Monetizing 5G Security

Moving from Cost Center to Profit Center

Enterprises are continuing to rethink connectivity and accelerate their digital transformation journey. The cloud-native versatility of 5G networks has a major role to play here. By securing these high-performance and low-latency networks that customers trust their critical use cases with, 5G network providers can help enterprises drive digitization and accelerate Internet of Things (IoT) adoption.

paloalto NETWORKS

Service providers have a great opportunity to build trust and capture market share among enterprises. In their quest to provide differentiated services for enterprises, mobile identifier-based enterprise-grade security can be service providers' greatest assets. The powerful combination of user (SUPI), device (PEI), and slice (NSSAI) identity data, and enterprise-grade Layer 7 security can unlock granular and intelligent mobile security on a level previously unseen:

- Identify compromised users and devices in real time.
- Segment user access based on security policies.
- Make the job of forensics quite a bit easier.

Business and mission-critical applications, including everything from energy to smart cities to utilities, critical infrastructure, manufacturing, logistics, and fleet management, are all expected to run over 5G networks. Regardless of the application, industry, or model of 5G service, there's one common need: enterprise-grade security. This is a 24/7 business-class level of security that includes visibility across the network and all connected devices; customized, manageable security policies fit for purpose; and granular, dynamic security controls. That's where the real opportunity lives for service providers delivering mobile services.

Enterprise-grade security means that organizations can see and stop advanced attacks against mobile users and devices in real time. Granular user and device-based security policies enable organizations to extend the Zero Trust approach to their 5G network segments.

Because enterprise-grade security is more than a reactive defense posture, it enables built-in value-added security services for new 5G architectures, including multi-access edge computing (MEC), private networks, and network slices that can better serve enterprise customers with new value-added security services. Thinking about 5G security differently opens new opportunities for service providers.

What's Driving the Market?

Enterprises see 5G as a driving force behind digital transformation. It can be a key enabler for any number of business improvements, including:

- The enterprise's desire for data-driven, instant time to market
- Operating expense optimization
- The ability to constantly adapt and evolve the business
- Mass customization
- A more mobile workforce
- Just-in-time logistics
- IoT

IoT alone is booming. It's estimated that there will be 27 billion IoT-connected devices by 2025.[1]

1. Knud Lasse Lueth et al., *State of IoT—Spring 2022*, IoT Analytics, May 2022.

The reliability and performance of 5G are what attract organizations to use it as a foundation for their digital transformation. The 5G standard adds some key security improvements over LTE. However, the built-in security capabilities aren't enough to safeguard business-critical operations and applications enterprises on their own. A small example here is enlightening. If you disconnect your laptop from the corporate IT network and connect it to the 5G network, is it more secure? Is it secure enough? How comfortable are you with that connection?

Sophisticated, evasive cyberattacks are on the rise. Global cybercrime costs, according to Cybersecurity Ventures, are expected to grow by 15% per year over the next five years, reaching $10.5 trillion USD annually by 2025.[2] All enterprise-sized organizations must now assume they will, at some point, be the target of an attack that has the level of sophistication of a nation-state attack.

The stakes are high. Digital transformation initiatives will directly affect business outcomes and revenue, worker safety, consumer safety, highway safety, society's critical infrastructure, supply chains, and even human lives.

The reliable, high-performance 5G connectivity fabric must be backed by enterprise-grade security that delivers:

Visibility: You can't secure what you can't see. It's critical that you are able to get granular about your mobile traffic, down to the specific user, device, and application involved.

Prevention: Enterprises can't afford downtime. Security for enterprise 5G must be able to prevent exploitation of network services and applications, thwart outbound malicious activity, stop packet-based attacks, and detect and prevent application-layer attacks.

Response: Granular visibility leads to granular response. Enterprise-grade security means responding to compromised users, devices, and applications in real time. Your incident response must be able to identify and take action across control and user planes of the network. Service providers have a critical key role in delivering this level of security and better serving their enterprise customers' security needs, but there's an opportunity to be had here and a chance to monetize 5G security, so it's a profit center not a black hole of costs.

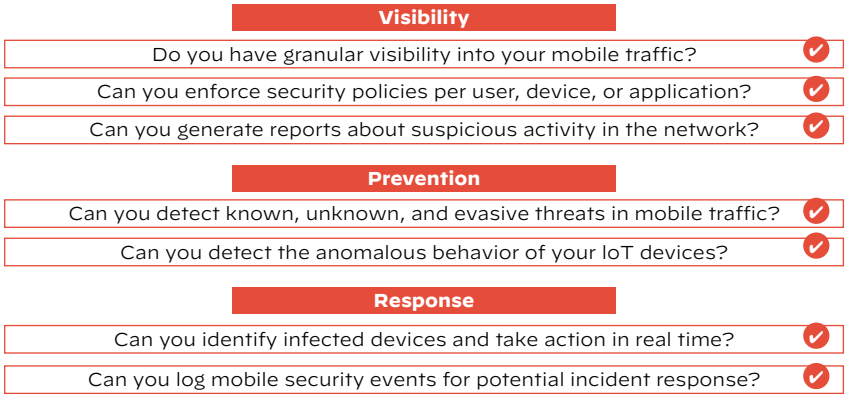

Figure 1: Palo Alto Networks checklist for enterprise-grade 5G security readiness

2. Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Cybercrime Magazine, November 13, 2020.

Three Models for 5G Security Monetization

5G Network Slice Security
Standalone network slices provide a private logical network that can cover a large geography and a variety of dedicated use cases.

5G Private Networks
A dedicated mobile network that can be positioned on-premises or in the cloud is the ideal choice for enterprises that require low latency, high reliability, and support for a high number of devices.

5G Multi-Access Edge Computing (MEC)
MEC uses an on-premises edge server to move mobile workloads and data closer to the end user.

Figure 2: Three models for 5G security monetization

5G Network Slice Security

Network slicing is about transforming the mobile network from a static, one-size-fits-all model to a new approach where logical networks and partitions are created with appropriate isolation, resources, and optimized topology to serve a particular purpose, service category, or individual customer. These standalone network slices provide a private logical network that can cover a large geography and a variety of dedicated use cases, such as vehicle-to-anything (V2x) communication, oilfield communications, machine-to-machine (M2M) communications, and more.

Although the design of network slices is theoretically supposed to ensure greater security, the reality is that the increase in slices brings increased complexity, leading to more configuration errors. Security researchers have also demonstrated a 5G slice escape. Gaining visibility and control of user traffic within individual network slices becomes a more critical task for security.

Applying a next-generation firewall (NGFW) at the N11 interface on a 5G network enables correlation of the Single – Network Slice Selection Assistance Information (S-NSSAI) with the IP traffic inside GTP-U tunnels. This makes it possible for the network operator to inspect user traffic and apply advanced threat prevention per network slice or group of network slices. Combining a real-time threat prevention engine with a comprehensive URL database and elements of application identification will limit unauthorized data and file transfers, detect and block a wide range of exploits, malware, and dangerous web surfing, as well as targeted and unknown threats.

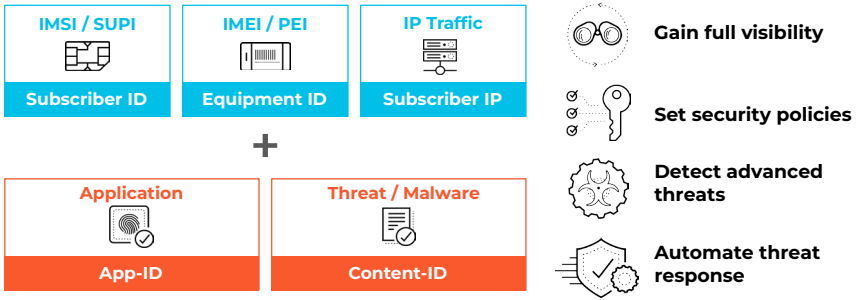

Figure 3: Correlation of user, device, and slice IDs on the user plane with a next-generation firewall provides visibility into potential threats and faster remediation

5G Private Networks

A dedicated mobile network that can be positioned on-premises or in the cloud is the ideal choice for enterprises that require ultra-low latency, the utmost in reliability, and support for a high number of devices. Dedicated bandwidth and infrastructure should be tailored to meet the needs of security-sensitive organizations, such as federal governments, public safety offices, schools, and manufacturers, as well as those operating in rural and remote locations, such as military organizations and mining, oil, and gas enterprises.

The flip side of this new private network approach is that it expands the attack surface and can enable actors with criminal intent to find new attack vectors against the enterprises that use it. Because private 5G networks are deployed as an extension of the enterprise infrastructure, the risk of lateral movement is higher.

As enterprises adopt and implement private 5G network trends, they must adopt a new approach to security. Process control environments, in particular, will need to establish a strong security posture with granular visibility in 5G traffic and automate security enforcement at the 5G user and 5G device level in real time to stop cyberattackers from infiltrating networks, disrupting critical services, destroying industrial assets, and threatening life and safety.

One of the most effective ways to deploy security for private 5G networks is to position an NGFW on the user plane (N3) and control plane (N4) interfaces. This deployment allows the firewall to be aware of mobile identifiers. Ingestion of device ID, subscriber ID, and slice ID data will enable the creation of dedicated security policies per user, group of users, or 5G slices. The firewall is also properly placed to see and stop advanced mobile traffic (Layer 7) threats across exploits, malware, malicious URLs, malicious DNS, spyware, command and control (C2), and data exfiltration in real time.

5G Multi-Access Edge Computing (MEC)

MEC uses an on-premises edge server to move mobile workloads and data closer to the end user. Data is stored and accessed locally while the control plane continues to the service provider's core. Applications perform better and processing tasks happen more quickly when they run near where they're being used. In this way, a MEC environment delivers high-performance, low-latency connectivity for mission-critical tasks. This is particularly important in enterprises such as manufacturing, where a slowdown or break in connectivity can shut down operations entirely.

Similar to private networks, the essence of 5G MEC security is to provide user traffic security at the granular user, device, and network slice level. Enterprise customers for MEC also often prefer to implement perimeter security between their MEC environment and the internet and/or enterprise network (N6). Additionally, as MEC deployments are connected to the service provider's 5G core, it is important to secure the connection between MEC and the core by applying PFCP stateful inspection and rate limit PFCP messages to prevent signaling DoS.

Enterprise-Grade Security Enablers for Monetization

Service providers will need to deliver a security platform with a great foundation. They should develop a robust and comprehensive end-to-end security strategy that encompasses all traffic (data and signaling planes) to protect their networks and provide a safe environment for their customers.

Any security strategy for 5G should start with Zero Trust, a strategic approach to cybersecurity that removes implicit trust all along the mobile landscape, regardless of what the situation is, who the user is, where the user is, or what application they are trying to access. With Zero Trust, the assumption is that every user, app, and transaction is suspect and must be carefully inspected and validated to remove the potential for a security infiltration. Zero Trust secures a network or organization by eliminating implicit trust and continuously validating every stage of digital interaction.

A Zero Trust approach protects all facets of the 5G infrastructure, including all layers, across applications, signaling, and user traffic, as well as all key interfaces. The premise is that you can't secure what you can't see, and you must secure the entire lifecycle of an attack—and lock down all the places where an attack may occur. In a 5G environment, this should include:

- Implementing detailed 5G security policies to control what apps and data users can access
- Defining identity to encompass all humans, machines, and processes that require access to protected assets
- Detecting and preventing threats in data transactions, whether they involve users, applications, or core network processes

For a more detailed explanation of Zero Trust for 5G, see Breaking Trust: Building Sustainable Security for 5G with Zero Trust.

The responsibility for securing the 5G network, its many assets, and everyone and everything that touches it is shared by the service provider and the enterprise. This is just a logical extension of the public cloud shared security models advocated by several of the large public cloud providers.

In short, the service provider is responsible for securing the infrastructure, while the enterprise is responsible for securing its own data. It's what enterprises have come to expect from previous generations of carrier networks.

Telco-Grade Meets Enterprise-Grade

5G security must be simultaneously telco-grade as well as enterprise-grade. Let us explain. When we say carrier-grade, we mean high-performance and highly reliable—what service providers are known for. Any security components introduced to the mobile network must support its general service level and availability requirements.

Enterprise-grade security is about the high performance and highly reliable levels of service and security feature sets conventionally offered to enterprises. This is where the opportunity lies for service providers.

Putting Automation and Integration to Work

Advanced automation and deep integration with cloud service providers, applications, and enterprise networks are key technology drivers for 5G networks. Mobile networks are more complex than ever before.

Security must be delivered with the same paradigm—automated, integrated, and customized. Similarly, as 5G cloud resources are scaled up and down based on the changing resource needs, we need the same for 5G security. That is, we need to automatically secure any new 5G services the moment they are spun up, thereby reducing the risk of human errors, increasing accuracy, and making sure they are never put into production without protection.

The only way to achieve this is to integrate security as part of the 5G cloud and service orchestration workflows.

By employing security automation, powered by artificial intelligence and machine learning, service providers can deliver a higher security level to their enterprise customers. This will also reduce the total cost of ownership.

Mobile identifier-based security is a fundamental enabler for effective security automation. When service providers employ 5G mobile identifiers to create granular policies and thorough threat correlation, they add yet another layer of security. With this approach, they can identify suspect apps and correlate users' IDs to them, apply policies, and identify infected users in real time. This greatly reduces the chance of a major security breach.

Security from a Network Service Provider: A Smarter Option

Anyone can connect a firewall to the gateway of a private network, slice, or MEC environment. In some cases, it will even be connected to an existing firewall, but the question to ask is, what is the added value that a network service provider brings to security? And the answer, as always, is in the data.

Mobile networks are not just a pipe carrying data from one place to another. They are one of the most advanced pieces of modern technology. Think of the sophisticated logic that can predict when a device will have bad service and automatically solve it by handing it over to another tower, providing a higher QoS class, and so much more. In the case of security, the value is in the user and device identities. Security can be much smarter and more efficient when you have a unique identification of the user.

The user identification data exists inside the service provider's mobile network, and only they can access it. The service providers are in a unique position to provide differentiated 5G security services for enterprises. For example:

- **Real-time identification of infected or compromised devices without the need for manual inspection, correlation of IP addresses, or any human intervention**. This is especially important in reducing security response time in mission-critical environments, such as hackers compromising assets in power plants, transportation, manufacturing facilities, or critical national infrastructure.

- **Granular security policies for applications**. You can restrict applications and processes to certain applications only. For example, a Siemens manufacturing robot has no reason to connect to any other application than the Siemens industrial control system.
- **Granular security policies for users and groups**. You can create different policies for different users or groups of users. For example, if an enterprise has subcontractors connecting to the network, they can be isolated into a dedicated segment.
- **Accelerated security investigation**. Digital forensics can be accelerated and achieved with reduced resources when the mobile identifier-based security logs are readily available to the investigators. A breach investigation cannot rely on temporary IP addresses generated by devices. Accurate analysis demands logging data on the level of unique mobile identifiers of the users (SUPI) and devices (PEI).

These granular 5G security capabilities, which service providers are in a unique position to deliver, will help build enterprises' trust in 5G networks. Service providers can also generate sustainable revenue streams from the same security capabilities.

Fast-Tracking Enterprises to Security Through a Fully Managed Service

The managed security service provider (MSSP) business model has been on the market for a number of years now. Among service providers, it's become common practice to offer cybersecurity services as an addition when selling common network services, such as a leased line or VPN service. Service providers are poised to transition to also selling 5G security in an MSSP package, but there are a few key enhancements that service providers may want to adopt if they want to be the trusted security advisor for an enterprise customer:

- 5G security should not be an afterthought. It should be part of the overall service creation process. Whenever enterprises order a 5G slice, multi-access edge computing (MEC), or a 5G private network, they should have the option to add security policies and security resources that are baked in from the beginning (day 0). Service providers can prepackage day 0 provisioning and simplify the ordering process for enterprises.
- Security absolutely needs to be monitored 24/7 with quick-response SLAs in case of an event.
- The service provider operations teams must be able to see and understand what is happening in their 5G networks to properly respond to security incidents. You can't protect what you can't see.
- Automation is a critical capability in 5G security. In almost every layer of the network, there needs to be an automated response to mitigate the risk, de-escalate the situation, and give enough time to the enterprise and service provider security experts to assess the situation.

Packaging and selling 5G security can be the most natural service for service providers to sell after connectivity. The enterprise market is well aware of

the security need. Service providers can add value using their network intelligence. More critically, a well-qualified 5G security operations center can provide enterprises with the trust they need to migrate their critical infrastructure networking to 5G.

Finding the Right Fit Among Partners

To implement this level of 5G security, service providers need partners that understand the particular challenges—and opportunities—of a 5G network. They should work with a partner that offers capabilities for:

- Seeing into and controlling enterprise 5G network traffic
- Detecting and stopping malware, viruses, URL, command and control, and other vulnerabilities within the user plane
- Quickly correlating, isolating, and quarantining infected devices from the network
- Creating dedicated security policies per user and group of users
- Packaging 5G security solutions by types of use case (e.g., MEC, slices, private 5G networks) that make it easy for service providers to incorporate into their portfolios

Palo Alto Networks 5G-native security allows service providers to safeguard their networks, users, and clouds, as well as back their customers with the enterprise-grade security they need for tomorrow's 5G economy. 5G-Native security offers a comprehensive approach to protecting all facets of 5G networks. Service providers can deploy a Zero Trust architecture for their own 5G network infrastructure and assist their customers in achieving the same for their 5G environments. From an enterprise and organization perspective, they should be able to extend the same Zero Trust approach they use in their other network segments to 5G.

Growing Market Share Through Better 5G Security

The 5G market is still maturing. Service providers have an opportunity to educate enterprises about the advantages of 5G, as well as to work with them on securing critical enterprise applications.

Service providers can accelerate the adoption of 5G services by backing these networks with the level of security, flexibility, and reliability that enterprises need for their business-critical applications. Service providers can do that by choosing partners that offer 5G-native security solutions to best-in-class capabilities across network security, cloud security, security orchestration and response, as well as attack surface management. Service providers should:

- Build enterprise-grade security in the new enterprise offerings (e.g., slice, MEC, private network) from the beginning.
- Identify new opportunities to serve enterprise customers with value-added security services.

- Promote the smarter security capabilities that come only from the user and device identification data inside the service provider's mobile network when paired with a 5G-capable machine learning-powered NGFW.
- Launch new services faster with automation-friendly security that keeps up with dynamic 5G service orchestration.
- Reduce incident response time with automation and orchestration tools for the 5G SOC.
- Secure their entire 5G infrastructure with a Zero Trust architecture where all layers, locations, attack vectors, and the whole software lifecycle are protected—the security foundation for the entire 5G infrastructure.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com