Security by design: How Verizon approaches 5G security

A primer for public sector agencies and private enterprises.

verizon business

Why read this paper?

5G has emerged as a powerful enabler of next-generation capabilities for the public and private sector, inspiring new and innovative use cases that deliver on the long-promised benefits of "digital transformation." This paper examines the cybersecurity considerations related to the ever-growing adoption of 5G. It provides assurance and evidence that security—like speed and low latency—is a key design feature of 5G technology. This paper also explains where and why specific security controls are built into Verizon's 5G networks—both public and private—and how these controls align with security frameworks and policy-makers (such as CISA, 3GPP, NIST and IETF) to enhance the confidentiality, integrity and availability of sensitive data traversing 5G networks.

Introduction

In just a few short years, "5G" has gone from business-buzzword to business-ready, with public sector agencies and private enterprises embracing the power and the possibilities of this high-speed, low latency form of cellular network connectivity. To call 5G a "game-changer" may have sounded like hype four or five years ago, but today it is the very real foundation for rapidly-maturing capabilities like smart grids, smart cities, telemedicine, and autonomous vehicles.

With 5G, government agencies and private businesses are exploring innovative ways to serve their constituents and customers while also increasing operational efficiencies through a host of now-common acronyms that harness the power of 5G. AR (augmented reality), VR (virtual reality), AGVs (autonomous guided vehicles), IIoT (industrial internet of things), (MEC) mobile edge computing, and AI and ML (artificial intelligence and machine learning) are just a few of the transformational technologies that make up the new alphabet soup of next-generation networking.

But while most media coverage of 5G focuses on its speed, one attribute of this network technology is often under-examined: How secure is 5G?

Non-standalone, standalone, public and private 5G networks

When 5G first started rolling out around 2018, it was initially built with a 5G radio access network (RAN) that used a 4G core. This meant 5G could be rolled out without the creation of completely new network infrastructure while still providing higher speeds and improved reliability. This approach is called 5G non-standalone (NSA), and it was a necessary intermediate step as the world transitioned from 4G to 5G.

> "5G has emerged as a powerful enabler of next-generation capabilities for the public and private sector ... this paper examines the cybersecurity considerations of implementing 5G and provides assurance and evidence that security—like speed and low latency—is a key design feature of 5G technology."
>
> **Quote attribution**

5G standalone (SA) was the next step and introduced the 5G core, which means that the entire network, from device to radio access network to core, is built specifically for 5G workstreams. Because of this, 5G SA can help take 5G benefits such as faster download speeds and greater capacity even further. Verizon's 5G core—and thus its 5G SA technology—is built on the Verizon Cloud Platform, which Verizon created specifically for telecommunications workloads. No other telecommunications company has taken this step; others are using cloud systems from public hyperscalers. Because it's built specifically for telecommunications workloads, it can support the advanced technologies and services that provide the reliability and performance customers expect now, as well as what they'll need in the future.

As the table below illustrates, there are enhancements to 4G LTE security as well as a number of new security features in the 5G SA architecture that did not exist in 4G LTE. Taken all together, these capabilities help eliminate many of the security attack methods favored by bad actors in previous generations of cellular technology.

Security comparison between 4G LTE and 5G

Function	4G LTE	5G (standalone architecture)
Privacy and Integrity Cipher	• Encryption on radio path • Control plan ciphering • 128-bit algorithms supported	**In addition to 4G LTE:** • 256-bit alorithms proposed for future release • Integrity implemented preventing unauthorized change of user data
Authentication Key Agreement (AKA)	Shared key provisioned Mutual authentication (UE and network)	**In addition to LTE:** • Access-agnostic authentication (EAP) is used • 5G-AKA and EAP-AKA supported for both 3GPP and non-3GPP • Protects the confidentiality of non-access stratum (NAS) messages
Subscriber Permanent Identifier (SUPI)	Identifier sent in plain text	Subscription Concealed Identifier (SUCI) is used instead of SUPI
Security Anchor Function (SEAF)	Not available	Allows re-authentication of the UE when it moves between networks
Home Control	Not available	• Home Public Mobile Network (HPMN) can verify UE is present • Useful in roaming scenarios with Visiting Public Mobile Network (VPMN) • Assists in fraud prevention
Network Exposure Function (NEF)	Not available	• NEF securely exposes capabilities to other Applicable Functions (AF) • Enables secure provision of information in the 3GPP network • Certificate based mutual authentication may be used
Security Edge Proxy Protection (SEPP)	No available	• Protects the home network edge, acting as the security gateway • Security between the home network and visited networks

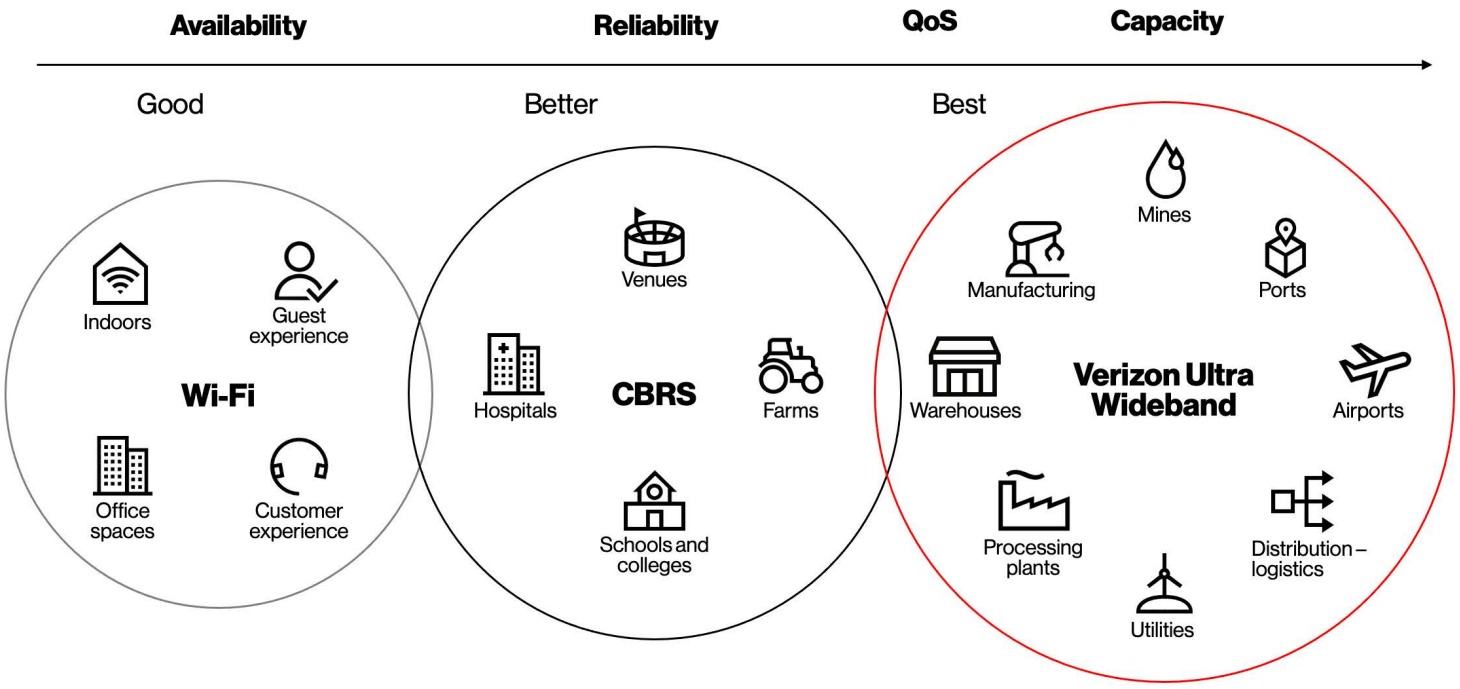
A further distinction that can influence overall security in both 4G and 5G networks is whether they are public or private. A public 5G network is simply the main domestic network built by Verizon and other operators to serve consumer and enterprise customers.

Unlike public networks, private 5G networks often cater for very specific use cases focused on a single enterprise or location. These networks often have more specific requirements than consumer mobile services, such as environmental monitoring or coordinating the safe movement of semi-autonomous vehicles. So while private 5G uses the same technology as public 5G, it offers a network that is exclusive to the customer, with the bandwidth dedicated to what the organization needs. This provides greater control over the data and network, meaning data is more secure since it doesn't traverse a public network.

Private 5G offers many additional benefits for those concerned about security. While the types of cyberthreats remain the same to public and private networks, the fact that the private network is often used exclusively in an area that is physically controlled and secured by an organization creates an additional level of protection. For example, for someone to get close enough to perform signal-jamming, they would need to be physically on site, which means getting past physical security and remaining undetected.

Private 5G networks are considered relatively easy to integrate for organizations that already have 4G LTE connectivity. They enhance organizational capabilities by providing high bandwidth, low latency coverage that can support scaled implementations of artificial intelligence and machine learning, virtual and augmented reality applications, remote monitoring, IoT devices and other networked devices.

Historically, Verizon has used CBRS spectrum – Citizens Broadband Radio Service – to supplement its low and mid band deployment of 4G LTE service and private network offerings. In 2022, however, Verizon expanded the 5G network to CBRS in parallel with its ongoing 5G deployment on C-band. This expansion delivered an increase in capacity and speed on the 5G Ultra Wideband network with the addition of 5G service running over CBRS spectrum.



Security and private 5G versus Wi-Fi

5G represents an evolution and improvement over 4G cellular technology,[1] given the incorporation of features such as user equipment authentication and authorization, end-to-end encryption, privacy enhancing features, and zero trust architecture, among others. These elements boost security by enabling 5G to natively secure communications across the network. Furthermore, private 5G can use licensed spectrum, which reduces interference issues from other wireless devices and enables network slicing, resulting in improved Quality of Service. Even private 5G on unlicensed CBRS spectrum affords a degree of security as it utilizes SIM cards rather than SSIDs such as WiFi relies upon. Wi-Fi, for its part, only uses unlicensed spectrum, making it subject to difficult-to-control interference in "noisy" environments, adding to the risk of connectivity failure or compromise.

It is expected that Wi-Fi will continue to play an important role in consumer and office LAN environments. In addition, due to better performance compared to Wi-Fi 5 for peak data rate, latency, density and energy efficiency, Wi-Fi 6 will be used for other basic enterprise use cases. Verizon manages Wi-Fi solutions at scale for customers today and expects to do so in the future, supporting customers' needs wherever they are on their digital journey.

Aligning 5G security with CISA recommendations and guidelines

The Cybersecurity and Infrastructure Security Agency (CISA) —an agency of the United States Department of Homeland Security responsible for strengthening cybersecurity and infrastructure protection—in 2021 issued a paper entitled "Potential Threat Vectors to 5G Infrastructure."[2] That paper noted three key attack vectors: policy and standards, supply chain and 5G System Architecture. Verizon's experience as the operator of one of the world's largest 4G LTE networks gave it a head start to meet the security challenges of 5G. In fact, early and ongoing work by Verizon to develop and deploy secure 5G connectivity directly addresses these threat vectors.

Policy and standards: In 2021, CISA announced the standup of the Joint Cyber Defense Collaborative (JCDC),[3] a new agency effort to lead the development of cyber defense operations plans, and to execute those plans in coordination with partners from the federal interagency, private sector, and state, local, tribal, territorial government stakeholders. The intent was to drive down risk before an incident and to unify defensive actions should an incident occur. Verizon was one of several founding members. Further, Verizon participated in the development of and influenced the 5G standards through the 3rd Generation Partner Project (3GPP), which has previously developed standards for LTE, LTE-Advanced and LTE Advanced Pro for commercial cellular/mobile systems.

Supply chain: Verizon's trusted supply chain is the foundation of its secure 5G network. Leveraging a diverse, competitive marketplace of trusted vendors of network hardware and software is a security imperative for Verizon and other 5G service providers. This is the fundamental principle of our supply chain security policy; it guides everything we do in vetting our trusted suppliers and in testing and configuring the equipment and devices we acquire from them. For both hardware and software, Verizon purchases all our 5G technology from a small group of sophisticated vendors with whom we have close, trusted relationships developed through thorough vetting and scrutiny, including pre-deployment testing of equipment. For instance, Verizon has long been aware of concerns about Chinese technology and does not use Huawei or ZTE when building its network infrastructure.[4]

Verizon has a complex and rigorous risk management framework for identifying and eliminating risks across our global supply chain for numerous products and services, including public cloud services. Verizon's contractual supplier security requirements, which are designed to address risk management goals, are based on Verizon's own corporate information security policies as well as open industry standards and control objectives found in National Institute of Standards and Technology (NIST) guidance and additional security standards regimes such as ISO2700x, SSAE16, PCI-DSS, HIPAA and others.

5G system architecture: Verizon is proud of its 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 network security 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), 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.

Verizon's 3GPP standards for security architecture in 5G adopted recommendations from the Internet Engineering Task Force (IETF) and National Institute of Standards and Technology (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.

By design, 5G SA features many additional security innovations to help mitigate unknown risks and ensure confidence in its use. These enhancements include:

Support for end-to-end encryption: Both in-band user data and out-of-band signaling is encrypted, 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.

NEW **A new Secure Edge Protection Proxy (SEPP):** This new 5G core element prevents threats from less-secure interconnected networks from harming the 5G networks to which they are connected. Further, identical network verification 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.

Network slicing: This is 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.

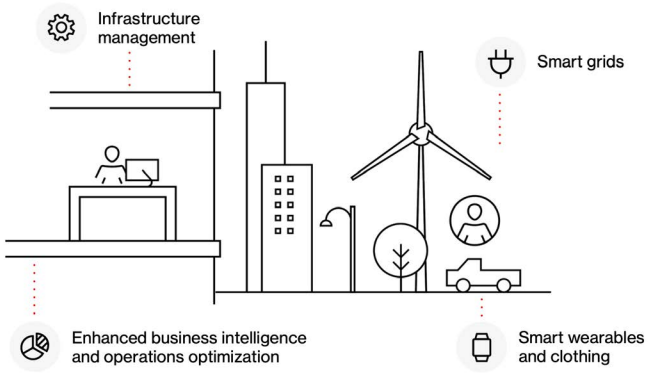
Device security: Verizon ensures that its smartphones and other retail 5G user equipment conform to not only industry security standards but to Verizon's own device security requirements and processes. For instance, Verizon mandates the use of Universal Mobile Telecommunications System (UMTS) SIM cards 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, Verizon tests, inspects and uses 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. The vSIM technology recently patented by Verizon should further increase security and enhance the user experience. The blockchain-based vSIM can be used by and transferred between different devices associated with the user account or temporarily assigned to other users. This extends the capability of "virtualization" into the end-user device. 5G, IoT and cybersecurity.

5G, IoT and cybersecurity: Ensuring system, application and data availability is one of the cornerstones of cybersecurity, along with the integrity of systems and data, and the protection of confidential information. Massive IoT deployments enabled by 5G require a security operations capability that can scale to secure the devices, manage vulnerabilities and ensure the secure transfer of data to analytics platforms. Monitoring for attacks on IoT devices, and having a security capability that can quickly detect and respond to attacks on these devices, is crucial. In more than one recent headline-making attack, compromised IoT devices were used in massive Distributed Denial of Service attacks that resulted in lower availability.

Cyberattacks on 5G-powered applications – including malware and ransomware attacks – can cause significant disruption to manufacturing processes, imperiling customer service and revenue generation, while also causing contractual liability, regulatory non-compliance, and reputational damage. Poorly-secured data-in-transit can lead to the theft of proprietary information and/or personal customer data. Human life is also at stake if 5G-enabled use cases do not factor security into their design and execution. An oft-cited example is the worst-case scenario involving a 5G-enabled autonomous vehicle: who wants to ride in the back seat of a self-driving car that isn't properly protected against cyber-carjacking?

Attacks on other public and private sector industrial facilities can lead to catastrophe. In fact, these kinds of attacks have already occurred, showing this is a very real risk. In 2014, a German steel plant suffered significant damage as the result of a cyberattack. And in early 2021, hackers attempted to poison the public water supply by infiltrating water plant industrial control systems in a Florida town.

Fortunately, Verizon is a leading contributor to industrywide 5G and IoT security initiatives – because security must extend beyond the network to the endpoint, including IoT devices and other emerging endpoints. Verizon understands how to apply network scanning, anomaly detection, segregation and other security techniques across OT and IT networks to optimize protection and performance.



Partitioned access control systems: Verizon enforces its established standards that require that an individual's access to its network, be it physical or logical access, is based on the principle of least privilege, providing the access an individual needs in order to do his or her job—no more, no less. The Mobile Switching Centers (MSCs), Network Equipment Centers (NECs), Network Operations Centers (NOCs) and other sites housing critical equipment are designed and equipped with access control systems with multiple, layered security access zones such as core equipment spaces, building services spaces, office spaces, public spaces, shipping/receiving spaces, etc. Critical spaces are surrounded and shielded by less critical spaces. Electronic keys control access to the buildings and interior spaces; mechanical keys are issued to only a few critical personnel as backups. Access to any of those spaces is controlled by the access control system for each individual, according to the legitimate need for his or her access. Since not all employees need access to all spaces all the time, the access control systems can be programmed to allow an individual's access by time of day, day of the week, per room or space, as required. The access control systems maintain log files of all access attempts, authorized or unauthorized. In addition, a facility's IDS may also be monitored by a third-party central station depending on the facility and local assessment of the security environment. Local personnel are on-call 24/7 to respond if necessary.

Network access control and cell site security: The primary concern regarding cell site security is that the distributed nature of 5G, including small cells, might increase the risk that bad actors could physically tap into Verizon equipment to eavesdrop or to disable it. Verizon's network infrastructure is monitored 24/7 to identify and address potential tampering. All of the relevant data flows—including between subscribers and 5G antennas, and among different parts of the 5G networks—are encrypted and subject to various controls (e.g., firewalls) to prevent an "infection" associated with one piece of equipment from affecting the rest of the network. If physical security were to be breached at the cell sites, specific controls are in place to limit the access of an attacker to the network. Unused network ports at the cell sites are disabled to prevent their use by attackers. Equipment at the sites is configured to be automatically provisioned so that attackers cannot overwrite the configuration locally. Finally, only network elements authenticated to the Verizon network are allowed to connect. Rogue systems are denied access and raise an alarm. Therefore, while bad actors may in some cases have the ability to disable or destroy distributed equipment such as small cells that sit at the edge of the network, this risk is more akin to that of a physical event—such as a powerful storm—than a cyberattack. Such an event (which can result in a temporary localized absence of service) may trigger Verizon's resiliency response plan, resulting in direct coordination with local, state and federal disaster management teams.

DLP: To identify issues not prevented by other controls, Verizon also uses detective mechanisms like intrusion detection and network Data Loss Prevention (DLP) to analyze network traffic for malware and unauthorized information transmissions. Looking forward, the use of AI promises a more efficient approach to security, allowing continuous monitoring for potential threats. The 5G network creates the opportunities for use of AI in the network through incorporation into the software-based architecture. Large amounts of data could be quickly analyzed for rapid detection of threats and immediately mitigated through the combination of AI capabilities with security automation.

Conclusion

From changing the very nature of collaboration and education to revolutionizing how data is used to control costs, improve services and keep people safe and healthy, 5G provides the foundation for profound change in business, government and society itself. As its use becomes more prevalent and pervasive, new and unexpected 5G-driven capabilities will emerge—as will new and unexpected threats. Neither the government nor any individual private sector entity can secure our nation's communications networks alone, which is why Verizon continues to invest heavily in partnerships with the government and other important stakeholders in the private sector to secure 5G.

Contact us

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

verizon business

1. verizon.com/business/resources/whitepapers/first-principles-for-securing-5g/
2. cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20%281%29.pdf
3. cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative
4. verizon.com/business/resources/whitepapers/first-principles-for-securing-5g/