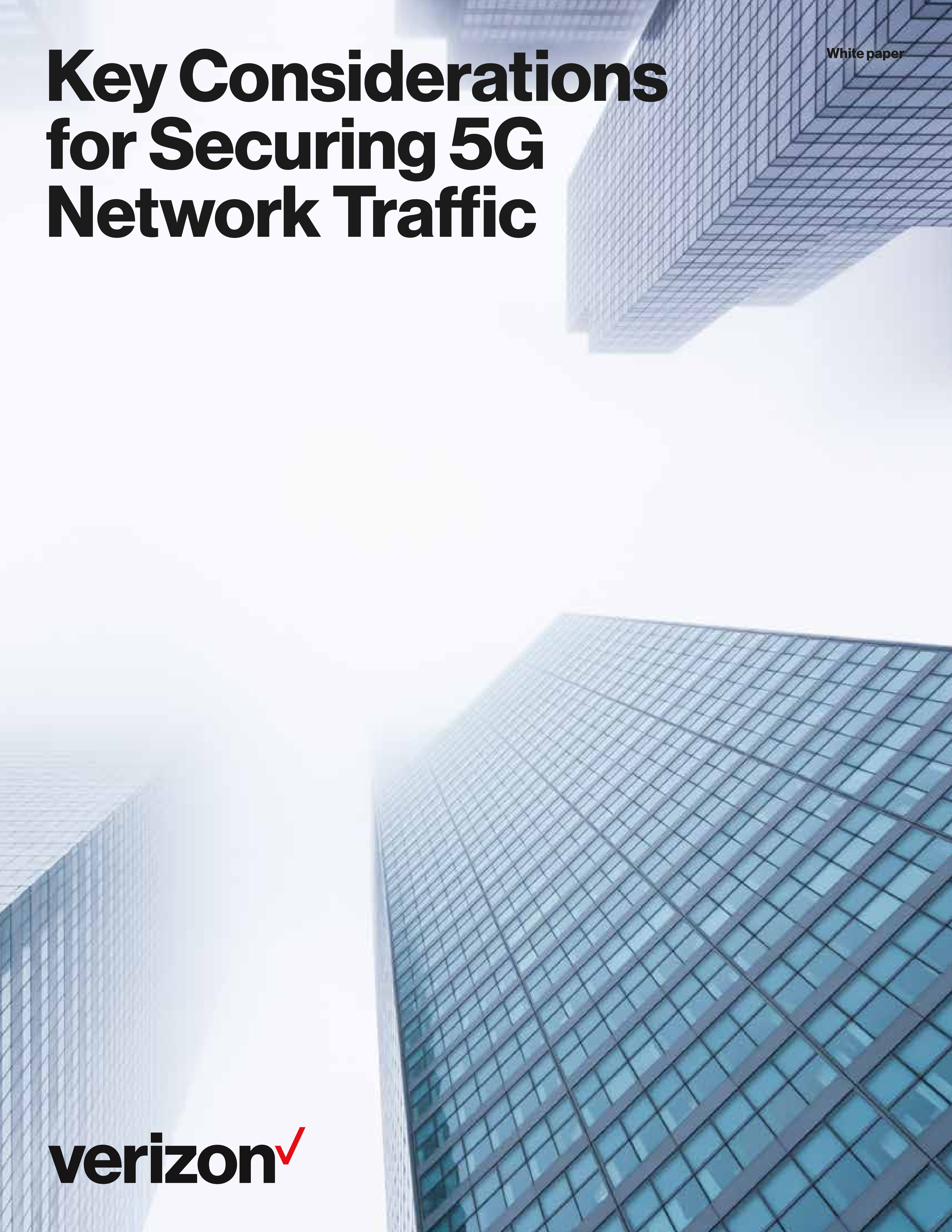
White paper

Key Considerations for Securing 5G Network Traffic



verizon

The enormous growth in enterprise data, driven in part by a dramatic increase in Internet of Things (IoT) adoption—from 31 billion devices to 75 billion by 2025[1]—is putting pressure on technology professionals to achieve higher network speeds and support greater device density, all while ensuring both the security and governance of data. This year's Verizon Data Breach Investigations Report (DBIR) found that nearly 90% of all breaches were financially motivated.[2] With so much proprietary data being generated, networked and stored, it's clear that the adoption of 5G technology will likely affect every company's overall security posture.

This paper looks at the reality of today's threat landscape and highlights opportunities and risk factors in new wireless use cases made possible by 5G.

The evolving threat landscape

The current state of network security informs the threats that enterprises can expect to see as they move toward 5G networks. The 2020 DBIR reports that 45% of all breaches were due to hacking, while 22% were caused by errors – either operational, by users or in misconfigurations. Nearly three-fourths of breaches were perpetrated by external actors, with organized criminal groups behind 55% of them.

Collectively, we are getting better at containing breaches; the DBIR found most were controlled in days or less. However, the criminal elements behind breaches are raising their sights, as 72% of breaches involved large businesses, even though more than half of victims had some personal data compromised as well. That breaches are a business is clear: 86% were financially motivated and 27% of malware incidents led to a ransomware demand, according to the report.

One of the factors in the growing number of breaches is the proliferation of endpoints, both traditional and machine to machine (M2M), including sensors and other IoT devices. With projections of nearly 15 billion M2M devices attached to IP networks by 2023,[3] devices will outnumber humans by at least a three-to-one margin in that time frame. It is difficult to gauge the impact that IoT devices have on current networks; unfortunately, many devices are configured and shipped with simple default passwords that are easily compromised by bad actors.

Enter 5G: Security boon or bane?

As enterprises plan broader adoption of emerging 5G services, there are some important factors to consider regarding services, devices and security processes that can lower their overall risk posture.

5G is simply a faster, more efficient way of moving IP traffic with lower latency over wireless connections and therefore does not present new attack surfaces itself. But it is reasonable to expect that as private 5G networks are deployed, they will face a progressive expansion of the threats already seen on 4G networks as well as the introduction of threats that are novel in both design and intent.

Thus, as 5G networks begin to introduce support for new use cases – many previously the sole domain of wired networks – additional vigilance will be crucial. For example, data-rich applications that call for more M2M interactions and employ a large number of wireless endpoints can create new attack surfaces for financial gain, including industrial espionage achieved by gaining access to information through unmanaged IoT devices connected to the network.

Although 5G leverages security measures that already exist in 4G, it has many additional security innovations to help mitigate unknown risks and ensure confidence.[4] These enhancements include:

- Support for end-to-end encryption of both in-band user data and out-of-band signaling, making it nearly impossible to intercept information over the air. Every access is authenticated by the home or provider network to ensure that the network that owns the subscriber verifies its legitimacy
- Identical network verification, whether connected via 5G or Wi-Fi, which helps eliminate rogue base stations acting as international mobile subscriber identity-catchers (IMSI-catchers). This network-agnostic authentication framework provides better home network control no matter how a device is being used and prevents snooping to catch credentials
- A new Secure Edge Protection Proxy (SEPP) that prevents threats from less-secure interconnected networks from harming the 5G networks they are connected to
- Network slicing, a mechanism that leverages software-defined network configuration to logically subdivide the physical network into multiple virtual "slices" of differing network capabilities, with the ability to isolate the network traffic from other slices. Previously, providing such differentiated capabilities and traffic isolation required building separate physical networks. With 5G network slicing, service providers can more precisely "tune" network capabilities to meet their specific application needs, segregating critical applications into their own slices, to reduce impact from other applications that may otherwise have been compromised

The 3rd Generation Partnership Project (3GPP) is the group that promulgates standards for 5G, specifically securing base stations, antennas and the core network by leveraging security protocols from organizations such as the Internet Engineering Task Force (IETF) and the National Institute of Standards and Technology (NIST). These enhancements in 5G standards are designed to address the security vulnerabilities of wireless communications.

Best practices in securing 5G

When it comes to data security, the best offense is a good defense. Here are some considerations when planning a 5G deployment.

Cybersecurity frameworks provide a methodological approach to the components of a security profile, so enterprises will not have to make it up as they go along. An excellent starting point would be the NIST cybersecurity framework, based on widely adopted standards and designed to reduce cyber risks to critical infrastructure such as 5G networks. The NIST framework helps organizations better understand the network's myriad components, especially where exposed interfaces exist. By breaking down a data security plan into equal components, interfaces, transition points and other aspects that provide vectors for bad actors to gain access, a framework can be the first line of defense.

Encryption should be used everywhere. 5G provides end-to-end encryption, both of setup signaling and during user data traffic transfers. However, it must be enabled to provide protection. Ensure that both data and signaling are encrypted as the default. Then, adopt a zero-trust stance for every application. Every single transaction should include authentication to help ensure the highest levels of security for all data and voice, regardless of its sensitivity. To maximize security, there should be no ring of trust and no perimeter, and everyone should be considered suspect and challenged. Today's networks are so complex that it is simply too hard to say where a trust boundary should be.

Just as important as adherence to standards is a deep understanding of the 5G supply chain. Enterprises should ensure that their 5G hardware—down to the chip level—is procured from trusted sources and that those devices are known to be free of backdoor access mechanisms. By the same token, every organization should have the assurance that the 5G firmware and software that power their devices is well understood from a safety perspective, and that they would not permit, for instance, some open source malware pulled from a code repository to infect devices or even a carrier's 5G core.

Finally, every organization should adopt enterprise best practices for securing all applications. Here are some best practices acknowledged by industry leaders:

Segregation of duties: This keeps a single individual from having the ability to subvert the overall security process.

Role-based access controls: Access to information or resources should be limited to only those authorized user roles or applications that require that access.

Principle of least privilege: Users should be granted only the minimum level of access to perform actions necessary for their job function.

Multifactor authentication: Wherever possible, require two or more authentications for a remote login to enhance overall security.

Modernization: Consider updating older, unmanaged assets that may be currently connected to the network. Ensure that older devices or sensors are properly secured, as they will present an attractive attack surface in an otherwise secure network configuration.

Governance: With the expected growth of wearable connected medical devices as part of the IoT movement, adherence to regulatory mandates such as HIPAA, payment card industry (PCI) and other governance guidelines will become a 5G issue. By working with device, software and network providers, organizations can ensure that these devices do not become the broken link in a secure data chain.

How Verizon helps

As one of the driving forces behind 5G, Verizon has become a provider of choice for many organizations that are transitioning to 5G wireless networks. With a global presence including more than 2,000 U.S. retail stores staffed with knowledgeable professionals, we have experience as an enterprise 5G user ourselves and have learned about security from our own adherence to PCI, HIPAA and other compliance mandates. We build on that experience and incorporate it into our own services and products offered worldwide.

At Verizon, security is baked into the 5G ecosystem. We adopt security protections through a strict vendor and product selection process, going beyond function selection to create a model for products with built-in security controls. This means not only hardening devices but hardening the physical and digital supply chains as well. When we make vendor software updates and patches available, we strive to ensure they are safe, secure and free from security holes.

We are proud of our involvement with a variety of industry partners and security bodies. As a founding member of two key 5G security organizations—the Council to Secure the Digital Economy and the O-RAN alliance—we are committed to leading the global effort to advance the security of the IoT and promote open, interoperable, standards-based virtualized 5G radio base stations and antennas. Verizon also partners with the Communications Information Sharing and Analysis Center (Communications ISAC),[4] which, as part of the U.S. Department of Homeland Security, is where the security organizations and other communications companies convene with U.S. government partners to promote the security and reliability of our nation's communications infrastructure and services.

As a result, Verizon's 3GPP standards for security architecture in 5G include recommendations from the IETF and NIST, such as mutually authenticating user equipment and the base station to prevent fraudulent access and disclosure of credentials to eavesdroppers, since nothing—signaling or data—should ever be transmitted over the air in the clear.

Verizon also ensures that our smartphones and other retail 5G user equipment conform to not only industry security standards but to our own device security requirements and processes. For instance, we mandate the use of a Universal Mobile Telecommunications System (UMTS) SIM card[4] equipped with a tamper-resistant element to prevent the exposure of network authentication and subscriber privacy credentials, which are stored on the UMTS SIM.

In that way, with the help of automated testing pipelines, we test, inspect and use standardized configurations to build a secure 5G network that focuses on every component of the network, including phones, MiFi devices and routers. Every component must conform to both industry standards and our strict device security requirements.

Our 5G services are powered by a new software-defined network architecture that can let enterprises isolate different applications and services into slices of resources and traffic, further enhancing security like virtual private networks do—only with simpler allocation and isolation. In this way, enterprises can separate and protect mission-critical systems from non-managed IoT devices, so a distributed-denial-of-service attack does not impact business-critical functions.

Finally, Verizon brings decades of experience in managing enterprise networks, and we are busy applying lessons learned from our prior network deployments to our 5G network and devices. We have the tools, products and people in place to help our partners and end-user customers understand their own security posture and plan to keep evolving their security strategies as 5G evolves.

Next steps

As the first company to launch a commercial 5G wireless service, Verizon is ready now to help secure your 5G environment. To learn more about how Verizon 5G can help ensure that your business maintains a strong security profile, please contact your Verizon Business Account Manager.

verizon✓

[1] "The Future of IoT Miniguide: The Burgeoning IoT Market Continues," Cisco, July 19, 2019.

[2] "2020 Data Breach Investigations Report," Verizon, 2020.

[3] "Cisco Annual Internet Report (2018–2023)," Cisco, March 9, 2020.

[4] "First Principles for Securing 5G," Verizon, December 2019.