White paper

Can the adoption of private 5G-enabled capabilities change an organization’s risk profile?

Secure network design and improved visibility into the device ecosystem pave the way for more effective risk mitigation.

verizon

paloalto NETWORKS

Introduction

In just a few short years, “5G” has gone from business-buzzword to business-ready, with private enterprises and public sector agencies embracing the power and the possibilities of this high-speed, low-latency form of cellular network connectivity. From revolutionizing how data is used to control costs, improve services, innovate product design, and help keep people safe on the job to changing the very nature of collaboration in health care and education, 5G provides the foundation for profound change in the connectivity used by business, government, and society itself.

The accelerated adoption of “emerging” technologies like AI, AR/VR/XR, Machine Learning, automation, edge computing, and IoT means more enterprises are re-evaluating the effectiveness of their current network infrastructure and performance. Many are turning - strategically - to private 5G to do this. As the use of private 5G becomes more common, new and unexpected 5G-driven capabilities will emerge -- as will new and unexpected threats.

The question, however, is not:
“How secure is private 5G?”

The question is:
“How will the adoption of private 5G-enabled capabilities change my organization’s risk profile?”

And the immediate follow-up question should be:
“Do we have visibility into any new risks so we can mitigate them to the degree needed?”

Security and innovation go hand in hand, according to a new research report

New research from Tech Target's Enterprise Strategy Group (ESG) suggests that many companies are now strategically pursuing both "IT transformation" and "business transformation" initiatives with very specific objectives and outcomes in mind. From enhancing cybersecurity and improving the customer experience to driving operational efficiency, these business objectives are causing many companies to revisit their network strategy and design. Private 5G networks, the study finds, will play a critical or significant role in a company's ability to achieve these objectives.

Sixty-four percent of IT and business leaders surveyed in the ESG report – Going Beyond Digital Transformation – said that learning to leverage edge computing to support data-driven decision making is a "top 5" priority, and 71 percent reported that 5G would play a "critical" or "significant" impact on their ability to do so.

When asked about their organizations' other IT priorities, respondents' most commonly cited responses included:

- Expanding the scope of our IoT deployment (41 percent)
- Ensuring security/compliance upon the movement of data (38 percent)
- Better understanding what data types will be generated and used for analysis (35 percent)

These priorities reflect the growing recognition that the convergence of IT, OT and private 5G networks calls for improved visibility into the security of the entire ecosystem, and for the design and implementation of appropriate controls to mitigate new and emerging risks.

The transformative power of private 5G

"Digital transformation" and 5G-enabled capabilities allow organizations to operate in ways once unimaginable. For example, with private 5G:

- "Smart" IoT/OT sensors can collect vast amounts of environmental data from a sprawling indoor/outdoor industrial facility, allowing for instant analysis and real-time decision-making about health and safety controls. This data can also be used to optimize power consumption (driving down energy costs and contributing to a company's sustainability efforts) and to monitor for potential/unfolding environmental disasters (fuel spills, emissions).
- Semi-autonomous drones can be used to inspect rooftop HVAC systems for wear and tear, and AI can be used to flag equipment in need of repair before it breaks ("predictive maintenance").
- Autonomous guided vehicles can move goods and products from one area to another without a human driver onboard.
- AI-enabled cameras can perform quality assurance on parts and goods during the manufacturing process to reduce error and waste and even predict an eventual equipment breakdown.

These and other operational capabilities – driven by 5G – are bringing IT and OT closer together. And while that convergence promises many rewards, new risks can emerge, too. Poorly secured and improperly configured OT and IoT devices, for example, can:

- Provide incorrect or corrupted data, causing harm to man and machine alike
- Be hijacked and used by cybercriminals as part of a "bot army" in DDoS attacks
- Imperil site security (HD cameras and proximity safety sensors going offline).
- If vulnerable to attack or disruption, business-critical network connectivity risks can include:
- Lost revenue (abandoned purchases due to slow point-of-sale system performance)
- Bodily harm (a runaway AGV hitting an employee)
- Reputational damage and/or regulatory penalty (EPA non-compliance, production downtime imperiling SLAs).

Without an appropriate level of visibility into the integrity and availability of the processes and technology that make "digital transformation" possible (and to the confidentiality of the data it possesses), an organization will struggle to properly settle on its risk appetite and deploy effective controls where needed.

Organizations embracing the zero-trust approach to security and its associated architecture are likely better strategically positioned to establish and integrate cyber resilience in the era of 5G. Their foundational commitment to "secure by design" can propel these companies significantly ahead, allowing them to gain a competitive edge.

Again, the question isn't: **"How secure is 5G?"**

The questions are: **"How will the adoption of private 5G-enabled capabilities (and the convergence of IT and OT) change my organization's risk profile and strengthen cyber-resilience, and do we have visibility into any new risks so we can mitigate them to the degree needed?"**

A suggested approach for securing private 5G-driven innovation

Verizon, a leading provider of private wireless networks for a wide array of industries, and Palo Alto Networks, a leading provider of cybersecurity solutions, have partnered to help enterprises extend their visibility into (and their ability to mitigate) potential vulnerabilities and other cyber risks associated with the new devices and applications being deployed on a new private 5G network.

Together, Verizon and Palo Alto Networks believe that for many enterprises, the rapidly accelerating convergence of private wireless, edge computing, and IoT will require a re-evaluation of their risk tolerance/risk appetite and the way they deploy their often-limited security resources against specific types of risk. For example, are enterprises putting “too much” emphasis on protecting data at rest when a “more impactful” risk is the potential loss of millions of dollars in productivity and revenue every 24 hours caused by a ransomware attack?

We suggest a 6-step approach to better securing your 5G-driven innovation and business transformation:

1. Assure that your to-be-chosen private network has inherent and appropriate security “baked in,” including end-to-end encryption and robust access control.

2. Enhance governance, oversight, and internal collaboration for new application deployment, to ensure business lines and operational teams don’t rush to deploy new 5G-enabled capabilities without evaluating the potential risks.

3. Extend visibility to the device ecosystem (scanners, tablets, sensors, AGVs) for IT and OT security teams and provide 24/7 real-time risk assessment on threats, vulnerabilities, exploits, risk, device context, and anomalous behavior. In networks encompassing IT, IoT, and OT devices, visibility into the state of specific devices (and the ability to perform behavioral analytics) is crucial to safety and security..

4. Segment and enforce least privilege access. Establish and enforce least privilege access through segmentation – an integral principle of the Zero Trust security framework.

5. Protect against known and unknown threats, leveraging threat intelligence to address known exploits, web threats, command and control (C2) activities, and malware, as well as prevent zero-day threats and immediate anomaly detection of IoT and OT behavior.

6. Integrate into existing security program capabilities (SOC, SEIM) the data gained from having extended visibility into the device ecosystem; this will offer a fuller view of risks and controls. When it expands its device ecosystem, an enterprise also creates a new (potential) attack surface that must be addressed.

How Palo Alto Networks drives more effective risk mitigation

Palo Alto Networks’ Zero Trust OT Security leverages AI and machine learning to autonomously discover and recognize all devices connected to a network and create a dynamically updated inventory enriched with data. Beyond the identification of IT, IoT, and OT devices, the solution offers comprehensive visibility into network behaviors, distinguishing normal patterns from suspicious activities.

Upon detecting a device vulnerability or anomalous behavior that poses a threat, Industrial OT Security, as part of the Zero Trust OT Security solution promptly alerts administrators, empowering them to investigate and address the issue.

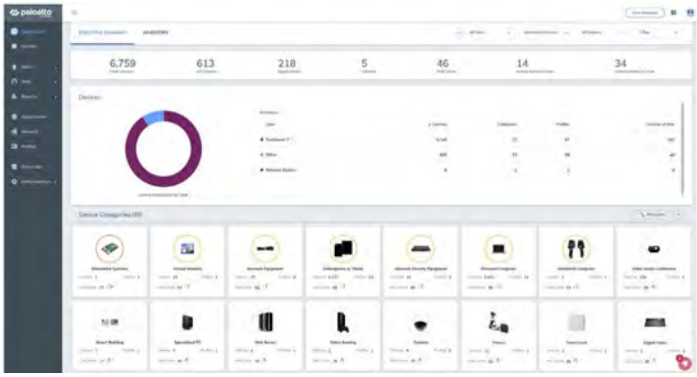
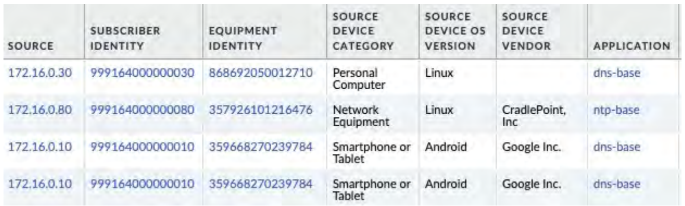


Figure 1 - Dashboard showing a summary of all devices discovered on a network

Palo Alto Networks' Next-Generation Firewalls (NGFWs) deliver instantaneous protection through the integration of inline deep learning. This form of machine learning is particularly adept at identifying unknown and elusive threats. Palo Alto Networks' deep learning system analyzes live traffic, ensuring that even the most sophisticated threats cannot conceal their true intent. Through real-time analysis of traffic, the security assessment seamlessly shifts from “offline” to “in-line,” enabling the prompt interception of evasive attacks.

Further, enterprises can leverage the visibility provided by Palo Alto Networks' Next-Generation Firewalls to more effectively segment devices from both the broader network and each other. This is achieved by crafting granular, context-enriched segmentation policies to prevent lateral movement of threats. Successful segmentation necessitates comprehensive insight into all applications within a private 5G network, ranging from traditional enterprise applications (e.g., databases and web servers) to OT/ICS protocols like Modbus and MQTT.

However, achieving robust security goes beyond mere application visibility. Palo Alto Networks integrates machine learning with its patented technologies such as Device-ID™, 5G Equipment ID™, App-ID™, and User-ID™, along with crowdsourced telemetry. This powerful combination swiftly profiles and assesses OT and IT assets, applications, and users. Such visibility empowers the implementation of fine-grained security policies, ensuring the least privileged access. Moreover, the generation of data-rich logs facilitates analytics and reduces Mean Time To Remediation (MTTR) when threats are detected.



SOURCE	SUBSCRIBER IDENTITY	EQUIPMENT IDENTITY	SOURCE DEVICE CATEGORY	SOURCE DEVICE OS VERSION	SOURCE DEVICE VENDOR	APPLICATION
172.16.0.30	999164000000030	868692050012710	Personal Computer	Linux		dns-base
172.16.0.80	999164000000080	357926101216476	Network Equipment	Linux	CradlePoint, Inc	ntp-base
172.16.0.10	999164000000010	359668270239784	Smartphone or Tablet	Android	Google Inc.	dns-base
172.16.0.10	999164000000010	359668270239784	Smartphone or Tablet	Android	Google Inc.	dns-base

Figure 2 - Examples of Device-ID information, Subscriber-ID (IMSI), Equipment-ID (IMEI), and Application-ID used for visibility and effective segmentation

Additionally, Palo Alto Networks' Cortex XSIAM provides a unified platform for centralizing data and Security Operations Center (SOC) capabilities, including XDR, SOAR, ASM, and SIEM. This consolidation eliminates the need for switching between different consoles, streamlining security operations. Cortex XSIAM is designed to seamlessly integrate with various security tools and vendors commonly used in 5G networks, such as firewalls, endpoint protection, and network monitoring tools. Leveraging machine learning, XSIAM continually learns from past incidents and responses, enabling it to adapt and enhance its automated response actions over time. This adaptive capability makes it more efficient in addressing similar security threats within the dynamic 5G environment.

How Verizon engineers its networks for enhanced security

Although 5G leverages security measures that already exist in 4G, Verizon has incorporated into its Private 5G network offerings additional security innovations to help mitigate unknown risks and ensure confidence. 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. The SEPP protects application layer control plane traffic between different network functions, negotiates cipher suites, handles key management, and performs topology hiding to external networks. It also discards malformed and untrustworthy N32 messages, among other duties.
- **Device security,** given that one of the key findings in the Verizon 2023 Mobile Security Index report was that 90% of successful cyberattacks and as many as 70% of successful data breaches originate at endpoint devices. Verizon takes device security very seriously, investing in testing labs and engineers whose sole responsibility is to ensure any device put on the Verizon network has been thoroughly tested and certified. As a result, any 5G end user device sold by Verizon for its Private Wireless Network has been certified in our labs using C-band or mmWave spectrum, depending on the device's capabilities.

As the table below illustrates, there are enhancements to 4G LTE security as well as a number of new security features in Verizon's 5G 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 (Stand-alone architecture)
Privacy and Integrity Cipher	• Encryption on radio path • Control plane ciphering • 128-bit algorithms supported	**In addition to 4G LTE:** • 256-bit algorithms 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 reauthentication 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 securedly exposes capabilities to other application functions (AF) • Enables secure provision of information in the 3GPP network • Certificate based mutual authentication may be used.
Security edge proxy protection (SEPP)	Not available	• Protects the home network edge, acting as the security gateway • Security between the home network and visited networks

Figure 3 - A comparison of security capabilities from 4G LTE to 5G

Conclusion

When an enterprise chooses to embrace private 5G to revolutionize its business and operations, it creates a rare and valuable opportunity to review and redefine the organization's risk tolerance, bolster cyber resilience, enhance security controls, and optimize the allocation of security resources. Seize this opportunity, using the 6-step approach described in this paper.

And remember - deploying a Verizon Private 5G network and adopting the Palo Alto Networks' Zero Trust OT Security solution doesn't mean “ripping and replacing” existing network and security investments, as both seamlessly integrate with existing infrastructure and operations.

For further information on how Verizon and Palo Alto Networks can help your enterprise transition to a private 5G-enabled future, please speak to your Verizon Business Account Manager.

verizon
paloalto
NETWORKS