Publication date:
May 2023
Author:
Hollie Hennessy
Mike Sullivan-Trainor
Rob Bamforth
Martin Hingley

Beyond Secure by Default

What you need to know about enterprise private 5G network security

Commissioned by:

TREND MICRO | CTONE

Brought to you by Informa Tech

Contents

Summary

Secure by default versus enterprise-grade private 5G security

The deployment of enterprise private 5G networks ushers in a complex array of new security requirements. With recent releases of 5G, 3GPP introduced security enhancements in the radio access network (RAN) and core network as well as in end-to-end areas such as signaling, slicing, and security assurance. This approach is known as “secure by design” or “secure by default.” But are these improvements enough?

The GSMA says:

5G has designed in security controls to address many of the threats faced in today’s 4G/3G/2G networks. These controls include new mutual authentication capabilities, enhanced subscriber identity protection, and additional security mechanisms. 5G offers the mobile industry an unprecedented opportunity to uplift network and service security levels.

While that is undoubtedly the case, enterprise private 5G raises the bar even higher by introducing both new endpoints and mission-critical requirements. The GSMA acknowledges:

5G provides preventative measures to limit the impact to known threats, but the adoption of new network technologies introduces potential new threats for the industry to manage.

Beyond 5G’s built-in security, enterprise-grade private 5G requires additional capabilities, including

- Increased visibility across integrated supply chains with suppliers and business partners requiring customized permission and access
- In addition to the secure signaling, private 5G requires threat detection and prevention across IT and operational technology (OT) endpoints
- For industrial use cases: customized services in a centrally managed platform to implement end-to-end security from the core to the edge
- For enterprise security: threat detection, visibility, and identification of gaps throughout the lifecycle of the infrastructure and applications

However, 5G networks are not designed for this level of complexity. As highlighted by Ericsson:

If you think about it, the 5G network is secure by default. You can just connect your 5G enabled device, and you already have a secure connection to whatever service you need. But at the same

time, we understand that not all devices are as secure as mobile phones. Not all devices share the heritage of secure, hardware-based identities like SIM cards and hardware security modules.

This paper will identify the limitations of 5G's secure-by-default approach for enterprise-grade private 5G networks and outline what solutions are emerging to address the gaps.

5G private network security posture

In order to define the gaps between public and private 5G, it is necessary to define the security posture required by the enterprise. First, private 5G networks, by definition, are exclusive to only those users authorized to access them. This raises the bar for security immediately in comparison with a public network, which is accessible to anyone who can connect.

Further, the security posture is determined by the use cases of the different vertical industries that are adopting private 5G networks. These are led by energy and utilities, manufacturing, and transport and logistics, all of which have different ecosystems requiring different security postures. Security requirements also differ by location: regulators in the main countries adopting private 5G, including Germany, the UK, Japan, Korea, China, and the US, have different standards and expectations.

With private 5G, the points where enterprise security and carrier security intersect will depend on the deployment model. Some will deploy private radio-access networks (RAN) to extend access to meet application needs (e.g., RAN deployed inside mines, factories, or campuses); others will use private core for greater control and data ownership or may opt for a more complex hybrid. In any case, there may be systems integration partners working with the enterprise, in addition to carriers and service providers.

Enterprise versus service provider security

In public networks, mobile network operators provide underlying communications infrastructure in a similar manner to how cloud providers offer the underlying compute power and storage. How networks or services are used, and by what, is the responsibility of the end customer, or enterprise. Even here there is a crossover of responsibility. Operators authenticate devices to use a network, but they are not responsible for who uses the device, what it does, or the device's own hardware, software, and data security.

For private 5G deployments, though enterprises can deploy a 5G network completely on their own, when licensing spectrum or installing RAN hardware, networks, and core functions, it is very likely that they will be working with a partner, systems integrator, or service provider. That partner may do more than an operator would and may manage more than just the network, but ultimately the enterprise is responsible. Even if it does not deploy and manage its own security, the enterprise must set up roles and responsibilities for people in addition to the processes and oversight. How far this goes down into the details of security will depend on the resources and capabilities available and on attitudes toward risk.

Visibility and monitoring

In whichever way responsibilities are shared and split between enterprise and partners, real-time security visibility of the entire landscape is essential. Private 5G networks are likely to be used as fundamental infrastructure for projects that were previously too expensive, difficult, or impossible to realize. New attacks may well take advantage of 5G's reach and speed. So, where possible, a proactive security posture must be taken with sufficient security visibility to allow for an immediate and targeted response in the event of attacks.

In an enterprise, this security visibility needs to span the entire organization's environment. Communication technology, or the 5G network, is just one element of this, as is visibility into assets, but this will need to extend into IT and into OT when relevant. An accurate view of the entire environment will be vital for recognizing, containing, and responding to attacks and for being able to assess the threat landscape in its entirety rather than in siloes.

Extending platforms to 5G using enterprise-grade security

Although 5G networks are designed to be secure by default, they are designed primarily from the perspective of an operator wanting to deliver a networking service to an authenticated device. Enterprise security requires more assurance that only authenticated users have access—and then only to the services and data for which they are authorized—and that all data and services are protected from malicious actors or actions. In conventional enterprise security, this means applying proactive protection, detection, and response to all elements (endpoints, networks, and infrastructure), encryption to secure data at rest and in transit, and authentication to ensure the identity of users and things. All these aspects of enterprise security can be applied to the systems, elements, and functions of a private 5G network to improve the security of the people, data, and processes that operate over it.

Extending zero trust into CT zero trust

Fundamental to this is the extension of one of the core design principles of 5G, namely the position of zero trust: assume all connections are exposed or tapped, so encrypt traffic and authenticate all use while applying the minimum privilege to accomplish the authorized task, extending across applications, network, devices, and users.

Many organizations are already adopting or planning to adopt a zero-trust model for access because of increasing use of cloud services and access over public networks (i.e., the Internet). Though private 5G networks are more secure than previous generations of cellular communications, there are specific communication technology (CT) considerations that must be considered when zero trust is being extended. As an example, there may be virtualized network functions executing in shared cloud-based resources, and there will be over-the-air communications that could be subject to jamming, interference, or replacement. In addition, the rollout of 5G allows for the connection to the network of an enormous number of endpoints and mobile devices, to which the zero-trust

principles must also apply. A zero-trust approach to 5G security is a necessity for a robust enterprise security posture, tailored to CT, as we see in the IT world.

Deployment and responsibility models

Mobile network operators deploying 5G will have several challenges, including the transitional phases when 5G will sit alongside earlier generations of mobile technology. The current implementations of 5G are based on what is known as non-standalone (NSA) mode, or E-UTRAN New Radio – Dual Connectivity (EN-DC), where mobile devices can access both 5G and 4G at the same time, but the core is 4G LTE.

This suits early-stage deployments for 5G devices but migrates to standalone (SA) mode, or SA-NR, where 5G RAN connects to a 5G core. Public 5G networks then replace earlier generations because they add better coverage, performance, volume of devices, and lower latency. But enterprises face different challenges, and the flexibility of 5G offers a few new deployment options that might suit specific needs:

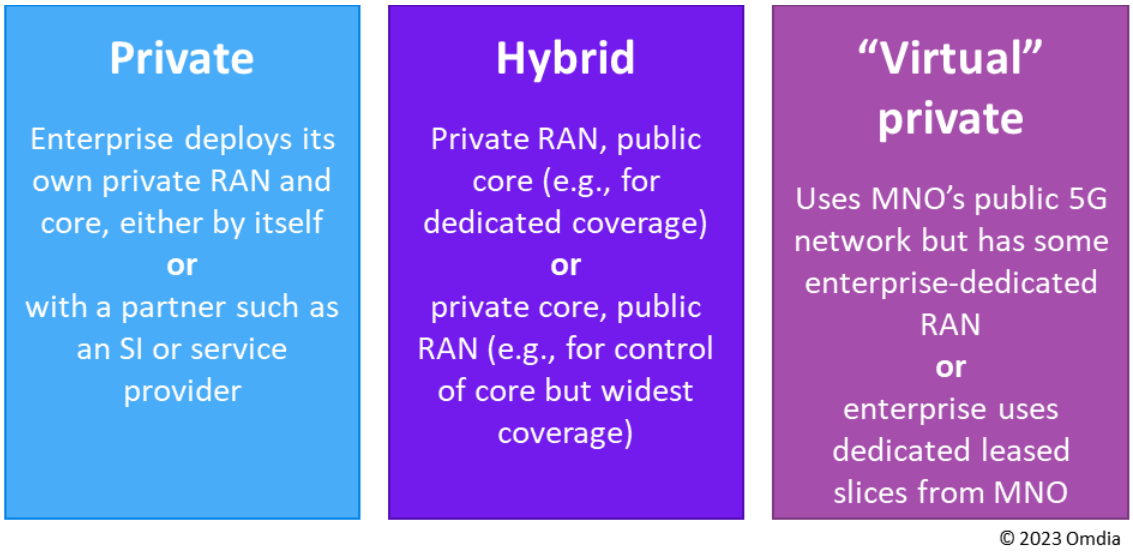
- **Private 5G.** A dedicated 5G network is deployed by an enterprise for the exclusive use of its own devices and RAN, with complete control over the core infrastructure. The deployment flexibility of 5G means that elements of the infrastructure can be hosted within the enterprise or in any cloud resources it uses. The enterprise is responsible, either directly or via a partner service provider, for the 5G network and for applying all necessary security and controls.

- **Private RAN hybrid.** This type of model is already in use with 4G to boost connectivity in large venues, campuses, and industrial complexes, but 5G RAN will allow greater bandwidth and more connections.

- **Private core hybrid.** Enterprises could look to take control of the core of their own 5G network but make use of public RAN for widespread connectivity.

- **Virtual private 5G network.** One of the innovations introduced in 5G is the ability to offer a network as a service, known as a "slice," across the many elements that form a network. This means that applications, groups, or users—or even entire customers with different network requirements—can be offered a separate slice with capabilities matching their specific requirements and isolated to ensure confidentiality, integrity, and performance. A leased private slice could be used by an enterprise like a virtual private network, although it should be noted that slices can span different operators, which may raise issues of security, interworking, and resilience that enterprises should consider.

Figure 1: Enterprise 5G private network deployment models



Source: Omdia

Though the technology behind 5G permits a great deal of potential for flexible deployment that goes beyond previous generations, commercial realities may dictate that specific approaches will dominate. At this stage of the market, it is clear that private 5G network deployment is a preferred offering for mobile operators, is being picked up by service providers and systems integrators, and offers much of the assurance that enterprises require. However, even with private 5G, there is a need to build a suitable security model.

Unique challenges of securing many small-scale networks with cloud / virtual functions

Software-defined networking / network functions virtualization

Much of the innovation in 5G comes from shifting the deployment from a traditional network made up of numbers of specialized and individually separate hardware elements to one where capabilities are delivered as software. Software-defined networking (SDN) further allows for decoupling control from data flow, offering more agile deployment with centralized control and programmable network services. Virtualized network functions (VNFs) can effectively be run on shared infrastructure at the edge as well as at the core, potentially simplifying network management, operation, and maintenance costs. These two technologies perform different roles, but when used together codependently in the 5G architecture, they offer a much more adaptable approach for network providers. However, this brings its own challenges:

- **Resource sharing.** Depending on how the systems are managed, demands on one aspect of the network may have consequences for the resources available elsewhere. For example, attacks on

a network function could affect other virtualized components running on the same physical server.

- **No gaps.** The physical isolation of hardware in traditional networks no longer applies: virtualized components can communicate directly and may be on the same hardware.
- **Virtualization integrity.** Abstracting to a virtualized layer does provide the benefit of unified resources, but if this layer is breached then all network functions can be vulnerable to attack.
- **Supply chain.** While open approaches allow for best-of-breed solutions and cost-effective options, they also bring the threat of supply chain compromise and the potential introduction of rogue network elements or credential mismanagement.
- **Development pipeline.** Increasing use of open-source software and continuous integration / continuous delivery (CI/CD) introduce new security challenges. There are tools and processes to deal with these in the development pipeline, but these need to be implemented as early as possible in the cycle to minimize the impact of flaws.
- **Blind spots.** Monitoring systems set up for physical systems are likely to be insufficiently fine-grained to closely detect and inspect traffic in virtual systems, making threats or anomalies potentially harder to spot.

Multi-access edge computing

Multi-access edge computing (MEC) changes the traditional client/carrier network model by allowing data and processing functions to be moved from the distant core closer to the end user or devices. This could introduce several threats from software vulnerabilities, rogue elements, or flaws:

- **Physical security.** Deployment of equipment and services at the edge, probably in many locations, makes them vulnerable to physical attack and damage or just physical access to IT equipment, which may then lead to compromise.
- **Edge software.** The use of applications, VNFs, and their supporting infrastructure at the edge could expose additional attack vectors to tamper with core system configurations, eavesdrop, or perform spoof activities. Once the MEC is compromised, this could be used to access the RAN or other elements of the architecture.
- **Application Programming Interface (API) abuse.** The use of standardized and common API frameworks improves the cost-effectiveness of 5G infrastructure but also increases the need for a cautious approach to authentication and access control.
- **Visibility.** MEC may not be viewed as part of the core, but its functions can be just as critical, and its use needs to be treated and monitored with real-time security management.

Cloud

To ensure that the 5G network has the scale and resilience required for the expected increase in performance and network capacity, its virtualized architecture is designed to take advantage of

cloud infrastructure. This poses a security challenge for network operators (and therefore to their enterprise customers) because of the multi-tenancy use of shared physical infrastructure. Mobile network operators and cloud providers share the responsibility of hardening cloud security through a broad set of mitigations:

- **Integrity.** Build a secure and trusted runtime environment and baseline, and protect against any misconfiguration, unauthorized modification, or tampering with configuration.
- **Isolation.** Use containers with limited and controlled permissions to run network functions and implement secure development pipeline and runtime practices.
- **Insulation.** Detect and prevent lateral movement between any logical boundary so that any breach has minimal consequences. Apply strong identity and access management controls and logging throughout. Use analytics to automatically detect anomalous activities and behaviors.

Enterprises that have a robust security posture will expect security hardening when using cloud-based services, and they should ensure that operator and service provider partners adopt similar principles.

Network slicing

The idea of network slicing is to provide a flexible approach to data, traffic, and security isolation through a network-as-a-service model, but it adds complexity to 5G for operators and needs careful management and monitoring to detect and protect against threats. Though 5G specifications are well defined in general, there is less clarity on how to ensure security in network slicing. With this in mind, and given that slices can and should span multiple operators, enterprises with robust security postures are likely to want to augment the capabilities of slicing using additional protection such as multilayer security, advanced encryption, or a zero-trust architecture. Even in this situation, slicing could still be used to offer separation for differential network performance or functionality but with additional layers of enterprise security on top.

Characterizing the threats

Though 5G has been designed to be more secure than previous cellular mobile infrastructure, it is also much more flexible in terms of deployment options and architecture. In many respects, it combines or converges both telecoms and IT architectures, so the threats and potential for attack can be viewed in different ways.

From the telecom architecture perspective, interfaces and systems that were once closed and proprietary are now more like IT: they are open, often software defined, and can take advantage of flexible delivery models such as cloud-based services. However, there remain critical telecom interfaces, such as in the radio network and in the core between carriers. There are threat models based on the 5G architecture, in particular the one that the EU agency for cybersecurity (ENISA) outlines in its report “The threat landscape for 5G networks,” which covers the breadth of 5G deployment and will be invaluable for network providers and carriers. However, as outlined above, 5G security needs for enterprises will vary and go beyond those applicable to telecom providers.

Comprehensive threat model (FiGHT, NIST, etc.)

Many involved in enterprise security will be familiar with the MITRE ATT&CK knowledge base, first released in 2012, which comprehensively defines the techniques and tactics used to attack as well as mitigations to detect and protect against threats. MITRE investigated the challenges with mobile networks and released the FiGHT (Five G Hierarchy of Threats) matrix in September 2022 to offer a similar framework for this space. This includes several techniques and subtechniques oriented around the tactics that might be used against a 5G system. It also outlines what to look for to detect a threat and what mitigations might protect against it.

The National Institute of Standards and Technology cybersecurity framework (NIST CSF) is not specifically designed in its current iteration (version 1.1, April 2018) for telecommunications networks. However, it is designed to be broadly applicable, and it has been used in relevant related fields such as connected-vehicle environments. In addition, given that the 5G architecture is more like a flexible and open IT solution, NIST CSF can also offer a suitable model to deal with the threats faced, based around the following functions:

- Identify - covers the development of an organizational understanding of how to manage cybersecurity risk.
- Protect - applying appropriate safeguards to prevent, limit, or contain the impact of an attack.
- Detect - see when and what sort of attack is occurring.
- Respond - actions to mitigate and limit the impact of an attack.
- Recover - restore capabilities afterwards.

While *identify*, *respond*, and *recover* relate to processes and the people involved in building and maintaining a robust approach to cybersecurity, *protect* and *detect* both align to capabilities that should exist in technology solutions put in place to provide that security.

By combining the FiGHT matrix of threat techniques with the relevant categories and subcategories of actions applicable to mitigate or protect against and detect those threats, it is possible to build a comprehensive threat model that extends across all aspects of the 5G architecture:

- **Device threats.** Threat to devices themselves can include malware, particularly for smarter user equipment based on popular operating systems. These need endpoint protection. However, all 5G-connected devices, down to tiny sensors, are exposed to attacks relating to the subscriber identity module (SIM) that provides the identity and authentication for a device on a cellular network. Some have been observed in 5G “in the wild,” including SIM credential theft, SIM cloning, fraud attempts such as SIM boxing to avoid termination fees, and location deception such as geolocation of devices based on radio signals or tracking device id moving from cell to cell. Others, such as endpoint denial of service through triggering fraud alert, sending fake registrations, consumption of data allocation by a malicious app, and adversary-in-the-middle eavesdropping, are still currently only theoretical but are nonetheless threats that need to be mitigated.

- **Air interface vulnerabilities.** The radio element of the RAN can be vulnerable to signaling threats such as jamming, eavesdropping, and overload or to tampering and spoofing involving the configuration of radio equipment or the use of rogue radio devices.

- **RAN concerns.** Edge equipment in the RAN could be tampered with to affect radio network configuration. This might be used to switch encryption off, allowing for eavesdropping, or to cause user equipment to bid down to a less secure (i.e., earlier-generation) mobile network. Though openRAN has the potential to reduce costs and increase flexibility and deployment options, by separating hardware and software and using open APIs to allow multi-vendor interoperable products, it also creates new attack surface. Faster-moving CI/CD software pipelines will need to incorporate security from the outset, and though standards should ensure interoperability, there may be gaps for malicious actors to exploit. The use of openRAN might keep network deployment costs down but increase the efforts applied to security and will require enterprises to assure themselves that they have applied security controls to all the key RAN elements. All equipment is subject to physical attack. This may be in the form of vandalism or damage to remove equipment from the network or the spoofing introduction of rogue equipment to eavesdrop.

- **Backhaul issues.** The 5G secure-by-design model assumes that any network link is open and might be tapped, so end-to-end encryption, including for backhaul connections, is vital and should be monitored. During attacks, changes in network configuration can occur to allow for traffic sniffing, so baselining and continuous detection and checking are required.

- **Core compromise.** The 5G core infrastructure makes extensive use of virtualization, allowing simplification of hardware and further deployment flexibility; for example, some functions can be outside the enterprise (or operator) network and in the cloud. This increases the opportunity for threats. Though there are security tools and control procedures for managing virtualization and isolating resources, and the increasing use of containerization, enterprises will have to think about how these apply not only to critical data and resources of their own but also critical elements of the network infrastructure. Management and orchestration processes for virtualization will need to be well thought through and correctly implemented. This may be an area where security tools need to go hand in hand with expertise from a third party, for example, a systems integrator with both telecoms and IT security expertise.

- **Interconnection failures.** The 5G architecture includes a new network function, the Security Edge Protection Proxy (SEPP), to securely interconnect between 5G networks maintaining integrity and end-to end confidentiality. However, enterprise application backends will also connect and communicate across the 5G networks.

Gaps in solution coverage

Solutions aimed at addressing the specific threats to an enterprise 5G network deployment need to pick up on both the traditional IT network security threats within the now-open telecoms architecture and those directly related to cellular-specific elements. Within the MITRE FiGHT

framework, threats are specified as to whether they are 5G specific or not, but even ones that apply elsewhere will also have an impact on 5G.

Traditional security tools have a significant part to play in securing enterprise 5G networks, from ensuring security as early as possible in the software development pipeline, applying web application firewalls, workload protection, and network traffic firewalling to 5G core and MEC virtualized functions and endpoint detection and response to user equipment and devices.

However, IT security solutions and tooling alone are not adequate to cover the CT environment. There is also a need for 5G/cellular-specific protection. In addition to the virtualized software elements, mobile networks rely on the authenticity of the SIM for identity and the reliability of radio transmission in the RAN. Different modes of attack (such as tampering from cloning, jamming, the use of rogue devices, or bidding down services) seek to exploit weaknesses at the edge of telecoms functions. There are also complex relationships and partnerships, not only in the supply chain but also in the interconnected nature of roaming during operations. There is a need to apply solutions aimed specifically at defending enterprise security needs in 5G networks.

In addition, as with previous generations, the 5G network architecture brings about its own interfaces, specifically between different functions. For example, the N6 function is the interface that connects the User Plane Function (UPF) and other networks and services; the N4 interface bridges the control plane and user plane. This specific architecture needs to be considered when applying cybersecurity to ensure adequate visibility into these interfaces.

This does not only require enterprise security tools to address specific aspects where 5G operations need to be monitored to detect potential compromise or breaches but also has an impact on the people and processes working in the organization to ensure security. Security teams in many organizations have worked separately from the network teams, but with the growth in adoption of security services edge (SSE) and secure access service edge (SASE), converged decision-making and operational management appear to be becoming more prevalent. This would be useful for 5G deployment too, because although the operational management will more likely involve a third-party network team, bringing disparate teams closer should make the complex task of managing 5G enterprise security easier.

The status of private 5G networks

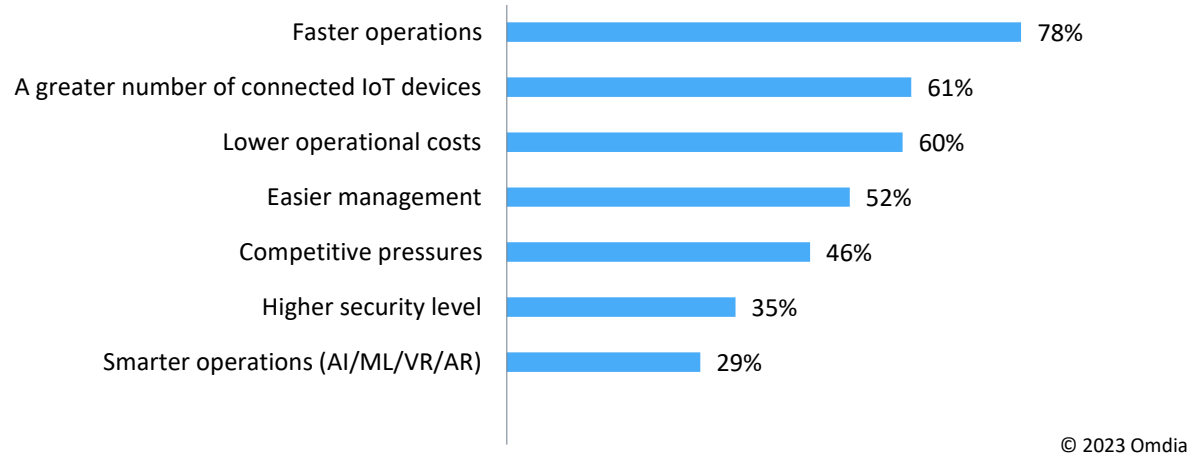
In order to gauge the state of enterprise private 5G network security, Omdia interviewed 150 enterprises, 58% of which had deployed such networks and 42% of which planned to do so within a year. In addition, 150 service providers that offer enterprise private 5G network security services were interviewed. Both surveys were across several countries, with the US, the UK, Germany, South Korea, and Japan represented, and included the most active industries in 5G private networks, including energy (oil and gas and utilities), healthcare (medical and pharmaceutical), logistics (airports, harbors, ports, and warehouses), manufacturing (connected cars, robotics, machine controls), and semiconductors. Enterprises had more than 5,000 employees.

The study found that 58% of the networks were deployed, with the remaining 42% planned, indicating a significant start for the market. However, only 35% of the deployed networks were in production with 65% in proof of concept. Forty-six percent expected to convert proofs of concept to production within the next year.

Most respondents (66%) were deploying the networks as replacements, with the remainder being greenfield. Chief among networks being replaced were physical networks (69%), Wi-Fi (42%), or LTE (32%).

Overall, organizations expected the private 5G network to improve efficiency and expand connectivity while lowering operating costs.

Figure 2: Reasons for deploying 5G

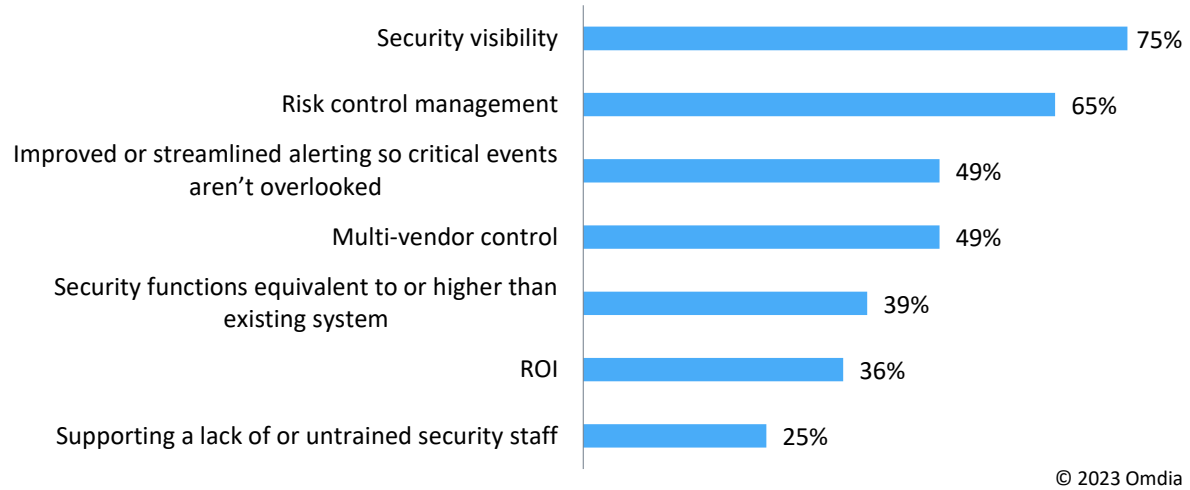


Source: Omdia

It is significant that while they expected lower operating costs, the organizations also expected to invest in new security tools, with 60% agreeing that new measures would be required to integrate private 5G network security with existing security infrastructure.

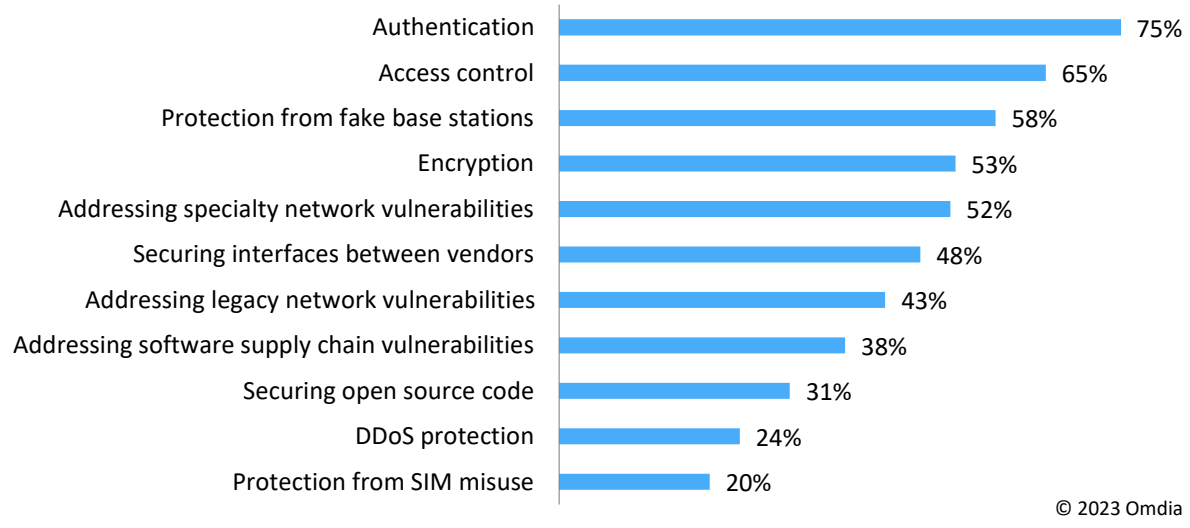
There is also an interesting difference in expectation between organizational leaders around security and the overall response base. Leaders expected greater visibility and risk management, while the overall view focused on authentication and access control.

Figure 3: Leaders' top security requirements for enterprise private 5G networks



Source: Omdia

Figure 4: Overall top security requirements for enterprise private 5G networks



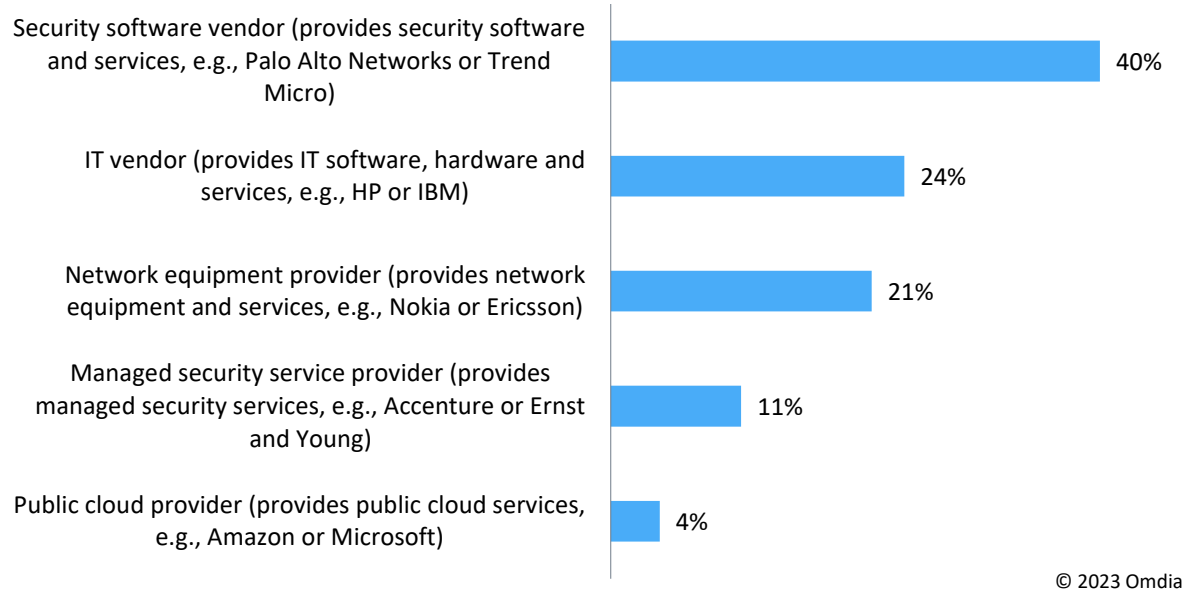
Source: Omdia

Most enterprises surveyed expect to manage planning, deploying, and operating 5G private network core, Internet of Things (IoT) endpoints, and the data network, though a few are looking to suppliers to do so. This suggests a deployment model where these elements are on-premises and within the enterprise's control rather than networks that are largely managed by the supplier or service provider. Still, a shared model is required because most enterprises expect the RAN and MEC to be planned, deployed, and operated by the service provider or supplier. For the security solution, this means a shared-responsibility model, where the enterprise will secure on its premises, and the service provider will secure the RAN and to the enterprise edge.

For a new deployment, most enterprises expect to spend 5–10% of the IT budget on 5G private network security. In terms of current annual budget, however, there are a few very large-scale projects requiring $10m or more.

Finally, most enterprises expect to acquire security solutions from a security-specific vendor for 5G private networks; but few 5G security supplier solutions are familiar to the enterprises.

Figure 5: Preferred supplier category for enterprise private 5G networks



Source: Omdia

Conclusion: Market opportunity and major challenge

The trends in enterprise private 5G network security point to a significant opportunity for organizations in terms of faster processing and more IoT devices enabling new and existing applications. Despite the secure-by-default approach, firms are expected to spend $2.5bn in 2023 and $12.9bn in 2027 on 5G security. The need for integration with existing security and addressing gaps in 3GPP standards will be the key drivers.

Apart from budgeting for this investment, organizations will have to come to terms with new shared-responsibility models and open-source technology. The overall cybersecurity risk will likely increase for mission-critical applications enabled by 5G private networks. However, the majority of organizations undertaking 5G private networks are mitigating the risk through enhanced security.

Appendix

Authors

Hollie Hennessy
Senior Analyst, IoT Security
customersuccess@omdia.com

Rob Bamforth
Supporting Analyst

Mike Sullivan-Trainor
Director, Cybersecurity Consulting
customersuccess@omdia.com

Martin Hingley
Supporting Analyst

Get in touch

www.omdia.com
customersuccess@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

About Trend Micro

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, our unified cybersecurity platform protects over 500,000 organizations and millions of individuals across clouds, networks, devices, and endpoints.

The Trend Micro One unified cybersecurity platform delivers advanced threat defense techniques, extended detection and response (XDR), and integration across the IT ecosystem, including AWS, Microsoft, and Google, enabling organizations to better understand, communicate, and mitigate cyber risk.

With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world.

TrendMicro.com

About CTOne

CTOne, a global cybersecurity leader in communication technology/ a subsidiary of Trend Micro, with over 30 years of experience in information technology (IT) security inherited from Trend Micro, CTOne bridges the communication technology (CT) gap by dedicating resources to the development of enterprise cybersecurity. On top of providing the most comprehensive solution in terms of mobile network communication protection, CTOne helps enterprises integrate IT and CT technologies for digital transformation, reducing operating costs, increasing productivity, and avoiding significant losses. CTOne is constantly on guard to ensure that daily business operations are protected to keep enterprises at the forefront of the market.

CTOne.com

Copyright notice and disclaimer

This report contains third-party IP owned by Omdia, a trading name of Informa Telecoms & Media Limited and has been licensed to Trend Micro.

The Omdia research, data, and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa Tech and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.