把握5G未来

网络安全是实现5G广阔前景的关键

pwc 普华永道

目录

概要：

重视机遇和安全的5G世界 3

进入5G时代 4

弹性设计 8

结论：

信任、弹性和实施，紧扣5G时代脉动 11

概要

重视机遇和安全的5G世界

世界各地的联网设备正在改变人们的生活和工作方式。这一变革中不可或缺的部分是将这些设备连接起来并使其能够彼此“交谈”的通信网络。在这一背景下，速度更快、带宽更高的5G网络是一项重大的进步，但仍需我们对其客观看待。尽管围绕5G的宣传甚广，但事实上，4G以及各种低功耗广域网（LPWAN）已经实现了5G所赋能的诸多服务项目。

即便如此，支持5G的核心技术在一些重要方面与以往相比仍有所突破，包括从根本上重新定义了通信网络的概念。前四代移动通信技术均基于物理架构实现。虽然5G也涉及到新硬件，但它首先是一个虚拟网络，并最终将实现网络和无线通信的融合。尽管这一突破将掀起一波创新浪潮，但5G带来的最大影响或许将通过无线技术的新用途或增强功能才能感受到：可能包括第四次工业革命（4IR）基础设施、智慧城市、自动驾驶汽车、远程手术和更强大的全新人工智能（AI）系统。

而改变就发生在新冠肺炎疫情这一全球性公共卫生紧急事件的大背景下。由于政府颁布的“居家令”，很多人将利用愈发依赖5G网络的通信技术在家办公。那些在数字化转型方面表现更优异的企业告诉我们，他们在技术、网络安全和弹性工作能力方面的投资，在应对新冠肺炎疫情时取得了回报。

然而这些变化也导致更为严格的网络安全审查。有评论人士认为，5G会增多受到对手网络攻击的潜在对象，因为与以往技术相比，5G连接的设备更多，且具有分布式边缘计算能力。不过，5G可能产生的漏洞更多来自于5G生态系统的其他因素，尤其是终端设备的安全。好消息是，5G网络面临的这些安全挑战是可以克服的，这为各方参与全球创新、实现5G技术应用的广阔前景提供了坚实基础。

进入 5G 时代

我们即将迎来一个由5G赋能的海量物联网（mIoT）支持和连接的世界。在这个世界，5G将为我们的智慧城市、4IR运营模式、智能家居、智能交通、智能医疗和无数其他潜在应用提供基础。普华永道最近在与世界经济论坛的合作中，发表了题为《5G的影响：创造跨行业和社会新价值》的报告，其中探讨了现有5G技术的广泛应用正如何改变商业环境。

如其他任何新技术一样，5G技术的引入要求我们重新审视网络安全方面的举措，但5G对于网络安全的高要求不应分散规划5G发展的组织、政府、城市和行业对5G重大机遇的注意力。事实上，通过了解和应对5G的特定风险，企业可以建立更强的弹性，并将5G作为公司创造收入和利润的突破点，以及为社会做出贡献的一股重要力量。随着新冠肺炎疫情以前所未有的方式改变着人们的生活和工作方式，这一新技术在当下变得更加重要。

谈到5G的不同之处，数字本身就能说明一切。5G的技术属性（见下页总结）意味着5G的速度比4G快大约100倍，并且可以连接更多的设备。此外，超低延迟（即接收请求响应所需的时间）也进一步扩大了5G的优势。

虽然消费者对于能在几秒钟内下载超高清电影的前景感到兴奋，但这些技术属性的真正益处将通过广泛的创新应用得到体现。这些创新应用不仅会改变我们娱乐休闲的方式，还将改变我们的工作方式和地点，改变我们出行和保持健康的方式——在5G应用中嵌入个性化的人工智能应用正发挥着越来越大的作用，帮助我们更加智能地应对日常生活和工作。

5G之所以能够实现其广阔前景，主要因为5G是一个通过分布式数字路由器运行的基于软件的网络，并通过将任务迁移至边缘来优化其处理速度和能力。这与前几代移动技术所采用的“轴辐式”（hub and spoke）配置形成鲜明对比。

“零信任”方法

确保5G网络安全是5G为消费者、企业和整个社会充分创造潜在效益，以及确保最终用户安全的关键。在新冠肺炎疫情大流行期间，随着越来越多的企业采取远程办公政策以及远程医疗应用的增加，5G网络安全变得更加重要。举例来说，员工在办公室以外工作导致企业IT基础设施外延，在受到网络安全攻击时，系统脆弱性会进一步加剧。此外，病人通过平板电脑、笔记本电脑或手机与医疗专家联系时，也需要确保病人敏感信息的安全。

要保护包括5G在内的所有移动网络免受网络安全威胁，关键的第一步是要了解漏洞有可能出现在哪里。漏洞主要出现在网络节点上，在这些节点上风险会从网络中的一个元素转移到另一个元素。与4G一样，在5G网络中，不同的企业通常会处于这些风险转移的任一侧，那么至关重要的就是要建立一个可以确保从网络一端到另一端始终保持安全的协调方式。考虑到技术工具的迅速发展，企业和网络犯罪分子也都在寻求利用这些发展优势，因此上述协调方式还需要灵活变通。

5G生态系统中所有的参与者，包括移动运营商、网络供应商、系统集成商和终端企业，应该在其被允许进入网络之前，先识别、分析和评估其每个组件的健康状况，并基于评估结果，在允许范围内对连接5G服务进行一些限制。这可以通过基于以下因素的战略来实现：

1. **零信任方法。**对于所有设备和软件，端到端的可靠安全态势将有助于减少整个5G生态系统的风险敞口。在连接到网络或资源之前，需要对设备的安全级别进行评估，然后，设备仅允许连接到资源，并且

5G技术属性

5G为网络的诸多方面带来了重大变化，包括核心和管理系统，以及从无线电到应用程序在内的所有协议层。5G的技术属性包括：

- **网络切片：**使服务提供商能够为特定用户组提供网络即服务（NaaS），让其根据具体需求灵活管理设备和服务。
- **增强型移动宽带（1-20 Gbps）：**可支持4K或8K分辨率的3D视频传输、在线游戏等应用。
- **超低延迟（<1ms）：**对于增强现实（AR）和虚拟现实（VR）、远程医疗和保健、智能交通和工业自动化等任务关键型服务非常重要。
- **大规模设备连接：**可支持车辆、移动用户、企业、物联网等设备连接。
- **高可用性和密集覆盖：**使5G能够为数十亿不同用户提供无限连接。
- **低能耗：**机器对机器（ M2M ）通信的电池使用寿命可达10年。

为了实现这些功能，5G配备了全新的空中接口，支持异构网络接入并且支持可变带宽。分组核心网的升级也正在进行，这样传统网络和5G移动服务可以共享基础设施，提升服务交付速度和运营效率。

应基于访问需求及设备的安全健康水平决定是否允许设备访问资源。此外，对所有软件配置，从核心到物联网设备，从固件到云，都必须保持一定的怀疑。在网络构建和部署之前，必须对资源中心进行验证，对代码库进行检查，以排除恶意软件。应用程序编程接口（API）应该根据风险级别进行分区和访问控制。

2. **通用加密。**为了尽可能降低数据泄露或损坏风险，电信运营商和其他5G参与者应该利用强大的加密方法来保护端点与服务之间的通信。这包括采用灵活的加密方法，并随着标准和风险的演变而逐渐增强加密。集中式密钥管理过程将有助于减少“中间人”攻击，即攻击者干预通信双方建立的联系，令双方认为他们是在直接与对方通信。

3. **人工智能编排。**机器学习（ML）和人工智能将在识别和降低时刻变化的风险方面发挥至关重要的作用，它们能够提供具有出色响应速度和准确性的洞见和智慧，以管理超密集机器类型通信和超低延迟应用的安全策略。人工智能和机器学习技术将在整个5G架构中被用于安全编排，包括流量分析、深度数据包检测（DPI）、威胁识别和感染隔离等活动。

人工智能：5G网络、应用和设备核心的强大工具

随着电信运营商开始部署5G，他们将不得不面对前所未有的网络复杂性。推动网络复杂性的关键因素包括5G网络的高密度分布、具有挑战性的大规模天线阵列配置以及整个网络基础设施的升级。电信公司还需要做好持续开发解决方案的准备，以满足来自物联网和相关智能系统的各种需求（包括已预测和未预测的）。这就要求对网络管理采取一种日益灵活且响应迅速的方法。

人工智能通过促进网络质量的动态参与，做到比当前更快速地检测和纠正网络问题，在应对挑战过程中发挥着关键作用。要实现网络切片的全部应用前景，人工智能也是必要的：它将帮助运营商优化其切片策略，反馈有关评价、评估和确定切片分配的工作。

放眼网络之外，最近的普华永道科技、媒体和通信出版刊物强调，人工智能和5G的融合将催生一波新的网联设备，并将在两个关键方面重新定义“智能”一词。首先，这些设备的用户界面将不仅基于触控，并且无论是否有触控功能，都会越来越多地基于语音操作。其次，设备将使用分离应用程序来触发用户要求的特定任务，并应用人工智能驱动的算法来预测用户需求并主动满足这些要求。

通过这些进步，人工智能和5G将给终端用户带来一系列影响。一是5G传输的数据会形成更加自动化和定制化的产品和服务，这将带来更大程度的个性化。二是随着人工智能增强人类能力，并在人类和机器之间建立更紧密的联系，人们的数字体验将变得更加亲近和人性化。总之，这些影响将推动生产力以及工作、空闲带宽的大幅提高，人们可以自由地进行他们真正感兴趣的活动。

人工智能还可以在5G世界的网络安全中发挥作用。这是因为人工智能和机器学习为组织提供了强大的新工具，以保护系统免受恶意攻击，亦即能够帮助组织对抗网络攻击者使用的日益复杂的工具。在普华永道看来，最有效的防御手段是利用人工智能对数据进行分类，并标记出来进行进一步的人工分析，然后再将人工分析反馈给人工智能，从而改善其未来预测。这一良性循环会为关键系统提供最佳防御，即为创新创造一个可靠安全的基础，从而在所有用例中发挥5G的广阔前景。

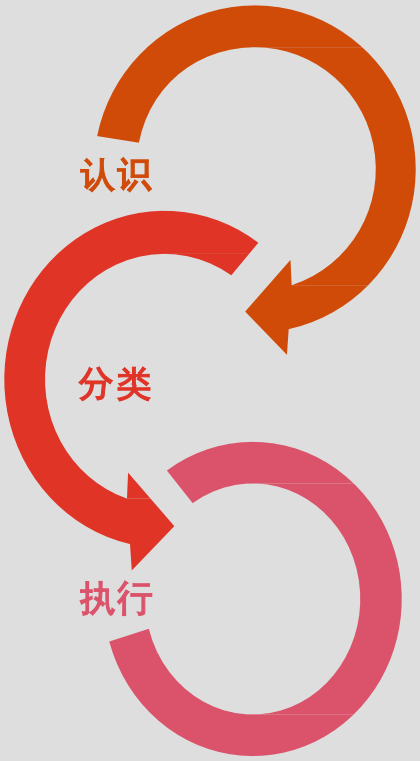
欲使包括5G在内的任何移动网络免遭网络威胁，关键的第一步是要了解漏洞有可能在哪里出现。

如果运用得当，该战略将有助于各组织共同协作确保5G环境安全，同时不会过度影响5G生态系统中各企业服务客户并与合作伙伴交互的能力。对于上述战略实施问题，一种行之有效的方法是采用被称为“零信任架构（ZTA）”的身份认证驱动模式。这一全面的信息和网络架构安全模式解决了“何人、何事、何处、为何以及如何”访问关键数据和网络架构资产的问题。

在零信任架构模式下，安全功能无论其部署于何处或者采用何种连接方法，都是为了执行策略并保护所有用户、设备、应用程序和数据资源，以及它们之间的通信流量。图1中描述的ACE模型（认识、分类、执行）可以帮助企业构建其零信任架构。

图1：为5G网络采用零信任理念

全面的信息和网络架构安全模式，必须解决“何人、何事、何处、为何以及如何”访问关键数据和网络架构资产的问题。这种以身份认证为驱动的信任体系通常称为“零信任架构（ZTA）”，使用ACE模型来部署安全功能，以用来执行策略并保护所有用户、设备、应用程序和数据资源，以及它们之间的通信流量，无论其位于何处或采用何种连接方法。



概述：发现并概述网络上的每个端点和应用程序。
评估：确定设备的安全态势。
识别：了解连接到网络的是哪些用户和设备、以及连接方式。
学习：通过监控和记录，持续评估设备和用户的行为。

权衡：评估受保护资产、数据和应用程序的价值、重要性。
风险评估：根据安全漏洞的影响进行风险评估。
分配群组：将数据、用户和端点映射到数据分类桶、组。
确定应用程序优先级：使用业务特权、数据分类桶和相关的风险评估来生成与优先级一致的安全策略。

限制：根据安全策略确定访问资格和执行边界。
隔离：确定如何检测、控制和隔离数据泄露和侵犯。
通知：建立数据泄露和安全侵害的通知机制。
细分：为基于身份认证的应用程序、端点和用户细分定义框架。
执行：根据定义的安全策略在执行边界内实现身份感知控制。

来源：普华永道分析

弹性设计

在5G时代，由零信任安全方法及其相关架构支持的企业能够很好地构建和嵌入网络弹性。普华永道最新的《数字信任洞察》报告对如何实现这一目标提供了极具价值的指导，该报告主要基于来自全球逾3,500家企业的调查数据。

研究发现，具有高网络弹性的企业在与制定弹性策略相关的三个领域的排名中均跻身前25%。从根本上讲，正是因为对“弹性设计”的重视使其遥遥领先于其他企业。因此，他们可以做到以下三点：

- **提高数据资产的可见性。**高弹性企业始终如一地跟踪其数据资产和现有流程如何影响其业务核心。《数字信任洞察》报告发现，91%的高弹性企业拥有一份准确的资产清单，并持续滚动更新。与之相比，其他受访企业中只有47%能够做到。这份清单还必须包含与第三方进行的合作，尤其是在业务要求与一系列供应商进行合作的情况下，需知这在5G世界中几乎是不可避免的。
- 在弹性方面处于落后水平的企业可以采取行动迎头赶上：通过构建自动化实时资产清单以及映射过程，实现整个网络持续且准确的可见性。低弹性企业也可以由此开始解决他们的漏洞。
- **测试容忍度。**高弹性企业着眼于大局，并且知道自己在处理风险情况方面的容忍度。我们的研究发现，在关键业务运营受到网络攻击面临中断时，只有不到三分之一的企业能够利用冲击容忍度，或企业为应对业务服务中断所准备的最大影响度来保护自己。而参与调查的其他一些企业，哪怕是规模最大的，在面临中断发生时，其关键业务服务也处于危险境地。

通过识别关键业务服务，使用指标来定义其对风险的容忍度，通过测试并将容忍度结果映射回业务服务，企业就能够应对不断变化的网络威胁。

- **调整和完善。**高弹性企业不断改进其商业策略：通过提高数据资产的可见性和测试风险容忍度，企业弹性不断增强。然而，面对技术的快速发展，我们发现只有34%的高弹性企业能够适应正在发生的变化。
- 为了确保全方位的保护，三分之一的高弹性企业在采用新技术时提升了弹性能力。这些企业通常依靠专门的团队来监控核心资产的性能和IT依赖性，并且能够利用从网络问题导致的中断所获得的经验教训，快速并持续重新设计其业务服务。作为准备工作的一部分，企业应通过自动化和流程编排来获得先进的威胁捕获能力。

总之，基于以上三个方面，企业能够从传统的灾难恢复和业务连续性模式转向弹性设计——这是诸多企业在新冠肺炎疫情危机复苏的过程中所需要做的事。弹性设计已经证明其可以保护组织、运营和系统免受网络威胁，这在5G和其他环境中同样重要且有效。

在弹性方面处于落后水平的企业可以采取行动迎头赶上：通过构建自动化实时资产清单以及映射过程，实现整个网络持续且准确的可见性。低弹性企业也可以由此开始解决他们的漏洞。

智慧城市：赋能未来城市环境

随着城市人口持续快速增长，传统基础设施面临的压力与日俱增，世界各地的城市都在竞相发展智慧城市。英国标准协会（BSI）将智慧城市定义为“在建成环境中对实体、数字和人类系统进行有效整合，从而为市民提供可持续、美好和包容性的未来”。这是一个非常恰当的定义，它强调了智慧城市在创建信息物理系统（CPS）的过程中应如何实现物质和数字世界的融合。

数字化可以增强一系列城市系统，以更有效地满足市民的需要——最明显的是在运输和楼宇设施管理等领域，以及在能源、水域、公共安全、废物管理和污染控制等方面。数字化还可以帮助应对诸如新冠肺炎大流行等公共卫生突发事件，通过建立模型、检测和预测，向政府提供实时数据，帮助其做出更明智的决策。5G将通过提供超高速、低延迟的平台来支持这些服务，从而帮助实现智慧城市的广阔前景。

维持智慧城市系统的安全显然至关重要，无论是涉及到运营基础设施，还是保护市民的个人数据隐私。只要我们确保所有智慧城市的系统和网络连接的设计、评估和调节都从根本上以安全为核心并基于零信任架构，那么上述目标就能实现。

结论：信任、弹性和实施，紧扣5G时代脉动

人们常说5G将改变世界，但重要的是保持清醒，不要被天花乱坠的宣传冲昏头脑。虽然世界正在发生明显的变化，但真正推动这种变化的是智能网联设备的普遍可用性。尽管这些设备所连接的网络很重要，但它也只是这个新环境的一部分。

尽管如此，5G的出现毫无疑问代表着网络安全领域的一个转变。在未来关键的工业和社会网络中，5G将成为一个重要媒介，自动化互联组件的工作流程和决策链将通过它来传播。如果没有5G，数量不断增长的数百万台网联设备将毫无用处，尤其对自动驾驶汽车等应用来说，网联设备的低延迟和超高速是先决条件。5G作为许多智能网联设备的“联网”组件，绝非言过其实。

在这种背景下，没有人会质疑在5G生态系统中有效确保网络安全的必要性。然而，值得注意的是，许多通常归咎于5G的安全漏洞实际上并非5G所特有。如果连接到5G网络的设备、加密算法或人工智能引擎被侵入或遭到破坏，这对5G运营商和用户来说都是一个问题，并非5G技术本身导致。在5G世界中，有效确保网络安全要求价值链中的每一个参与者都要发挥自己的作用。这就是我们提出应采取一种零信任架构并辅以“弹性设计”支持的原因——目的是将网络安全置于5G部署的核心。

为达到这一目的，企业领导人需要关注构建网络安全的三个基础：**信任**，以推动网络安全措施的采用；**弹性**，以预防、安然度过破坏性的网络攻击，并在攻击后恢复；**实施**，快速行动以解决新生和现有的威胁。以上三点是构建稳健网络战略的基础，可确保企业快速、安全地部署5G，让个人、企业和社会作为一个整体，自信安全地享受5G这一强大新兴技术的巨大潜力。

联系方式

欲进一步了解普华永道如何赋能您的5G未来之旅，请联系：

科技、媒体及通信

中国

周伟然
普华永道全球科技、媒体及通信行业主管合伙人
+86（755）8261 8886
wilson.wy.chow@cn.pwc.com

高建斌
普华永道中国科技、媒体及通信行业主管合伙人
+86（21）2323 3362
gao.jianbin@cn.pwc.com

英国

Kirolous Zikry
普华永道英国科技、媒体及通信行业高级经理
+44（77）2563 3388
kirolous.s.zikry@pwc.com

网络安全和隐私保护

中国

黄景深
普华永道中国网络安全和隐私保护服务主管合伙人
+852 2289 2719
kenneth.ks.wong@hk.pwc.com

李睿
普华永道中国网络安全和隐私保护服务主管合伙人
+86（10）6533 2312
lisa.ra.li@cn.pwc.com

李扬
普华永道中国网络安全和隐私保护服务主管合伙人
+86（10）6533 7800
dennis.y.li@cn.pwc.com

英国

Richard Horne
普华永道全球网络安全和隐私保护服务主管合伙人
+44（77）7555 3373
richard.horne@pwc.com

Grant Waterfall
普华永道欧洲，中东和非洲网络安全和隐私保护服务主管合伙人
+44 77 1144 5396
grant.r.waterfall@pwc.com

加拿大

Marin Ivezic
普华永道加拿大工业和物联网网络安全和隐私保护服务合伙人
+1（416）687 8672
m.ivezic@pwc.com

匈牙利

Peter Durojaiye
普华永道匈牙利网络影响中心总监
+36（70）685 0360
peter.a.durojaiye@pwc.com

www.pwccn.com

普华永道秉承“解决重要问题，营造社会诚信”的企业使命。我们各成员机构组成的网络遍及157个国家和地区，有超过27.6万名员工，致力于在审计、咨询及税务领域提供高质量的服务。如有业务需求或欲知详情，请浏览 www.pwc.com。

本文仅为提供一般性信息之目的，不应用于替代专业咨询者提供的咨询意见。