针对服务提供商和供应商下一代
业务与技术解决方案的独立市场
研究及竞争分析

HEAVY READING
WHITE PAPER

5G 安全策略考虑因素

Heavy Reading 为瞻博网络制作的白皮书

JUNIPER NETWORKS

作者：HEAVY READING 首席分析师 JIM HODGES

简介

在多个方面，5G 必将成为未来的一项颠覆性技术。它不仅可提升网络速度，还会促使各种各样的新服务和垂直应用诞生，包括对基于物联网 (IoT) 的应用的支持。如今，RAN、核心和传输架构已完成重要创新和设计。然而，在制定 5G 演进策略时，服务提供商必然会考虑独特的设备和应用要求对安全产生的影响，因此安全仍为其最关心的问题。

要在众多垂直行业中成功部署 5G 网络，最基本的问题仍为安全。5G 网络会连接大量的设备，并为具有不同安全需求的不同应用和客户提供服务。5G 应用的多样性及其规模、吞吐量和延迟要求使得难以在安全管理和安全策略的效率、一致性和准确性方面取得平衡。此外，多接入边缘计算 (MEC)、虚拟化、控制用户平面隔离 (CUPS) 和网络切片的应用，为服务提供商带来了新的攻击面，为此，必须加以妥善应对。

本白皮书介绍了 5G 的全新特性、5G 的安全隐患以及服务提供商在向 5G 过渡时需要面对的安全挑战和机遇。

与 4G 相比，5G 有什么特色？

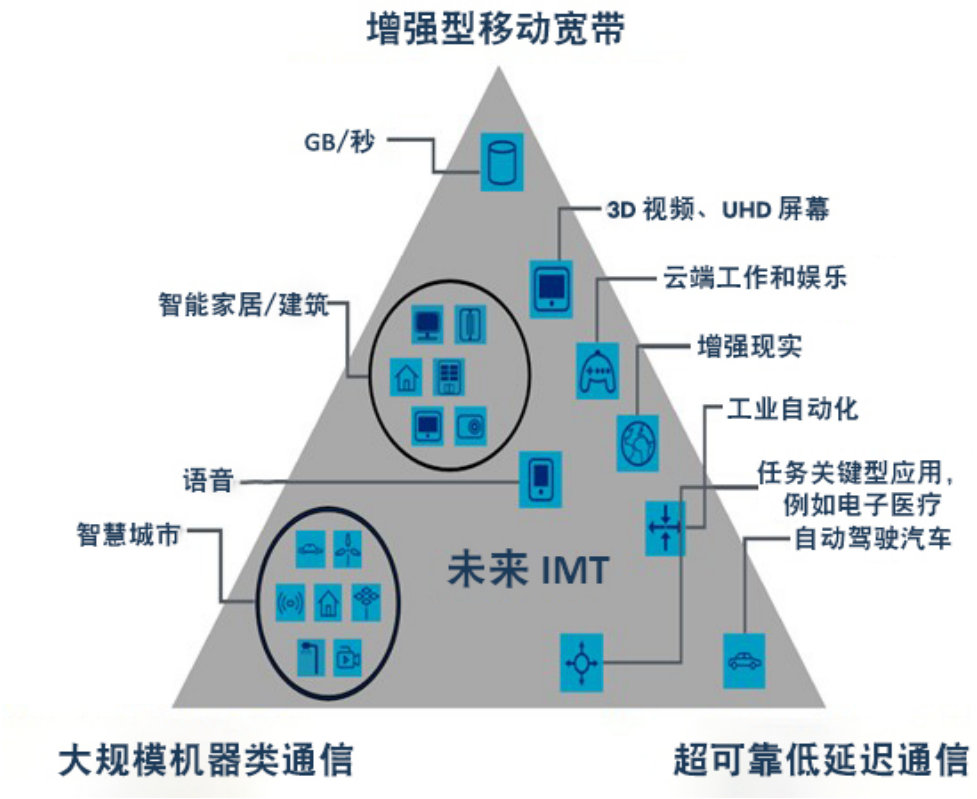
5G 旨在大幅提升性能，包括可实现 1 毫秒延迟和 10 千兆位/秒峰值数据速率，这一切都代表着从 4G 网络的巨大飞跃。这些宏大的性能目标会影响到 5G 网络的安全性能演进。

与前几代相比，5G 是第一个支持多种不同用例的移动架构。为了提供一个结构来组织特定领域及其各种用例，国际电信联盟 (ITU) 发布了 5G 服务层次结构。

如**图 1** 所示，该层次结构将 5G 服务划分为三个特定的领域，它们分别是传统增强型移动宽带 (eMBB) 领域以及两个新领域：大规模机器类通信 (mMTC) 和超可靠低延迟通信 (URLLC)。每个领域都有自己独特的安全要求。通过一个集成的 5G 网络保护如此多样化的接入和服务需求，其难度可想而知。

例如，5G 可实现大规模物联网应用，例如作为智慧城市基础的交通传感器和车辆到基础架构 (V2I) 服务。确保黑客无法访问这些数据、劫持物联网设备或破坏服务至关重要。

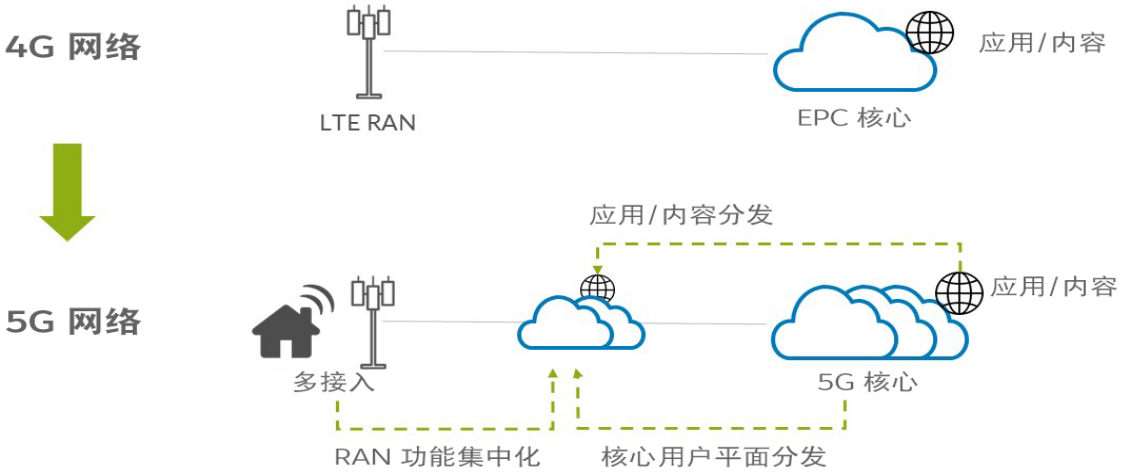
图 1：ITU 5G 服务层次结构



资料来源：ITU-R M.2083-0

为了实现这些不同的性能指标，5G 采用了几种新的网络设计方法，包括 MEC、控制和用户隔离 (CUPS) 以及网络切片。正是由于网络架构的这些变化（如**图 2** 所示），安全架构也必须同步发展。新技术的引入带来了新的攻击面，为此，安全策略必须加以应对。本白皮书的下一部分将分析这些潜在的风险场景。

图 2：从 4G 到 5G：网络架构的演进



资料来源：5G Americas 发布的《5G 安全演进》(The Evolution of Security in 5G) 数据解读

策略考虑因素 1：安全性能和安全运维必须同步提升

与 4G 一样，5G 也同样不是一步建成的。相反，5G 将与 4G 并行发展，并在未来十年分阶段演进。因此未来数年，4G 仍继续存在。

据 GSMA 预测，到 2025 年，4G 仍将在全球网络连接中占据 59% 的份额，恰恰证明了这一点。* 大多数 5G 部署将从 5G 非独立 (NSA) 架构开始，将 5G RAN 与现有 4G 核心搭配实施，以便更快地启动 5G 服务。

因此，服务提供商的 5G 安全战略必须首先评估现有的 4G 网络安全性，以确保 4G 与 5G 的实施保持一致。从逻辑上说，要开始此评估，首先就要确定其 4G 网络安全性是否能够支持 5G NSA 带来的网络容量增加。在大多数情况下，安全性要求升级物理基础架构以实现纵向扩展，同时要求升级虚拟基础架构以实现横向扩展和纵向扩展。

如果不进行这类投资来扩展性能，安全性将成为整体网络性能的瓶颈。在产品层面上，应评估当前移动安全用例（如 3G/4G Gi/SGi 防火墙、安全网关 (SEG) 和 Gp/S8 漫游防火墙）的吞吐量、连接规模和会话建立速度等安全性能。

另外，还需要检查分布式拒绝服务 (DDoS) 保护用例。随着物联网的兴起，互连设备因规模庞大而安全能力普遍有限迅速成为黑客的首选目标。

例如，仅 2016 年，Mirai 物联网僵尸网络在全球就破坏了近 100,000 台互连设备。这些设备会对域名系统 (DNS) 服务提供商 Dyn 发起 DDoS 攻击，其峰值速率为每秒 1.2 兆兆位 (Tbit/秒)，从而造成 4 个小时以上的服务中断和停机。Mirai 事件只不过是个开端。从那以后，JenX、Hajime、Satori 和 Reaper 等变种相继出现，并变得越来越复杂，越来越难以防御。

不幸的是，5G 技术会通过增加可用带宽来提供一个更强大的网络，这一点却会助力遭到入侵的设备生成攻击流量，从而使问题雪上加霜。随着 DDoS 容量耗尽攻击的频率、规模和复杂度不断提升，带外清洗中心和人工干预等传统防御措施已变得力不从心，并且成本高昂。

发生大规模容量耗尽攻击时，将可疑流量重定向到清洗中心会增加延迟并带来巨大的财务负担，因为缓解成本与数据流量的大小直接相关。服务提供商应考虑采用现代化的新型 DDoS 防护措施，其中包括遥测、机器分析和基于网络的缓解，以自动执行更智能、更经济的检测和缓解过程。

除性能外，安全运维还必须扩展和支持具有物理网络功能 (PNF) 和虚拟网络功能 (VNF) 的分布式电信云环境。因此，需要一个统一的安全管理系统来管理物理和虚拟域，并为这些域提供一个统一视图。换句话说，安全管理需要实现全方位的系统级可见性。另一方面，此战略还需要通过可编程的安全策略来实现自动化策略编排，以确保网络安全、可靠，从而满足服务级别协议的要求。

此外，5G 基础架构的异构性和复杂性还要求在多个域的多个层面（例如切片、服务或资源）应用安全性。因此，服务提供商要在安全运维上防患于未然，安全自动化和编排至关重要。

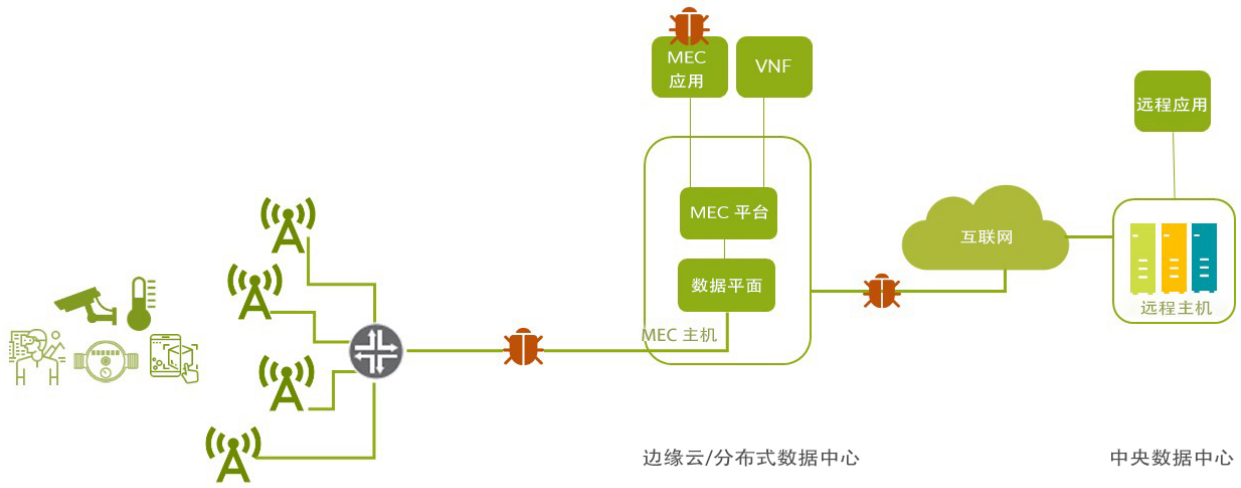
* GSM 协会发布的《2019 移动经济研究报告》(*The Mobile Economy 2019*)。

策略考虑因素 2：网络架构的演进和新兴技术的兴起带来了新的攻击面

边缘计算作为云计算的演进，可以使应用托管和数据处理从集中式数据中心转向网络边缘，且更接近移动应用。要满足 5G 的苛刻要求，边缘计算十分重要，尤其是那些注重低延迟和带宽效率的用例更是如此。

ETSI 的多接入边缘计算 (MEC) 行业规范组 (ISG) 为 MEC 定义了一套技术标准。这些标准支持多种不同的技术，包括 5G NSA、分布式计算以及网络设备和计算服务器的虚拟化。所有这些技术都可在一个开放式生态系统中进行互操作，而服务提供商可以在该生态系统中部署分布式应用。然而，MEC 环境的异构性和多样性（**如图 3 所示**）为恶意攻击和隐私泄露带来了新的攻击面，并可能对整个 MEC 系统构成重大威胁。

图 3：MEC 攻击面



资料来源：瞻博网络

一种可能的部署模型是，在与某些 VNF 相同的物理平台上运行 MEC 应用。这些 MEC 应用可能是不受移动服务提供商控制的第三方应用，因此会带来一个问题，即这些应用可能会耗尽网络功能所需的资源。

另外，应用设计不当可能还会为黑客创造新的攻击途径，供其潜入分布式数据中心并影响该平台上运行的网络功能。同样，攻击者可以通过插入恶意应用来实现同一目的。如果较为敏感的安全资产在边缘的虚拟化功能方面遭到破坏，则攻击者可能会恶意利用这些资产来获得连接，或者实施欺诈、窃听或数据操纵攻击。

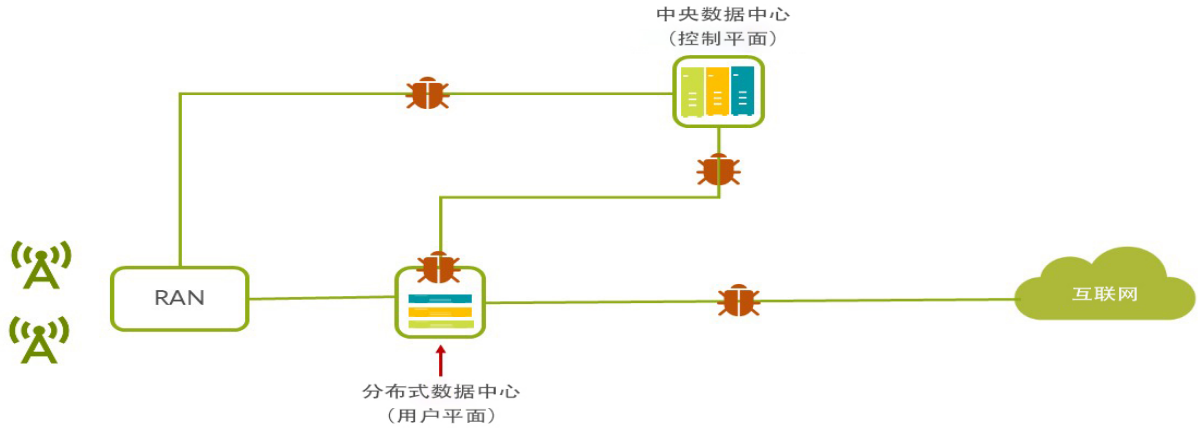
这些攻击方法不一定是全新的。但由于 MEC 架构是全新的，安全问题的潜在破坏性和严重性可能得不到充分的认识。因此，在选择供应商时以及在部署商用大规模边缘云之前，服务提供商应确保安全解决方案足够灵活，以便在初始部署时可以应对各种威胁问题。

分布式核心攻击面

在 4G 演进型分组核心 (EPC) 中引入 CUPS 可视为迈向 5G 核心架构的重要一步。CUPS 是 3GPP 第 14 版标准的一部分，因为它能够利用现有的 4G EPC 在网络上分配用户平面资源。在最终部署 5G 核心网络基于新服务的架构之前，可以通过这种方式分配资源。CUPS 可以使运营商独立地定位和扩展 EPC 节点的控制平面和用户平面资源。它适用于视频等高带宽应用。由于核心用户平面更靠近最终用户，因此运营商无需将流量一直回传到中央数据中心，从而降低了延迟和回传成本。

虽然 CUPS 本身不是 5G 功能，但它遵循 5G 网络部署所固有的新信任边界和威胁面。这意味着，包括 Sx 和 SGi 在内的任何接口均可能成为发起 DoS 或 DDoS 攻击的目标，如**图 4** 所示。

图 4：分布式核心攻击场景



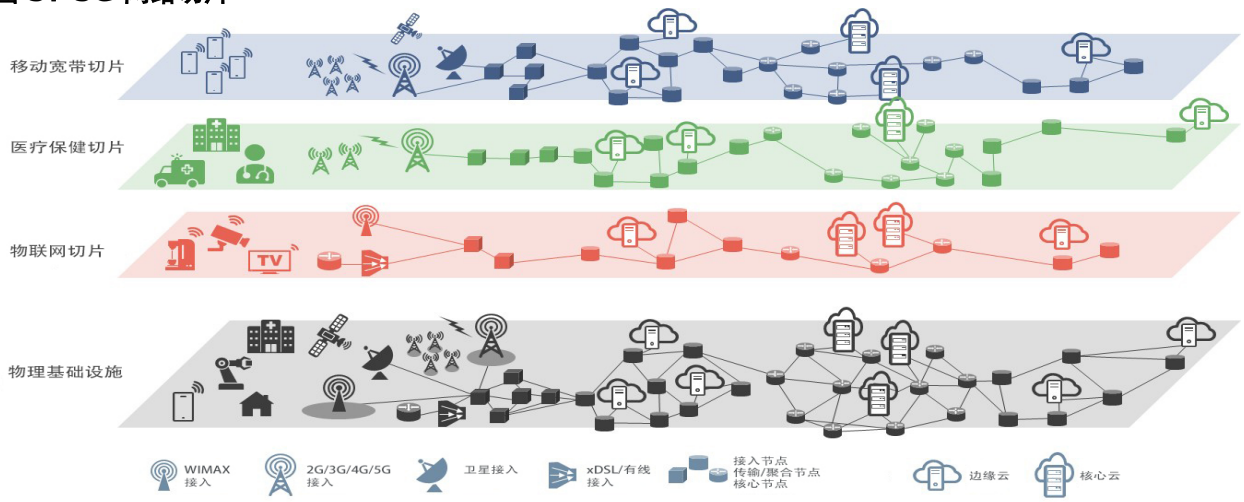
资料来源：瞻博网络

网络切片攻击面

网络切片是一种特定的虚拟化形式，可以使多个逻辑网络在共享物理网络基础架构上运行。通过网络切片，移动服务提供商可以对其网络资源进行分区，以处理不同用户具有不同性能和功能要求的多种用例。此外，他们还可以在一个物理基础架构上复用这些用例。

例如，现在可以创建不同的应用切片类型来支持多种服务，包括工业物联网和医疗保健等垂直市场应用，如**图 5** 所示。

图 5：5G 网络切片



资料来源：IEEE 发布的《通过 SDN/NFV 实现 5G 网络切片：概念、架构和挑战》(Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges)

由于 5G 将支持多种用例和新服务，因此网络切片有望在 5G 网络中发挥关键作用。这些新的用例和服务会对网络功能提出不同的要求。如 ITU 5G 服务层次结构所示，在吞吐量、服务质量、延迟和安全性等方面，性能要求可能有很大差异（参见**图 1**）。

一个经常提到的 5G 示例是，通过共享给定的物理网络来同时运行大规模物联网、移动宽带 (MBB) 和 URLLC 应用。比如说，物联网通常支持非常多的设备，但每台设备的吞吐量可能非常低。相比之下，MBB 则支持较少的设备，但每台设备都会发送或接收高带宽内容。

这些各不相同的服务切片性能特征会直接影响安全协议的选择以及策略的实施。例如，一个切片中的服务可能需要极长的设备电池续航时间，因此会以其他某种方式限制安全协议（例如，重新身份验证的频率）。又比如，一个切片中的服务可能非常注重隐私，因此需要非常密集地执行安全过程（例如，频繁地重新分配临时身份）。

此外，服务提供商还需要考虑这些切片彼此隔离的程度。不法分子会通过安全度"较低"的切片获得更广泛的网络访问，这会构成一大安全问题。

在如**图 6** 所示的攻击场景中，攻击者会耗尽一个切片的资源。在这种情况下，攻击者可能会耗尽多个切片共有的资源，从而导致其他切片遭受 DoS 攻击或发生服务降级。

图 6：切片容量耗尽攻击场景

资料来源：瞻博网络

策略考虑因素 3：安全性作为差异化优势推动收入增长

服务提供商 5G 安全策略的最后一个考虑因素是，如何利用安全性来打造网络部署的独特优势并从中获得商业回报。

对于包括制造业和交通运输业在内的众多需要大量部署物联网应用的行业来说，采用网络切片等 5G 功能有利于推动其收入大幅增长。与消费者不同，这些垂直行业中有许多行业对安全性的要求更为严格。因此，许多行业已建立了自己的专用连接网络。为了使 5G 产品成功进入这些垂直市场，服务提供商应突显其在安全方面的能力，以满足这些客户的需求并解决他们关心的问题。

在物联网方面，服务提供商会通过一个有效的切入点谈及企业物联网，那就是网络连接。虽然物联网连接本身潜力巨大，但服务提供商还可以利用其他许多机会。例如，安全性。安全始终是企业采用物联网的首要关注点，同时也是一大技术障碍。

由于在这些行业中，许多企业可能并不具备相关内部技能来保护其应用，因此他们会求助于服务提供商来满足其独特的安全要求。这一步十分重要，它可以使服务提供商不仅限于提供基本连接服务，还可以不断演进，为极具吸引力的产品提供物联网连接和安全性。

另一方面，5G 安全即服务（SECaaS）也可以让安全性成为推动收入增长的一个因素。5G 之所以极具吸引力，很重要的一点是，它可以使垂直行业通过使用共享基础架构降低成本/提高效率。某些垂直行业可能仍希望自行控制安全性，而另一些行业则可能会选择将某些安全服务外包给 5G 网络来进一步节省成本。这些服务可以包括在网络中实施策略（防火墙、设备访问控制）和/或使用网络提供的身份验证/地理定位功能。

借助软件定义的网络和虚拟化技术，可以为特定应用或用户部署安全配置。通过将应用专用的网络连接彼此隔离，5G 服务提供商可以为用户提供个性化的安全功能，并将其作为增值服务，例如监控分析和深度数据包检测。

同样，对于服务提供商在其 MEC/边缘云环境中托管第三方应用的情形，还可以为这些应用提供安全/保障服务。其中一些服务示例可能包括，在安装时以及升级和服务器重新启动期间，对应用执行完整性保证检查。再比如，可以将安全服务 API 公开给足够可信的第三方 MEC 应用以进行用户识别。

总结

安全性是成功交付 5G 服务的重要一环。服务提供商必须将其安全策略作为 5G 演进路线图的重要部分进行妥善规划。

当前的移动网络安全性能和运维必须能够纵向扩展和横向扩展来满足 5G 要求，而不是成为瓶颈。此外，由于边缘计算、CUPS/分布式核心和网络切片带来了新的攻击面，服务提供商必须采用适当的安全措施来缓解威胁。最后，5G 和物联网时代的安全性不应仅视为一种义务。服务提供商应考虑将安全性定位为一种服务差异化优势，以及一项重要的创收因素。