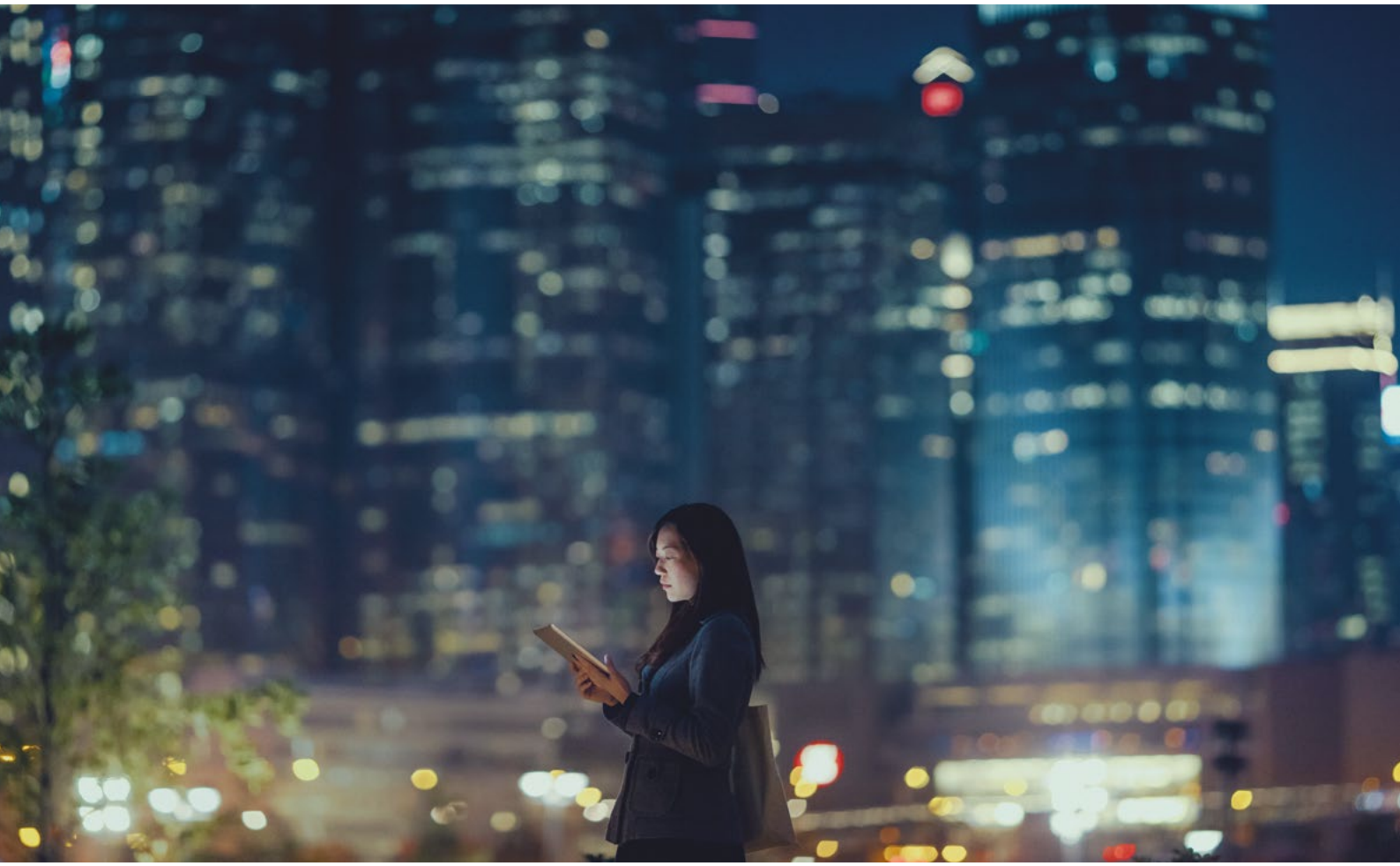
NOKIA



Cybersecurity in the age of 5G technology

Reducing risk and complying with security frameworks and toolboxes

Application note

Overview

Addressing cybersecurity risks in 5G networks

5G introduces new network technologies to connect devices critical to wider infrastructure and enable the development of a digital economy and society, making security and privacy high priorities. The European Commission has created a coordinated European approach to mitigate the main cybersecurity risks arising from 5G networks.

Its 5G EU Toolbox sets out nine risk scenarios and mitigating measures. This paper describes the three most relevant technology-related risk scenarios that can be addressed by CSPs: misconfiguration of networks; lack of access controls; and exploitation of IoT (Internet of Things), handsets and smart devices. As well as detailing the necessary measures required in each scenario, the paper outlines the Nokia approach and solutions available.

NOKIA

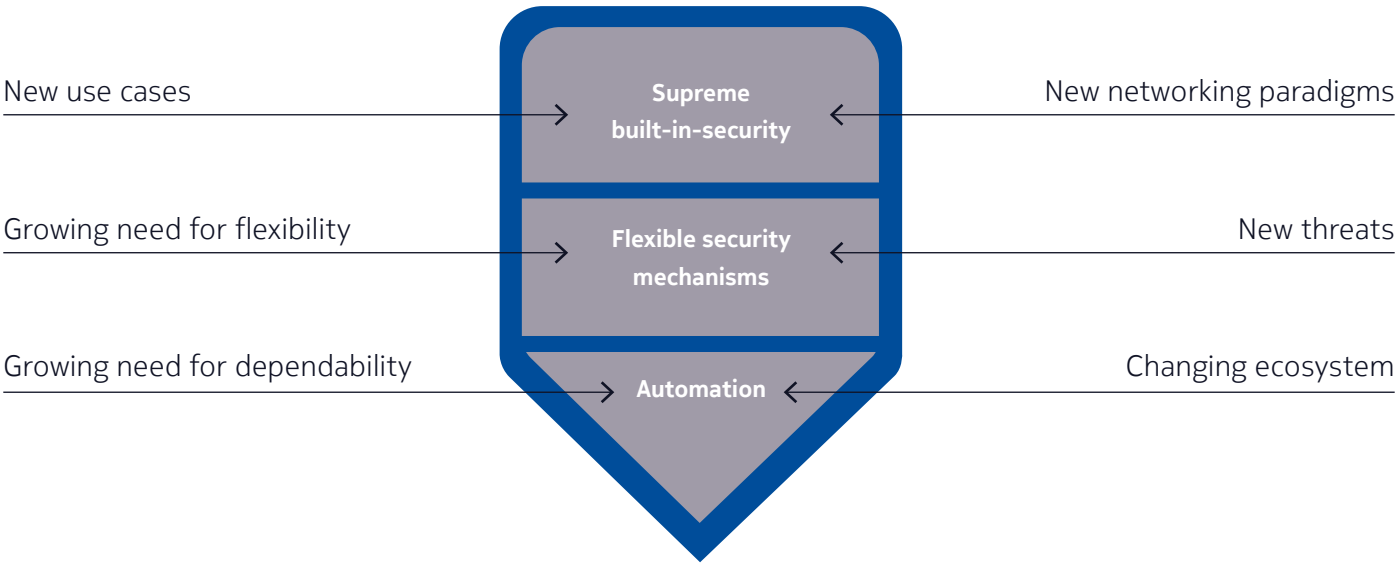
Contents

The importance of 5G cybersecurity

Wireless communication is inherently vulnerable and needs protection against interception and tampering. Encryption has been used on the radio interface ever since GSM brought 2G. The next two generations of mobile networks — UMTS and LTE — significantly enhanced security. Besides encryption of user traffic, these networks also provided mutual authentication between mobile terminals and the network, as well as integrity protection and encryption for all control and management traffic. These UMTS and LTE security features ensure high security and privacy for subscribers, as well as helping networks to combat various forms of attack.

The network changes that go hand-in-hand with the arrival of 5G mean that some elements of security now need to be reconsidered.

Figure 1. New network technologies and new capabilities, as well as changing ecosystem demands and rising cybersecurity threats all call for a rethink of network security



5G enables networks to be used in exciting new ways, but the growing variety of new devices and applications operating over the same network put security and privacy considerations front and center. 5G networks will connect devices that are critical to wider infrastructure, so data protection and access management features must be embedded in 5G solutions. 5G will also be a key enabler for the development of a digital economy and society, making security concerns everyone's business, including organizations such as ISO, IEC, NIS and others.

5G will affect almost every aspect of EU citizens' lives. The European Commission has therefore launched a coordinated European approach to mitigate the main cybersecurity risks arising from 5G networks. This resulted in the creation of the 5G EU toolbox, which recommends key actions to be taken at the EU level and by Member States. The rest of this paper will show how Nokia can help Communications Service Providers (CSPs) to deploy the security measures outlined by the EU toolbox.

EU toolbox of risk mitigating measures

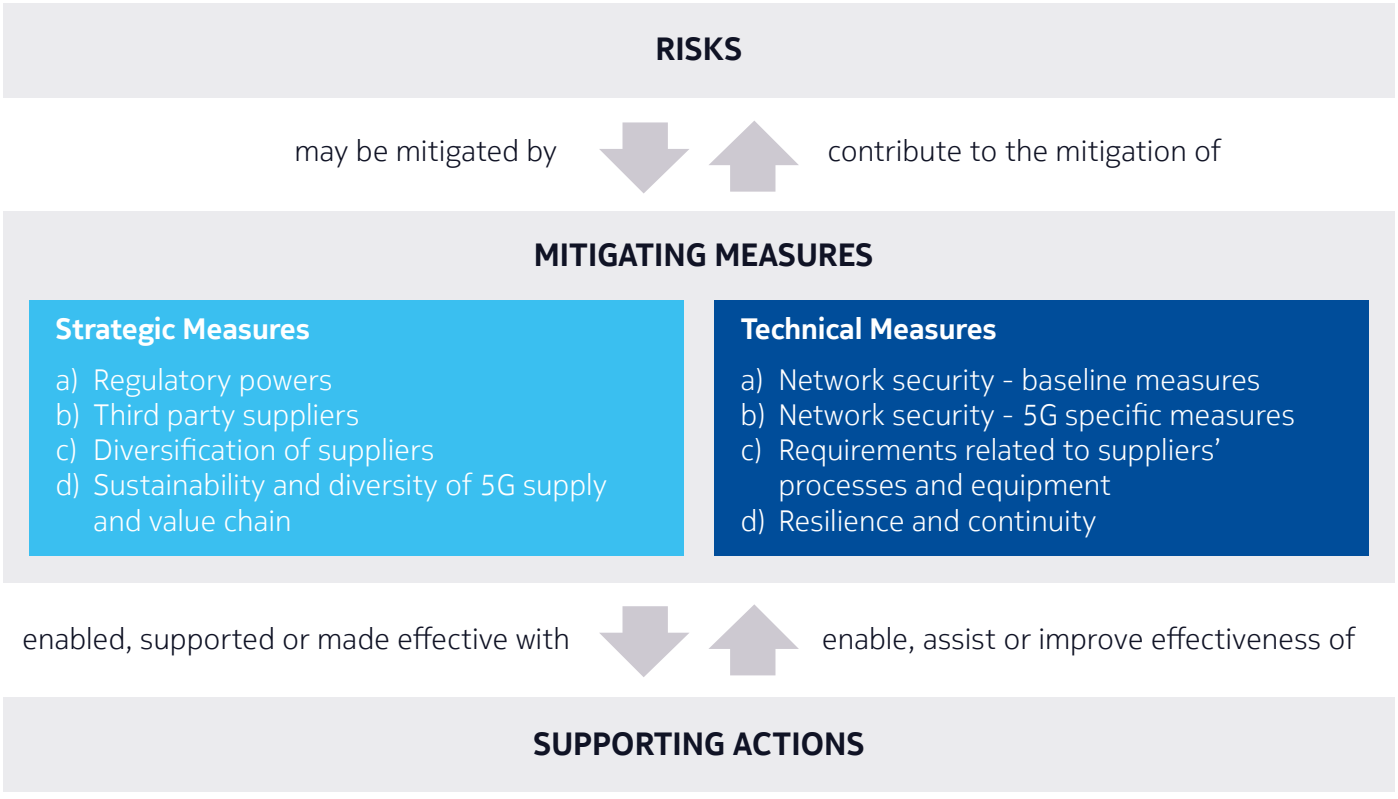
The European Commission published the Cybersecurity-of-5G-networks-EU-Toolbox-January-29-2020.pdf at the end of January. The toolbox identifies a common set of measures to mitigate the main cybersecurity risks arising from 5G networks.

The toolbox concludes that the current policy and framework for security in communications should be reassessed and Member States must take mitigating measures.

The EU Toolbox for 5G Security was developed by the NIS Cooperation group, which includes representatives of the EU Member States, the European Commission and the EU Agency for cybersecurity (ENISA). 5G cybersecurity is one of several work streams within the group. ENISA supports the group in all its activities, such as drafting guidelines and reference documents for good practice and developing collaborative procedures.

The toolbox identifies nine risk scenarios and mitigating measures. Most of the issues identified arise from the increasing use of cloud technologies and the dynamic network configurations arising from the proliferation of new 5G services.

Figure 2. The EU Toolbox for 5G Security identifies strategic and technical measures to mitigate security threats, along with relevant supporting actions



The toolbox aims to relate the emerging risks of 5G to the appropriate mitigating measures and supporting actions.

The main mitigating measures are grouped into strategic and technical categories, while a set of supporting actions are also proposed to reinforce their effectiveness.

Strategic measures include increased regulatory powers for authorities to control network deployments, as well as specific measures to address risks related to non-technical vulnerabilities, such as interference by or over-dependency on a third country. Other considerations include promoting a 5G supply and value chain. However, it is the technical measures that are probably more important here because they are under the control of CSPs.

It is important to note that strategic and technical measures cannot be used interchangeably. Increased technical safeguards cannot mitigate strategic risks and addressing strategic risks will not lessen technical vulnerabilities.

From a technology perspective, CSPs and their suppliers are the most relevant stakeholders for security within the 5G ecosystem. On the one hand, CSPs have a decision-making role, making them responsible for the overall security of their networks. On the other hand, telecom equipment manufacturers such as Nokia are responsible for providing the software and hardware that can implement the security features that CSPs demand.

Risk scenarios and mitigation plans

The toolbox identifies and provides risk mitigation plans for each of the risk scenarios identified in the EU coordinated risk assessment report. The plans each combine several mitigation measures.

As a leading supplier, Nokia can provide tools and solutions to mitigate the technology-related risks identified by the EU. This paper focuses on the three most relevant risk scenarios 1, 2 and 9: misconfiguration of networks, lack of access controls and exploitation of IoT (Internet of Things), handsets and smart devices. The following technical measures provide the tools to address these three scenarios.

Figure 3. Three risk mitigation scenarios that this paper addresses

Risk Scenario	Technical Measure
Risk Scenario 1: Misconfiguration of networks	**Technical Measure 1:** Ensuring the application of baseline security requirements (secure network design and architecture)
Risk Scenario 2: Lack of access controls	**Technical Measure 3:** Ensuring strict access controls
Risk Scenario 9: Exploitation of IoT (Internet of Things), handsets or smart devices	**Technical Measure 5:** Ensuring secure 5G network management, operation and monitoring
	Technical Measure 10: Using EU certification for other non 5G-specific ICT products and services (connected devices, cloud services)

According to the EU toolbox, “technical measures include measures to strengthen the security of 5G networks and equipment by reinforcing the security of technologies, processes and physical factors. The effectiveness of the technical measures in terms of risk mitigation will vary depending on the scope of the measures and on the types of risks to be addressed. In particular, technical measures alone would not allow [CSPs] to address non-technical vulnerabilities (e.g. risk of interference by a third country or dependency risks).”

NOKIA

Risk scenario 1: Misconfiguration of networks

Even if network components are initially configured correctly to comply with security policies, challenges can still arise during network operation. Misconfiguration is a constant threat that can only be countered by an automated audit and mitigation process. This will maintain security as configurations are updated.

Automated audits of security and application parameters are especially relevant with the introduction of dynamic, distributed and complex network deployments. These go hand-in-hand with multi-tier cloud-based architectures, which will become the norm in 5G networks that use Virtual Network Functions (VNFs) and, increasingly, Cloud-native Network Functions (CNFs).

The distributed nature of the required data center infrastructure and network functions present more challenges. Future network architectures will consist of multiple central, tens of regional and potentially thousands of edge data centers to deploy functions near the edge of the network. This optimizes delay and bandwidth for end-user devices.

Today's data centers, already deployed for previous network generations, are managed as separate entities. Each center has its own local authorization database and is configured according to the needs of the network deployment. Many parts of a deployment include automatic configuration and execution of hardening scripts. However, some aspects of configuration can only be done manually, resulting in potential discrepancies and misconfigurations.

There is an urgent need for intelligent network automation solutions that give CSPs comprehensive network and infrastructure visibility. These solutions need to respond rapidly to changing network conditions with minimal CSP intervention.

It will be essential to verify current network parameters and compare them to a gold standard, obtained either from a validated lab configuration or captured from the network by an initial audit.

Such automated audits will be able to spot changes made to critical assets, such as modified user privileges, added accounts, suppressed login credentials, FW states, etc, whether the changes were made by a privileged account, managed via an identity and access control, or made locally on the network element.

How Nokia helps

Security misconfiguration is a common problem. It can happen in a number of different ways, such as through insecure default configurations or credentials, unprotected files, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers or verbose error messages containing sensitive information. All operating systems, frameworks, libraries and applications must be securely configured, as well as regularly patched, upgraded and hardened in a timely fashion.

While security misconfiguration in traditional data centers puts companies at risk of unauthorized access to application resources, data exposure and in-organization threats, the advent of the cloud has increased the threat landscape exponentially.

With so much complexity in a heterogeneous environment, human error or malicious configuration may well take place outside of the control of the CSP, making it mandatory to put complete security processes in place and have tools to manage automatic audit and remediation.

It is also essential to manage other vulnerabilities by ensuring that the latest software releases and security patches are implemented automatically in the network.

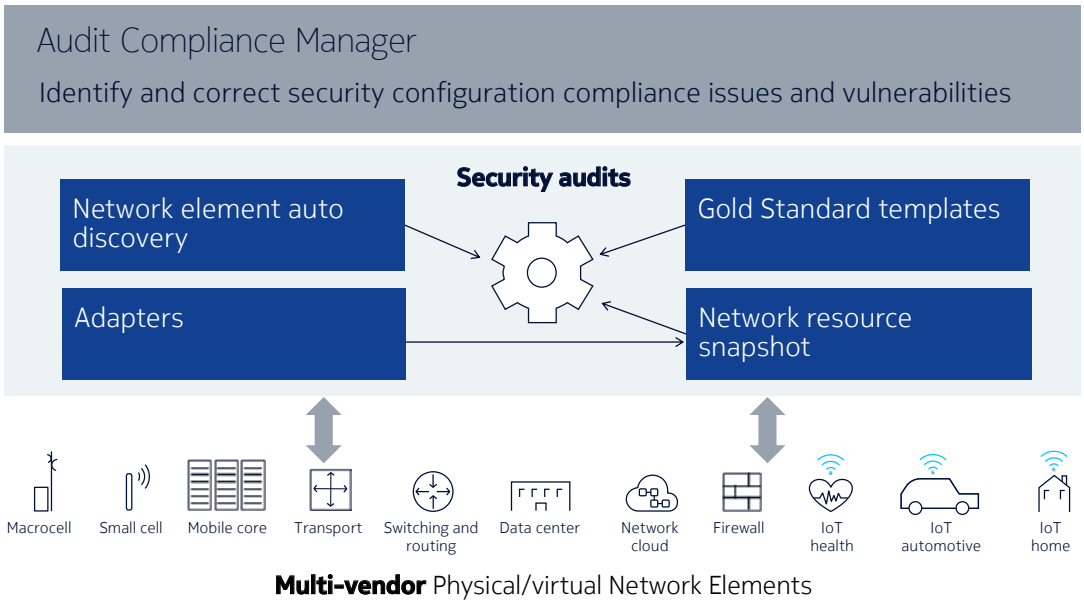
Security breaches on critical servers and applications could compromise the entire network. Security hardening and systematic compliance therefore needs to be enforced on each server/application and continuously audited, assessed, enhanced and reinforced. Issues with incorrect security configuration can otherwise leave systems vulnerable from the start, or the configuration may be compromised later.

Nokia NetGuard Audit Compliance Manager (NACM) automates the audit and analysis of all the parameters in physical and virtual networks. NetGuard ACM extracts real-time parameter settings from physical and virtual network functions and analyzes the data integrity by comparing the results to industry gold standards. It also flags up any mismatches to help prevent service degradations and process inefficiencies.

The flexibility delivered by Software Defined Networking (SDN) and Network Functions Virtualization (NFV) creates a dynamic environment, where service parameters and settings are frequently changed by both humans and autonomous processes. Combined with the Ethernet and IP protocols used by LTE, Video, IP Multimedia Subsystem (IMS) and cloud technologies, today's networks support millions of configuration parameters, so it is vital to maintain and assure data integrity.

NetGuard ACM therefore simplifies and accelerates the fine-tuning of network settings and parameters to ensure successful new service activations by delivering business process automation. It can also play a role in enhanced service assurance methodologies, improving the customer experience by automating and accelerating parameter and configuration checking.

Figure 4. Nokia NetGuard Audit Compliance Manager automates the audit and analysis of all the parameters in physical and virtual networks



Risk scenario 2: Lack of access controls

Today the management of Authentication, Access Control and Authorization is dispersed and often done in a siloed way that gives rise to important security control issues:

- Multiple users can share the same network accounts (admin, root and so on), accessing them using shared or default passwords and with no way to trace which user made any changes

- People external to the organization cannot get temporary access
- There is no automated process for access approval
- There is no consistency between network element user/credentials and central user management systems (user central point of control)
- Only the root administration is deployed, with no ability to manage role hierarchy based on roles and sub-roles
- The granularity of authorization is too limited
- Managing roles and privileges is extremely complex
- Nodes may have limited user/profile capabilities. If the scope of the authorization domain is too large, CSP personnel who are normally unauthorized to make changes may inadvertently make unwanted modifications
- Authentication policy (rules, One Time Password (OTP) and so on) is limited
- There is no centralized delegation capability
- There is no traceability of individual user actions
- There is no authorization formatting for interacting with the nodes

The EU toolbox recommends implementing adequate, flexible and verifiable technical measures to ensure strict network access controls are applied. The principle of least privilege should apply, ensuring people only have the access they strictly need. Duties should be properly segregated, and procedures should be in place to ensure the rules cannot be bypassed and that they evolve over time in step with the evolving network.

How Nokia helps

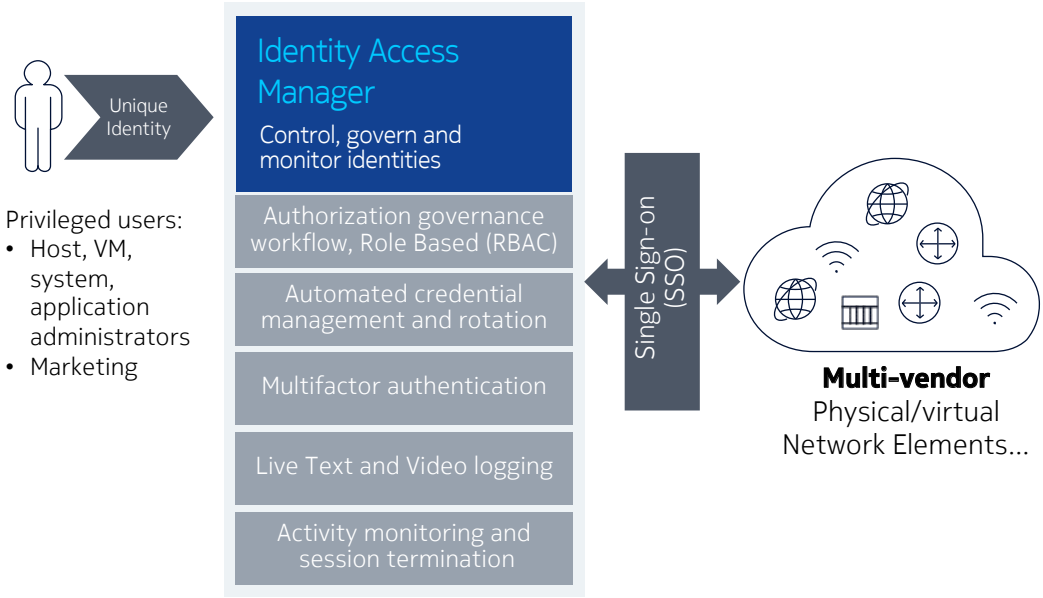
User Management defines user groups, complete with rights adapted to suit the role played by members of the group. It should be separate from network element Access Management. User Management should be able to check the status of each employee, while Access Management should safely store all network element passwords and hide those from users. All activities carried out under a specific user identity should be logged and analyzed to flag up abnormal behavior or for later examination after an incident. This last is a compliance requirement.

Applying the principle of “Zero Trust” means organizations accept the risk of identity theft or malicious activity by their own staff and subcontractors as a reality. They must combine two approaches to detect and mitigate such events and limit the impact on network operations. First, generate an audit trail for all user identities, complete with anomaly detection. Second, audit the security configurations on network elements to check whether they have been compromised.

NetGuard Identity Access Manager (NIAM) introduces the following principles:

- Separation of people from credentials with central management of network element credentials
- Full real time overview of activity on all network elements
- Full audit trail based on identification of individuals not roles
- Detection of any access bypassing the central system

Figure 5. NetGuard Identity Access Manager high level architecture



Nokia's experience in the telco space makes it possible to provide adaptors to support a full multi-vendor implementation, including Command Line Interface (CLI) or proprietary sessions next to Secure Shell (SSH). In addition, it helps CSPs to reduce the possibility of access by subcontractors by implementing comprehensive Privileged User Management capabilities and by separating user access from device access. Anomalous behavior can also be detected via User Behavior Analytics, which includes Nokia's NetGuard Security Management Center (NSMC) module.

Attacks by internal users can do the most damage and are the most difficult to find. These attacks may originate with genuine insiders or they may have had their credentials stolen. NSMC employs machine learning to generate per-user profiles of behavior based on ingested NIAM data. Suspicious user sessions can be terminated or locked out via the NSMC playbook (security operations workflow) to trigger action by NIAM. The suspicious user's NIAM account is locked pending Administrator investigation and action.

NIAM additional adapters also play a crucial role in access control management. The list of important adapters includes but is not limited to:

- Single sign on (providing a secure connection to network elements)
- Password rotation (automating the process of periodic credential changes)
- Account management

Network password rotation can be labor-intensive and time-consuming. NIAM maintains network credentials and updates automatically at the same time as the Network Management and Care systems, with tested credential rotation procedures in a multi-vendor network.

Nokia's NSMC is a security operations analytics and response system that aggregates, analyzes and correlates security data from a variety of sources, enriching it with context from the CSP to help security teams assess and control business risks, improve decision making and control costs. It enables trends or anomalies to be identified quickly and initiates automated responses by triggering cyber playbooks. It also detects and manages any incidents.

In addition to incident management, the NSMC solution includes an automated workflow/orchestration component that automates security service deployments, manages security policies and provides security policy lifecycle management. Nokia's solution makes use of cyber playbooks to drive automated actions in response to various threats and security alerts. Playbooks can integrate with other systems such as threat intelligence feeds and trouble ticket systems such as Remedy Action Request System (ARS), as well with network management solutions.

The NSMC aggregates inputs from various network and system data sources and correlates the data to identify patterns that match specific threats. For example, NetGuard ACM carries out regular audits and reports the misconfiguration of systems. The audit results are published to NSMC for analysis, so it can raise the alert about any incidents likely to impact on system security. The cyber playbook kicks off an automated workflow and triggers the reconciliation of the system configuration.

There are several important scenarios in which the NSMC will detect and mitigate the risk of network misconfiguration, as follows:

- A single security configuration violation
- Repeated security configuration violations
- Disabling of the firewall central management
- Bypassing single sign-on.

Advanced Persistent Threats (APTs) can go undetected for six months or more, causing significant damage. A combination of NIAM, ACM and SMC can significantly decrease the scope of damage by detecting the incident earlier.

Risk scenario 9: Exploitation of IoT, handsets or smart devices

GSMA Intelligence forecasts that IoT connections will reach almost 25 billion globally by 2025. This is a massive opportunity but it also poses several security risks. How do you ensure the security of billions of devices, as well as the network they are running on? How do you prevent a hacktivist group or state-backed actor taking control of IoT devices to attack the network by overwhelming the signaling plane?

As highlighted in the EU toolbox, it is important for CSPs to implement monitoring measures in their operation centers. Instead of scanning files, Nokia recommends a more efficient solution that looks at network communications between devices and the command and control (C&C) infrastructure. With network-based sensors, CSPs can monitor the network traffic between user endpoints and the internet, looking for evidence of malware infection. This includes malware C&C traffic, exploit attempts, hacking activity, suspicious behavior and Distributed Denial of Service (DDoS) activity.

Furthermore, alerts must be sent to a central alert reporting cluster where they are analyzed and stored. Interfaces provide real-time information feeds to Security Orchestration, Automation and Response (SOAR) systems, Security Information and Event Management (SIEM), firewalls and policy enforcement systems. Nokia also recommends implementing an automated end-user notification system and a self-serve remediation portal. CSPs must also protect network management traffic to avoid unauthorized changes to the network or service components.

How Nokia helps

Nokia's NetGuard Endpoint Security (NES) solution is an end-to-end, consumer-facing malware detection, notification and remediation service. It provides real-time network-based detection and analytics for all devices, whether or not the device has its own anti-virus or other protection systems. The solution is deployed offline, receiving a copy of the traffic to be inspected from the network. The system detects the communication signatures of malware rather than software signatures. It also detects anomalies based either on predefined or automatically learned traffic patterns.

For example, to protect against a DDoS attack coming from endpoints on the network, whether from users or IoT devices, NES can detect the creation of a Botnet in real time and block or disturb the communications to and from the C&C controlling the infected devices. NES can then either tell the subscribers or the IoT vendors to start cleansing their devices, or initiate processes within the CSP's organization to update the firmware of the devices using device management tools, such as Nokia's IMPACT IoT platform.

IMPACT IoT platform is integrated with NES and the NSMC to protect IoT devices without the need for security software clients on the devices. This closed loop security enables CSPs to detect anomalies when an IoT device is behaving strangely and detect viruses when an IoT device is sending suspicious messages. This horizontal platform provides secured services for device onboarding, device management, data collection, event processing, analytics and application enablement.

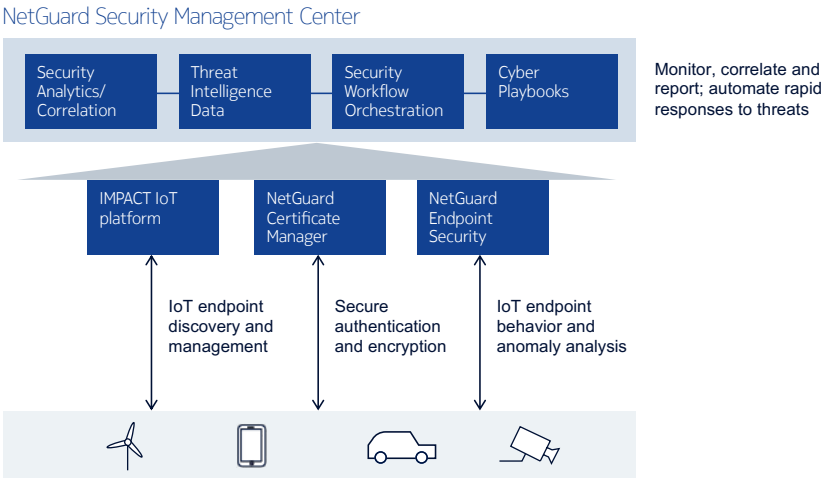
Of course, it remains very important to ensure that the device is not vulnerable. To accomplish this, IoT devices must be:

- Securely managed in terms of software, firmware and patching
- Have secure communication in terms of authentication, integrity and confidentiality
- Securely monitored to ensure they have not been compromised
- Provide automated and rapid response when a device is compromised.

Figure 6. Nokia's IoT security product suite provides the functions needed to ensure devices are protected

IoT devices must:

1. Be securely managed (firmware, configuration and patching)
2. Have secure communications (authentication, integrity and confidentiality)
3. Be securely monitored for malware activity
4. Provide automated rapid response when a device is compromised



Network security teams are supported by the detection of rogue IoT devices and their automatic removal from the network

NOKIA

Conclusion

Network hardware and software suppliers play a critical role in securing 5G network across Europe. A risk assessment should therefore be conducted at the European level, involving the relevant national authorities.

The criteria for assessing a supplier's risk profile are outlined in the toolbox and the EU coordinated risk assessment document: "the likelihood of the supplier being subject to interference from a non-EU country (presence of certain factors, which are also listed in the EU coordinated risk assessment report); the supplier's ability to assure supply; and the overall quality of products and cybersecurity practices of the supplier". This assessment should neither be a self-assessment and nor should it be conducted by other market participants given the obvious conflict of interests.

Security requirements and considerations must be an intrinsic part of new 5G architectures, not an afterthought. Get it right and CSPs, vendors and enterprises can deliver new services with confidence, trust and privacy. 5G services will increasingly form a part of the critical infrastructure in almost every country. It is important to invest in 5G security now to avoid unexpected costs later on from countering attacks or from the consequences of leaving high-value data unprotected.

The European Commission's "Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures" offers valuable guidance on the risks associated with 5G services, as well as the technical and strategic measures needed to mitigate them.

Nokia takes security seriously and we want to ensure that our customers build and operate secure 5G networks.

Nokia has already played an important role in securing critical networks for more than 15 years and our technologies and expertise can help protect 5G networks and services in the future. More than 500 security projects worldwide already rely on Nokia and we regularly leverage our work in security standards forums to design solutions that fully address the security requirements of complex networks.

NOKIA

Abbreviations

APT	Advanced Persistent Threat
ARS	Action Request System
C&C	Command and Control
CLI	Command Line Interface
CNF	Cloud-native Network Function
CSP	Communications Service Provider
DDoS	Distributed Denial of Service
ENISA	European Commission and the EU Agency for cybersecurity
EU	European Union
FW	Firmware
IMS	IP Multimedia Subsystem
IoT	Internet of Things
NACM	NetGuard Audit Compliance Manager
NES	NetGuard Endpoint Security
NIAM	NetGuard Identity Access Manager
NSMC	NetGuard Security Management Center
OTP	One Time Password
SDN	Software Defined Networking
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
SSH	Secure Shell
VNF	Virtual Network Function

Additional resources

Security challenges and opportunities for 5G mobile networks

5G security – a new approach to build digital trust

End-to-End Security Architecture for 5G 3GPP Radio Transport

5G Radio Insider Threat Security Controls

5G Continuous Audit

Strong Access Management for 5G compliance

References

1. EU Coordinated Risk Assessment on Cybersecurity in 5G Networks' https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

About Nokia

We create the technology to connect the world. Only Nokia offers a comprehensive portfolio of network equipment, software, services and licensing opportunities across the globe. With our commitment to innovation, driven by the award-winning Nokia Bell Labs, we are a leader in the development and deployment of 5G networks.

Our communications service provider customers support more than 6.4 billion subscriptions with our radio networks, and our enterprise customers have deployed over 1,300 industrial networks worldwide. Adhering to the highest ethical standards, we transform how people live, work and communicate. For our latest updates, please visit us online www.nokia.com and follow us on Twitter @nokia.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: SR2004043356EN (July) CID207438