FAST TRACK TO THE 5G EDGE

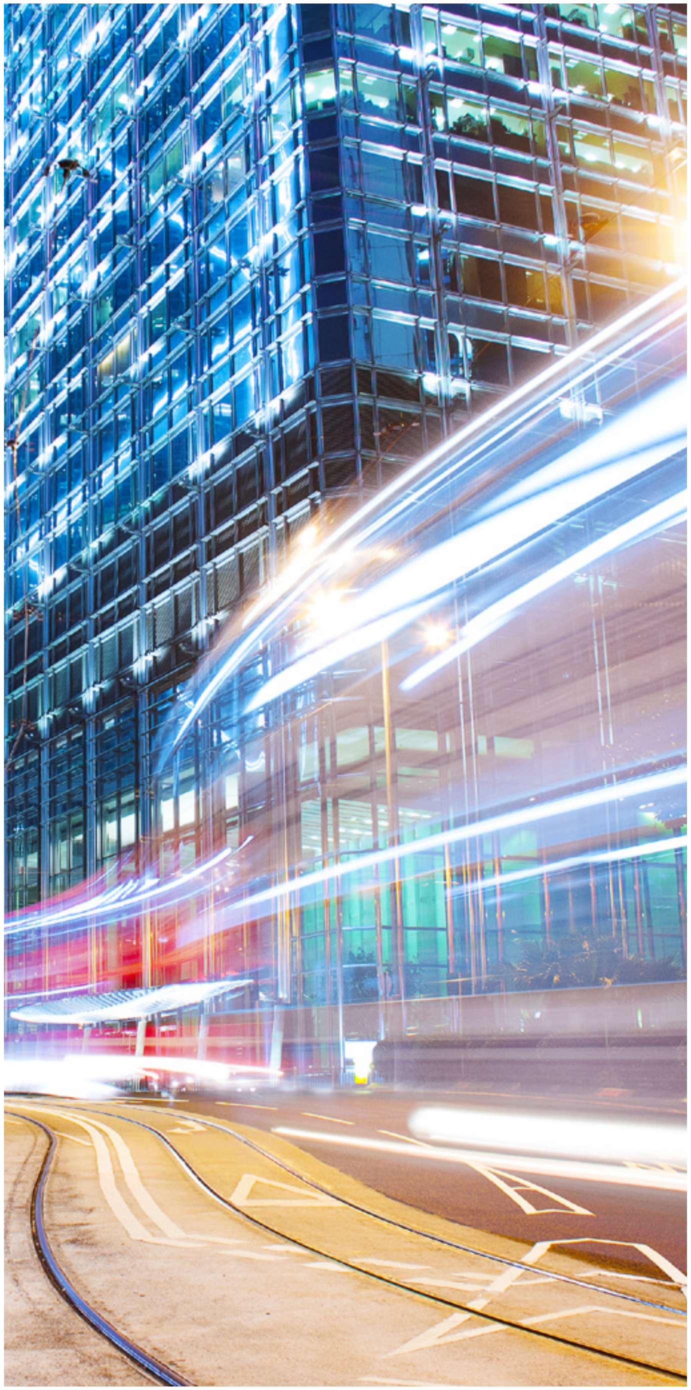
CLOUD-NATIVE INFRASTRUCTURE ALL THE WAY TO THE EDGE

INTRODUCTION

5G Standalone (SA) introduces a new operational and service paradigm for service providers. It eliminates the hardware-centric, centralized architectures of the past and embraces a cloud-native, distributed infrastructure for building and operating networks.

The approach uses microservices, running in software containers on a service-based architecture (SBA), to deliver services all the way from the core to the edge and far edges of the network. Edge services, deployed in multi-access edge computing (MEC) environments close to customers, ensure customers receive the best possible network performance and quality.

Service providers also have much to gain from this architectural shift. With a cloud-native architecture, you can achieve the type of digital transformation enterprise companies need to become more efficient and competitive. You can use the capability to quickly roll out and upgrade services to hundreds and thousands of edge locations. You can also operate your networks with the agility and scalability we normally associate with hyperscale companies like Google, Amazon Web Services, Microsoft Azure, or Apple. Having a cloud-native SBA architecture all the way to the edge is an essential building block in a 5G network.



GETTING YOUR CLOUD-NATIVE 5G ARCHITECTURE TO WORK—ALL THE WAY TO THE NETWORK EDGE

The success of 5G SA depends on successfully implementing the network foundation: cloud-native infrastructure running container-based microservices on a service based-architecture (SBA). To succeed, you need to apply the architecture consistently across the network, from the core to the edge and even far edges. You can use multi-access edge computing (MEC) deployments to extend your architectures to edge locations.

Kubernetes, another ingredient in 5G networks, provides a unifying technology that pulls it all together. Kubernetes is the de facto standard for managing and orchestrating container-based microservices, and almost all service providers will use it as the basis for the SBA. Kubernetes is a good choice: it's flexible, scalable, and efficient; it can run network functions as microservices; and it turns network management into a seamless process. With Kubernetes, you can use software tools to move capacity and network functions across your networks, spin up network slices, and automate control mechanisms.

AT-A-GLANCE REQUIREMENTS FOR SUCCESSFUL CLOUD-NATIVE DEPLOYMENTS

KUBERNETES

Tailored for 5G service providers

BIG-IP

BIG-IP SERVICE PROXY FOR KUBERNETES

Networking into and out of clusters

THREE REQUIRED CAPABILITIES

Traffic control, security, and visibility

ASPEN MESH

Networking within clusters

KUBERNETES CHALLENGES AND REQUIREMENTS FOR SERVICE PROVIDERS

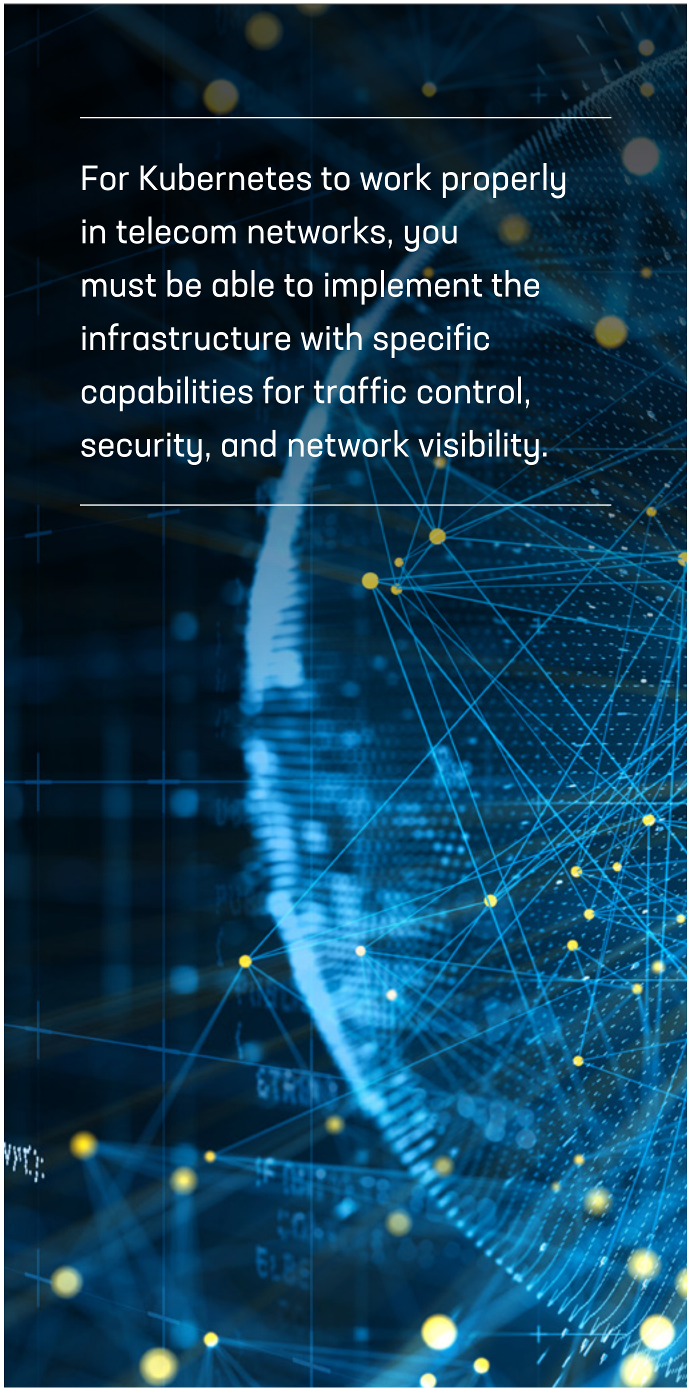
Service providers recognize the central role container-based microservices play in 5G, but you must be able to define, manage, and control your own cloud-native infrastructure to support your network functions and applications. However, Kubernetes does present some challenges: It was designed originally for IT networks, not telecommunications implementations, so it has no awareness of telecom protocols. It can’t accommodate the many types of traffic that are unique to service provider networks, and it doesn’t meet some of your particular demands for managing network traffic as it moves into, out of, and within Kubernetes clusters.

For Kubernetes to work properly in telecom networks, you must be able to implement the infrastructure with specific capabilities for traffic control and security. You also need network visibility to ensure proper revenue controls. Here’s more about what you need, and why.

Traffic control: You need intelligent traffic management tools to facilitate the transition from 4G to 5G protocols, support new capabilities such as network slicing, and enable ultra-reliable low-latency communications, massive machine-type communications, and enhanced mobile broadband for consumers.

For traffic coming into and out of the infrastructure, Kubernetes must meet specific requirements. For example, as service providers roll out their 5G cores, many will leverage their existing 4G billing and charging systems to speed delivery of new 5G-based services and get faster returns on their investments. Their Kubernetes clusters must support both 4G and 5G protocols during this transition, such as 4G signaling protocols like Diameter and SCTP. The infrastructure must also provide traffic management capabilities for load balancing and routing. These capabilities are necessary to ensure incoming traffic is distributed efficiently across servers and the network can operate with high availability and eliability.

Traffic within clusters has similar challenges. In particular, you must be able to control and manage traffic within a cluster to facilitate service discovery, routing, policy enforcement, and more.



For Kubernetes to work properly in telecom networks, you must be able to implement the infrastructure with specific capabilities for traffic control, security, and network visibility.

Security: Service providers require robust security for ingress traffic—that is, traffic coming into clusters—to establish the first line of defense against threats. The infrastructure must provide distributed denial-of-service (DDoS) attack protection, signaling firewalls, and web application firewalls at the ingress point to prevent malicious traffic from entering the cluster and impacting 5G core network functions and customer applications.

Traffic within clusters must also be secured. You must be able to authenticate services and ensure encryption for traffic between network functions.

Visibility: Service providers need the ability to observe traffic flowing into and within the infrastructure so you can optimize operational efficiencies, facilitate troubleshooting, and provide proper revenue assurance.

Ingress traffic has specific visibility considerations and requirements. For example, you may invest substantially in revenue assurance, and you must be able to trace traffic for compliance and billing purposes. The entry point to the Kubernetes cluster is the key network location for gathering this information. The information must be granular enough to provide visibility into per-subscriber traffic to help troubleshoot network problems that affect evenues.

Traffic visibility within clusters has similar requirements. You must be able to observe, monitor, and trace traffic within clusters to ensure network health and determine the root cause of failures that may occur. Visibility within clusters also enables you to comply with regulatory requirements for lawful intercept.

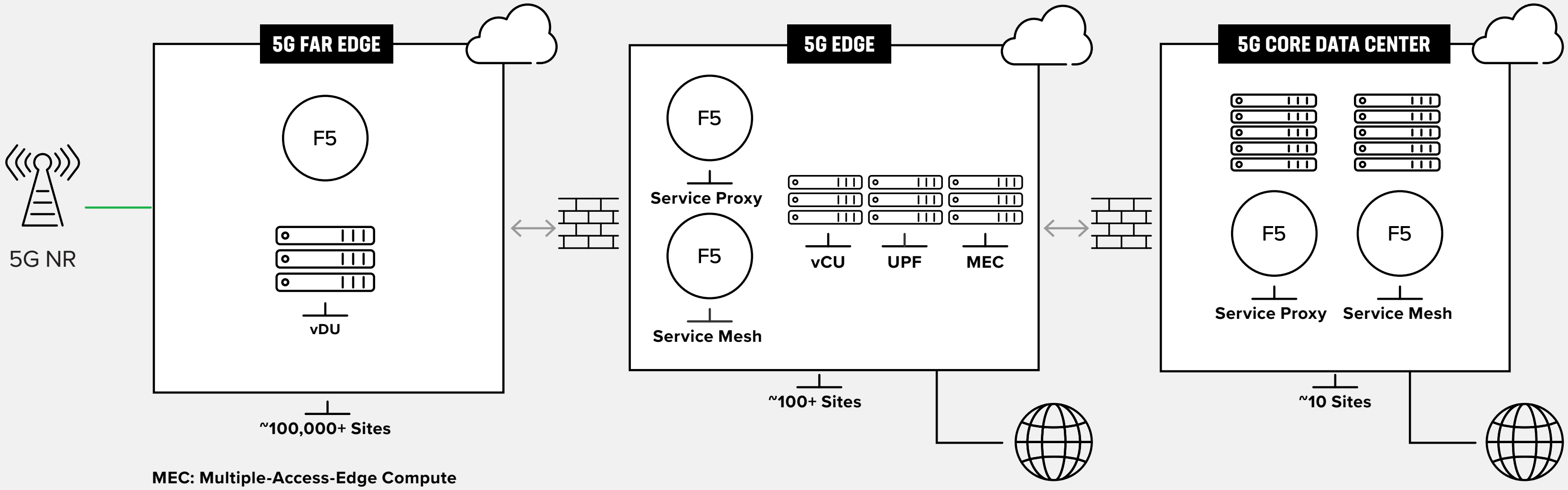
F5 SOLUTIONS FOR CLOUD-NATIVE 5G INFRASTRUCTURE

F5 provides two solutions to help you use Kubernetes to support the networking and security requirements in 5G systems. The solutions include F5® BIG-IP® Service Proxy for Kubernetes (SPK), which addresses issues for ingress and egress traffic from a Kubernetes-based cloud infrastructure, as well as carrier-grade F5 Aspen Mesh™, which addresses traffic challenges for traffic moving between cloud-native network functions (CNFs) and applications within a cluster. The solutions are shown in Figure 1.

You can use these solutions to build your 5G infrastructure with the consistency required to support network functions and applications at the far edge, edge, and core. The solutions are scalable and can support one, multiple, or thousands of deployments depending on network location, density, or edge service needs.

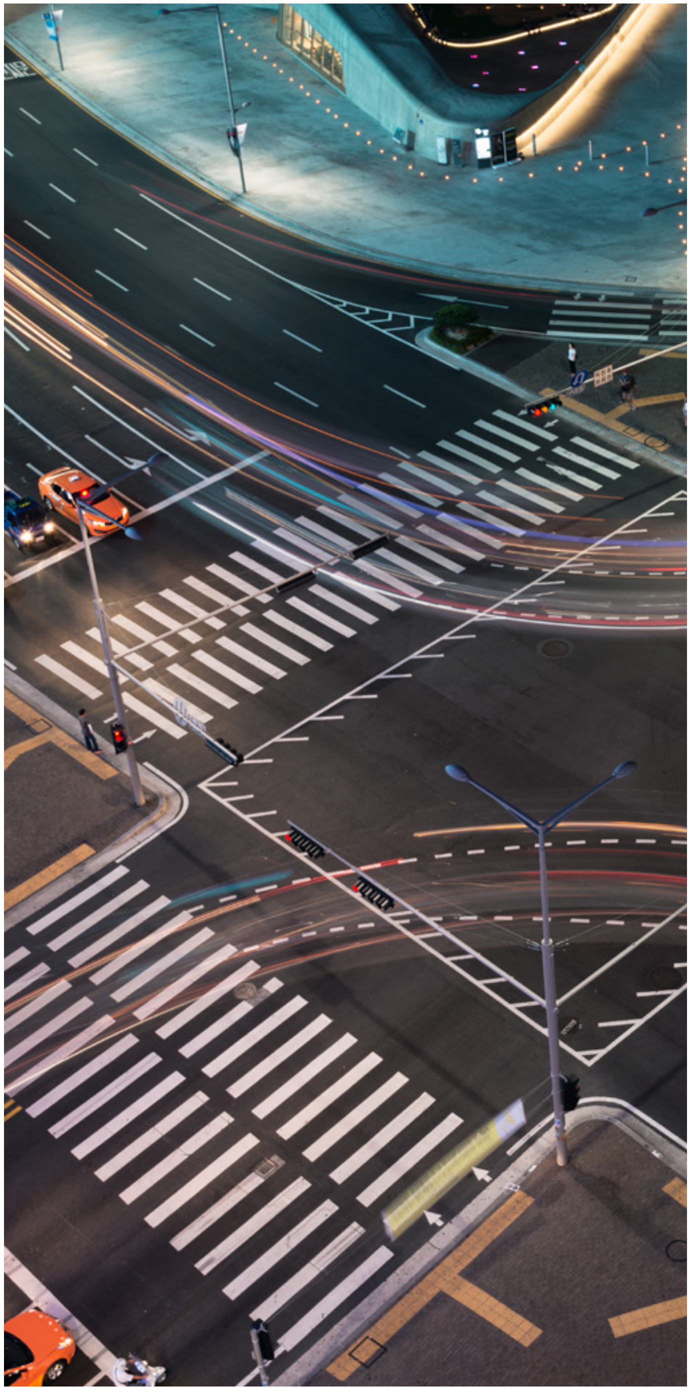
> Service providers should choose network cloud platforms that provide supreme visibility, support high capacity, and efficient scale.[1]

F5 INFRASTRUCTURE SOLUTION SCALING CAPABILITY



MEC: Multiple-Access-Edge Compute
vDU: Virtual Distributed Unit
vCU: Virtual Central Unit
UPF: User Plane Function

Figure 1: BIG-IP SPK and Aspen Mesh enable you to support cloud-native infrastructure functions and applications at far edge, edge, and core network locations.



NETWORKING INTO AND OUT OF KUBERNETES CLUSTERS WITH BIG-IP SERVICE PROXY FOR KUBERNETES

F5 designed BIG-IP SPK to help you deploy cloud-native infrastructure across your footprints. The solution uses Kubernetes approaches for configuration and orchestration, adding industry-leading multi-protocol signaling support, security, and visibility for traffic coming into and out of a Kubernetes cluster.

For traffic control, BIG-IP SPK intelligently handles the most common telco messaging protocols and enables service discovery for automating network function configurations.

For traffic control, BIG-IP SPK intelligently handles the most common telco messaging protocols and enables service discovery for automating network function configurations. It performs the load balancing, routing, and rate-limiting roles service providers use to maximize traffic speed, optimize capacity usage, and intelligently scale traffic across the Kubernetes environment.

BIG-IP SPK implements security at container ingress points with multiple solution options to prevent DDoS attacks, volumetric attacks, or just “bad” traffic from entering the Kubernetes cluster. The service includes a signaling firewall, F5 Advanced Web Application Firewall™ (Advanced WAF), and distributed denial of service (DDoS) protection to steer harmful traffic away from the network, with an option to leverage Intel SmartNIC capabilities for high performance. The BIG-IP SPK security service also hides the topology of the cluster’s internal structure so third parties can’t see into the cluster configuration or access details about network functions and management.

BIG-IP SPK gives you the tools to observe all traffic as it enters and leaves a cluster. It provides the traceability, statistics, and analytics you need for compliance and billing, and ensuring all revenues are accurately received.

NETWORKING WITHIN CLUSTERS WITH ASPEN MESH

Microservices are modular, autonomous services that are installed in the network in software containers and interact with one another to perform a service. Without a way to view and manage microservices, a network could have a universe of software components that can't be efficiently visualized or controlled and must be managed individually. A service mesh can manage all this complexity so you know what's going on in your Kubernetes clusters and can streamline operations to run efficiently, reliably, and securely. This is a critical capability for the MEC architectures you'll use with 5G.

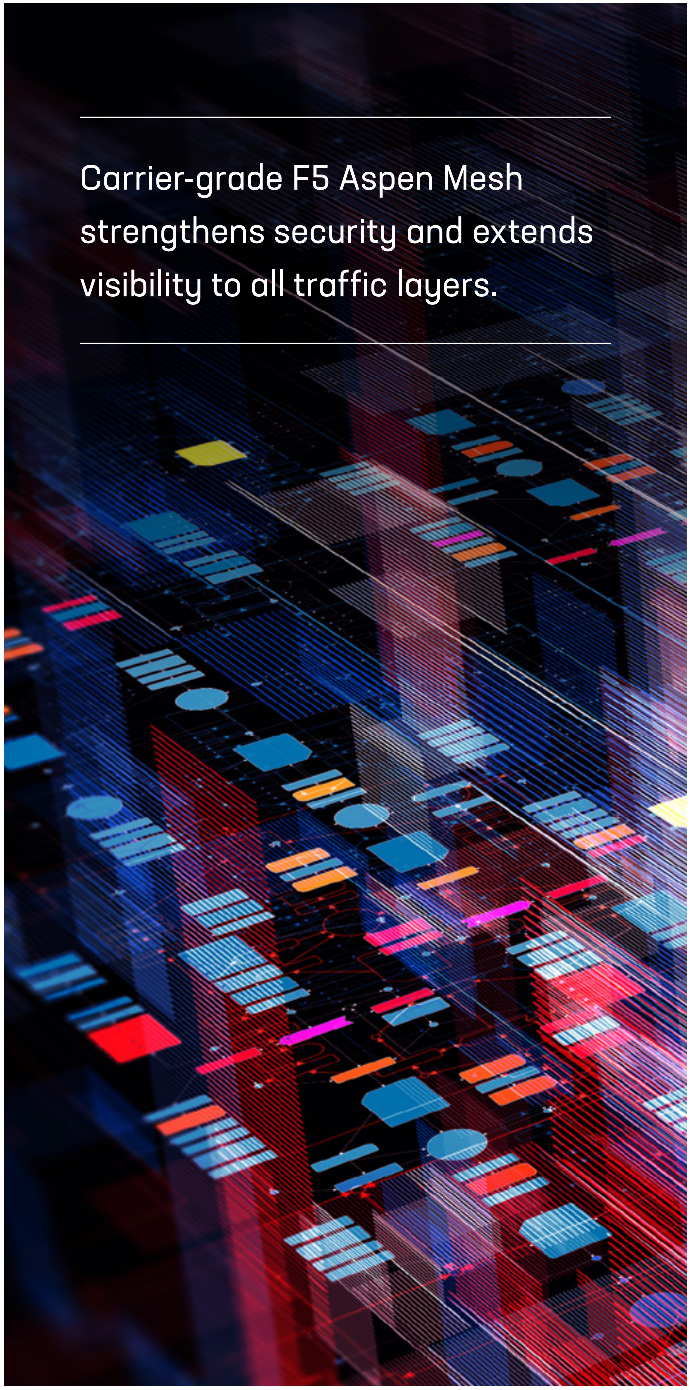
Carrier-grade F5 Aspen Mesh, designed to be owned and managed by service providers, is purpose-built for 5G cloud-native infrastructures and MEC environments. The service mesh builds on open source Istio and provides the added capabilities you need for traffic control, security, and visibility within your Kubernetes clusters.

Service mesh traffic control and policy management capabilities facilitate seamless, multi-tenant environment operations. You can use the capabilities to efficiently route service communications, and configure and enforce business and compliance policies. It's scalable and can meet traffic demands as they scale exponentially.

Aspen Mesh strengthens security. It provides a consistent way to encrypt and authenticate all traffic between multi-vendor network functions. It employs the strongest mTLS authentication techniques to ensure carrier-grade and 3GPP-compatible certificate authority.

Aspen Mesh visibility extends to all traffic layers. It reveals traffic flow within each Kubernetes cluster and dependencies between services.

In addition, F5's service mesh provides packet capture capabilities that standard Kubernetes does not provide. Packet capture is important for troubleshooting communication issues between CNFs within the cluster and for compliance with governmental requirements, such as lawful intercept.



Carrier-grade F5 Aspen Mesh strengthens security and extends visibility to all traffic layers.

24.6 billion

ESTIMATED IOT CONNECTIONS BY 2025

5G UBIQUITOUSLY CONNECTING EVERYONE TO EVERYTHING WHICH UNDERSCORES THE IMPORTANCE OF REACHING FOR THE EDGE.[2]

REACHING THE 5G EDGE WITH F5

Service providers are stepping into new territory as they build 5G standalone networks that run on cloud-native infrastructure, service-based architectures, and hundreds if not thousands of edge compute facilities. The work is challenging but the outcome, a digital transformation of the telecom network, positions you to deliver a better customer experience, support 5G's compelling use cases, and adopt innovative business models that can increase revenues and profitability.

Given the complexity of the deployments, many service providers will turn to industry partners to help them build out the new infrastructure and deliver services at the edge. In particular, you need specialized solutions and expertise to implement Kubernetes cloud-native technologies that were originally designed for IT networks, not telecom.

As an application, security, and delivery company, F5 has vital know-how and solutions to help you address these strategic challenges. Our extensive heritage in enterprise networking, service provider networks, and 4G gives us unique experience to help you deploy the new platforms and run 5G services like enterprise workloads in the cloud.

Learn more about F5 service provider solutions at **F5.com/serviceprovider**.

SOURCES

[1] “Cloud Native networking for a 5G era” report, ABI Research, (March 2020), page 13
https://www.abiresearch.com/blogs/2020/04/06/cloud-native-networking-5g-era/

[2] The Mobile Economy 2020, GMA Associates
https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Global.pdf

FAST TRACK TO THE 5G EDGE

Digital transformation is underway across telecom networks. F5 has specialized solutions to help you implement Kubernetes cloud-native technologies all the way to the edge. Discover how a standalone 5G network equips you to deliver customer experience, while boosting revenues and profitability.

Learn more about F5 service provider solutions at **f5.com/serviceprovider**

US Headquarters: 801 5th Ave, Seattle, WA 98104 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com