问方面仅 UPF 做转发时， Internet 安全访问遵从 UPF 所在边缘云的组网安全要求。

5.2.5 组网方式5：仅做转发，UPF部署在客户机房

UPF 部署在园区仅做流量转发，运营商不提供 MEP；其组网安全要求相比方式 1 的不同点体现在安全域划分方面，园区 UPF 与核心网间进行安全隔离。UPF 与园区客户私网、APP 之间应进行安全隔离。APP 与 APP 之间应进行隔离（如划分 VLAN/VXLAN）。Internet 访问方面，仅 UPF 做转发时，Internet 安全访问由客户来决定，建议客户私网和 Internet 之间进行安全隔离。

5.3 基础设施安全

基础设施安全需要从硬件基础设施安全、虚拟基础设施安全等方面实施。具体安全要求包括:

（1）硬件基础设施安全主要包括物理环境安全和资产管理要求，主要包括：边缘计算系统机房出入口应配置电子门禁系统，控制和记录进入的人员，机柜应具备电子防拆封功能，应记录、审计操作机柜的行为等。硬件基础设施应支持管理物理资产，实现物理资产的发现（纳管）、删除、变更及拓扑呈现，支持对虚拟机的端口（监听端口）、软件（软件资产）、进程（运行进程）、账户（账户资产）进行采集、记录等。

（2）虚拟基础设施安全主要包括宿主机安全、镜像安全、虚拟化安全和容器安全等，具体包括：

- 宿主机应禁用软盘、USB 接口、串口及无线接入等不必要的接口，应进行安全加固，如禁止多个管理员共用一个帐户、设置合理的口令策略和访问控制策略、禁止安装不必要的系统组件、禁止开放不必要的服务和端口等。
-
- 虚拟机镜像、快照等需进行安全存储，防止非授权访问；应提供存储镜像的完整性和机密性保护，支持镜像的完整性校验，应支持镜像安全传输。

（3）虚拟化安全应支持同一物理机上不同虚拟机之间 vCPU、内存以及 I/O 等资源的隔离，应支持虚拟化软件的安全加固，以及虚拟机迁移安全等。

（4）容器安全应覆盖整个容器的生命周期，可以从开发、部署、运行三个阶段来进行安全防护。

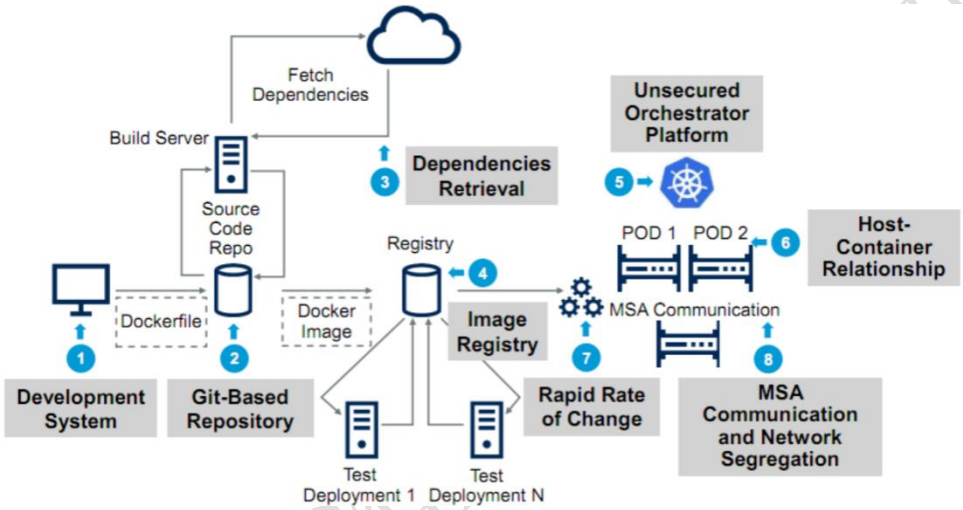

图 5-1 Gartner 的容器全生命周期攻击面分析[7]

参照上图 5-1，开发阶段应要求开发者对 base 容器镜像以及中间过程镜像进行漏洞扫描检查，同时对第三方甚至自有应用/代码进行安全检查。部署阶段应由 MEC 平台对镜像仓库进行安全监管，对上传的第三方/自有容器镜像进行漏洞扫描，控制有高危漏洞的容器镜像的运行使用。运行阶段首先应支持容器实例跟宿主机之间的内核隔离；其次，应支持容器环境内部使用防火墙机制防止容器之间的非法访问，应可持通过第三方进程监控或流量监控对运行时容器实例的非法/恶意行为监控，可在容器管理平台部署 API 安全网关来对容器管理平台的 API 调用进行安全控制。

5.4 UPF安全

UPF 安全包括系统安全和业务安全：

（1）系统安全方面应支持网络管理域、核心网络域、无线接入域相互隔离，数据面与信令面、管理面相互隔离；应支持 TEID 的唯一性，支持对 UPF N3、N9 和 N4 接口传输的用户数据和信令分别进行完整性、机密性、防重放攻击保护。

（2）业务安全方面应支持防移动终端发起的(D)DOS 等攻击，支持对终端数据报文/协议进行过滤，支持对终端用户的上行流量的源地址进行匹配，对下行流量的目的地址进行匹配，并丢弃非法地址的报文。应支持设置终端互访策略，支持信令和用户面数据流量的控制，防止来自 SMF 的信令或 APP/终端的数据造成的(D)DoS

攻击。位于第三方机房的 UPF 应支持内置安全通信功能，如支持 IPSec 协议和内置虚拟防火墙功能，实现安全保护和控制等。

5.5 MEP安全

边缘计算平台（MEC Platform，MEP）不仅提供边缘计算应用的注册、通知，而且为应用提供 DNS 的请求查询功能、路由选择功能，本地网络的 NAT 功能，同时可以基于移动用户标识的控制管理能力，满足业务分流后的用户访问控制。MEP 还提供服务注册功能，将 MEC 平台的服务能够被其他服务和应用发现，也可以通过 API 接口的方式对外开放 MEP 的能力。

根据边缘计算架构，MEP 部署在虚拟化基础设施上，应满足 5.3 章节的安全要求。MEP 应对 API 接口访问进行认证和授权并支持数据传输的机密性、完整性、防重放保护。并且，MEP 应支持防(D)DoS 攻击，敏感数据保护等。

5.6 第三方/自有应用安全

MEC 平台的第三方/自有应用可部署在虚拟机或容器中。对于虚拟机形态的第三方/自有应用应考虑虚拟化相关安全。在虚拟化网络的 VPC 边界应部署南北向的虚拟化网络安全设备，如虚拟化防火墙、入侵防御、WAF 等；在虚拟化网络 VPC 内部的子网和虚拟机之间应部署东西向的虚拟化网络安全措施，如微隔离等；在虚拟化主机内部应考虑部署主机防病毒、EDR 等主机安全方案。

对于容器形态的第三方/自有应用，由于是 PaaS 形态，安全能力建设需要依赖运营商提供的安全服务，运营商包装容器安全服务需要的产品技术和方案参见 5.3 基础设施安全章节中的容器安全部分。

5.7 边缘计算编排管理系统安全

MEC 的编排管理系统架构与 NFV 的编排和管理系统类似。从 ETSI MEC 系统参考架构（图 3-1）中可以看出，MEC 的编排管理系统包括 MEO、MEPM 两部分，南向接口面向 VIM 和 MEP，北向接口面向运营商的运营管理系统。运营管理、MEO、MEPM 之间的接口都属于 API 调用，并不直接面向用户和互联网，除应做好严格的访问控制外，还可部署 API 网关对 API 的调用进行安全控制。

5.8 接口和通信协议安全

边缘计算系统中的标准接口应支持通信双方之间的相互认证，并在认证成功后，使用安全的传输协议保护通信内容的机密性和完整性。

边缘计算系统的管理维护接口应支持对接入者的身份认证，并在身份认证成功后，使用安全的传输协议保护通信内容的机密性和完整行。

边缘计算系统应使用安全的标准通信协议，如 SSHv2、TLS v1.2、SNMPv3 及以上版本，等，禁止使用 Telnet、FTP、SSHv1 等。

5.9 网络能力开放

5.9.1 概述

运营商网络支持网络能力向边缘应用开放，MEC 中边缘应用通过调用运营商网络能力（如用户位置、QoS 等），可进一步增强业务功能和体验。网络能力开放带来好处的同时也引入了新的安全威胁，应对 API 进行安全的管理、发布和开放。对作为 API 调用方的边缘应用进行认证和授权，从而保证边缘网络能力开放的安全性。目前，关于能力开放可以参考 3GPP SA6 组定义的 3GPP TS 23.222 [5]为 API 服务调用定义的 CAPIF 框架，如下图 5-2 所示，其中核心功能 CAPIF core function 负责处理 API 请求者的请求和授权。

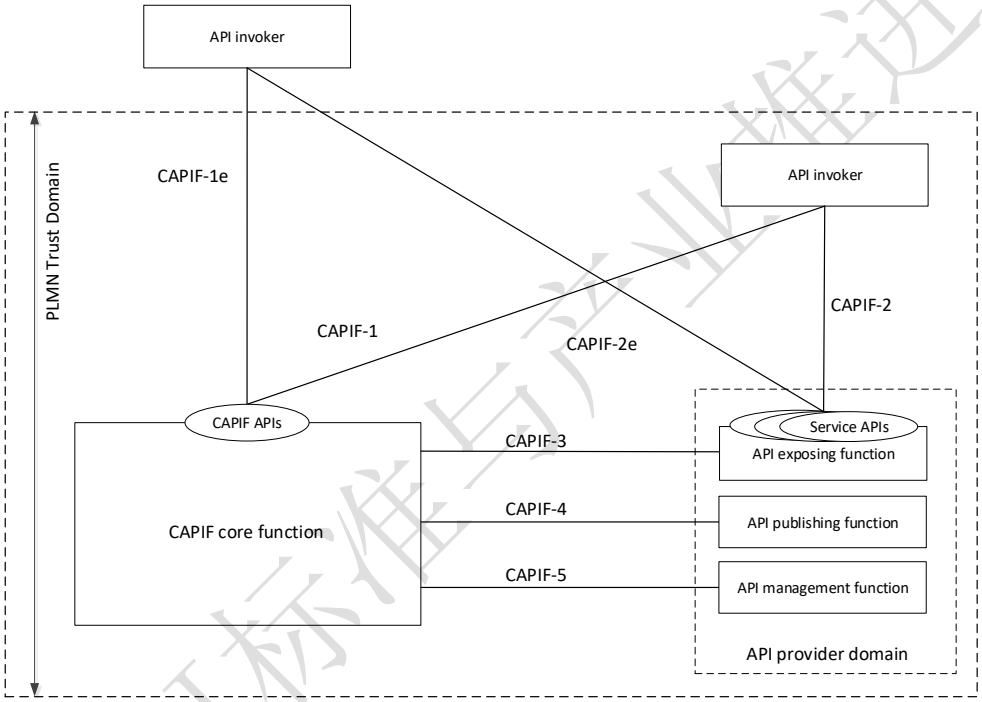

图 5-2 3GPP CAPIF 框架

5.9.2 CAPIF架构适配

3GPP SA6 定义的 3GPP TS 23.758[6]定义的应用层 MEC 架构如下图 5-3 所示。在边缘侧包含边缘应用服务器（Edge Application Server，EAS）与 ETSI MEC 架构中的 MEC APP 对应，边缘使能服务器（Edge Enabler Server，EES）与 ETSI MEC 架构中的 MEP 对应，而边缘数据网络配置服务器（Edge Data Network Configuration Server，EDNCS）为 EES 的管理模块，可以部署在 MEP 或 MEPM。这些服务器之间存在 API 调用关系，这些服务器与运营商网络之间也存在 API 调用关系。如果需要复用 CAPIF 框架来实现这些服务器之间的服务调用管理，则需要将 MEC 的各服务器以及运营商网络之间的调用授权关系与 CAPIF 进行映射，从而复用 CAPIF 已有的调用流程和机制。

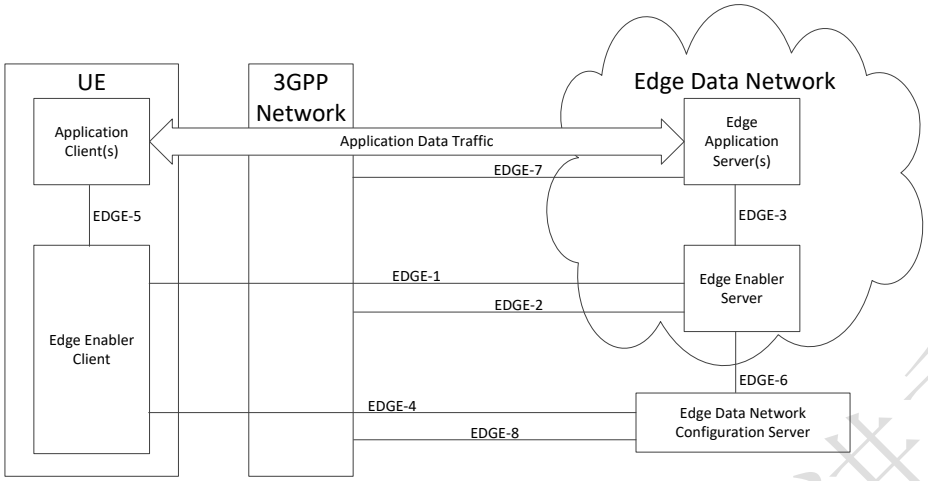

图 5-3 3GPP MEC 应用架构及接口

针对 CAPIF 的部署方式不同，典型的映射有两种方式，一种是分布式，一种是集中式。对于分布式的映射，除了运营商网络部署的 CAPIF core function，每个边缘计算网络部署有独立的 CAPIF core function，负责对运营商网络中 API 提供的服务进行调用；对于集中式的映射，边缘计算网络的服务调用由运营商中的 CAPIF core function 进行管理，不再单独部署分布式核心功能。

有了上述映射关系之后，MEC 场景下边缘服务器之间进行 API 调用，或者边缘服务器调用 3GPP 网络开放的北向 API 均可以复用 33.122 所定义的安全机制。

5.9.3 用户授权的能力开放

边缘应用服务器需要调用运营商网络的能力开放，其中可能涉及 UE 的敏感信息（如位置）。使用这些信息需要获取用户同意，且用户需要完全掌握哪些应用可以以什么频率获取用户或用户设备的指定信息。当核心网收到边缘应用的用户位置请求时，可以通过信令面向用户发送位置请求，在获取用户同意后，核心网才会将获取的用户位置信息返回给相应的边缘应用。

5.9.4 边缘服务授权

移动网络运营商需要对UE使用边缘计算服务进行授权，只有具备合法授权的用户才能使用对应的边缘计算服务。对于非运营商部署场景，边缘服务提供商也应该采取类似的授权机制保证边缘计算服务不被非法访问。例如，当用户访问边缘应用时，核心网需要获取用户签约数据，若用户未签约则拒绝用户的访问，或者核心网与用户所访问的应用交互获取用户授权信息，只有用户具备合法的授权才允许用户访问边缘服务。

5.9.5 应用切换过程中的服务认证和授权

因为 UE 位置移动或者是负载均衡等因素，边缘应用服务器会发生切换。需要考虑将必要的上下文安全地从源边缘应用服务器传递到其他服务器（边缘应用服务器或云应用服务器）以保证用户服务连续性。常见的切换触发有四种触发方式：EAS 发起、EES 发起、UE 侧应

用客户端发起以及 UE 侧使能客户端发起。以 EAS 发起的为例，应用上下文通过源和目标 EES 传递到目标应用服务器，从而使的目标应用服务器可以对 UE 进行认证和授权，保证应用切换过程中 UE 的业务连续性。

5.10 用户接入安全

用户接入安全是指对接入到运营商核心网络、边缘计算节点的终端进行身份识别，并根据事先确定的策略确定是否允许接入的过程。边缘计算节点面临海量异构终端接入，这些终端采用多样化的通信协议，且计算能力、架构都存在很大的差异性，如在工业边缘计算、企业和 IoT 边缘计算场景下，传感器与边缘计算节点之间众多不安全的通信协议（如 Zigbee、蓝牙等），缺少加密、认证等安全措施，易于被窃听和篡改，因此，应根据安全策略允许特定的设备接入网络、拒绝非法设备的接入。

5.11 数据安全

数据安全要求对用户数据中的隐私（比如身份信息、位置信息和私密数据等关联到个人的数据）和身份（比如用户所知、用户拥有（如智能卡）、用户具有信息（如生物特征等））进行保护，采用加密（含对称加密、非对称加密等）或脱敏（比如匿名或假名等）等主流数据安全技术，并且进行安全存储以防数据丢失，保障用户数据的机密性和完整性。

5.12 管理安全

MEC 的管理安全主要包括安全事件、用户行为、关键数据以及平台基线、生命周期等相关的管理，如下图 5-4 所示。

MEC 的安全管理具体建议如下:

（1）安全事件管理：实现 MEC 系统中安全事件可预警、可追溯。安全事件管理通过收集物理安全设备、虚拟安全设备、应用层安全设备相关告警日志，上报至态势感知系统进行分析，进行安全预警；同时将告警信息进行归档，方便后续日志追溯。

（2）用户行为管理：实现人员操作行为可追溯，预警人为操作所产生的风险。通过统一接入门户对宿主机、虚拟机、云管理平台、MEC 管理平台以及虚拟网元、第三方应用的用户进行统一管理。记录其登录登出以及相关的命令操作，通过 UEBA 技术绘制用户行为肖像并生成相应安全策略。当用户出现异常操作时，发生告警并阻止相关操作。

（3）关键数据管理：实现关键数据流转路径可追溯，防止数据泄露。对用户信息、配置信息、镜像信息、软件包等关键数据的流转进行记录，形成数据流转路径。当发生数据泄露事件时，为事件追溯提供证据。

（4）平台基线管理：通过对宿主机、虚拟机、物理网络设备、虚拟网络设备、镜像、应用软件包（网元、第三方应用）进行安全基线核查，确保平台本身以及上层应用的安全性，减少安全风险，提高安全防护水平。

（5）生命周期管理：对接入到 MEC 的设备进行生命周期管理，定期远程更新所有边缘设备，维护管理补丁升级和固件升级，及时修补漏洞。

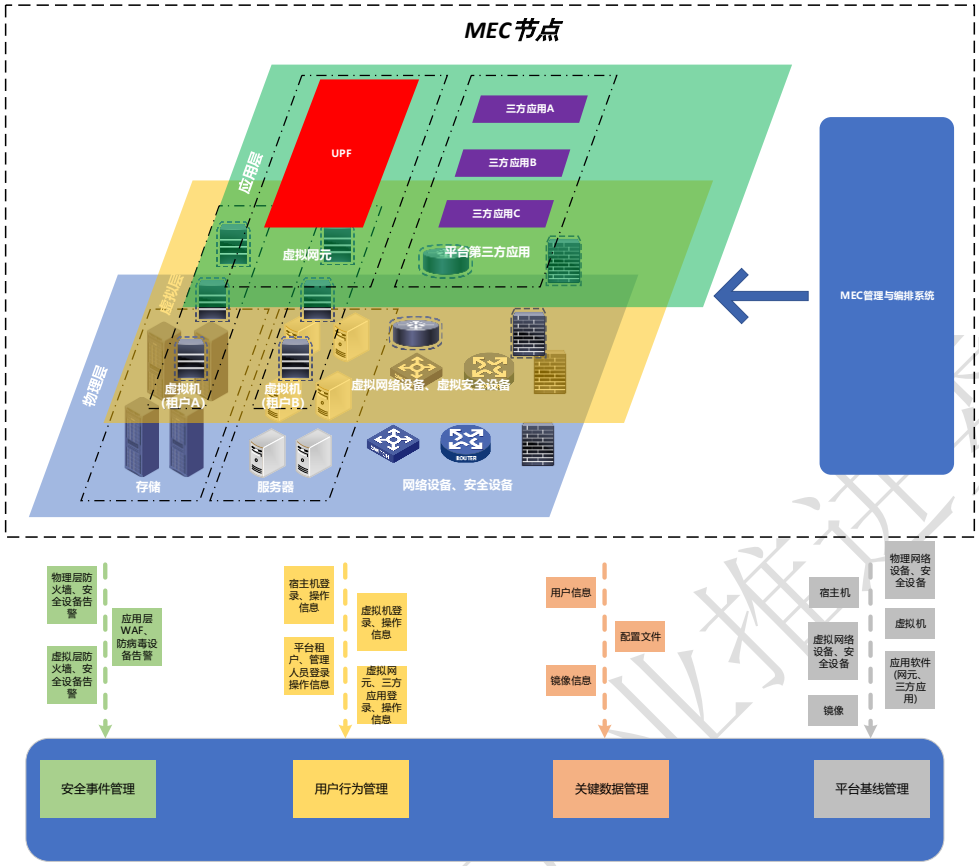

图 5-4 MEC 管理安全框架

六、 边云协同安全要求

边缘应用和云端应用的协同要求对应的安全防护体系应考虑边云协同的安全需求。例如，在基于人工智能技术的应用中，云端应用负责训练，边缘侧的应用负责对实时的数据分类处理，云端会将模型和参数推送到边缘侧，边缘侧也会将需要训练的数据上传到云端，云边两侧的数据传输需要进行安全监控，以防有针对模型、参数和训练数据的投毒，或者针对相关接口未授权的访问。又如，在车联网等移动场景中，智能终端会经常移动，那么相关的业务应用会预测物体运动轨迹，从云端调度最近的边缘节点，启动对应应用的边缘服务。此时，该边缘应用的安全防护应用也应快速准备好资源，做好数据接入准备，并且从云端获得相关的安全防护策略。从而，安全应用接受云端控制器的调度，紧跟业务边缘应用，最终安全策略在全局时刻能保持一致。

以 KubeEdge[1]为例，当前云端需要指定边缘应用部署的节点，例如，某物联网应用可以根据某个资源部署策略进行部署，云端调度器会根据策略将边缘应用部署到相应的节点上。此时，云端安全应用应该能够监听到该事件，并获得边缘应用部署位置，然后通知边缘侧的安全执行器。后者可根据边缘节点设置，以 sidecar 的方式嵌入到该边缘应用的 pod 中，或者以特权容器的方式在边缘应用所在的节点上进行部署。当物联网设备移动到另一个边缘节点附近时，云端调度器则需要向该新的节点部署边缘应用。此时，云端安全应用也应感知到该变化，并在新的节点上及时部署资源、流量和安全策略。

从架构来看，边缘计算平台和云平台是层次化的结构，但从业务逻辑上看，两者是一体

[1] https://kubeedge.io/

的。所以为了保证边缘应用安全，比那云协同应当确保云端和各个边缘侧的安全策略是一致、全局统一的，应确保云端和边缘节点之间的数据和控制通道的机密性、完整性和可用性，应对云端镜像仓库、边缘节点本地的边缘应用镜像进行安全性评估和完整性校验等。

七、 边缘计算安全关键技术

7.1 基线核查

MEC 的能力开放功能为各个企业提供了能够定制化运营商服务的能力，其中企业可以将自己的 APP 直接部署在 MEC 平台上来实现某些服务能力。

MEC 平台中第三方 APP 具有以下特点：

（1）APP 所使用的依赖组件可能并不受 MEC 平台管理，不能确保其使用的依赖组件符合 MEC 平台安全要求。

（2）APP 的安全防护水平参差不齐，不能确保三方 APP 的安全防护水平符合 MEC 平台安全要求。

通过基线核查技术，对所有部署在 MEC 的 APP 部署包进行基线核查（包括代码审计、依赖组件检测等），确保部署在 MEC 平台上的 APP 的安全防护能力与 MEC 平台安全防护能力相符合，减少第三方 APP 给 MEC 平台带来的风险。

7.2 数据采集及异常协议流量分析

边缘计算节点分布式部署，对传统的流量采集和分析方式（即针对核心网链路采集，使用专线回传全量采集数据，部署协议分析平台集中分析）带来了挑战。边缘计算节点可以通过部署虚拟化探针，实现在边缘计算节点虚拟化环境中的协议流量采集，并通过分布式部署在边缘计算节点的异常协议分析系统，在边缘计算节点本地分析和监测来自用户终端和边缘计算节点中第三方应用的异常业务行为和异常协议流量，再将筛选后的数据发送回核心分析平台，从而实现在减少回传数据量的同时，通过本地化的分析提高分析响应时延和处理效率。异常协议流量分析的重点是分析发现可能对边缘计算系统、网络和业务产生严重影响的异常协议流量和异常业务使用，为边缘计算节点所部署的安全防护设备提供响应策略和部署依据。

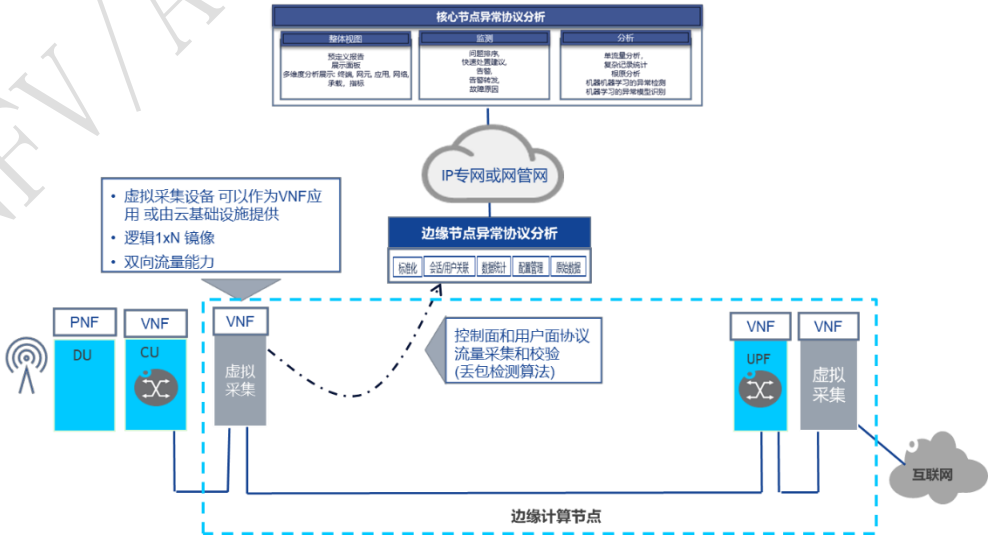

图 7-1 数据采集及异常协议流量分析

同时，边缘计算节点的异常协议流量分析平台可以根据分析每个应用层功能的网络业务特性和管控要求输出精细化的安全策略，下发给边缘计算节点中的安全模块，由安全模块实施这些安全策略。安全模块也可以根据需要采集流量日志，作为数据源提交给异常协议流量分析平台，经数据关联后进一步进行异常流量分析或验证安全策略实施的效果。

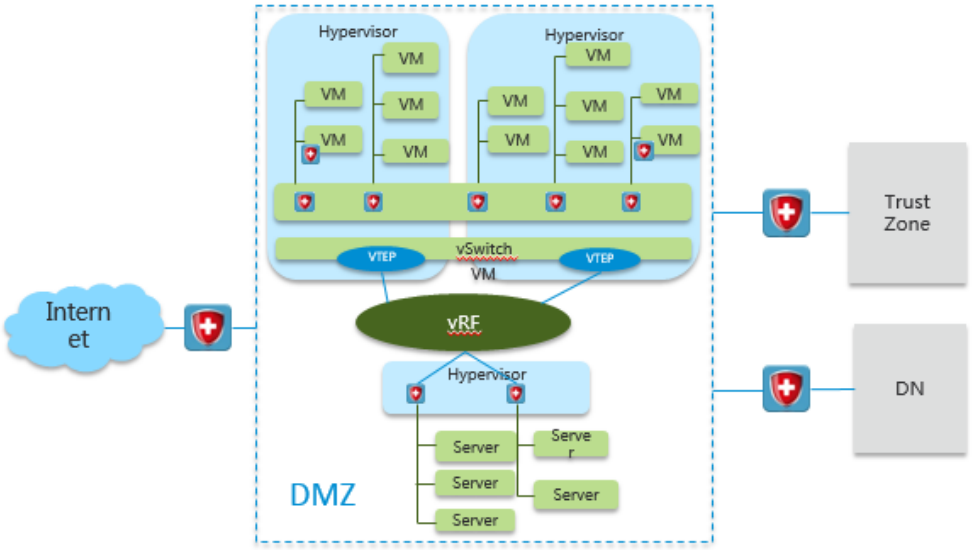

图 7-2 边缘计算节点安全模块

7.3 可信计算

边缘计算靠近用户，相比核心网，位于相对不安全的物理环境中，存在攻击者近距离接触边缘计算节点的设备，进行攻击的风险。所以，通过引入可信计算技术，实现从基础实施、系统启动到上层应用，逐级验证完整性，保证边缘节点中的设备处于可信的状态。

图 7-3 边缘计算场景的可信计算完整性度量

上图描述了边缘计算场景的可信链构建过程。通过可信芯片，逐级度量，实现从 Host 到 Guest 的全流程可信链建立。通过该可信链，实现可信的虚拟化运行环境，可信的虚拟化生命周期管理；可信管理系统可通过与 MANO 交互，将可信状态同步到编排系统。

7.4 安全能力开放

通过网络功能虚拟化和服务化的思想，构建服务化安全功能。通过对传统安全功能的虚拟化，提供满足不同安全需求的虚拟安全功能单元，例如防火墙、接入认证、IPSec（网际协议安全 Internet Protocol Security）、SSL（安全套接层协议 Security Socket Layer） VPN（虚拟专用网络 Virtual Private Network）、入侵检测、病毒检测等。各虚拟安全功能单元通过按需调用不同基础安全服务功能集来满足安全功能可重构，实现安全功能服务化。

在切片或应用编排部署过程中，安全能力开放引擎结合应用的安全需求调用安全功能，使安全资源、网络资源、数据资源在网络切片中独立提供，从而实现边缘网络的安全保障，满足业务安全要求。

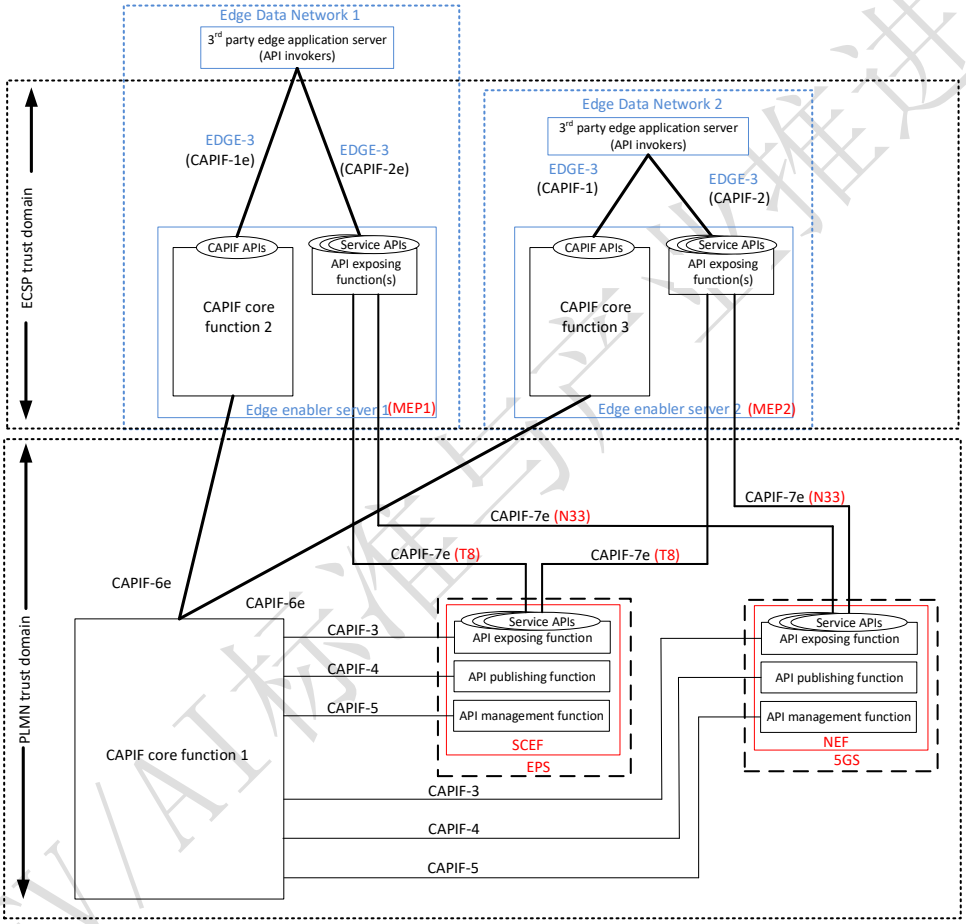

图 7-4 MEC 安全能力开放架构

上图 7-4 以分布式 CAPIF 为例，描述如何通过 MEC 的能力开放架构实现向 APP 开放安全能力。在运营商网络域，部署有 CAPIF core function 以及 API 功能（API 管理、发布以及开放），其中对于 4G 网络的 API 功能则集成到 SCEF 网元中，对于 5G 网络的 API 功能集成在 NEF 中。同时， CAPIF core function 本身也可以集成在 SCEF 或 NEF 中。边缘平台则作为 3GPP 网络域的 API 调用者。

而对于边缘平台，也部署有独立的 CAPIF core function，以及 API 开放功能。其中 CAPIF core function 和 API 开放功能集成在 EES 服务器，也就是部署在 MEP 中。而边缘应用则是边缘平台 CAPIF 框架下的 API 调用者。

边缘应用既可以调用边缘平台 MEP 本身提供的开放能力，也可以通过边缘平台调用

3GPP 网络提供的开放能力。对于前者在边缘平台的 CAPIF 框架进行认证和授权，对于后者则同时需要引入 3GPP 网络域的 CAPIF 框架进行认证和授权，从而充分保障边缘能力开放安全性。

八、 边缘计算安全解决方案案例

8.1 垂直行业通用安全解决方案

虽然垂直行业的安全需求存在差异，但是也存在一些通用的安全威胁和安全需求。例如，终端被病毒感染后，向托管在运营商边缘节点的 APP 发送恶意流量；行业数据在传输时被拦截，导致信息泄露或数据在存储时被篡改、非法访问；运营商边缘基础设施、UPF 或 MEP 的漏洞被利用，导致 APP 敏感数据被非法访问等；APP 与私网之间的数据被拦截或篡改等；APP 自身感染病毒或者 API 被非法访问导致数据泄露等。运营商可以利用网络能力为行业客户提供通用的安全方案，具体包括：

（1）终端安全：通过边缘节点的安全监控系统对终端异常流量进行监控，定期给用户推送异常流量提醒，使用户能够及时发现安全风险，采取安全防护措施，如安装或升级防病毒软件。

（2）数据安全：根据客户的业务需求，开启空口信令的完整性、机密性保护以及空口数据的完整性和机密性保护。并且，对存储的数据分别使用 AES 和 SHA256 实现数据的加密和完整性保护，设置用户名/口令或者生物认证等访问控制。

（3）网络安全：客户 APP 所在边缘计算节点的通信网络包括机房、组网、基础设施、UPF、MEP，实现为 APP 提供运行环境、网络资源等。具体安全机制包括：

- 机房物理环境遵照等级保护等相关标准的安全要求进行设计。
- 组网安全根据 UPF 和 MEP 部署位置，划分安全域，设置防火墙等安全设备实现隔离和访问控制。
- 基础设施按照基础设施安全要求实现资源的隔离、安全加固，实现最小化权限运行。
- UPF 和 MEP 实现自身安全加固，基于证书认证通信对端身份，基于 OAuth 2.0 实现 API 调用的授权等。

（4）业务安全：通过安全合规工具对 APP 的操作系统、数据库和中间件的配置进行安全检查，对不符合项进行整改。边缘节点可以给 APP 提供防火墙、IPS、WAF 等安全服务。

除了上述通用的安全解决方案，针对行业客户特有的安全需求，运营商也可以提供特有的安全解决方案。以下章节将针对文中的 4 种典型边缘计算场景，给出特有的安全解决方案。

8.2 垂直行业特有安全解决方案

8.2.1 智慧工厂安全解决方案

安全是智慧工厂有序发展的必要保障，控制安全是智慧工厂特有安全要求。控制安全是指可编程逻辑控制器（Programmable Logic Control，PLC）等工业控制系统生产控制系统的安全，应从控制协议安全、控制软件安全及控制功能安全三个方面加强安全，可采用的安全

机制包括协议安全加固、软件安全加固、恶意软件防护、补丁升级、漏洞修复、安全监测审计等。另外，智慧工厂的生产数据敏感性高，一般都会有数据不出场需求，所以可以通过部署专属 UPF、设置专门的 DNN 或者 UL CL 等，实现行业客户的数据流智能终结在客户指定的 APP 上。

8.2.2 智能驾驶安全解决方案

安全是智能驾驶持续发展的基本前提，特有的方面为自动驾驶系统安全。自动驾驶系统安全旨在减少已知的潜在意外行为（被控制等）和未知行为潜在行为以达到可接受的残余风险水平。在系统开发阶段，主要措施是假设存在某种潜在危害，并采用迭代开发、验证的方法进行功能实现。在架构设计上，主要采用独立分层和纵深防御安全架构，并集成独立微控制器和专用加密硬件。当车辆在不同边缘计算节点之间切换时，可通过云边协同的方式保证 APP 安全策略的连续性。

8.2.3 智慧城市安全解决方案

智慧城市中的安防监控数据可用于调查取证，监控数据涉及到个人隐私（如居住房间、生活习惯等），所以运营商还应提供隐私保护方案，即对用户的位置信息等使用 AES 等安全算法进行加密保护。

8.2.4 超高清视频安全解决方案

超高清视频的内容会分发给多人观看，应保证内容安全，所以运营商还应提供内容安全方案，即对内容在上载到 MEP 上之前，对内容包的数字签名使用内容提供方的公钥进行验证，并使用关键字搜索等内容安全技术手段，对内容进行安全审核，防止非法内容的传播。

九、 总结

本研究报告分析了运营商边缘计算的安全威胁，提出了边缘计算安全要求、等保要求（见附录），并进一步分析了边缘计算安全关键技术，安全解决方案案例，给运营商边缘计算的安全提供了技术参考。由于运营商边缘计算的网络架构、部署模式以及商业模式等还在逐步发展中，所以本文中的安全威胁、安全要求以及关键技术、解决方案还会随着运营商边缘计算业务的规模商用进行持续更新和优化。

十、 缩略语

缩略语	英文全称	中文含义
AI	Artificial Intelligence	人工智能
EAS	Edge Application Server	边缘应用服务器
EES	Edge Enabler Server	边缘使能服务器
EDNCS	Edge Data Network Configuration Server	边缘数据网络配置服务器
API	Application Programming Interface	应用程序接口
CAPIF	Common API Framework	公共 API 框架

十一、 参考文献

[1] GSMA 智库、ECC《5G 时代的边缘计算：中国的技术和市场发展》

[2] ETSI GS MEC 003 V1.1.1 (2016-03) Mobile Edge Computing (MEC); Framework and Reference Architecture

[3] ETSI GS MEC 017 V1.1.1 (2018-02) Mobile Edge Computing (MEC); Deployment of Mobile Edge Computing in an NFV environment

[4] CCSA 5G 核心网边缘计算总体技术要求

[5] 3GPP TS 23.222 V17.0.0 (2020-03) Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs

[6] 3GPP TR 23.758 V17.0.0 (2019-12) Study on application architecture for enabling Edge Applications

[7] Container Security . 0 (2019-12) Study on application architectu, Anna Belak, Gartner Security & Risk Management Summit 17 –20 June 2019 / National Harbor, MD

十二、 附录：等保要求

12.1 概述

以下参考等保 2.0 云计算扩展要求，提出了边缘计算节点符合等保要求的建议措施。边缘计算节点的等保测评等级建议为三级，也可根据客户需求调整评测级别。

12.2 物理环境安全

【基本要求】

应保证云计算基础设施位于中国境内。

【建议措施】

建议边缘计算节点服务器、存储设备、网络设备、边缘云管理平台、信息系统、等运行业务和承载数据的软硬件均位于中国境内。

12.3 通信网络安全

【基本要求】

a) 应保证云计算平台不承载高于其安全保护等级的业务应用系统;

b) 应实现不同云服务客户虚拟网络之间的隔离;

c) 应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力;

d) 应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略;

e) 应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。

【建议措施】

建议提供边缘计算服务平台和边缘计算服务客户承载的业务应用系统相关定级备案材料，确保边缘计算服务客户承载的业务系统定级不能大于边缘计算服务平台的定级，同时边缘计算服务平台上的不同边缘计算服务客户的边缘应用或应用系统网络是相互隔离的，并且边缘计算服务提供商提供相应的安全接口规范，提供給边缘计算服务客户使用以及第三方安全机构使用，使边缘计算服务客户能够根据业务自身的安全需求在边缘计算服务平台选择相应的安全组件（如：通信传输、边界防护、入侵防范等安全防护机制组件），自主定义相应的安全策略。

12.4 区域边界安全

12.4.1 访问控制

【基本要求】

a) 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则;

b) 应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。

【建议措施】

建议为运行在边缘计算服务平台上业务系统提供设置访问控制的能力,同时边缘计算服务平台和边缘计算服务客户的网络要相互隔离,并且在不同等级的网络区域边界部署访问控制设备，设置访问控制规则，拒绝该非法访问。

12.4.2 入侵防范

【基本要求】

a) 应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等;

b) 应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等;

c) 应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量;

e) 应在检测到网络攻击行为、异常流量情况时进行告警。

【建议措施】

建议边缘计算服务平台能够具备能够检测虚拟机与边缘服务器之间、虚拟机与虚拟机之间、容器与容器之间、边缘节点与外部的异常流量的检测机制，并且对网络攻击行为进行记录，记录应包括攻击类型、攻击时间和攻击流量等内容，并进行告警。有条件可部署抗 APT 攻击系统，网络回溯系统、威胁情报检测系统、入侵检测系统等安全组件。

12.4.3 安全审计

【基本要求】

a) 应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启;

b) 应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。

【建议措施】

建议边缘计算服务客户在远程管理业务系统时能够通过堡垒机或者 vpn 连接再通过堡垒机进行操作，堡垒机具备命令审计对违规命令进行阻断操作数据操作审计机制，对于违规操作可进行阻断处理,同时边缘计算服务平台自身应具备对边缘计算服务客户的虚拟机或容器操作指令进行记录;

12.5 计算环境安全

12.5.1 身份鉴别

【基本要求】

当远程管理云计算平台中设备时,管理终端和云计算平台之间应建立双向身份验证机制;

【建议措施】

建议当对边缘计算服务平台进行远程管理应建立双向身份验证机制。

12.5.2 访问控制

【基本要求】

a) 应保证当虚拟机迁移时，访问控制策略随其迁移;

b) 应允许云服务客户设置不同虚拟机之间的访问控制策略。

【建议措施】

建议边缘计算服务平台配置安全组，微隔离安全防护机制，或者高级的分布式防火墙产品，保证虚拟机与虚拟机能够自主设置访问控制策略，同时虚拟机漂移后策略能够跟随迁移，保证业务系统安全。

12.5.3 入侵防范

【基本要求】

a) 应能检测虚拟机之间的资源隔离失效，并进行告警;

b) 应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警;

c) 应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。

【建议措施】

建议边缘计算服务平台配置入侵防御安全防护机制，或者高级的分布式防火墙产品，对虚拟机到虚拟机之间的攻击进行检测并阻断，同时虚拟机漂移后策略能够跟随迁移，保证业务系统安全。

12.5.4 镜像和快照保护

【基本要求】

a) 应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务;

b) 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改;

c) 应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。

【建议措施】

建议边缘计算服务平台具备统一镜像管理安全服务，如：对镜像进行漏扫扫描、恶意代码检测等等，同时对敏感的资源才用加密、访问控制、完整性校验等技术手段进行保护，防止镜像被恶意篡改或非法访问。

12.5.5 数据完整性和保密性

【基本要求】

a) 应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定;

b) 应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限;

c) 应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施;

d) 应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密

过程;

【建议措施】

建议边缘计算服务平台为边缘计算服务客户提供数据隐私保护服务、数据安全传输服务、密钥服务，确保边缘计算服务客户自信实现数据加解密过程。边缘计算服务提供商为边缘计算服务客户提供数据管理权限授权流程、授权方式、授权内容的机制，同时保证所以数据在中国境内，符合国家相关政策。

12.5.6 数据备份和恢复

【基本要求】

a) 云服务客户应在本地保存其业务数据的备份;

b) 应提供查询云服务客户数据及备份存储位置的能力;

c) 云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致;

d) 应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。

【建议措施】

建议边缘计算服务平台具备数据多副本机制，能够为边缘计算服务客户提供备份机制，把数据能够备份到本地，同时提供数据迁移机制，确保边缘计算服务客户数据能够迁移到本地计算环境或者其它边缘计算服务平台。

12.5.7 剩余信息保护

【基本要求】

a) 应保证虚拟机所使用的内存和存储空间回收时得到完全清除;

b) 云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。

【建议措施】

建议边缘计算服务平台具备安全删除数据的功能或机制,保证边缘计算服务客户删除业务数据时，不会有残留信息。

12.6 安全管理中心

12.6.1 集中管控

【基本要求】

a) 应能对物理资源和虚拟资源按照策略做统一管理调度与分配;

b) 应保证云计算平台管理流量与云服务客户业务流量分离;

c) 应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计;

d) 应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。

e) 边缘计算服务提供商实现边缘计算服务平台统一更新，同时为边缘服务客户提供边缘设备统一更新服务平台。

【建议措施】

建议边缘计算服务平台建立资源统一管理调度与策略分配机制，同时保证边缘计算服务平台的管理流量和业务流量进行分离。边缘计算服务平台能够对基础设施所涉及的硬件或软件（如：编排系统、边缘服务器、边缘管理平台等）进行状态监测、安全监测、版本管理、补丁管理。

12.7 安全建设管理

12.7.1 边缘计算服务提供商选择

【基本要求】

a) 应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力;

b) 应在服务水平协议中规定云服务的各项服务内容和具体技术指标;

c) 应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等;

e) 应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除;

f） 应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除;

【建议措施】

边缘计算服务客户所部署的应用系统等级保护不得高于边缘计算平台的等级，并且能够为边缘计算服务客户提供差异化的安全能力，使其对业务系统进行自主安全防护。边缘计算服务商需要提供服务水平协议或服务合同中确认安全服务商和云服务供应商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任，以及合同到期边缘计算服务提供商完整提供客户数据，并承诺相关数据在边缘计算服务平台上清除，不得泄露边缘计算服务客户数据。

12.7.2 供应链管理

【基本要求】

a) 应确保供应商的选择符合国家有关规定;

b) 应将供应链安全事件信息或安全威胁信息及时传达到云服务客户;

c) 应将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。

【建议措施】

建议边缘计算服务提供商定期供应链安全事件报告或者威胁报告，并及时通知边缘云服务客户。

12.8 安全运维管理

12.8.1 边缘计算环境管理

【基本要求】

云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。

【建议措施】

建议运维人员的运维地点是否位于中国境内，对于从境外对境内　边缘云服务平台实施远程运维操作的行为需判断是否遵循国家相关规定。

SDN/NFV/AI标准与产业推进委员会

地址：北京市海淀区花园北路52号

邮政编码：100191

联系电话：010-62300069

联系邮箱：snai@caict.ac.cn

传真：010-62300094

网址：www.sdnfv.org