WHITE PAPER

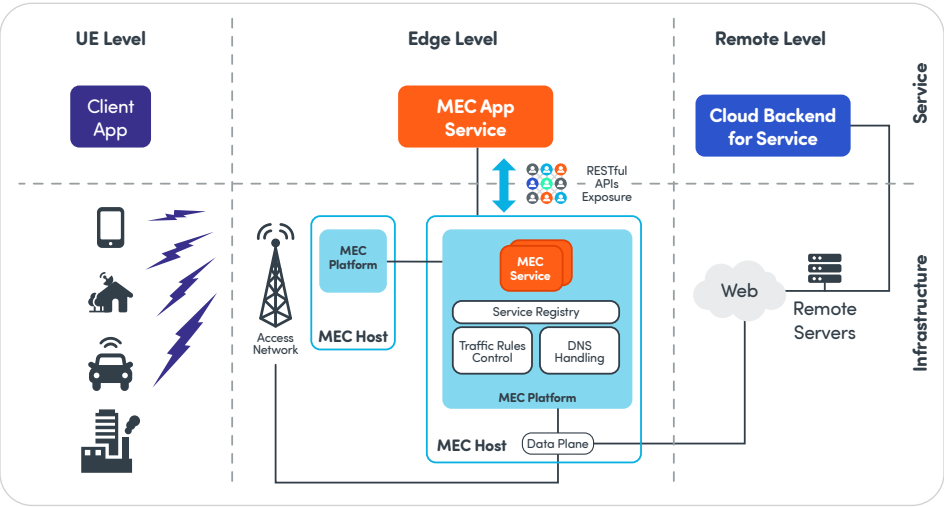
The Fundamentals of Ensuring 5G MEC Security

What is 5G MEC?

5G introduces heretofore unseen capabilities for mobile internet. Its ultra-low latency and ultra-fast connection speeds will not just transform mobile connectivity but empower a variety of new use cases such as autonomous vehicles and smart cities.

Empowering 5G, multi-access edge computing (MEC) is a technology that helps deliver these ultra-low latency and high bandwidth speeds by placing computing and processing capabilities as close to the end user as possible, at the edge of the mobile network. As well, the cutting-edge of advantage in cloud and next-gen mobile gaming, requiring the lowest latency and highest performance possible for users, in essence defining the next generation of networking, is powered by MEC.

This allows data to be processed and stored locally, reducing latency, and improving performance and speed. MEC is particularly powerful when used in 5G networks that follow 3GPP standards and use cloud and virtualization technologies such as network function virtualization (NFV) and software-defined networking (SDN). 5G networks provide a dynamic environment for edge computing, while MEC enhances 5G's capabilities by offering ultra-low latency, extended bandwidth, and higher performance.



MEC applications, interaction, and service exposure in a 5G Network

Both 5G and MEC rely on virtualized and disaggregated software components running on geographically distributed and open hardware. While this architecture offers many benefits, it also exposes MEC and its stakeholders to a range of constantly evolving cyber threats. The impact of these attacks can extend across the environments and networks in which MEC is implemented, so it is important that 5G MEC is developed with security in mind from the earliest stage of planning and development.

Introduction

Multi-access edge computing (MEC) represents a game-changing capability in 5G environments for organizations, delivering faster speeds and enhanced bandwidth, thereby fostering a new level of products and services to their customers. To achieve that, a new level of complexity is introduced into the 5G equation, and with that comes a drastically expanded threat surface which must be accounted for with comprehensive end-to-end coverage.

This white paper examines the range of threat vectors and factors that are associated with MEC solutions and offers insight into proven testing strategies to assure the validation of the entire MEC solution so that it can deliver on its promise.

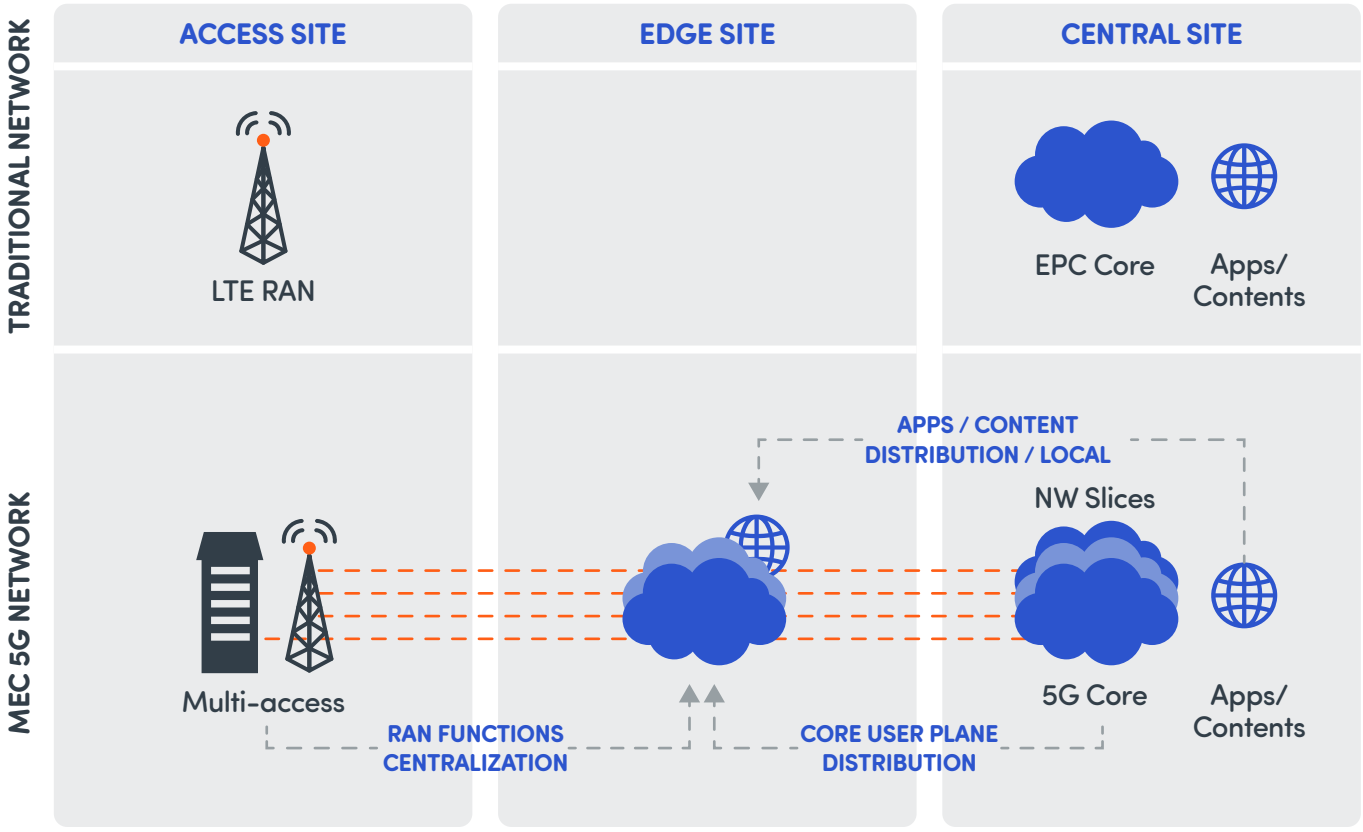
How MEC Works

MEC essentially changes how data travels through a mobile network. In a traditional network architecture, transactions travel through the Radio Access Network (RAN), then through the 5G Core, and back again.

With MEC, the speed and performance of mobile networks are improved by processing and storing data locally, at the edge of the network. This is achieved by placing servers and hosting infrastructure close to the end user and the 5G Core network. MEC can be deployed in a variety of ways, including on physical hosts like gNodeB base stations, in the cloud, or in a hybrid model that combines both physical and cloud-based deployment.

MEC data centers can collect local information and network data in real time, which can be used to gain insights about specific use cases or environments, and to report on operating conditions for easier and faster maintenance. This allows for faster access to those applications and services, and enables enterprises to create new and enhanced products and services for their customers.

MEC data centers also use local resources, allowing services that rely on them to remain resilient in the event of problems or outages on the broader network. However, MEC solutions also introduce new connections and components that could be attacked individually, so it is important to have the right security measures in place and to properly test them before the deployment.



MEC changes how data travels through a mobile network.

Security Threats to 5G via MEC

One of the fundamental qualities of MEC solutions is that they are largely open environments for third parties to enable better performance for users. MEC data centers will host a large variety of stakeholders, applications, application programming interfaces (APIs), data, and technologies which will constantly interact.

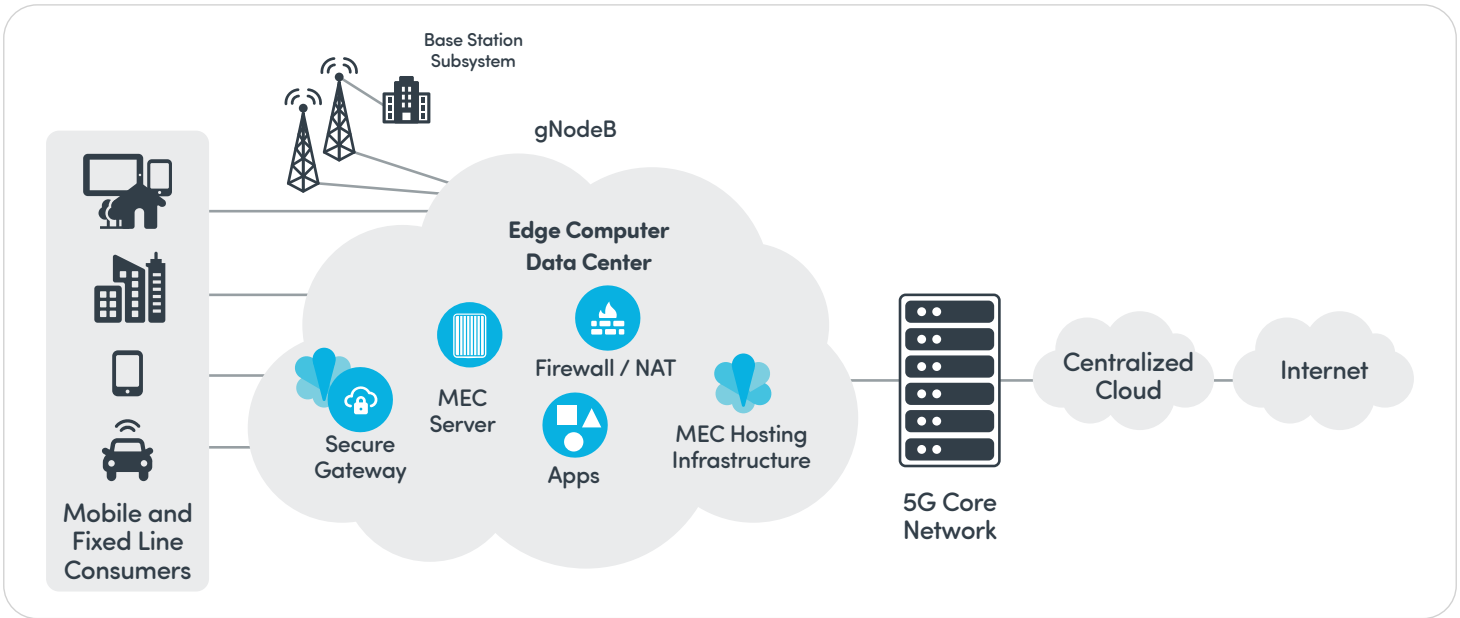
The open environments, along with a variety of stakeholders, applications, APIs, data, and technologies hosted in MEC data centers, make them vulnerable to abuse, exploitation, and misuse. These vulnerabilities can occur in the form of abuse of assets, supply chain compromise and misconfiguration, and weak security controls. MEC data at rest and in transit represent expanded security vulnerabilities due to the open and multivariate nature of the environment. To address this, it is important to secure each component and the way they communicate. Applications should be logically separated, and data should be segmented appropriately, while their interactions should be policed and monitored.

There are a range of threats that a MEC data center could face when it goes live. A successful attack on a MEC solution could lead to exploitation of the MEC ecosystem and even be used as a vector for a broader attack on the 5G Core network or supply chain. To protect against these threats, it is critical to have a comprehensive security framework in place and to properly test it before deployment.

Abuse of Assets

The first point of concern is that the internal assets of the MEC data center might be abused by attackers, co-opting the architecture of MEC solution to their own ends. These threats include:

- **Zero-day vulnerabilities.** If an attacker exploits a gap in either the MEC solution's software or hardware, they could leverage undiscovered vulnerabilities, leading to a zero-day attack which could exploit the multi-faceted MEC environment or its stakeholders.
- **Tampering and exploitation.** If attackers access software that's deployed on a MEC data center, they could manipulate the software or tamper with crucial systems.
- **Availability and performance degradation.** A successful attack on a MEC data center could degrade performance and disrupt service availability.
- **API exposure.** MEC solutions host a range of services and applications and must therefore open APIs for third parties to integrate with and access those services. This fundamental capability of MEC solutions can potentially lead to API exposure, and create opportunities for attack, abuse, and exploitation.
- **Component manipulation.** The MEC hosting infrastructure is also a potential point of concern. It could be physically accessed by malicious parties who would then gain control over the MEC solution and connected systems.



MEC data at rest and in transit represent expanded security vulnerabilities

Supply Chain Compromise

The MEC ecosystem connects users, technologies, enterprises, vendors, customers, and 5G networks, making it vulnerable to supply chain attacks. A successful attack on the MEC solution could compromise the broader supply chain and affect the users and systems within it. Some potential threats include:

- **Development manipulation.** Attackers could interfere with the development process of various stakeholders within the MEC ecosystem, including applications, APIs, and technologies, as well as the development of the MEC solution itself. This could be done by manipulating development tools or the overall development environment, potentially leading to the creation of vulnerabilities or the introduction of malicious code.
- **Source code manipulation.** Attackers may target the source code repositories or open source libraries used within the MEC ecosystem to insert malicious code or tamper with legitimate code. This could be done through the manipulation of development tools, the development environment, or through the insertion of malicious code into open source dependencies. These attacks could potentially compromise systems or data within the MEC ecosystem and the wider supply chain.
- **Update/distribution manipulation.** Adversaries may manipulate the update and distribution mechanisms for the MEC solution, as well as the applications, APIs, and technologies used within the MEC ecosystem. They could then send out malicious updates to legitimate systems or distribute malicious software under the guise of legitimate software updates, potentially impacting the MEC solution and its stakeholders
- **System image compromise.** Attackers could manipulate any system images within the MEC ecosystem, potentially obscuring malicious activities or deleting, corrupting, or altering backups. This could affect the MEC solution and its stakeholders.
- **Software component replacement.** Attackers could potentially manipulate the MEC solution and its stakeholders by replacing legitimate software components with malicious ones. This could include replacing software distributed through update or distribution channels, modifying open source dependencies, or selling modified or counterfeit products to legitimate distributors. The goal of these tactics may be to compromise data or systems, and they may be targeted at a specific victim set or distributed more broadly with additional tactics being deployed against specific victims.
- **Counterfeit sales.** Attackers may compromise the MEC ecosystem by using a successful attack to fraudulently sell counterfeit software and hardware components to legitimate customers. This could be achieved through the manipulation of product delivery mechanisms or the modification of products prior to receipt by the final consumer, potentially leading to data or system compromise.
- **Shipment interdiction.** By attacking a MEC solution, assailants may be able to insert themselves fraudulently into a supply chain and interdict shipments sent legitimately.

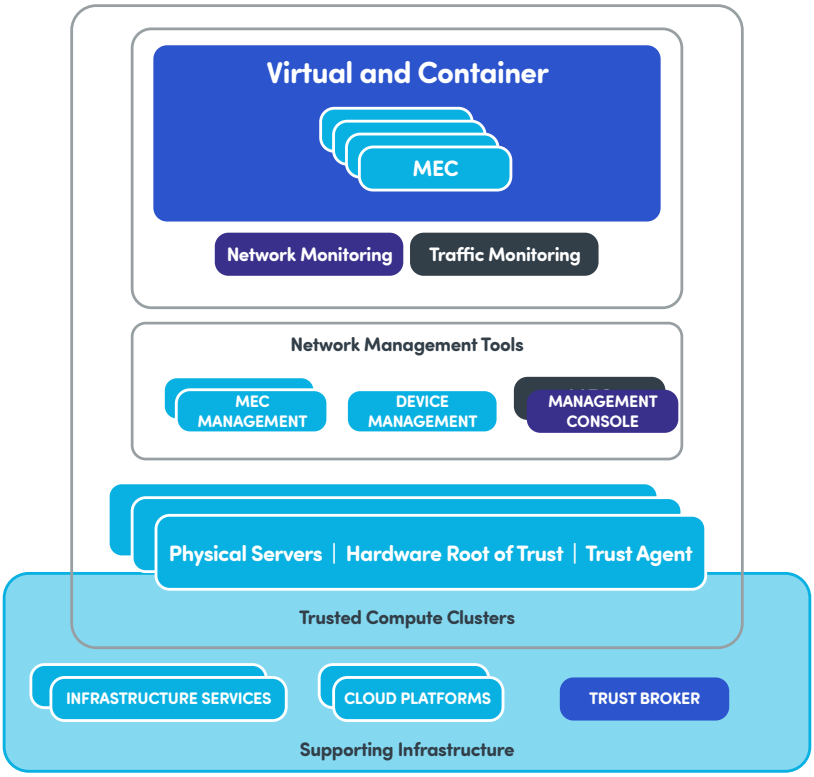
Misconfigurations and Weak Security Controls

Improper or poorly implemented security controls and practices are an enduring challenge in all parts of IT. Similarly, they will be a problem for MEC solutions. Attackers can exploit these gaps to gain unauthorized access and potentially expose sensitive information. The unique nature of the MEC environment also brings additional problems. The types of vulnerabilities that can arise from misconfigurations and weak security controls include:

- **Manipulation of target environment.** If threat actors can exploit a MEC environment's insufficient security controls, the attackers may be able to infiltrate a MEC solution and in doing so, manipulate the victim's environment to hamstring operations, degrade MEC defences, or open new attack vectors.
- **Compromise of integrity.** An attack on a MEC solution could compromise network integrity of data communication that are not integrity-protected.
- **Misconfiguration.** Attackers could revert the configuration of software components or systems to default or insecure settings.
- **Tampering with security controls.** Attackers might infiltrate a MEC system in order to turn off or misconfigure security features.

Threat Vectors and Their Risk Factors

The potential attacks and damages that can be wrought upon MEC solutions and their stakeholders are diverse. The key to mitigating them requires a clear understanding of the risk factors that might permit those threats to emerge. MEC solutions face many of the same threats that other IT systems do, but their vulnerabilities may emerge in unique ways.



The MEC ecosystem

Platform Security and Integrity

The security and integrity of the MEC platform relies on the resilience of the tools and processes that protect and manage it. This is the starting point when planning and developing MEC security and understanding the associated list of potential vulnerabilities.

Operations, Administration and Management (OA&M) Security. OA&M functions are those which oversee the everyday workings of a MEC system. They control privileged access within the ecosystem. This is an essential requirement for interfaces which legitimate parties use to operate these assets. Gaining unauthorised access to these access privileges will put attackers in the MEC driving seat.

Best practices for OA&M security must ensure access to these assets is carefully controlled and monitored, with only those who are officially approved to have access being granted privileges to do so. All users should be authenticated and authorized, and their access monitored, logged, and audited. As such, identity and access management (IAM) controls should be implemented for OA&M interfaces and secure communication channels must be put in place.

Access security can be bolstered by incorporating multiple factors of authentication for use of these interfaces, such as PKI-based certificate authentication and biomarkers, can also be implemented to enhance access security.

Encryption. 5G MEC systems will be replete with important data about services and technologies, as well as potentially sensitive user data. As a result, that data will need to be encrypted to avoid unauthorized access and privacy violations, whether accidental or malicious. Failing to do so offers opportunities to attackers, presents the threat of noncompliance with numerous regulatory agencies around the world that require personal data be encrypted both in transit and at rest. As such, all communications must be encrypted and centrally managed across the MEC system.

Key and certificate management systems. Keys and certificates will be crucial to securely manage various interactions. As some of the most sensitive assets that an edge environment maintains, they need to be closely managed and monitored. Certificates, for example, often expire without the knowledge of administrators, leading to serious security incidents. From that point of view, clear benefits result with the use a certificate lifecycle management (CLM) system which maintains oversight the validity of certificates throughout the MEC environment.

Similarly, keys need to be stored securely, closely monitored and controlled lest they fall into the hands of malicious parties and give them the ability to access and decrypt crucial MEC data. A hardware security module (HSM) can ensure cryptographic assets such as keys and certificates are securely created, stored, and protected from tampering.

Cryptographic algorithms. The strength of the algorithms used to encrypt data are of particular importance. Most modern-day encryption algorithms are exceptionally hard to break for all but the most motivated and resourceful threat actors. Still, they should be considered a vulnerability in 5G MEC, especially those algorithms utilized in safety-critical or national infrastructure-based use cases. Furthermore, the advent of quantum computing will, according to the U.S. National Institute of Standards and Technology (NIST), provide the means to break all current encryption. Strong cryptographic algorithms – and measures to resist quantum threats – are a necessity for planning and development of MEC deployments for the future, to maintain private information security and ward off advanced threats without interruption.

Network Security

Network security is essential for protecting sensitive data and the MEC ecosystem from unauthorized access, misuse, modification, destruction or improper disclosure, denial of service, and network-accessible resources. Maintaining complete visibility and control over all workloads in a dynamic and ever-changing MEC environment is a significant challenge. Security strategies must evolve to keep pace with the growing number of security risks in MEC environments. These challenges pose a significant threat to data and MEC ecosystem security, from the complexity of data centers, to the outdated nature of manual security controls, and the ever-increasing cleverness and frequency of cyberattacks.

Best practices for MEC network security must ensure automation is incorporated into the framework of infrastructure security to eliminate human error, which otherwise expands the threat surface. This enhancement capability provides robust and comprehensive scalability to ensure holistic security. Another crucial aspect is establishing trust in virtual and cloud platforms by verifying, assessing, and testing the availability, integrity, and confidentiality of integrated firewalls, security groups, and micro-segmentation based on workload and trust compute hosts. Micro-segmentation can be achieved through automated network configuration and provisioning, and containers, built on a microservices model, are becoming increasingly common to support scalable workload isolation. Furthermore, VPNs are critical for securing hybrid environments.

Adopting a multi-layered approach that leverages automation, network segmentation, and the latest network security technologies is essential to ensure comprehensive security in MEC environments.

Virtual and Container Security

Virtual machine (VM) and container service platform threats represent significant vulnerability to MEC solutions. Threats include DoS, VM/container escape, VM/container compromise, image authenticity, side-channel attacks, orchestration and management security breaches, and cloud service consumer misconfigurations.

Orchestration and management security is essential to infrastructure protection. It controls the orchestration of containers and virtual systems and represents a vital element of the platform. The security integrity of the entire infrastructure can be compromised by unauthorized access and manipulation of the orchestration and management plane.

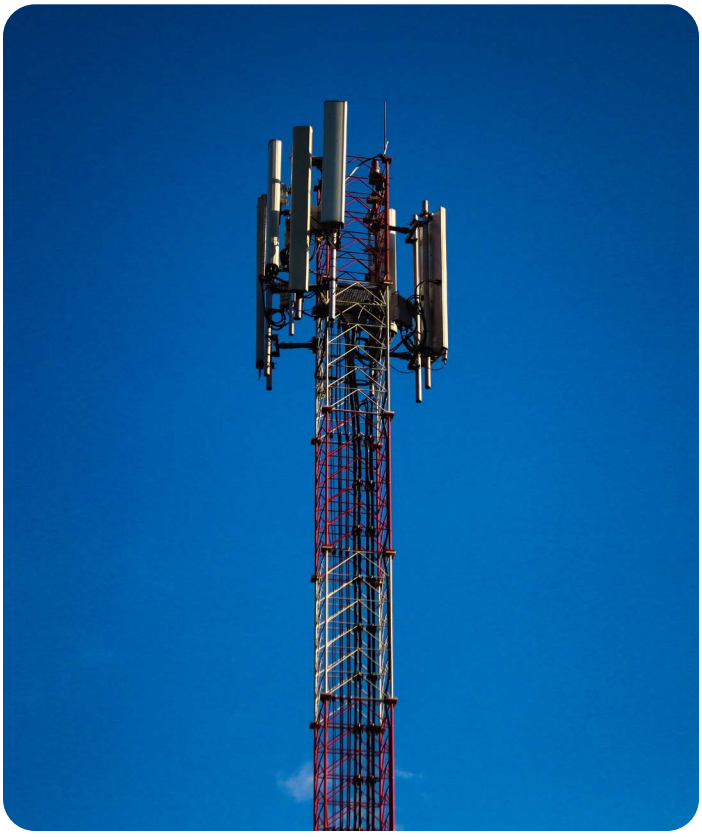
Moreover, resource consumption also poses a significant threat in a multi-tenant virtualization environment. If one tenant engages in extreme resource consumption, it can create a DoS event for adjacent tenant systems. The action can also result in compromising or seriously degrading solution functionality. In addition, colocation attacks, such as VM/container escape or side-channel attacks, can compromise adjacent tenant compute workloads with resource deprivation. Data confidentiality, integrity, or availability may also be at risk.

Physical Security

MEC systems will be hosted on geographically localized hardware. MEC hosts are decidedly external to a centralized data center, and they will exist in physically accessible environments which can be exploited or harmed by "real world" actors and leveraged to attack the MEC software itself. Physical attacks can compromise the integrity of the MEC solution, interfere with apps and services, and infrastructure within, and extract sensitive data such as user information or cryptographic keys.

Natural disasters such as floods, fire, and earthquakes can also damage the MEC host and the systems within, leading to physical exploitation or compromising the security of the system.

MEC hardware must be resistant to tampering, physical deterioration and damage. They also need to be closely monitored to either catch physical intrusions, damages or behavioral anomalies coming from the host. In essence, proper physical and environmental security of edge computing facilities must be assured which includes security monitoring of edge computing facilities to ensure a secure service environment.



Application Security

MEC solutions will host a large variety of applications, and through software vulnerabilities in those applications, serious threats can arise. The entry points that application vulnerabilities provide can permit a variety of attacks. Attackers can gain unauthorized access to data, they can elevate their privileges and exploit a variety of MEC components and internal assets.

Web applications are one of the largest attack surfaces. A recent Forrester Survey found that 39 percent of external attacks directly targeted web applications. Much like application programming interfaces (APIs), they're often susceptible to injection attacks or server-side request forgeries.

Application security can be poorly implemented. Authentication or access controls might be misconfigured, allowing improper access or privileges to the wrong parties. Security controls could be insufficient, out of date, or set to default. Furthermore, the actual design of those applications might leave exploitable gaps such as excessive and unnecessary ports or potential for integrity violations.

The importance of regularly patching and updating applications to address known vulnerabilities cannot be overstated. Additional recommendations include:

- **Conduct regular vulnerability scans** and penetration testing to identify and address any potential security weaknesses in the applications.
- **Ensure secure coding practices are in place** during the development of applications and perform code reviews to identify and fix any security issues.
- **Implement robust access controls** and authentication mechanisms to prevent unauthorized access and ensure proper authorization of users.
- **Use encryption** to protect sensitive data and prevent data breaches.
- **Keep security controls up to date** with the latest patches and software updates.
- **Conduct regular security audits** and assessments to evaluate the effectiveness of security controls and identify areas for improvement.

API security. One of the main characteristics of a MEC solution is that it can open itself to third parties to host their services, thus delivering benefits for both the third parties and its users. However, opening those APIs to third parties also presents the potential for vulnerability exploitation on a variety of levels.

If APIs are insufficiently protected or managed – for example, by allowing clear-text authentication or anonymous access – they can become exposed. Attackers could then manipulate, compromise, or damage the MEC solution. If user authentication is implemented poorly, attackers can pretend to be a legitimate service, or users, and fraudulently connect with an API.

In other cases, important data can leak from APIs only to be captured by malicious parties. Many API deployments give an excess of data in order to filter it properly. For example, unauthorized access to the location API for the MEC location service can expose sensitive location data and seriously violate user privacy.

MEC solutions may similarly be subject to the range of common security challenges APIs face. The *OWASP API Security Top 10* vulnerabilities lists many of them. Many APIs grant too much access to users, allowing threat actors to extract too much information about the broader system, or manipulate controls to achieve results that threaten the MEC solution's integrity and functionality. Injection attacks are also a continuing problem for APIs in which attackers can send specific commands to the API to expose important information or execute various actions.

API gateways. API gateways secure the APIs and provide functionalities such as authentication, authorization and access control, rate limiting, and data encryption. **It is the core of API security**. In addition to the basic capabilities found in API gateways, organizations should implement a comprehensive and forward-looking API security solution to protect current and future APIs to ensure enduring data integrity and confidentiality.

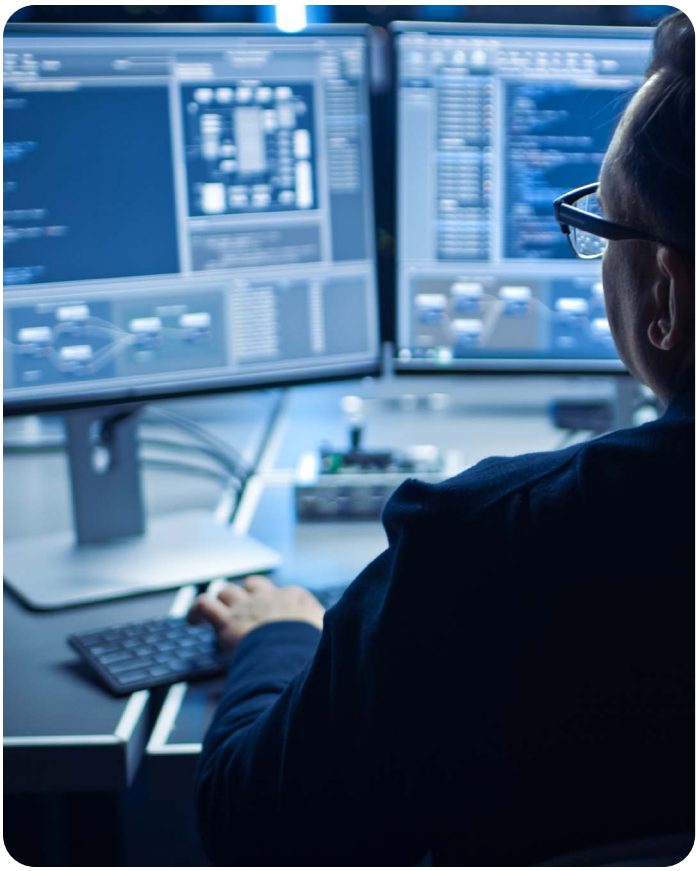
Monitoring API usage. Logging and monitoring the usage of the APIs is essential to detect any suspicious activity by first acquiring raw user data to establish the usual user behavior patterns. Threats are detected by identifying unusual and malicious patterns so they can be stopped in real-time. Insufficient monitoring and logging results in untraceable user behavior patterns. This allows threat actors to compromise a system and remain undetected.

Advanced API testing strategies. MEC APIs represent a major attack surface which requires a new approach to validation. Testing the security of the APIs using **automated test tools** helps address the growing complexity test teams face to ensure reliable coverage. They also provide the building blocks of machine learning (ML) for future security testing evolution. **API penetration testing** identifies security vulnerabilities that attackers might exploit to gain access to sensitive data or perform other malicious actions. This type of testing involves mimicking approach that malicious actors would use to find exploitable weaknesses. This includes testing for SQL injection and cross-site scripting (XSS) attacks, and other API level vulnerabilities. This type of testing should employ industry-recognized methodologies such as the OWASP (Open Web Application Security Project) testing guide and OWASP Application Security Verification Standard

Requirements of 5G MEC Security – The Need for Testing

Security testing is a crucial aspect of any 5G MEC deployment. While low latency and optimized performance are key benefits of multi-access edge computing, security is the foundation which ensures it and prevents the infrastructure from falling prey to data theft, downtime, and more.

These threats must be understood and ultimately mitigated if 5G and MEC's true potential is to be realized. Security will be a firm expectation for all stakeholders in the MEC ecosystem and in order to assure them of a MECs trustworthiness, rigorous and comprehensive testing in both the development and live environments is crucial.



Assessment Strategies for 5G MEC Security

Recognizing that MEC solutions are architected in multiple ways, where individual implementations vary in a variety of bespoke environments, Spirent SecurityLabs has many years of experience delivering testing solutions in this space. This includes a special focus on 5G security. With this extensive background, SecurityLabs created of a set of essential testing strategies to assess the security posture of the MEC solution – whether public or private – before deployment, to identify and prioritize vulnerabilities.

Focused on Network Functions (NFs), the testing strategy includes, but is not limited to, the criteria found below.

MEC Security Architecture Review. This will first involve conducting a security architecture review to understand what processes and controls already exist within the environment, as well as to identify where a MEC solution might be vulnerable in its design of network segmentation and overall architecture. This review will consider cross-functional threats and vulnerabilities that may arise from the interactions of different components within the MEC solution. This review phase may also include a review of the MEC solution's physical security components within the service environments, providing a comprehensive understanding of the status of defence strategies already in place, with consulting available for any aspects that might be recommended for inclusion.

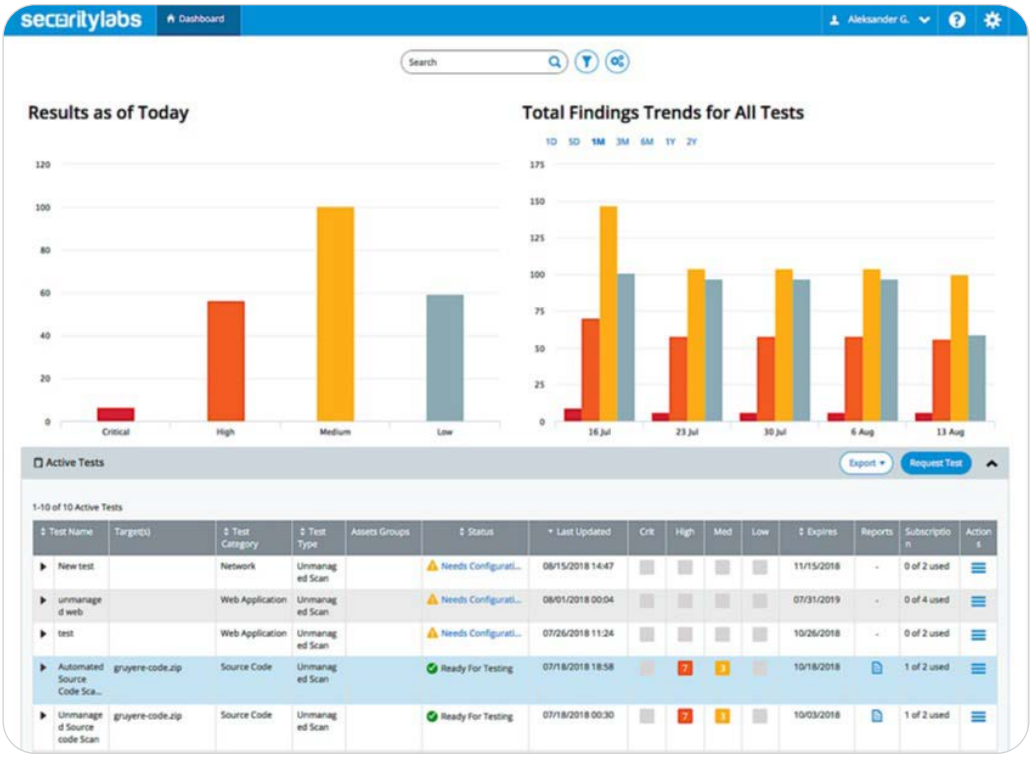
Network Penetration Testing. Components of the next stage will include testing the MEC solution through the white box and black box methodology, known as internal and external testing. The network penetration testing aims to simulate real-world attacks and provide a point-in-time assessment of vulnerabilities and threats to the MEC solution's network infrastructure. The network penetration tests are conducted on the perimeter from outside a firewall as well as behind the firewall or using VPN for assessing the network layer. This testing aims to assess how threat actors might exploit the environment under real-world conditions.

Host Security Assessment. This stage of testing assesses the internal controls that are in place within the MEC solution and examines their effectiveness. This supports the requirements of an evolving security posture which must undergo a regular cycle of review and adjustment of measures already in place. This review will encompass an examination of each host for vulnerabilities in areas such as patch management, credentials management, authentication management, event logging and sessions, misconfigurations, policy violations, and system hardening. The primary objective is to prevent privilege escalation and lateral movement in the network, ensuring that the system is secure from all angles, including compliance with security standards and alignment with organizational security policies. In addition, other security controls as defined per 3GPP Security Assurance Specifications (SCAS) standards would be part of this testing strategy. This assessment should align with the current security requirements of the MEC system and account for the associated upgrades and updates of a MEC solution's security hardware and software components.

Virtual and Container Security Audit and Testing. This stage assesses cloud, virtual, and container security, including cloud platforms like AWS, Azure, and Google Cloud, orchestration systems like Kubernetes and OpenShift, and custom solutions. The primary objective is identifying vulnerabilities threat actors can exploit to compromise the infrastructure. The virtual and container security audit and testing will focus on critical security areas, including but not limited to unauthorized access, compromise of a container or image, misuse of a container to attack other containers or the host operating system, escape from a container (container breakout), lateral movement, data breaches, and any other exploitation opportunities.

Hardware Security Assessment and Testing. Supply chain compromise, particularly in the form of counterfeit hardware, remains a persistent threat to the security of MEC solutions. Counterfeit hardware poses a risk due to its low cost of manufacture and the potential for high profits. To combat these threats, hardware security assessment and testing should be conducted to ensure the integrity and security of the hardware components. This type of testing should include, but is not limited to: device firmware analysis, binary code analysis, insecure boot process, JTAG/UART review, fuzzing, underlying software and application evaluation, evaluating communication channel, encryption, elevation of privilege, man-in-the-middle (MITM) attacks, code injection, memory leaks, serialization, and hardware reverse engineering.

MEC Application and API Penetration Testing. MEC application-layer pentesting identifies insecure application architecture, design, and configuration. This type of testing employs industry-recognized methodologies such as the OWASP testing guide and OWASP Application Security Verification Standard. The application and API test will focus on critical security areas, including but not limited to injection attacks, authentication mechanisms, session security, input validation, encryption usage, cryptographic weaknesses, business logic flaws, and policy compliance.



This assessment model has been utilized with a number of major North American Tier 1 operators:

- **MEC Security Architecture Review**
  - Insecure network segmentation
  - Misconfigured firewalls and monitoring systems
  - Poorly configured cloud security
  - Weaknesses in remote access
- **MEC Network Penetration Test**
  - Insecure PKI setup
  - Misconfigured firewall rules
  - Inadequate, misconfigured, or missing network access control
  - Unpatched network devices
  - Data exfiltration and egress protection bypass
  - Unsecured protocols
  - Security misconfigurations
  - Insufficient authentication
  - Default credentials
  - Insufficient privileged account management
- **MEC Host Security Assessment**
  - Insufficient protection of Kerberos ticket
  - Insecure file system permissions
  - Privilege escalation
  - Insufficient logging and monitoring
  - Unsecured network services

- **MEC Virtual and Container Security Audit & Testing**
  - Weak secrets management
  - Insufficient pod/container isolation
  - Inadequate patch management
  - No resource limits
  - Misconfigured network policies
  - Lack of restrictions on container images to private registry
  - Lack of mTLS and unrestricted pod-to-pod communication
  - ARP & DNS spoofing on Kubernetes
- **MEC Application and API Penetration Test**
  - Unauthenticated API
  - Broken access control
  - Insecure deserialization
  - Insufficient session expiration
  - Remote code execution (RCE)
  - Lack of resources & rate limiting
  - Weak JSON web token (JWT)
  - Sensitive information disclosure in JWT token
  - Application path disclosure
  - Improper exception handling
  - Verbose error message
- **Hardware Security Assessment and Testing**
  - Unencrypted communications
  - Hardcoded cryptographic keys
  - Reprogrammable components
  - Insecure boot process
  - Weak and non-standard cryptographic algorithms
  - Weak and common credentials
  - Unencrypted storage
  - Accessible serial console
  - Outdated software
  - Insecure APIs
  - High privileged running services

Assessment Report. Once testing is complete, assessment reports should be available that include an overview of all the issues that pose security risks to the MEC assets and network. A testing report should provide a list of prioritised security risks to the assets and its network found in the MEC solution, along with the potential impact those vulnerabilities represent. As well, included in the report should be detailed guidelines for remediation, with recommended steps to achieve a secure MEC solution.

This process will not only help clients find and address their vulnerabilities and security issues, but bring in key stakeholders, educating them on those impacts and mitigation strategies.

Accounting for New Cybersecurity Frameworks. Any testing strategy for 5G MEC security should also account for the new cybersecurity frameworks which have come out since the emergence of 5G, which resulted in more sophisticated threats and a broader threat surface. This elevated the urgency and importance of holistic security and necessitated employing new frameworks of security management. They include:

- **Secure Access Service Edge (SASE).** A cloud-centric distributed security architecture securing users and applications as opposed to subnetworks and IP resources
- **Zero Trust and Zero Trust Network Access (ZTNA).** Eliminating the notion of trust, necessitating that access must be granted for each application transaction
- **Transport Layer Security (TLS).** Use of encryption targeted at preventing malicious unauthorized altering of transmitted data between endpoints and eavesdropping
- **Mutual authentication.** Where the sender and recipient must verify the other party is genuine and trusted

Benefits of Proactive 5G MEC Security Testing

Knowing your weakness is a major strength. Having this insight means once issues are identified, they can be triaged addressed quickly before they become customer user issues impacting customer satisfaction and the flow of revenue streams. Other benefits include:

- **Lower costs** through reduced development time, pre-emption of failures in the field, visibility into whether investments are paying off as expected
- **Proactive visibility** of security posture helps organizations prepare for and pre-empt catastrophic and costly security breaches
- **Reduced risk of breaches**, fines for compliance violations, and inability to respond to new threats by validating security functions behave as expected
- **Lower customer churn** rates through data-driven insights into how well new services are performing
- **Faster innovation** and time-to-market as developers spend less time troubleshooting, testing and fewer refinement cycles
- **Ability to scale new services** with confidence that performance and security will not be compromised
- **Differentiated services** with tangible, reliable, sustainable advantages in security and performance

Qualifications for Comprehensive 5G MEC Security Testing

Ensuring qualified testing experts are engaged in the process is the key to secure 5G MEC solutions. Many in-house security teams are yet not familiar with the 3GPP 5G SCAS standards, since the requirements for 5G security are comparatively new. With 5G MEC, that characteristic of new technologies and requirements is also a concern for test team qualification. In the case of 5G security, Spirent's SecurityLabs test experts found over 75 security gaps across authentication, authorizing, encryption and system hardening. which could have resulted in:

- Unauthorized access
- Insecure transmission
- Service exposure
- Unauthorized access to NFs

These were all cases where the vendor representations indicated the solution components were ready for deployment. However, the status of network configurations and application software updates, and other factors, cannot guarantee these components are secure. Employing a seasoned testing team with holistic knowledge of 5G and 5G MEC solutions is critical to achieve reliable security in new and existing MEC solutions. Any security testing solutions must support the original goals of a MEC solution, which facilitates enhanced performance and delivering optimal latency. Too often, the security testing process, and the controls that are put in place, can impede these operational deployment goals.

Recognizing the significant list of requirements for holistic 5G MEC security, organizations at times, see the benefit of supplementing their inhouse capabilities with a qualified testing partner. This option often provides subject matter expertise development to in-house testing teams, as well as saves on costs due to the elimination of ramp-up time required for expert testing in this space. A test partner who has a full spectrum understanding of the nuances and complications of 5G network infrastructures and the variety of MEC implementations, as well as the challenges face individually and in general, are key elements of a qualified testing partner.

About Spirent

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks. We help bring clarity to increasingly complex technological and business challenges. Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information visit: www.spirent.com

Conclusions and Takeaways

Understand the vulnerabilities and severity of risks in 5G MEC cybersecurity. These cover abuse of assets, supply chain compromise and misconfigurations and weak security controls.

Account for threat vectors and their risk factors. These include platform security and integrity such as Operations, Administration & and Management (OA&M) Security; User authentication, Encryption; Key and certificate management systems, as well as cryptographic algorithms. Additionally, network security, virtual and container security, physical security, application security and API security should be taken into account.

Adopt a mature 5G MEC security testing strategy. Here the concept of building security from the planning and development phase, rather than bolt it on later, is key. A mature testing strategy should include, but not be limited to: Security Architecture Review; Network Penetration Testing; Host Security Assessment; Virtual and Container Security Audit and Testing; Hardware Security Assessment and Testing; MEC App and APIs Penetration Testing.

Consider an expert testing partner. A qualified test partner in 5G MEC must understand the fundamentals of all the associated technologies, how they operate, and crucially, how they can be attacked. The partner should possess the same creativity and innovative cunning an attacker might use and so can security test MEC technologies in a way that few others can. The partner should have an established track record of testing engagements in communications and security industries. With this the test partner offers expertise but also years of data to establish reliable baselines, develop best practices, test, assure and ultimately prepare clients for the rigorous real-world conditions that their MEC infrastructure will be put under.

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com

Rev B | 01/24 | www.spirent.com