radware

Sharpening the Edge: 5G Networks, Edge Computing, IoT and Their Implications on Cybersecurity for Service Providers

WHITE PAPER

SHARE THIS WHITE PAPER

TABLE OF CONTENTS

Introduction

Service providers are undergoing a technological revolution in the name of agility. They're transforming computing infrastructures to gain service dexterity, provide new and improved applications to digitally native consumers in an app-driven world and deliver interactive content delivery services to new generations of customers who demand them.

The overarching goal? Leverage automation and a new generation of software- and service-defined architectures to improve the digital experience for consumers and businesses alike, all the while providing a secure experience.

To accomplish this, service providers are undergoing several business and architectural transformations:

- They're moving to a demand-driven, software-orchestrated network that enables faster time-to-service and deployment life cycles and real-time provisioning of underlying computing and network resources. This allows for easier consumption of resources and provides end-user autonomy.
- They're moving to the "edge." Service providers are transitioning away from core network designs by deploying new network infrastructure at the edge that will host key application resources, thereby reducing latency.
- This push toward the edge is being driven in large part by the upgrade to 5G networks. At its core, 5G is an upgrade in the mobile architecture that pushes new computing elements and services closer to the edge in order to scale and improve network performance. 5G networks rely on the aforementioned virtualized and distributed network functions that span remote locations and are heavily dependent on robust, secure interworking between remote and local virtualized network functions.
- They're transitioning to support the growing number of internet of things (IoT) devices and use cases, requirements for increased multimedia bandwidth and network-enabled security. Service providers must deliver scalable and cost-effective solutions.
- Lastly, service providers are improving their overall security posture to stay ahead of an increasingly dynamic and dangerous cyberthreat landscape. They're implementing new security architectures/solutions that are capable of moving at the speed of business and can operate in a highly distributed, multicloud architecture.

5G Networks, Edge Computing, IoT and Cybersecurity

The move to edge computing environments, the deployment of 5G networks, the mass adoption of IoT devices and the need to keep all of this secure have had far-ranging impacts for service providers.

For edge computing to thrive, the underlying architecture will be distributed in the cloud and will no longer be dependent on dedicated appliances. The corresponding implementation and deployment of carriers' networks will evolve to expand capacity, reduce latency and lower costs/power requirements.

To reinforce this open environment, organizations driving network agility will have to virtualize their network functions, resulting in less control over the physical elements of the networks in exchange for the cost benefits of flexible resource allocation. Services are also no longer restricted to service providers' networks or content and will exist in external network domains, increasing the geographical coverage for subscribers. This means that services can rely on physically closer, virtualized network resources for more efficient delivery of content to the connected device.

As part of the transition to edge computing, service providers will implement network slicing in which network providers "slice" portions of network resources to offer specialized services for specific application types, all the while remaining in the same physical infrastructure.

5G networks piggyback with network slicing because that will bring higher bandwidth and lower latency for today's digitally native consumers. In addition to serving as the foundation for the aforementioned digital transformation, 5G networks will also deliver the integral infrastructure required for increased flexibility. Driven by global demand for high-speed internet access, the business landscape will only increase in competitiveness as service providers jockey to deliver improved network capabilities.

But these transformations come with new cybersecurity risks. As network architectures evolve to support third-party applications, increased consumption of multimedia content and the interaction of data and services via IoT devices, they will create security vulnerabilities if cybersecurity isn't prioritized and integrated into the network from the get-go.

Current carrier networks are not capable of handling the security requirements of multicloud, widely distributed networks. The same capabilities that allow edge computing platforms to deliver lightning-fast connectivity also allow hackers to execute larger, more sophisticated cyberattacks. SOC engineers at service providers already face difficulty in predicting and preparing for today's attacks, becoming easy prey in the multicloud universe.

When combined with IoT devices, unprepared service providers can be overwhelmed by the next generation of security threats. For example, 5G networks shift the current network paradigm by redefining what "fast-paced" will be. The digital and virtual transformation utilizes more cloud applications dependent on various APIs, multiplying the complexity of interconnected devices that rely on more responsiveness, such as virtual healthcare solutions. This becomes a key issue for 5G network managers because of the increased number of potential vulnerabilities if they are not properly protected.

Take network slicing as another example. Network slicing offers traffic segmentation that is designed to isolate disruptions, but it also complicates network security because it requires more multitenancy and policy management to remain contextual.

But these risks come with new opportunities. Securing both 5G networks and edge computing architectures should not be viewed as an operational cost but rather as a new business opportunity/competitive differentiator that is integrated throughout the overall architecture. Just as personal data has become a commodity, service providers will require a security architecture that keeps data secure while improving the customer experience via a mix of availability and security functions. New outbound protection requirements have emerged to identify anomalous behavior to help identify misuse of resources and provide a meaningful remediation model to large-scale IoT deployments.

Network Security in an API- and App-Driven World

In a world driven by apps, how do service providers accommodate the masses, meaning the masses of IoT devices, applications, consumers and bandwidth requirements and third-party access required to manage applications?

Underscoring all of this are APIs, which are a double-edged sword. While APIs are the cornerstone of this ubiquitous connectivity and integration, they also represent a massive security threat. Traditionally, application and API exposure had been constrained to IDC infrastructure. This meant that a secure data center (DC) or security gateway framework was used to harden the exposure of numerous applications in the same physical location. These applications communicated to the internet via a common path. In the scope of security design, this was a relatively easy problem to address.

In the modern landscape, applications will pay for edge computing resources and require direct access. It means constant interaction with third parties and computing fabrics via APIs.

API and application protection becomes a key component in modern edge security. 5G networks rely heavily on HTTP/2 and APIs, thereby inadvertently exposing critical infrastructure to tech-savvy hackers. Malicious network traffic can evade networking monitoring and attack detection solutions and erode computing resources.

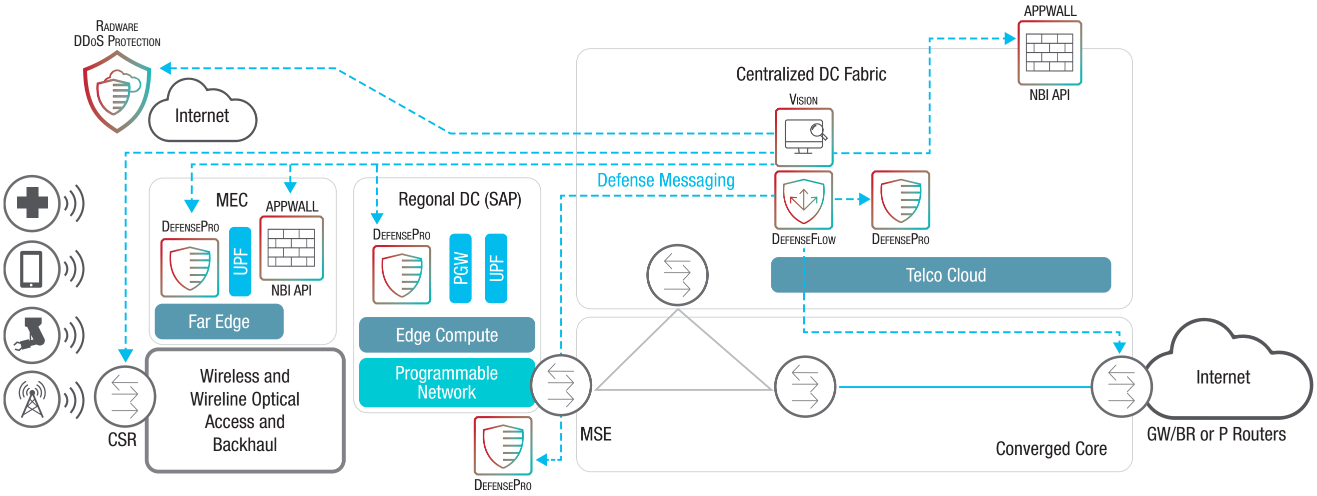
In this app-driven world, how do service providers protect themselves from third-party access? First, they must scale protection strategies and architectures to defend against volumetric attacks while addressing new complex attack surfaces, which require more sophisticated defenses. Automated software delivery will be critical and will allow service providers to address the complexity of a widely distributed architecture in a repetitive model. Network and security alignment will improve resource allocation while optimizing consumption-based delivery from edge computing systems.

When cybersecurity is built into the networks from the get-go, attacks can be addressed locally, avoiding backhauling attacks and driving efficiency back into the core computing environments. This scalable infrastructure protection strategy also serves as a point of escalation for more sophisticated or persistent attacks seen in gateways, applications and APIs.

Network Protection Moving Forward

So in this newfound world, what are the primary security strategies that carriers must embrace to provide consumers and businesses with a secure experience? First, there should be an expectation that these instruments of innovation will dramatically increase the threat landscape if implemented incorrectly. Overall, there are three primary strategies that service providers need to execute to “sharpen the edge” and safeguard widely distributed architectures.

- Protect the network from the internet
  - Service providers must protect the core network and service gateways from inbound attacks.
- Protect distributed applications and APIs on edge computing platforms
  - Distributed applications and APIs are targets across the network. Safeguarding them is critical.
- Protect the core from the access network
  - Infected mobile and IoT devices can be harnessed into large-scale bot attacks that enter the service provider’s network from the RAN.



- Multiple security layers (centralized DCs, peering and cloud, service aggregation PoPs (SAP), far edge (MEC))
- Distributed mitigation and telemetry (DDoS + WAF (VNF))
- API and high-speed TLS security
- Service provisioning and life cycle automation with cross-functional integration via REST API
- Flexible licensing to complement mixed virtual and physical environments as well as transformation and migrations

Attack Mitigation Protection for Service Providers

By protecting Service Providers against known and emerging network and application threats in real time, Radware's layered approach is designed to help organizations mitigate attacks that can be detected and offer a security solution that combines detection and mitigation tools from a single vendor. Radware's solution provides maximum coverage, accurate detection and the shortest time to protection.

Radware's Attack Mitigation Solution (AMS) offers a multivector attack detection and mitigation solution, handling network layer and server-based attacks, malware propagation and intrusion activities. Complete with anti-DoS, network behavioral analysis, encrypted traffic protection, intrusion prevention system (IPS), web application firewall (WAF) and in-the-cloud DDoS mitigation in one integrated system, this solution is designed to mitigate multivector attacks to protect an ISP's core resources.

Half of the top 25 carriers worldwide use Radware's AMS.

To mitigate network attacks that threaten to saturate bandwidth, Radware's AMS includes an attack life cycle workflow automation engine that allows for the escalation of attacks to scrubbing centers, the peering edge or a cloud-based DDoS scrubbing service optimizing where mitigations take place while also optimizing the network. This multitiered service model is further extensible to universal customer premise equipment (uCPE), virtual network function protections and computing fabrics, regardless of their connectivity or physical location. Enhanced with a central monitoring and reporting system, the solution provides ongoing unified situational awareness of the network and applications using a single security information and event management (SIEM) engine for all components.

Conclusion

The convergence of these technical revolutions is placing new demands and driving change within service providers. The move to edge computing environments, the deployment of 5G networks and the mass adoption of IoT devices have placed new cybersecurity demands on service providers at a time when the world is becoming increasingly insecure. But with change comes opportunity.

LEARN MORE FROM
ACG RESEARCH

By securing the customer experience, service providers have an opportunity to transform cybersecurity into a competitive advantage. They can establish a competitive advantage and fundamentally increase their addressable market by creating a secure environment that protects customers' data and devices, building trust with new generations of consumers who demand security of their personal information.

With the new reality of network slicing and highly distributed network functions, service providers will be overburdened unless they employ an automated, self-learning defense mechanism. For service providers, the economics of an increase in security staff is not an option when moving toward 5G — it just doesn't scale from a cost perspective, and it puts human engineers at the disadvantage of ever-increasing machine-based bot attacks.

Questions: Tell us more
or give us a call at
877.524.1419 to reach a sales
professional.

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, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.