Manufacturers get industrial strength security with private 5G.

verizon

Contents

Why read this white paper?

5G technology has quickly evolved from aspirational to business-ready, and many organizations are already realizing the benefits of private 5G. Forward-thinking corporations – particularly in the industrial and manufacturing spaces – spent the last few years developing use cases for 5G that they hoped would transform the way they operate. Now they are seeing it happen, for real – on the factory floor, in the laboratory, and out in the field. The promise of the "Fourth Industrial Revolution" is becoming a reality.

But security, as always, remains a concern.

5G technology is engineered with enhanced security controls to better protect sensitive data and systems, but 5G won't automatically solve deep-seated, legacy deficiencies in an organization's security program. If a corporate security team's oversight efforts have traditionally struggled to keep pace with the business-lines' aggressive push for transformative technology, such as cloud, mobile, and the Industrial Internet of Things (IIoT), it will continue to struggle after it adopts 5G.

That said, there is a path forward to a more secure business driven by 5G.

The NIST CSF (the US Department of Commerce/National Institute of Standard and Technology Cybersecurity Framework) provides the guidance that organizations need to improve security across the IT estate and mitigate the risks inherent in certain 5G use cases. It is viewed as a global standard which other standards, such as ISO 27110, are aligning to.

This paper:

- Describes the differences between public and private 5G
- Explores the use of private 5G in industrial settings – and the associated cybersecurity considerations that must be addressed
- Details how the NIST CSF can be leveraged to enhance security as organizations embrace 5G and "Industry 4.0".

Collaboration between security teams, IT and network teams and non-IT business executives is key to fully – and securely – realizing the benefits of 5G technology. We hope this white paper provides a common frame of reference to enable that collaboration.

A good problem: So many options for advanced connectivity.

In many industries – manufacturing, distribution centers, mining and energy production – use cases built on advanced networking capabilities are transforming every aspect of the business.

Machine-to-machine communication is rewriting years-old standard operations procedures, and the IIoT is generating massive amounts of data that, when analyzed in near-real time, can be aggressively capitalized. Emerging use cases such as time-sensitive networking over wireless and autonomous guided vehicles (AGV), or bandwidth-hungry use cases such as connected video cameras and augmented/virtual reality, also demand a robust networking foundation.

But which underlying network technologies are best suited to the business's unique requirements? Private 5G? Public 5G? Wi-Fi 5 or Wi-Fi 6?

And what about the security considerations for each?

5G versus Wi-Fi.

The use of 5G technology for business-critical networks offers a number of benefits over non-cellular technology (such as Wi-Fi 6) – especially for large industrial companies. Both technologies are undergoing major advances to support emerging use cases and requirements inspired by and relating to, Industry 4.0 trends.

5G represents a dramatic step forward with regards to enhanced throughput, service deployment, and latency reduction, along with data volume handling, and overall reliability. The technology is an evolution and improvement over 4G cellular technology, with the 3GPP (3rd Generation Partnership Project) standard body providing guidance around security best practice for providers. What this means is that 5G networks are secure by design, resulting in 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, 5G uses licensed frequency bands, which reduces interference issues from other wireless devices, and enables network slicing, resulting in improved Quality of Service. 5G also provides flexibility around service deployment, due to its use of a number of technology solutions used in the cloud, and with virtualization at its core. This means 5G can support mobile edge computing, enabling cost-efficient ways of tackling latency issues, among other things. 5G also provides ubiquitous access, roadmap flexibility and support for WAN and LAN technology.

In contrast, Wi-Fi 6 only uses unlicensed spectrum frequency bands, making it subject to difficult-to- control interference in “noisy” environments. With Wi-Fi mainly used at home and for office LANs, the device ecosystem is more focused on these environments. As a cellular technology, 5G is also suitable for mobile, fixed, nomadic, indoor, and outdoor use.

Despite these drawbacks, Wi-Fi is likely to continue to play an important role in consumer and office LAN environments, particularly with improvements that Wi-Fi 6 offers over Wi-Fi 5, including better performance around peak data rate, latency, density, and energy efficiency.

User equipment authentication and authorization, end-to-end encryption, privacy enhancing features, and zero trust architecture, among others... boost security by enabling 5G to natively secure communications across the network.

The 5G Choice: Public or Private?

A distinction with cellular technologies is whether they are public or private. Unlike public networks, private networks often cater for very specific use cases focused on local area coverage that often have more specific requirements than consumer mobile services. Again, examples include production line management or AGVs.

So while private 5G uses the same technology, 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 cannot be shared externally. As a result, it becomes a viable option for use cases where IoT devices, such as sensors or cameras, remain on the customer premises and don't need to be roaming.

Private 5G also offers benefits for those concerned about security. While the types of cyberthreats remain the same, the fact that the network is being 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. Remember, a layered defense, combines physical and logical security controls.

Type of 5G network - main attributes

Public

- Uses mobile network operator expertise, solutions and a wide range of spectrum
- Full provision from and interoperability with a public network
- Quality of Service improvements for prioritizing critical devices and applications
- Enables edge computing within the public network with the option of on-site gateways that offer lower latency and localized data storage and processing

Private

- A dedicated network enabling high levels of security and privacy
- Isolated network that doesn't touch a public mobile network
- Full control over design, deployment timeline and operation
- Full control over SLA
- Edge computing offering lower latency and localized data storage and processing
- Outsourcing of some or all of design or management of network
- Direct responsibility for spectrum access and usage

Modified from: https://www.gsma.com/iot/wp-content/uploads/2020/10/2020-10-GSMA-5G-IoT-Private-and-Dedicated-Networks-for-Industry-4.0.pd

5G and key security considerations for industrial settings.

Complex and critical environments that rely heavily on industrial control systems (ICS) wand operational technology (OT) would do well to evaluate the use of private 5G. The type of connectivity that takes place on crowded factory floors and sprawling seaports, for example, has the very real potential for signal interference from physical structures and even from other wireless signals. Private 5G works particularly well in these settings due to its ability to provide consistent and reliable speeds and low latency, minimizing the risk of interrupted connectivity.

Availability, as security practitioners know, 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 call for a security program 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 DDoS attacks. Cyber-attacks 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 or personal customer data.

Human life and limb is also at stake if 5G-enabled use cases do not factor security into their design and execution. An oft-cited example is the worse-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 industrial organizations – power plants and water treatment 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[1]. And in early 2021, hackers attempted to poison the public water supply by infiltrating water plant industrial control systems in a Florida town[2].

How NIST CSF can help secure your private 5G network

The NIST CSF offers a proven approach to cybersecurity program design that, when applied to a private 5G network and the applications it enables, can greatly reduce risk. The NIST CSF stresses the need for organisations to develop five key capabilities:

Identify
Know the internal and external threats to your assets and to your organisation.

Protect
Secure critical infrastructure, assets and data, no matter where they are located, from cloud and mobile to IoT.

Detect
Enhance and accelerate the ability to detect compromises of systems or data.

Respond
Develop and maintain a plan to quickly and effectively manage a security incident.

Recover
Plan for resiliency to maximize system uptime and minimize costly business interruptions.

[1] https://www.bbc.com/news/technology-30575104

[2] https://www.bbc.com/news/world-us-canada-55989843

The industry-wide framework consists of three main components:

Framework Core

Implementation Tiers

Profiles

The Core consists of three parts :

Functions

Categories

Subcategories

And includes five high-level functions:

Identify

Protect

Detect

Respond

Recover

These level down into 23 categories split across the five Functions. See below:

Function	Category
Identify	Asset management Business environment Governance Risk assessment Risk management strategy Supply chain risk management
Protect	Identity management and access control Awareness and training Data security Information protection, processes, and procedures Maintenance Protective technology
Detect	Anomalies and events Security continuous monitoring Detection processes
Respond	Response planning Communications Mitigation Improvements
Recover	Recovery planning Improvements Communications

[1] https://www.bbc.com/news/technology-30575104

[2] https://www.bbc.com/news/world-us-canada-55989843

A closer look at the NIST CSF.

Identify

A key starting point when developing a security program is to identify what devices are on the organization's network, and what data is residing on each asset. Fundamentally, you can't protect what you don't know about. As part of this exercise, organizations need to identify their "crown jewels" – that is, the key assets that would fundamentally impact the ability for a company to operate if they were compromised or made unavailable.

Ultimately, businesses need to ensure they have a complete picture of their operating environment. As organizations think about the impact of adding a private 5G network to their network footprint, it is critical to understand what exactly is being added. It won't just be the private 5G network and the hardware and software elements that are installed, but also the various components that support the use case and leverage this technology.

In addition, it's crucial to understand where the data that is being collected is processed and then stored for later access. You also need to prioritize the various use cases in terms of the role they play in the success of the business, and the combination of technology and data that will be needed to achieve them.

The other key element for this stage is for organizations to identify and understand their risk profile. Corporations today might have many different departments that operate in different ways, as well as subsidiaries that operate in different industry verticals. This adds to the complexity of setting up a security program, and means data needs to be collected and contextualized to determine the risk profiles of different networks.

When it comes to private 5G, some of the considerations around risk, particularly for the industrial vertical, have been discussed earlier in this document. The industrial operations built around proprietary technology, and provided by IT and OT specialist providers, also need to be factored into an organization's risk profile and how they could impact ease of recovery.

Related to this, many companies operating in an industrial environment have historically used proprietary technology within an isolated private network to provide a certain layer of security. The types of use cases that private 5G supports often require access to public cloud environments.

These types of changes to network architecture will have an impact on an organization's risk profile and need to be incorporated. On top of that is identifying and regularly assessing what security technology, people and processes are in place and whether there are any gaps. Typically, this is achieved through annual independent assessments. Underlying all of this are the security outcomes an organization is seeking to achieve, including the level of risk mitigation, compliance and privacy.

Protect

Technologies that offer protection are the foundation to a security program. How these technologies are set up has had to change as organizations have moved from a traditional fixed perimeter approach – such as a castle and moat – to a corporate IT environment that includes a hybrid network with virtualized components, networking elements (on premises and in the cloud), software as a service, and employees who increasingly work remotely.

The protection put in place needs to reflect this new model. High levels of protection are core to the security built into private 5G networks that use encryption and incorporate Zero Trust principles. The focus therefore needs to be on protecting the different elements of the use cases that private 5G networks support.

There are different types of technology that can be considered for this. For example, network slicing can provide an extra level of protection by separating network capacity for different use cases and data, keeping it away from other data that travels across the network.

Endpoint protection is also a key consideration. While endpoint devices such as laptops and mobile devices can support sensors for security, IoT devices require a more specialized type of endpoint technology that reflects their size and capacity.

As well as endpoints, private 5G use cases require applications and data processing that need to be protected. But how and to what level depends on the type of technology being used, what level of protection is built in, and whether public cloud is used, and the associated risks this brings. With the sophistication of attacks and the different types of threat actors only increasing – and the ongoing need to protect the company's crown jewels – Zero Trust continues to be the foundation for developing a sound approach to the "Protect" pillar of the NIST CSF.

Finally, as reliance increases on employees being the front line of a company's security program, it's important to ensure that any changes in threats, technology and process are incorporated into employee training and awareness activities.

Detect

The general mantra when it comes to cybersecurity is, "It's not a case of if you will be breached, but when". When it happens, speed of detection is key. As reported in Verizon's 2021 Data Breach Investigations Report, almost 20% of breaches remain undetected for months or more.

The speed of detection is incredibly important given the types of risks to the business that were discussed earlier in this paper, not least of which is the threat to human life. Detection is therefore a key part of any security program. So, as organizations start to introduce private 5G and associated use cases, they need to consider what updates are needed to their detection technology to include any changes to network, applications and data storage.

A potential challenge, particularly for companies with highly industrial environments, is whether their detection technology can ingest the often proprietary log data that is created. In those situations, organizations need to ensure their detection technology can ingest and meaningfully process these data types. They might also need to look at leveraging network analysis technology that can interrogate network traffic, and use it to look for suspicious activity, including evidence of exfiltration.

Respond

A key part of this pillar is planning, which is incredibly important for security operations to succeed. This means regular trial runs and walking through what responses to different threats look like. Independent assessment of the security setup is also highly recommended.

Organizations must also plan in a way that is specific to their industry. The way in which they need to respond differs from other sectors. Therefore, technology partners should also understand the industrial environment to assist with this planning.

As companies start using private 5G technology and their associated use cases, and adjust their protection and detection programs, their response planning must also adjust and then be tested to ensure it has been hardened and continues to be robust.

It's also important to have additional resources as backup in the event of a breach. Most organizations can't waste resources by having people waiting around for a breach to happen. While breaches are likely to happen, it might not be for some time, meaning these employees are sitting idle. Industrial organizations should therefore have staff with secondary duties who can respond when a breach happens or have a third party on call – or a mixture of both.

Recover

When looking at this pillar, industrial companies will need to go back to the considerations around the specific needs of their business and the affected endpoints to minimize the impact to the business.

With a private 5G network, organizations will be introducing new technology vendors, so they need to understand what assistance might be needed from them as part of the recovery process and incorporate that into recovery planning.

Conclusion.

With 5G, the future of business is here – and private 5G provides the next-generation network underpinnings to transform industry. Smart business leaders and their counterparts in IT and security must collaborate like never before to realize the rewards – and manage the risks – of the Fourth Industrial Revolution.

By leveraging the security controls inherently built into 5G along with the NIST CSF, organisations can chart a secure pathway to endless innovation.

Visit verizon.com/business/en-gb/solutions/5g/ to learn how Verizon 5G is changing everything.