5G Cybersecurity Guidance

Introduction and Scope

Next-generation telecommunications services based on 5G promise faster mobile broadband, massive IoT connectivity, and ultra-reliable, low latency communications, helping to realize everything from pervasive fixed wireless Internet access to connected industries and smart cities. At the same time, the services-based architecture inherent to 5G will enable network operators to simplify infrastructure management, automate service delivery, and generate new streams of revenue from tailored enterprise offerings. 5G presents a foundation for building smart nations and powering economic growth, but this foundation is fraught with risk as 5G architectural characteristics and anticipated use cases open up a significantly larger attack surface[1]. It is crucial that governments and industry partner to engineer cybersecurity defenses into 5G infrastructure with the goal of protecting critical services and realizing 5G's full social and economic potential.

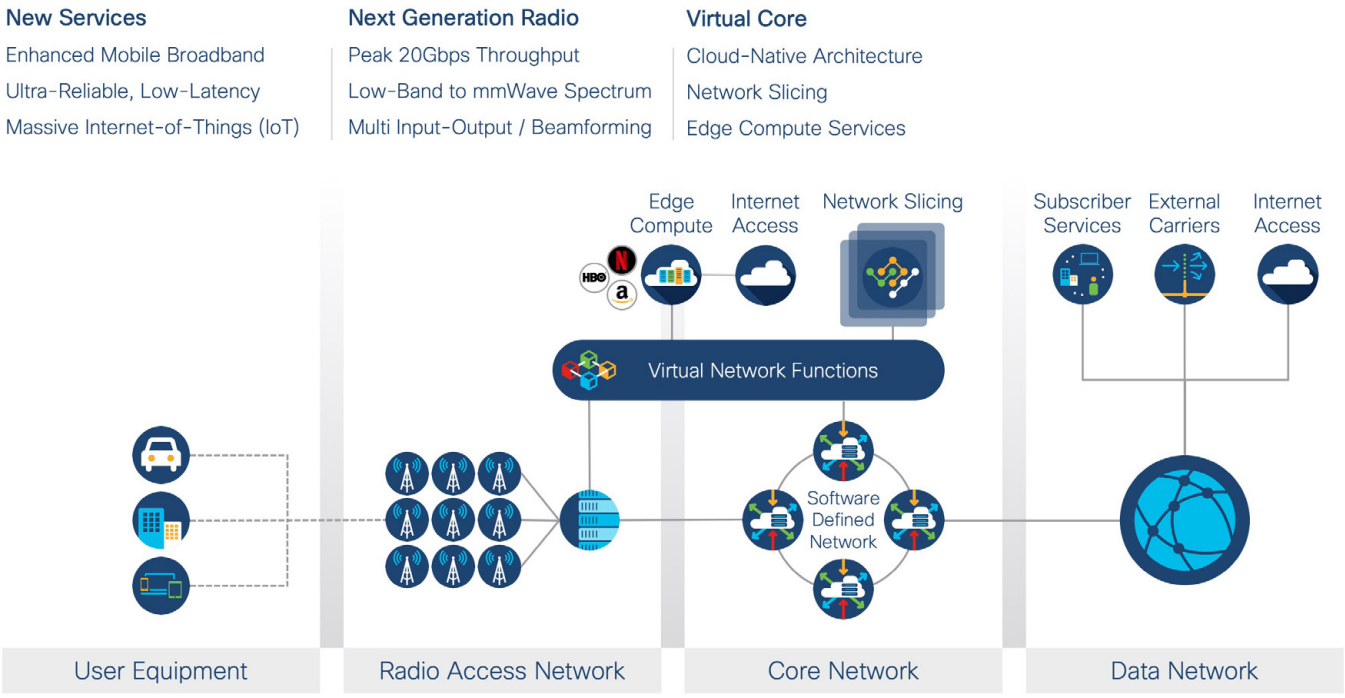
This paper provides high-level insights regarding 5G cybersecurity risks to an operator's core network infrastructure and presents six key recommendations for strengthening 5G against cybersecurity threats. These recommendations inform a security architecture strategy that builds on inherent security services defined in the 5G standard. This paper does not specifically address security within the user access environment, though much of the guidance would still apply as best practices for strengthening enterprise, industrial, and IoT networks that leverage 5G services.

Overview of 5G

The 5G cloud-native architecture, as specified by the 3rd Generation Partnership Project (3GPP) working group, standardizes the core functional elements and interfaces for next-generation mobile services. 5G is a software-centric architecture built with Software-Defined Network (SDN) services and Virtual Network Functions (VNF) that run in a distributed environment. This approach facilitates separation between user and control plane functions, allowing 5G carriers to achieve greater service automation, agility, and scale at a lower operating cost. By comparison, 4G is based on monolithic applications tied to dedicated hardware platforms, making it difficult for operators to independently scale and customize services.

From a logical perspective, the 5G architecture is divided into four areas: **User Equipment**, **Radio Access Network**, **Core Network**, and **Data Network**. The most significant 5G evolutions are found in the Radio Access and Core Networks. The Radio Access Network leverages new wireless technologies that deliver faster speeds – up to 20x faster than 4G – and lower latency while accommodating higher user densities. The Core Network provides a distributed, flexible, high-capacity service backbone that enables new 5G capabilities such as network slicing[2] and edge computing[3]. Taken together, 5G offers operators a platform for expanding mobile broadband access and performance. At the same time, it optimizes the network to deliver better consumer services while enabling new enterprise offerings in manufacturing, logistics, agriculture, and more.

5G Architecture



5G Network Architecture

5G Cybersecurity Risks

5G is susceptible to many of the same cybersecurity risks found in today's existing telecommunications and enterprise networks. Moreover, 5G is subject to new avenues of attack against core network services due to its complex ecosystem of technologies, stakeholders, and operations. These include:

- **Services-Based Architecture**: 5G represents a major transformation in how telecommunications services are built and delivered. Fundamentally, 5G architecture is based on decomposed, virtualized, and distributed network functions. These functions rely on containerized applications, open interfaces, and orchestration platforms to coordinate service delivery. Taken together, these infrastructure abstractions expose new points of attack and lead to challenges in implementing and managing security controls in a highly virtualized environment.

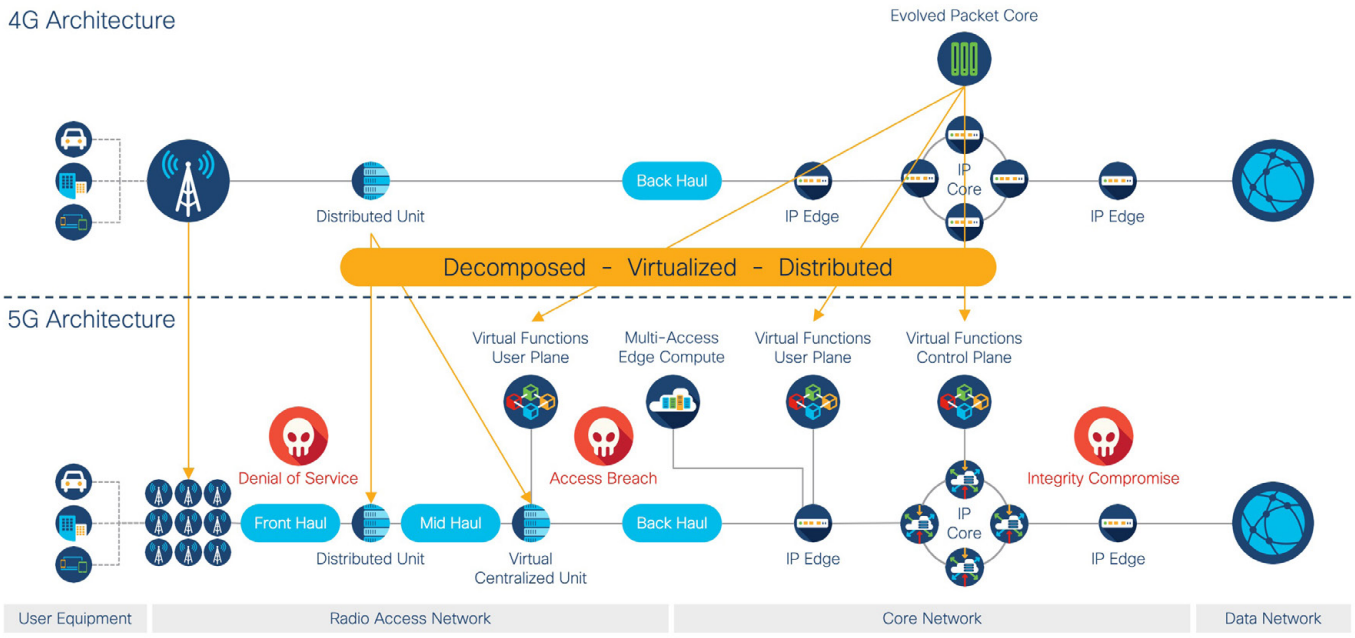
- **API-Based Communication**: The 5G services-based architecture leverages Application Programing Interfaces (APIs) to enable communications between service functions and optimize infrastructure deployment, configuration, and management. Poorly coded or insecure APIs can expose core services to attack and place the entire 5G network at risk.

- **Enterprise, Industrial, and IoT Services**: 5G represents a shift from traditional consumer smart phones to advanced enterprise services. 5G is expected to be widely adopted in enterprise, industrial, and IoT use cases, enabling greater workforce mobility, automation, and countless new applications. Incorporation of 5G into these environments requires a deeper level of integration between end-user networks and 5G service interfaces, exposing both enterprise owners (in particular, operators of critical information infrastructure) and 5G carriers to new risks. Ultimately, an attack that successfully disrupts the network, or that steals or undermines the integrity of confidential data, could have a far greater economic and societal impact than previous generations. For example, industrial and IoT devices can be particularly vulnerable as they often rely on legacy equipment and lack adequate cybersecurity protection. Attacks on vulnerable devices can impact critical services that depend on the 5G network with real-world consequences. Conversely, a large collection of compromised industrial or IoT devices can be manipulated into launching attacks against the 5G infrastructure and disrupt services for all users.

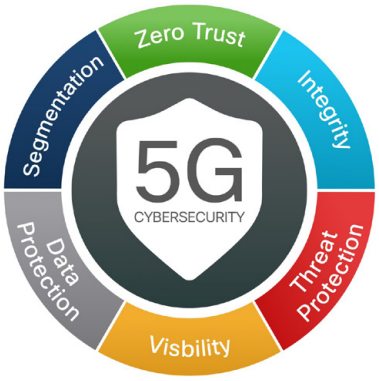
- **Multi-Access Edge Computing**: To facilitate high-speed, ultra-reliable, and low latency services, 5G employs edge computing to bring performance-sensitive applications closer to end users. In effect, operators can distribute user-facing applications within their own infrastructure across virtualized data centers located near mobile radio access nodes or inside enterprise customer data centers and third-party cloud environments. This decentralized approach can blur operational boundaries and increase security management complexity. Moreover, edge computing introduces new opportunities for attacks against application services integrated with 5G infrastructure and may create further avenues for attackers to pivot threats towards core 5G services.

Cybersecurity risk is driven by the nature of threats. Threats are defined by the ways an attacker can compromise system vulnerabilities or weaknesses, impacting the confidentiality, integrity, and availability of a system. There are many variants of threats to 5G infrastructure, but they can be organized according to impact into three, broad categories:

- **Denial of Service**: Attacks that cause service outages through either virtual or physical means. Examples include hardware vandalism, radio signal jamming, and traffic flooding.
- **Access Breach**: Attacks that lead to unauthorized system access, manipulation, or a data breach. Examples include malicious changes to system configurations, exploiting software vulnerabilities, communications hijacking, and disclosure of sensitive data.
- **Integrity Compromise**: Attacks that impact infrastructure integrity through hardware, software, communications, or operational tampering. Examples include implanting malicious hardware components in system devices, altering operating system code, modifying data, and circumventing organizational security policies.



4G and 5G Architectural Differences & Threat impact



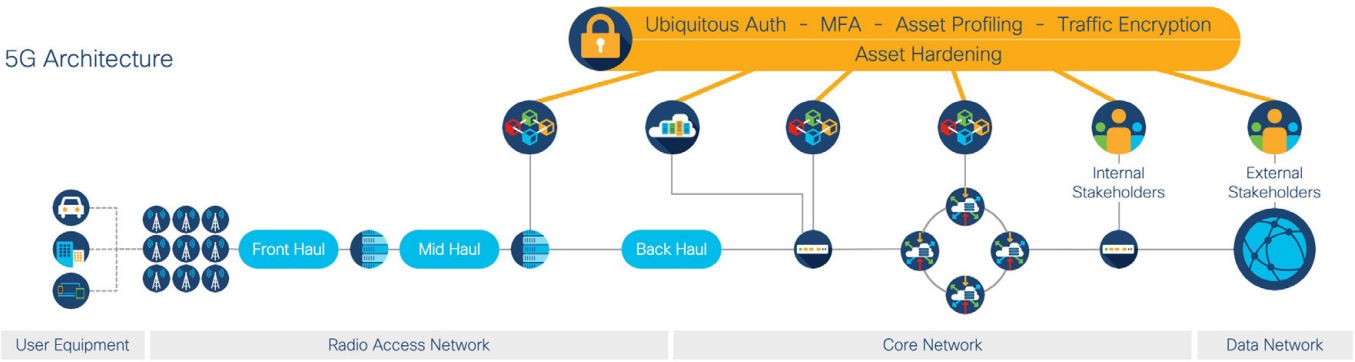
6 Recommendations for Mitigating 5G Cybersecurity Risks

5G leverages many of the same technologies and architectural approaches used in building modern enterprise networks and cloud services. However, with few 5G network deployments so far, established cybersecurity best practices and architectural patterns have yet to emerge. As such, 5G deployments should build on mature cybersecurity standards employed in enterprise and cloud environments. Examples include the NIST Cybersecurity Framework and ISO Information Security Management System series. Operators should also leverage internationally-recognized product testing, assurance, and certification regimes (such as the Common Criteria) to enable the deployment and use of trustworthy products. With international and 3GPP standards as a security baseline, 5G operators should adopt the following six, key cybersecurity recommendations as part of an architectural strategy for addressing the risks described above with the overall goal of reducing the attack surface, continuously mitigating threats, and protecting data and privacy.

Zero Trust

Treat 5G infrastructure as an untrusted environment[4] and explicitly authenticate and authorize interactions between all assets in all areas (workforce, workplace, and workloads[5]) – both inside and outside the network – prior to allowing access; secure and limit interactions to the minimum necessary; and continuously monitor asset security posture, adjusting access rights accordingly. Key capabilities include:

- **Asset Hardening**: Reduce the attack surface for each asset by following best practices to lock down local access controls, configurations, and services.
- **Ubiquitous Authentication and Authorization**: Authenticate and authorize access between all assets taking into account contextual factors that include user identity, device type, and geographical and/or network access location. Non-user assets such as machine devices and application workloads can leverage certificate-based authentication and authorization.
- **Multi-Factor Authentication (MFA)**: Use multiple, strong methods to authenticate and authorize user access to assets (e.g. account name + password + one-time token) taking into account contextual factors that include device type and geographical and/or network location.
- **Asset Profiling**: Validate and track the security posture of all assets, allowing or denying access based on assessed risk.
- **Traffic Encryption**: Secure communications between all assets using strong encryption technologies.

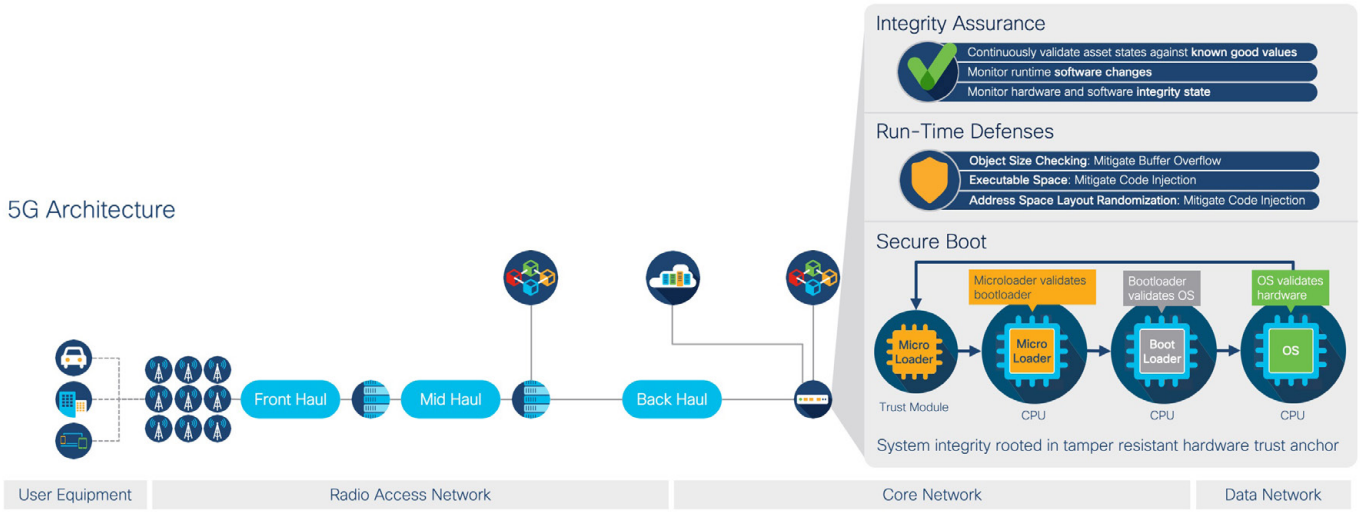


Zero Trust Environment

Integrity

Validate vendor supply chain security and secure development practices, employ trustworthy products, and continuously monitor hardware, software, and operational integrity to detect and mitigate infrastructure and service tampering. Key capabilities include:

- **Vendor Security Assessment**: Validate the strength of a vendor's supply chain security program, secure product development and management lifecycle, vulnerability and data disclosure, and overall information security practices. It may also be prudent to verify product security through direct assessment and testing of the vendor's design and implementation in vendor-managed facilities.
- **Secure Boot and Runtime**: Ensure assets leverage secure boot processes based on anti-tamper technologies such as hardware trust anchors and software image signing to assure the authenticity and integrity of hardware and software components. Assets should employ runtime defenses to assure the integrity of running processes and mitigate memory-based attacks such as buffer overflows and code-injection.
- **Integrity Assurance**: Continuously monitor hardware and software to validate integrity and detect tampering issues based on verifiable evidence that enables prompt corrective action.
- **Operational Integrity**: Implement appropriate policies, governance, and operational practices to detect and prevent insider abuse.

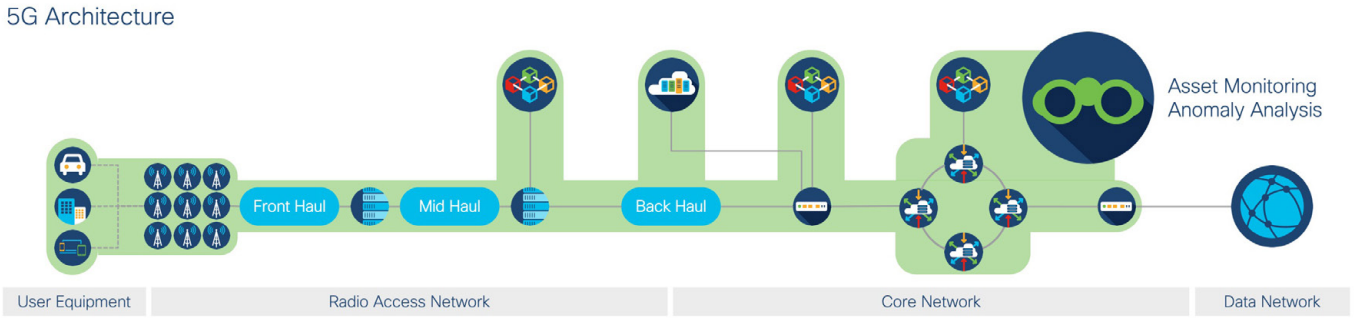


Asset Integrity Protection

Visibility

Enable full visibility across the infrastructure to identify all assets and continuously monitor asset security logs and anomalous behavior and communications patterns to reveal potential security risks. Key capabilities include:

- **Asset Monitoring**: Enable security tracking, logging, telemetry, and centralized monitoring for all assets, including endpoint, network, and server devices and applications.
- **Anomaly Analysis**: Leverage machine learning systems to monitor for and detect unusual asset behavior or communications patterns. As decryption of network traffic for threat inspection may impose unacceptable latency or violate privacy requirements, machine learning techniques should be tuned to detect anomalies in encrypted traffic flows as well.

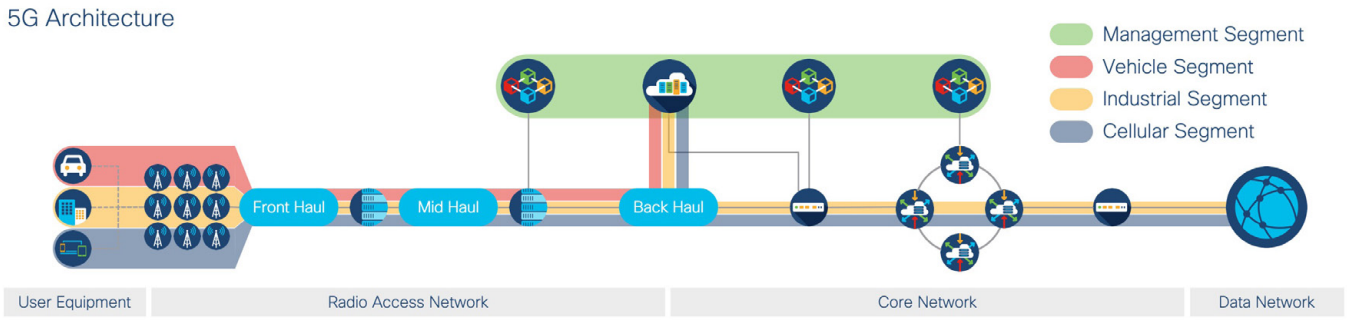


Full Infrastructure Visibility

Segmentation

Implement end-to-end segmentation to partition asset groups, reduce the attack surface, and limit the impact of compromise. Key capabilities include:

- **Software-Defined Segmentation**: Place assets into logical security groups that leverage network-integrated access controls and policy services to limit communication flows between groups. 5G network slicing features should be leveraged as a component of an end-to-end segmentation strategy.
- **Network and Application Firewalls**: Implement firewall gateways to inspect and explicitly allow or deny transactions between critical assets or asset groups.

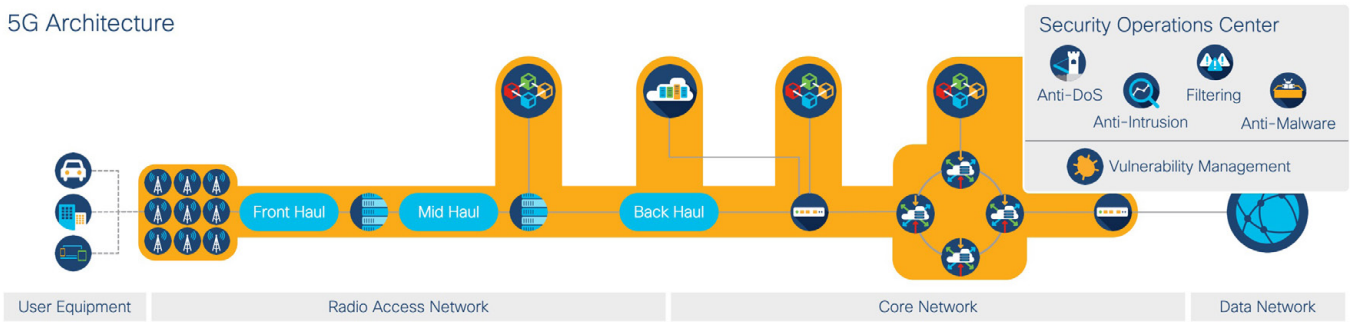


Software Defined Segmentation

Threat Protection

Implement defensive security controls and continuous monitoring backed by machine learning capabilities, and establish incident response operations to detect and mitigate threats to assets. Key capabilities include:

- **Vulnerability Management**: Adopt internationally-accepted standards and best practices on coordinated vulnerability disclosure and handling to effectively identify, mitigate, and remediate security vulnerabilities (e.g. software patching) in a timely manner.
- **Denial-of-Service Defense Systems**: Monitor network traffic to detect and mitigate network flooding attacks.
- **Intrusion Detection and Prevention Systems**: Monitor network traffic to detect and mitigate unauthorized access or attempts to exploit system vulnerabilities.
- **Malicious Traffic Filtering Systems**: Monitor network traffic to block malicious or unwanted traffic such as spam or attempts to interact with malicious domains and websites.
- **Anti-Malware Systems**: Monitor network traffic and endpoint and server devices to detect and block malware files or malware execution.
- **Security Operations Center**: Establish a centralized security monitoring, incident response, and threat intelligence organization responsible for rapidly detecting and mitigating security breaches. Adopt integrated cybersecurity capabilities and automation tools that simplify and streamline security operations.



Threat Protection Services

Data Protection and Privacy

Implement policy-driven security practices and controls to protect data and privacy, harnessing many of the key capabilities listed under the previous recommendations. Data protection and privacy represents the application of policies, practices, and technical controls to protect user rights and secure data against unauthorized data access or use. Security policies and controls should be applied in a manner consistent with regulatory requirements and best practice to protect sensitive data and ensure those who are authorized to access and process data do so ethically and responsibly. Data protection and privacy should also address steps to be taken in the event of a breach or compromise and the mitigation and recovery procedures to contain the damage and inform the affected parties in accordance with applicable laws and regulations.

Conclusion

5G is an evolving architecture with few implementations and many unanswered questions. What is clear is that cybersecurity is foundational to realizing dependable and resilient 5G services in any form it takes. Government regulators and network operators must work hand-in-hand to ensure cybersecurity best practices and capabilities are designed into 5G infrastructure and operations right from the start. With an ever-evolving threat landscape matching the pace of innovation, it is crucial that network operators approach 5G build-out with a zero trust mindset, prioritizing infrastructural and operational integrity, ensuring full visibility across the network, partitioning traffic flows appropriately, continuously defending against attacks, and placing data protection and privacy at the heart of service delivery.

References

3GPP TS 23.501 Release 15, December 2019

3GPP TS 33.501 Release 15, June 2018

ENISA THREAT LANDSCAPE FOR 5G NETWORKS, November 2019

EU toolbox on 5G Cybersecurity, January 2020 (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468)

NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1, April 2018

NIST SP-800-207 [DRAFT] – Zero Trust Architecture, September 2019

NIST SP 800-190 – Application Container Security Guide, September 2017

The Evolution of Security in 5G – A "Slice" of Mobile Threats, July 2019 (https://www.5gamericas.org/wp-content/uploads/2019/08/5G-Security-White-Paper-07-26-19-FINAL.pdf)

Enabling Rakuten Cloud Platform with Cisco NFVI and Orchestration Solutions, February 2019 (https://blogs.cisco.com/sp/enabling-rakuten-cloud-platform-with-cisco-nfvi-and-orchestration-solutions)

Securing the 5G Core (5GC) and Evolved Packet Core (EPC) with Cisco Security, March 2019 (https://www.cisco.com/c/en/us/solutions/collateral/service-provider/service-provider-security-solutions/white-paper-c11-742166.html)

5G Security Innovation with Cisco, June 2018 (https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/service-provider-security-solutions/5g-security-innovation-with-cisco-wp.pdf)

Sources

[1] Although there is a larger attack surface in 5G based on new use cases and architectural and operational differences from earlier architectures (e.g. 3G, 4G), the 3GPP security standards for 5G include specific features and mechanisms to help mitigate this risk. Vendors and operators should consider these features carefully for any 5G deployment.

[2] Network slicing enables the creation of multiple and distinct virtual networks across a shared infrastructure.

[3] Edge computing enables the placement of performance sensitive applications closer to end users. This is described in more detail later in the document.

[4] Zero Trust represents an overarching access security model that deliberately avoids assuming implicit trust between elements in a network. This is particularly important in 5G as various external stakeholders may need to access infrastructure components or services for management, maintenance, or monitoring purposes. For example, enterprise users may need select access to 5G slice management services. Third party vendors may need access to select components for configuration or troubleshooting. Properly implemented, Zero Trust can provide appropriate stakeholder access while securing 5G services against misuse.

[5] The workforce area concerns user and device access to applications. The workplace area concerns user and device connections across networks. The workload area concerns connections between applications and services.