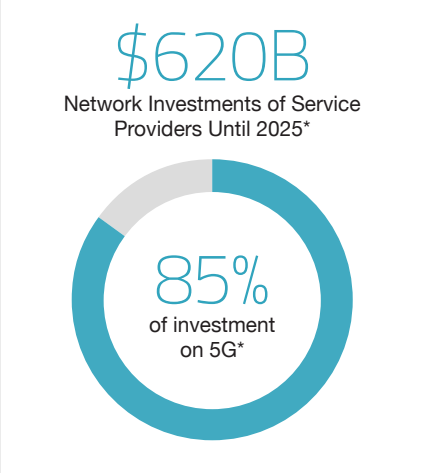
Radware 5G Protection

Table of Contents

5G Networks, Edge Computing and Ultra-Low-Latency Applications

Service providers are undergoing a technological revolution, transforming their networks and computing infrastructure to dramatically change the user experience and support new services in an app-driven world tailored to industry and business objectives.



*According to GSMA – The Mobile Economy 2022

To do so, service providers are embracing ultra-low-latency designs, fully automated software delivery and increased levels of operating efficiency. Edge computing and application delivery designs address a wide variety of quality-of-experience goals while increasing the distribution of resources, policies and controls. 5G networks promise to change the way humans interact with machines to deliver real-time intelligence meant to improve the digital experience.

At the cornerstone of these technological revolutions will be the need to deliver a safe and secure digital experience.

5G Promise and Potential

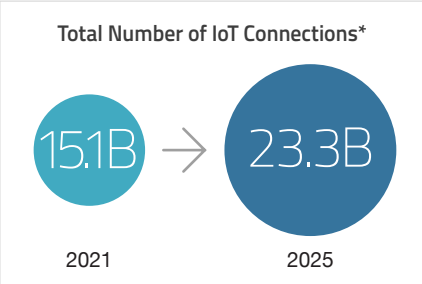
5G promises to be a game changer. It will reshape private and business communication in ways we've yet to imagine, but what exactly are the benefits we can expect?

Enhanced Mobile Broadband Performance

Data speeds will increase up to 20Gbps, and even basic user IoT equipment should be able to generate up to 1Gbps of bandwidth. Increased data speeds will improve the quality of experience of many services, such as over-the-top (OTT) services, online gaming and more.

Crowded Access Network

The IoT ecosystem is growing, and businesses are using IoT to improve efficiency and to create new business opportunities to increase revenue. 5G will boost IoT adoption by creating new business models with the help of higher bandwidth, reduced latency and network virtualization.



*According to GSMA – The Mobile Economy 2022

Ultra-Reliable Low-Latency Communication

Services that could not be adopted at high scale until now will now emerge. Artificial intelligence (AI), virtual reality (VR), Industry 4.0 applications, medical-critical services, autonomous mobility, and more will be able to utilize the 5G's ultra-low-latency requirements. Service providers will be able to deliver a sub-10-ms reliable latency performance, which will open the door for new services and great customer experience.

Dynamic Customer Experience

5G networks are known for their lightning-fast data connection and low latency, but 5G will also simplify network slicing by creating multiple virtual networks within one physical system. Network segmentation enables many new opportunities for service providers. For example, markets driven by the IoT can enjoy a more dynamic and granular IoT experience, starting with a basic, cost-effective solution, and up to a premium ultra-low-latency service to support bleeding-edge services.

Business

Service providers' main objective is to enhance their infrastructure monetization. Improved performance and the dynamic quality of experience will open the door to new services that, until recently, were limited or completely absent from the service providers' portfolio. New services, such as AI, VR, Industry 4.0 applications, medical-critical services, autonomous mobility and more will allow service providers to gain new market share.

Challenges

5G transformation will require a new mindset, as the need for agility, flexibility, scalability and performance drives dramatic changes in the network topology, core network and radio access network (RAN).

Network topology has changed from a centralized model to a widely distributed, cloud-native fabric that features an "edge" model, and from one main gateway to a distributed network with multiple internet break points.

The 5G core is based on what is called a service-based architecture (SBA), which implements a cloud-native design approach so that all network elements are now communicating using API over HTTP/2 and can be outsourced easily to the cloud. RAN is also evolved to support higher cell density, higher bandwidth and ultra-low latency.

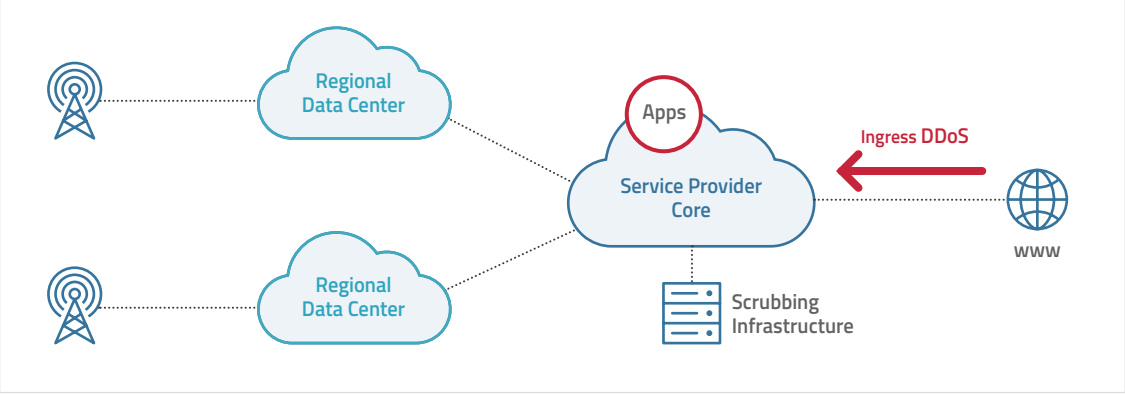


Figure 1

Network topology before 5G

Figure 2

5G network topology

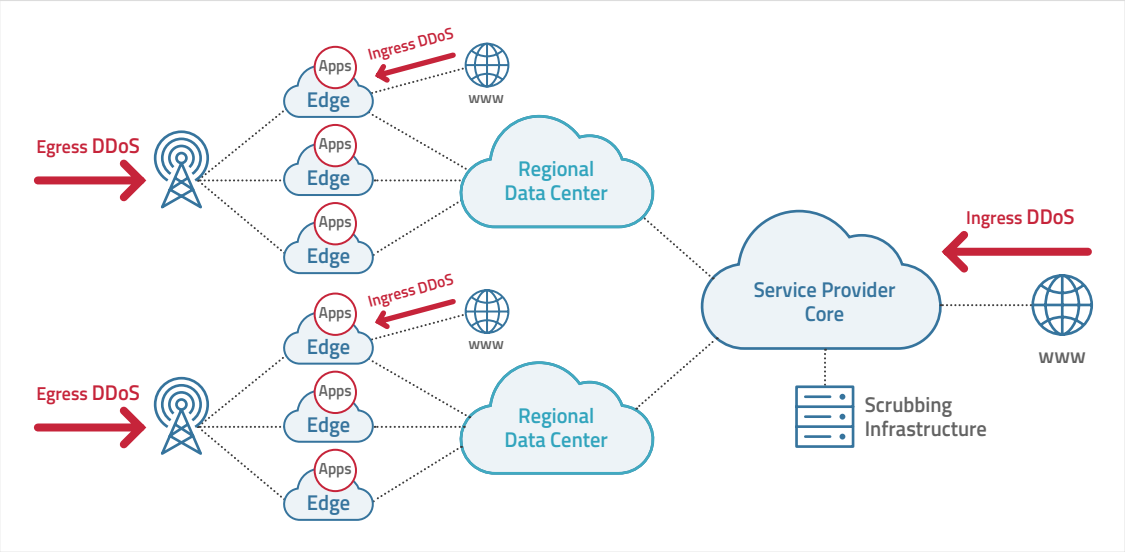
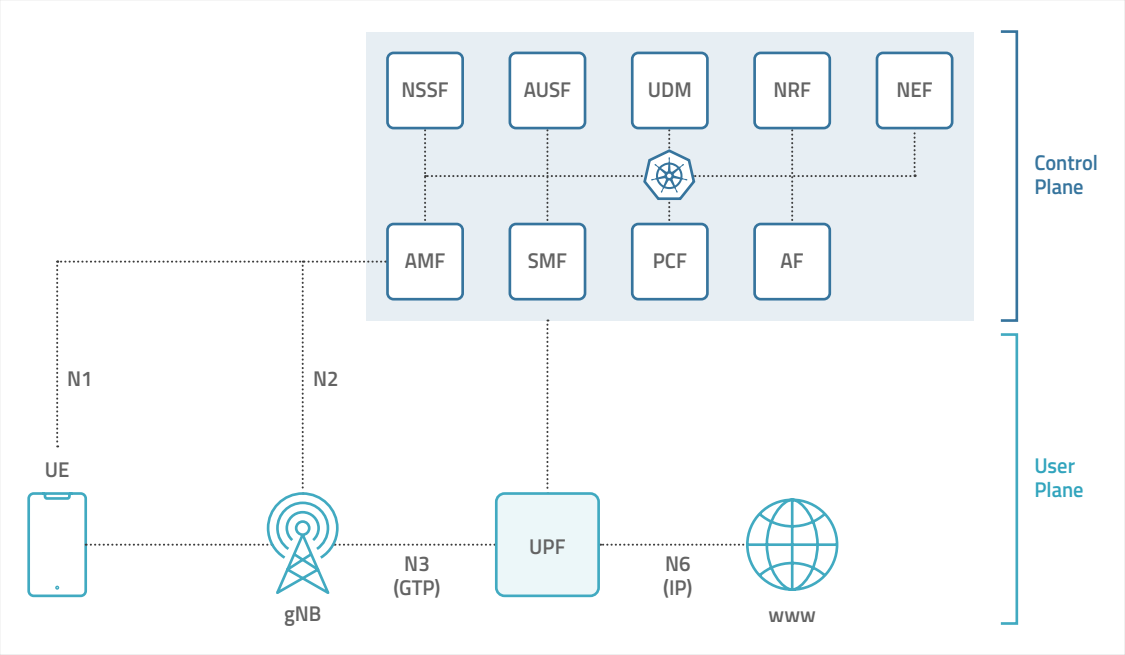


Figure 3

5G core, service-based architecture



5G networks will support growth in user equipment, availability of new services, lightning-fast connectivity and better user experience. However, the change of network topology, core architecture and RAN capabilities has far-ranging impacts on service provider cybersecurity strategies and postures.

Main 5G Security Threats

Ingress DDoS Attacks

Distributed architecture increases exposure to destructive distributed denial-of-service (DDoS) attacks. Now the core and the edge have internet-facing functions (e.g., an N6 interface connecting UPF to an external data network).

Larger, More Sophisticated Egress Attacks

Low-latency capabilities, improved cell density and higher bandwidth will generate IoT growth. This crowded access network will only aggravate the hectic access threat landscape, such as DDoS flood attacks from IoT devices or other terminal equipment via an N3 interface.

Attacks on Distributed Applications and Core Network Functions

Multi-access edge computing is part of the 5G transformation and will have different requirements. For example, a simple Facebook metaverse interaction will push Facebook to have a closer presence to its customers just to facilitate real-time requirements of the augmented reality interaction. Of course, Facebook is not alone. We will have more virtual and augmented reality services along with new medical services, industrial services and more.

Ultra-low latency, high bandwidth and ambitious quality of experience will not only affect the presence of edge consumer and enterprise applications but also extract the core network elements closer to the edge to align them with the new requirements.

Sharing edge-compute real estate with enterprise applications and distributing critical network function outside of the traditional defense border creates new security vulnerabilities.

Service providers must also protect APIs and availability of any 5G core elements, both distributed and undistributed. Protecting third-party applications is a concern as well as they can expose your network to east-west attacks and other collateral damage.

Public Cloud Vulnerabilities

Service providers with a cloud-native infrastructure are still perceived as early adopters, but service providers will consider public cloud resources to increase points of presence. Before this migration will start, security must be considered as a high priority to ensure data is protected against emerging public cloud vulnerabilities and threats.

Currently, service providers are challenged to handle the full security requirements of 5G networks. The same capabilities that allow service providers to deliver lightning-fast connectivity with ultra-low latency also allow hackers to execute larger, more sophisticated cyberattacks. The virtual transformation of the core network also adds complexity and dependency on APIs to enable crucial new services, such as autonomous mobility and healthcare services.

Service providers must equip themselves with a new and different security posture else they be overwhelmed by the next generation of security threats.

Radware Solution

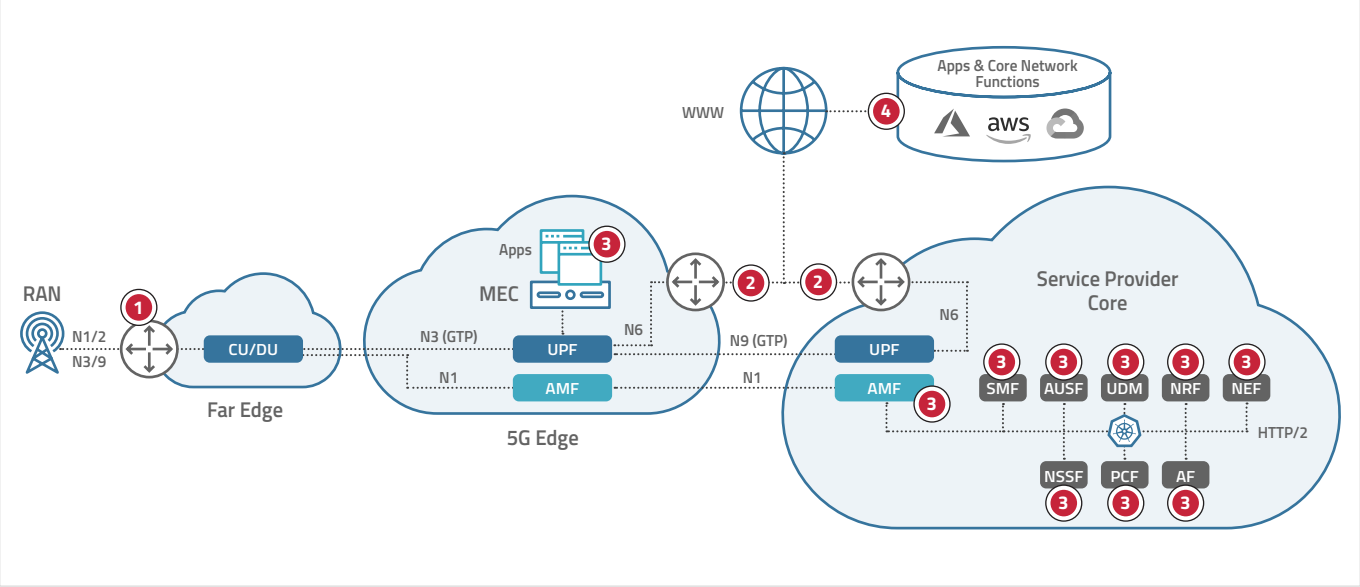
The 5G network is completely different from past architectures. A different threat landscape requires a different security posture. Radware delivers the industry's most complete 5G security solution to protect network and ultra-low-latency services at any scale, including 360-degree protection for network access and both edge and core network architectures.

Radware's 5G protection is focused on four main use cases:

1. **Mobile Access Protection** – Latency-agnostic protection to a crowded mobile access network
2. **Edge and Core DDoS Protection** – DDoS protection at any network with open borders
3. **Edge and Core Application Protection** – Web and API protection designed for 5G-service mesh architecture
4. **Public Cloud Support** – Protection of a public cloud infrastructure against new cloud threats

Figure 4

Radware 5G protection

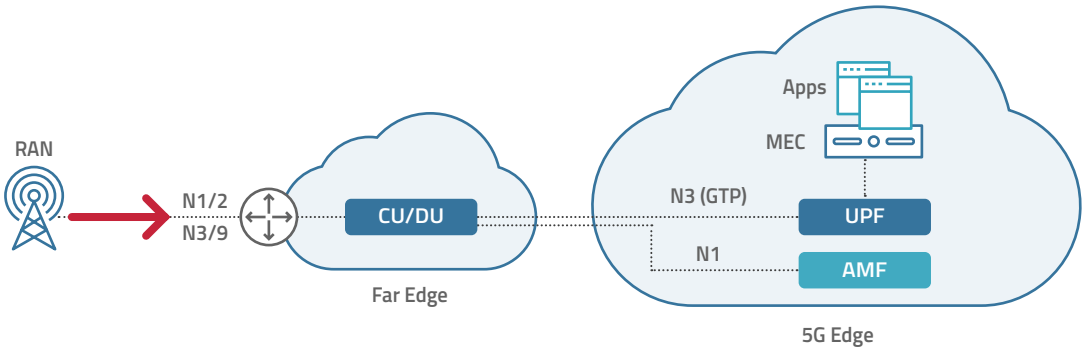


Mobile Access Protection

Low latency, high bandwidth and top-notch quality of experience are facilitated by the 5G network topology and enhanced RAN. These capabilities create a need for a new access network security posture closer to the attackers.

Figure 5

Access network attacks



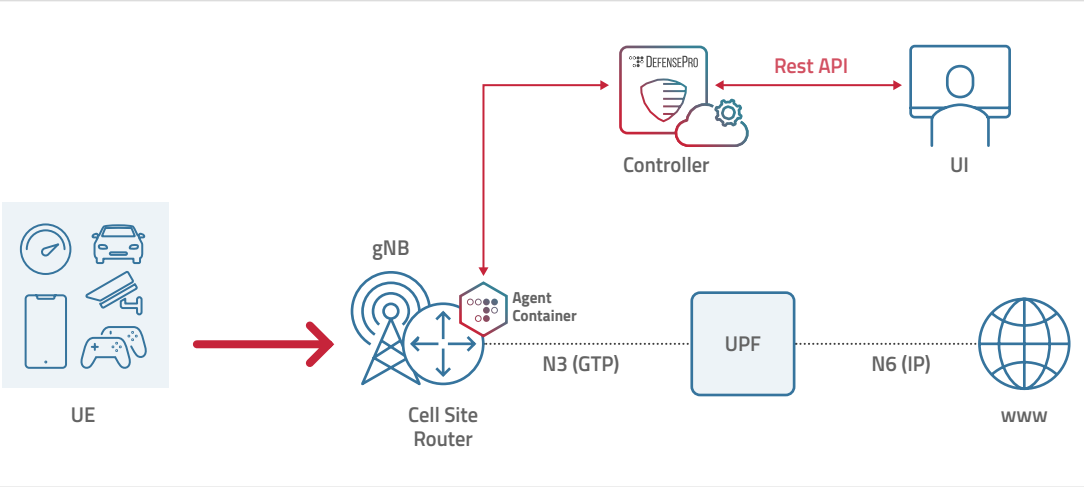
This new network faces four primary challenges:

- Inspecting N3 high-bandwidth data encapsulated in GPRS Tunneling Protocol (GTP)
- Protecting against different terminal equipment more powerful than ever
- Orchestrating thousands of distributed-access network locations
- Keeping the ultra-low-latency promise

Radware's innovative solution is built on a container-based agent implemented in the cell site router protecting the network closer to the source. The solution can be easily distributed across the 5G topology while using innovative security algorithms to deliver the granularity and dynamic ability needed.

Figure 6

Deployment of access network protection



Radware's solution ensures the promised ultra-low-latency requirements, high bandwidth, scalability and demanding quality of experience while providing unmatched DDoS and network anomaly protection against attacks coming from the access network.

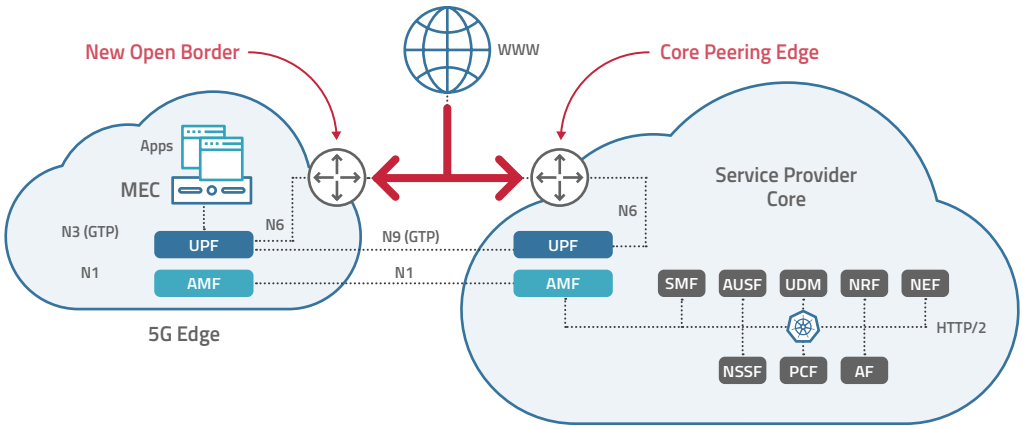
Main Advantages of Radware Mobile Access Protection

- Low latency agnostic, none-intrusive, out-of-path process.
- Unmatched air-gapped behavioral DDoS protection
- In router integration for better detection and mitigation
- Dynamic and ultra-granular detection. Support GPRS Tunneling Protocol (GTP) inspection
- Orchestration of large-scale distributed agents by a central controller

Edge and Core DDoS Protection

Figure 7

Open borders and peering edge attacks



New Open Borders

Design requirements of 5G network architecture shifts the network-critical elements from the core closer to the edge to facilitate the new emerging real-time services. Ultra-low-latency requirements opened the door for new local break points connecting the UPF to external data networks (N6 interface).

Exposed open borders are a security threat. Service providers need to protect the edge services and network infrastructure from ingress DDoS attacks coming from the internet toward the service provider's edge services and infrastructure.

Radware's DDoS protection can protect any new edge with multiple vendor-agnostic deployments.

Core Peering Edges

Mobile core networks have always been open to ingress DDoS attacks at the peering edges, and 5G networks are no different. The N6 interface is also a security threat from the peering edges.

Protecting the N6 at this location is done mainly by utilizing NetFlow BGP to redirect detected attacks to an out-of-path scrubbing center.

Main Advantages of Radware DDoS Protection

- Automatic and behavioral protection
- Zero-day attack protection
- Phantom flood attack protection
- Comprehensive orchestration
- Flexible and vendor-agnostic deployments

Edge and Core Application Protection

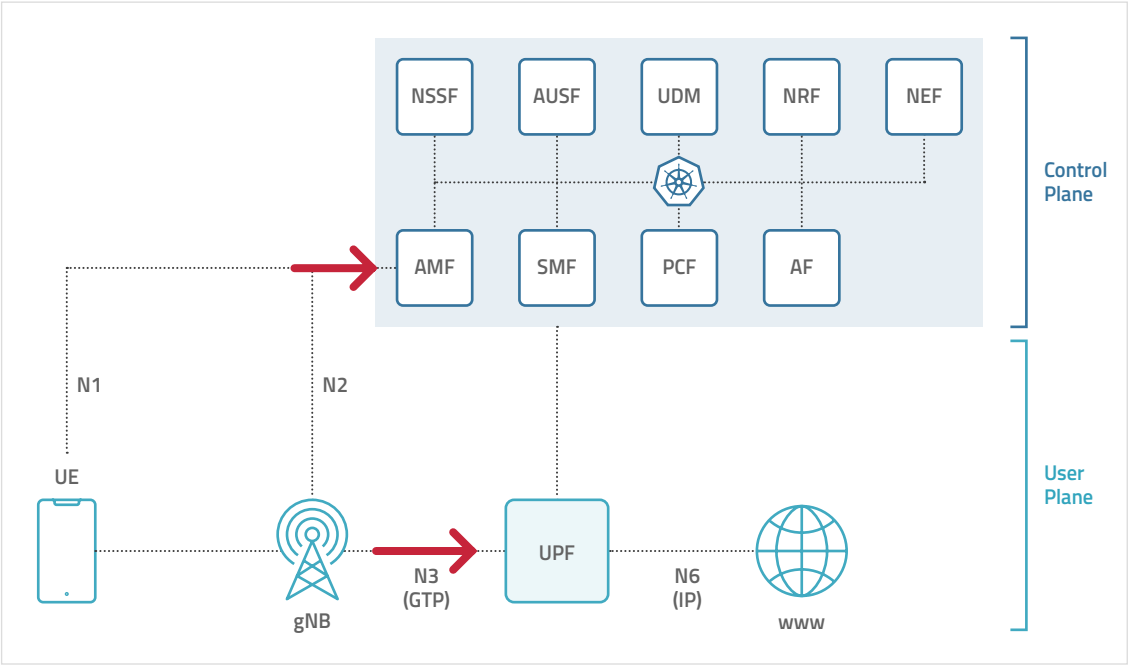
Radware web application and API protection (WAAP) offers great security for both 5G network functions and any third-party applications hosted on the edge.

5G Core Application Protection

5G core services are exposed to attacks from interfaces N1/N2 and N3. Flood attacks can be blocked using Radware's access network protection using the in-router solution, but network functions should be protected from AMF signaling leakage as well.

Figure 8

Control plane attacks

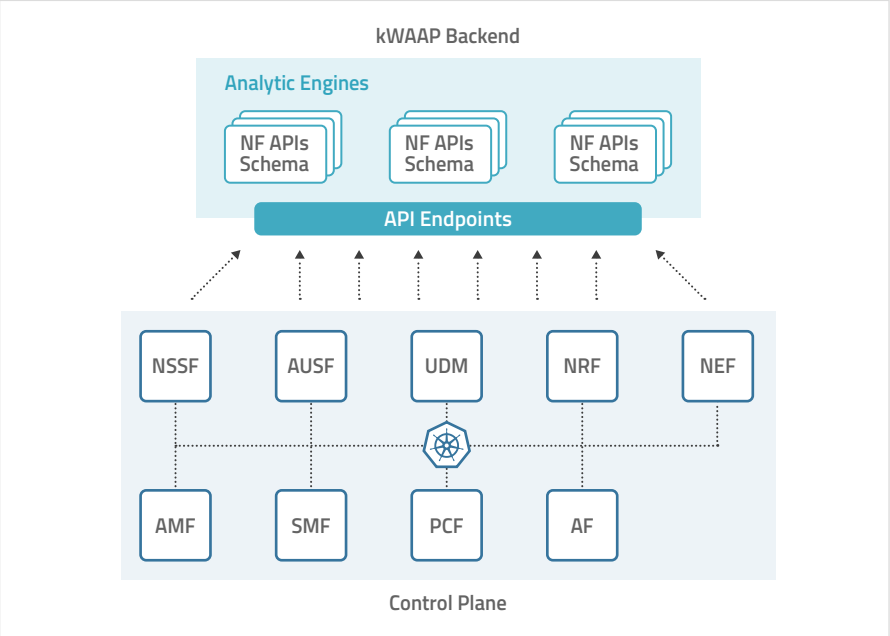


Radware's WAAP protection is an air-gaped, container-based solution that can work also using Kubernetes orchestration. The solution is deployed as a native citizen within the worker's cluster.

Radware WAAP protection secures any 5G service element against web and API injections, lateral movements, exfiltrations, and zero-day usage and application attacks by checking API transactions.

Figure 9

Radware WAAP Deployment



5G transformation is a complicated process, and although SBI service mesh architecture is the goal, it is not the starting point for many service providers. That is why Radware is flexible enough to deliver application and API protection at any step in this transformation process.

5G Edge Application Protection

The core network holds the critical network functions, but the presence of edge enterprise applications is also a growing threat for 5G networks. Ultra-low latency, high bandwidth and the ambitious quality of experience will push more enterprise services closer to the user. As a result, they will expand the edge computing's threat landscape. Enterprise applications add vulnerabilities, such as east-west attacks, lateral movement and more.

Radware's WAAP protection can reduce the mobile edge threat landscape by providing comprehensive application and API protection to any distributed application running on edge computing.

Monetize Your Security Efforts

Protecting third-party applications will reduce exposure and eliminate any vulnerabilities to edge computing, but service providers can use this security concern as an opportunity to deploy a SaaS muti-tenant model and to monetize their security resources.

Radware's security posture is designed to work as a multi-tenant offer and can easily transform the security effort to an SaaS opportunity.

Main Advantages of Radware WAAP Protection

- Protection designed for container-based architecture and Kubernetes orchestration
- Zero-day application attack protection
- Negative and positive security model
- Web and API protection
- Lateral movement protection
- Exfiltration protection

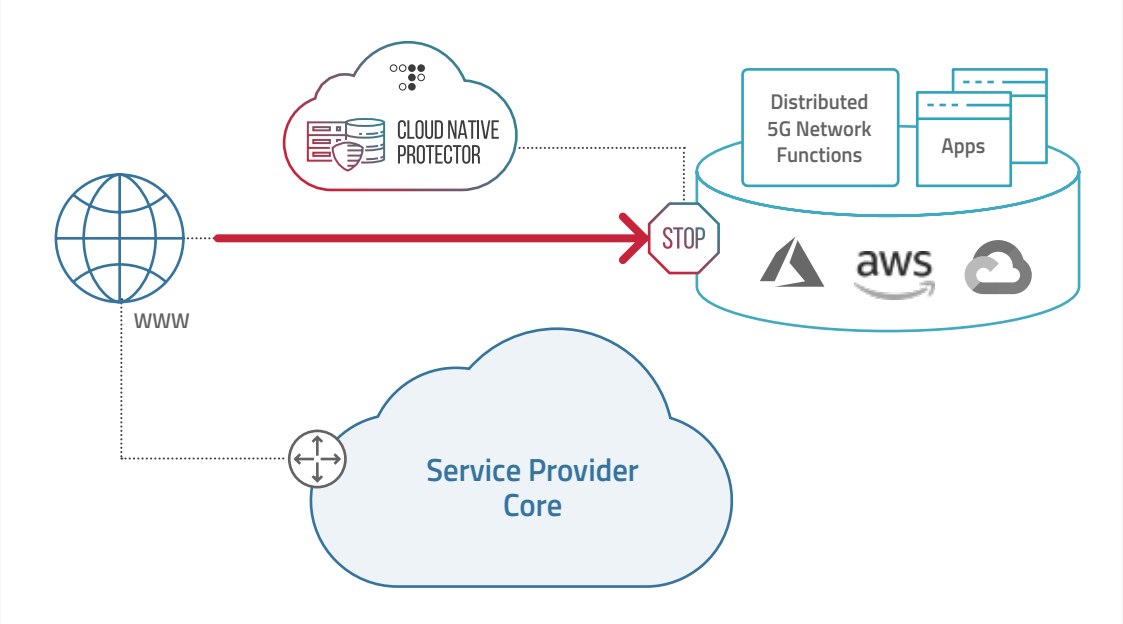
Public Cloud Support

The transition to completely cloud-native 5G infrastructures will start by companies leveraging public cloud resources to increase network coverage and then beginning to outsource critical network functions.

5G services that reside on public cloud platforms are exposed to different security threats from inside and outside the cloud environment. Redware's Cloud Native Protector provides comprehensive protection for services hosted on the public cloud with multi-layer defenses that secure the cloud environment against identity and access abuse, protect against malicious user behavior and secure the overall security posture of the public cloud environment.

Figure 10

Public cloud attacks



Main Advantages of Radware Cloud-Native Protection

- Identify public exposure, misconfigurations and compliance violations
- Prevent credential abuse and data theft
- Correlate sporadic events to attack storylines
- Protect against automated bot attacks

Important Elements for a Great 5G Security Solution

Service providers are not capable of handling the full security requirements of 5G networks without changing their security posture, but what exactly should a service provider look for when searching for the best 5G protection solution?

5G protection must meet the design requirements of the 5G architecture and be able to protect the dynamic threat landscape. Critical capabilities are:

Specification Alignment

3rd Generation Partnership Project (3GPP) is the main standards body developing technical specifications for cellular networks, including security specifications. These specifications are the foundation on which other security elements are built; some of these security elements are defined as optional or are more open to flexible interpretation. Aligning and understanding these security guidelines is important for any security vendor and service provider to deploy and manage a robust and secured 5G network.

Agnostic to Low-Latency Requirements

One of the key use cases of 5G is ultra-reliable low-latency communication as it will open the door for new services that will change our daily lives, such as medical, social, transportation, entertainment and more. However, supporting sub-10-ms reliable latency performance will also affect the security, as security elements must be able to detect and mitigate attacks faster than even. Security elements at the RAN must be stateless and agnostic to the latency requirements.

Protection Consistency in a Multi-Cloud Environment

The design requirements of the 5G architecture are revolutionary and are completely different from 2G, 3G and 4G; the edge approach and the software delivery model will enable deployment of applications and core network elements in a distributed and disaggregated cloud environment and, in some cases, in public clouds. This, of course, will make it harder to have a consistent security posture on all the different environments.

A great 5G solution will be able to maintain consistent security policies across multi-cloud environments via identical security controls and visibility into all assets.

Distributed and Scalable Security Designed for Service Mesh Architectures

The 5G core network evolved from a closed and inflexible environment into a set of interconnected network functions (NFs), with authorization to access each other's services using REST interface using HTTP/2.

The new core network design makes container orchestration an obvious choice for service providers. It will enable flexibility, scalability and a perfect solution for the 5G network topology disaggregation.

5G protection must deliver state-of-the-art application and API protection that is natively built for a container-based architecture and orchestration ecosystems like Kubernetes.

Summary

Unmatched Protection

Behavioral-based and automated algorithms for granular and dynamic protection

Solution Natively Built for 5G

Technology specifically designed for 5G threat surfaces, agnostic to ultra-low-latency services, with edge-oriented protection and aligned with 3GPP specification

Frictionless, Multi-Cloud Support

Rapid scalability and seamless deployment, with a pure software delivery model and both public and private cloud support

Radware provides comprehensive 5G security designed and built to meet the full security requirements of 5G networks. Radware's 5G protection supports 3GPP specifications and ultra-low-latency applications and provides multi-cloud support.

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.