Protecting the core: Securing subscriber data in modern telecom networks

White paper

Subscriber data is an element of trust between communication service providers (CSPs) and their users. As threats become more sophisticated and harder to detect, protecting this data requires more than traditional security measures. At Nokia, security is embedded from the ground up. Through a 'Design for Security' approach, layered defenses, and proactive monitoring, Nokia delivers comprehensive protection for modern telecom networks.

Silent intrusions in telecom networks

Some of the most damaging recent telecom breaches have gone undetected for months or even years. In a recent case, attackers gained access through poorly secured remote engineering portals, reaching lawful intercept systems and subscriber metadata pipelines. They used implants like BPFDOOR, a passive Linux backdoor known for evading firewalls and logging, to maintain persistent, low-profile access deep inside the network.

These deliberate, multi-layered breaches are crafted to blend into core telecom processes. With adversaries increasingly automating parts of their campaigns, this represents a massive challenge especially for security teams relying on static indicators, log-based hunting, or general-purpose detection tools that don't understand telecom's specific behaviours.

Strategic role of subscriber data management in modern networks

Subscriber data management (SDM) solutions are essential to the operation of modern mobile networks. They manage the full spectrum of subscriber data from personal details and billing information to network credentials, preferences, and access entitlements. For users, a breach of this data can lead to anything from inconvenience to real-world disruption.

For CSPs, the stakes are consistently high. A compromise in SDM not only risks serious regulatory consequences but also erodes subscriber trust, a far more difficult and expensive loss to recover from. Even when no direct misuse is detected, reputational damage alone can have a lasting impact.

SDM systems have also evolved far beyond static databases. They now play an active role in real-time policy decisions, authentication, and service delivery. In this way, SDM has become a strategic part of the network's control fabric, and with that comes a heightened security responsibility.

Adversaries recognize the value. Access to SDM can provide insight into user behavior, enable subtle manipulation of access policies, or offer persistence within the network's identity layer. Protecting SDM is therefore not just about data protection, but also about safeguarding how the network functions at its core.

To stay ahead, CSPs need more than traditional security controls. They need telecom-aware detection strategies, behavioral baselines, and an understanding of how SDM is being used in context, because increasingly, it's not just what attackers target, but where they aim to blend in.

How Nokia SDM ensures a robust subscriber data protection

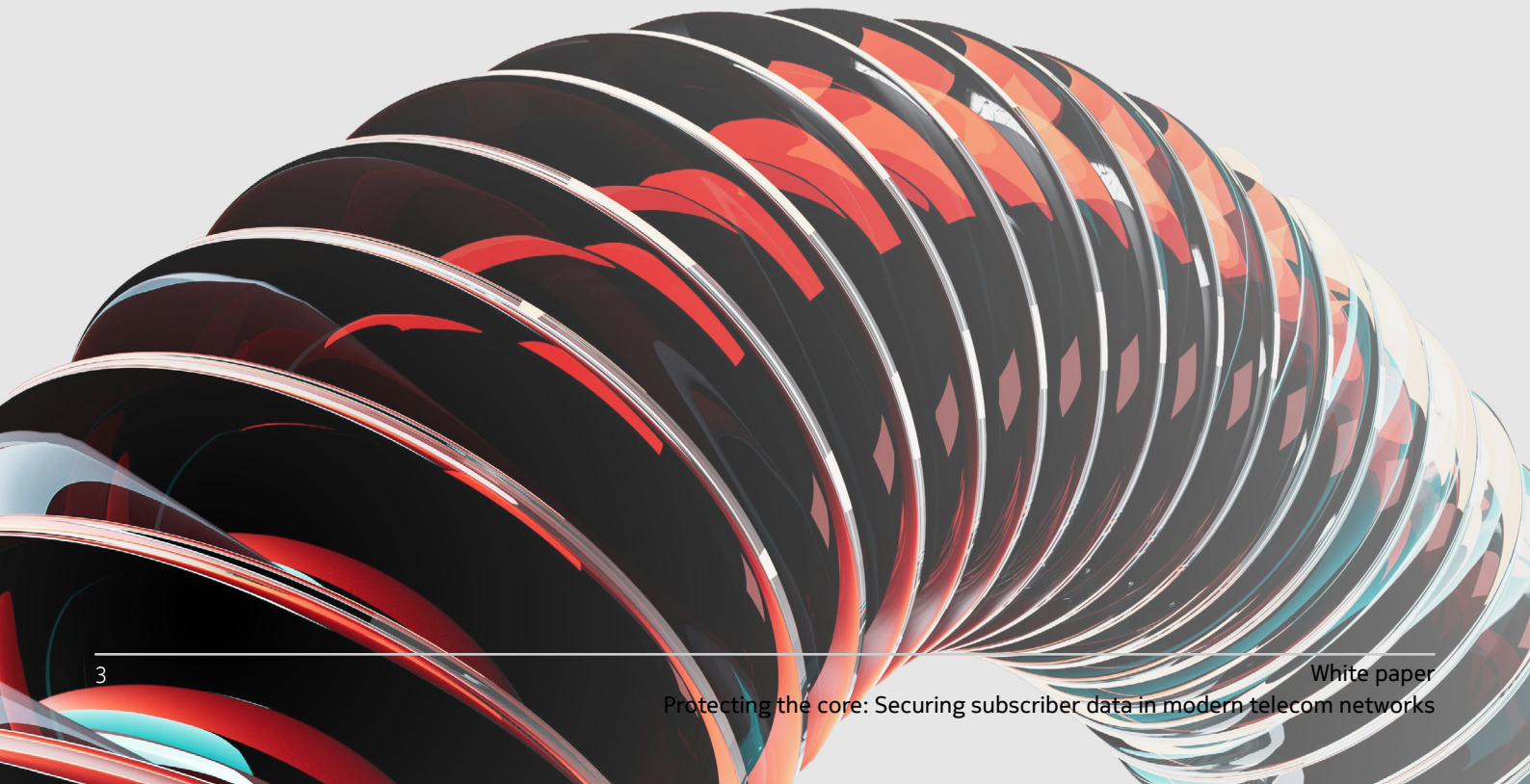
Nokia Subscriber Data Management solution (SDM) takes a pro-active approach to security, going beyond the basics. Nokia SDM protects itself and the key network assets critical to 5G network security with tamper-proof, robust systems built to Zero-Trust principles.

The security design of Nokia SDM directly reflects the principles of the 'Design for Security' (DFSEC) approach. DFSEC integrates security throughout the product development process, resulting in a more robust and resilient product architecture and inbuilt security measures. This strategy enhances our ability to pro-actively address modern threats and mitigate liabilities.

Nokia SDM offers also other safety features such as georedundancy by deploying SDM across multiple geographically dispersed data centers. The distributed architecture ensures business continuity, even in the event of regional outages or disasters. The cloud-native design further contributes to scalability and flexibility, allowing for rapid adaptation to changing demands and seamless failover between sites.

At the heart of these multi-layer security measures lie the SDM encryption practices. All sensitive subscriber data is encrypted both when stored in the SDM database (at rest) and when transmitted between different components of the system (in transit). The encryption algorithms used are industry-standard and regularly updated to address evolving threats.

The use of High Security Modules (HSMs) provides an additional layer of physical security to critical secrets and operations within the Nokia SDM. HSMs are specialised hardware devices designed to protect cryptographic keys and perform secure cryptographic operations. As the HSM is physically isolated and secured, it is a crucial component in safeguarding sensitive data. Within Nokia SDM, HSMs play a vital role in several scenarios, ensuring that the secrets are never handled unencrypted outside the HSM.

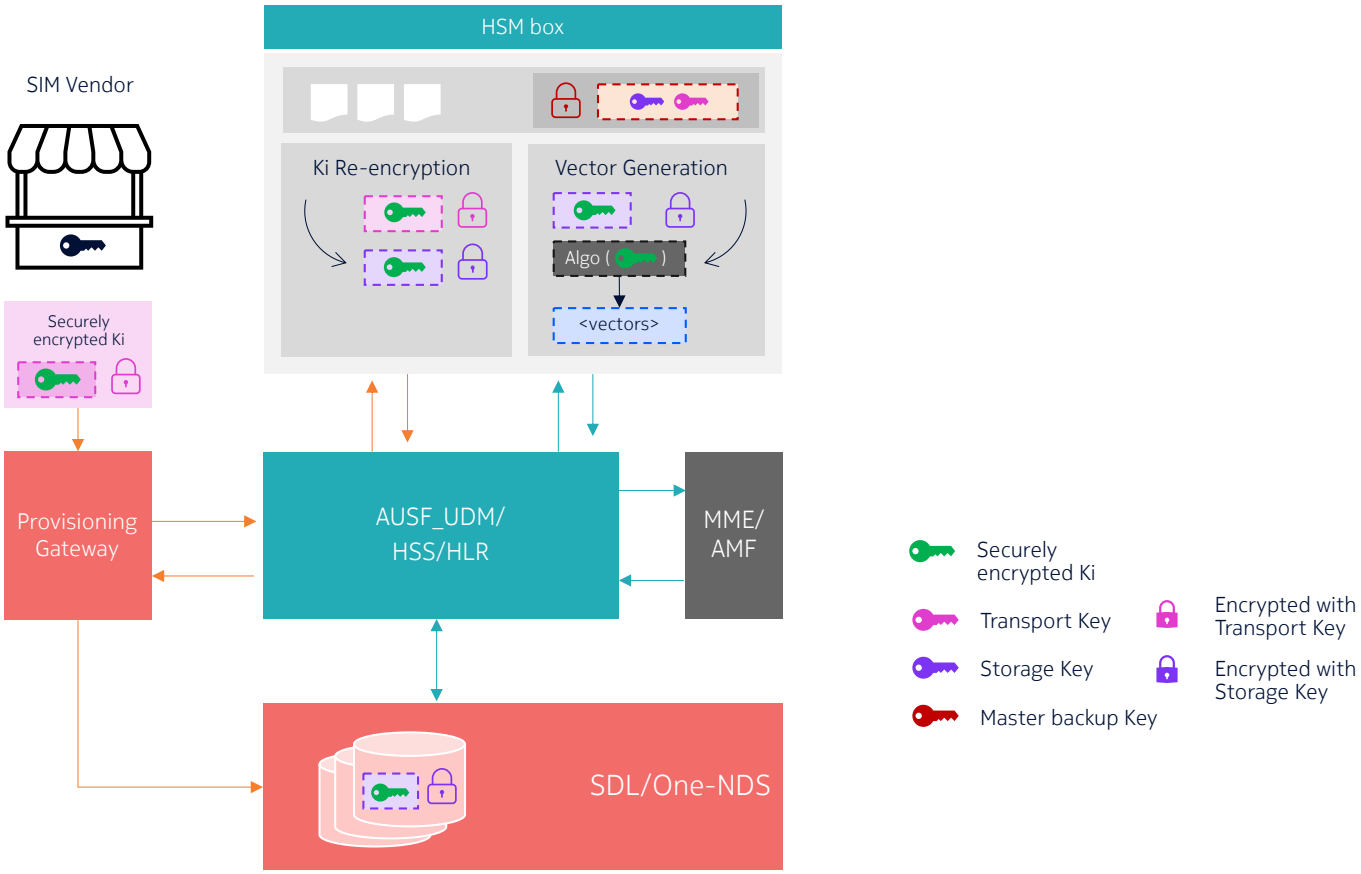


Encrypting security keys in Nokia SDM

Your phone (UE) and the network's SDM system share a secret code (*Ki*). This code is used to create security tokens (authentication vectors) that prove your phone's identity when making calls or connecting to the network. Nokia SDM protects the *Ki* with the highest level of security, using a physical hardware security module (HSM) for exclusive handling and encrypted storage within the UDM/SDL.

To ensure the security of the critical *Ki*, a multi-phased encryption method is employed. While the initial encryption provides a strong foundation, to rely solely on the SIM vendor's transport key would introduce a single point of vulnerability. Therefore, the Nokia SDM implements additional layers of protection of the *Ki*.

The *Ki* is irst encrypted with a transportation key by the SIM vendor. The de-encrypted *Ki* is then re-encrypted with a separate storage key, managed by the Nokia SDM within a secure HSM, providing a second layer of protection.



This multi-phased approach ensures the isolation of *Ki* from other system components, preventing unauthorized access.

Telco-grade protection for critical network functions

Networks face an increasing volume of stealthy, complex attacks that easily bypass traditional perimeter and signature-based defenses. Threats like GTPDOOR and BPFDOOR exemplify a new class of malware engineered to exploit telecom-specific pathways and maintain covert, persistent access. These threats don't generate obvious indicators; they operate quietly, often below the visibility of IT-centric security tools.

Protecting the "crown jewels" of the telecom core, such as the SDM, HLR/HSS, GGSN/UPF, and signaling elements, requires more than generic endpoint security. Operators need a detection and response strategy designed specifically for telecom: one that can monitor dynamic workloads across VNFs, CNFs, and bare-metal nodes, while remaining invisible to the real-time operations those functions deliver.

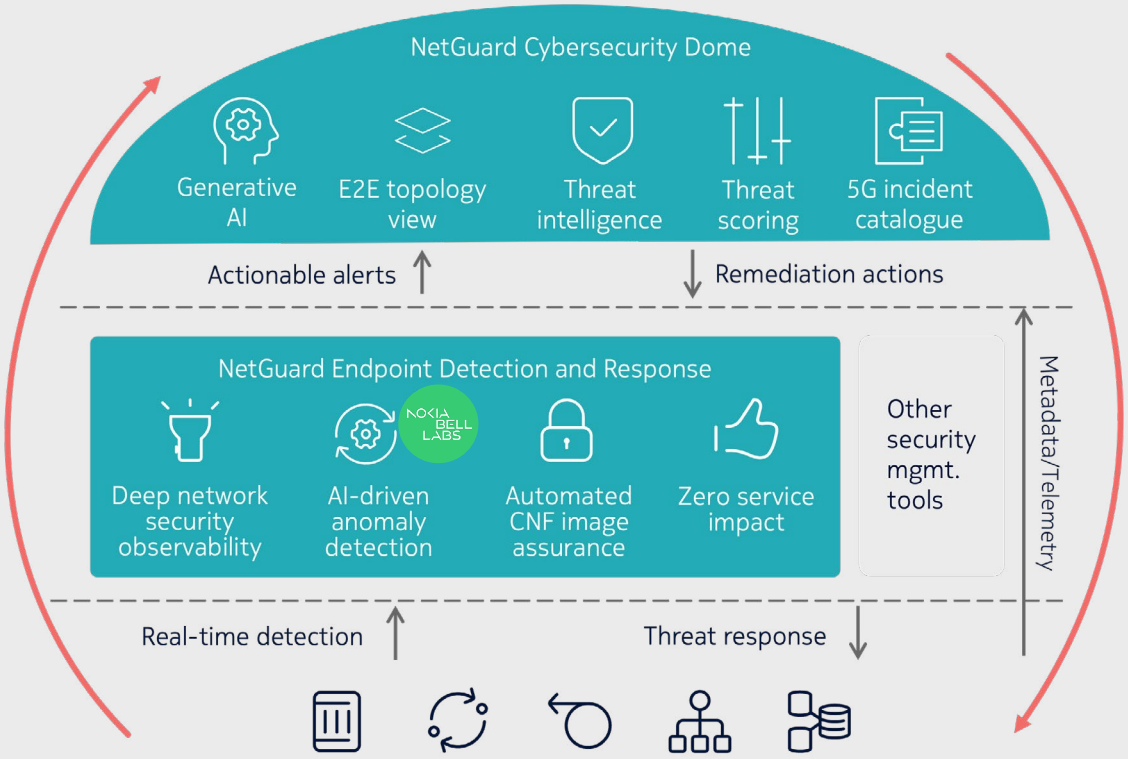
NetGuard Endpoint Detection and Response (EDR) is built for exactly this. It combines host-level visibility and network traffic intelligence to provide continuous, real-time detection of both known and novel threats. Here's how it works:

- Lightweight EDR agents and sensors: Deployed on virtualized hosts and CNFs, EDR agents capture anomalies in process behavior, system activity, and file integrity in real time without degrading quality of service. Network sensors monitor network traffic, detecting lateral movement, C2 activity, and possible multi-stage attacks even on legacy or third-party systems where agents can't be installed.
- AI-based anomaly detection: Identifies zero-days in real time using a novel clustering method with only a few packets per cluster and achieving <1% false positives and >98% detection accuracy. Developed and patented by Nokia Bell Labs.
- Central analysis engine: Collected data is streamed to a centralized server where it is validated, correlated, and analyzed using MITRE ATT&CK techniques.
- Automated CNF image assurance: Validates container images pre-deployment to block tampered or vulnerable workloads, reducing supply chain and runtime risk.

Security assurance across domains

To stop stealthy, multi-stage attacks before they reach critical assets, telecom operators need security observability and an orchestration framework that connects insights across core, transport, RAN, and cloud to ensure fast and accurate response.

NetGuard Cybersecurity Dome provides this comprehensive security assurance. It unifies detection and response through a centralized Extended Detection and Response (XDR) platform, correlating data across domains, security controls and users to uncover hidden threats and automate response. With AI-driven threat scoring, predictive analytics, and telecom-specific playbooks, it allows SOC teams to act decisively — before attackers gain persistence or cause disruption.



Enforcing Zero Trust and hardening privilege

Recent telecom breaches also reinforce the need for a hardened Zero Trust model, where access is never assumed and always verified. The Nokia Privileged Access Manager ensures that only the right people and systems can reach sensitive assets by enforcing least privilege across IT and OT environments.

Nokia Certificate Lifecycle Manager supports telco-scale environments, automating the management of 100M+ PKI certificates from enrollment to audit, ensuring encrypted communications and strong identity assurance across all layers.

Strategic risk management and consulting

Most breaches stem from unaddressed risks, rather than tool failures. Effective security starts with a clear view of your risk posture. Nokia's security consulting services help telecom operators:

- Identify telecom-specific risks across network layers
- Prioritize controls based on actual threat exposure
- Align security investments with 4G/5G transformation goals
- Meet evolving global and regional compliance requirements

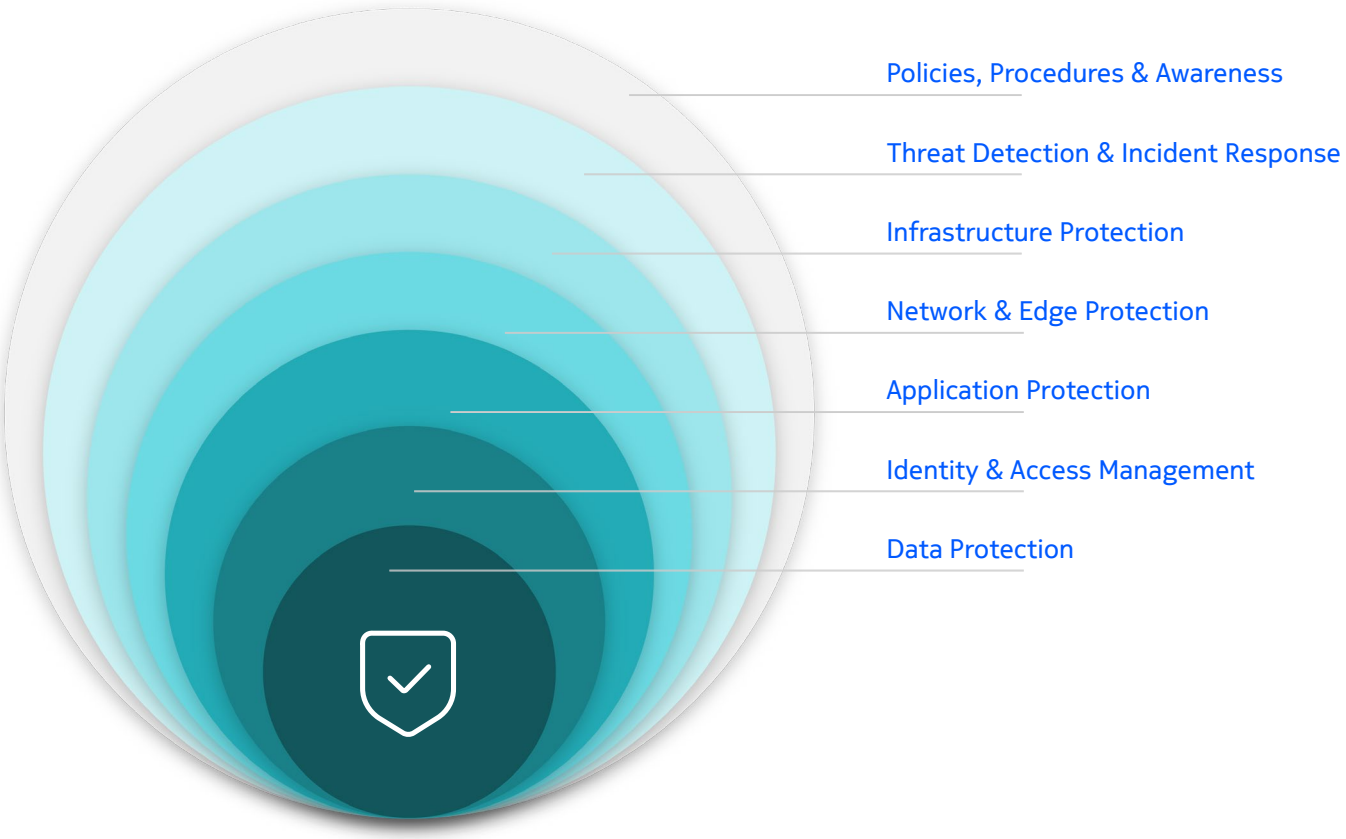
Telco-native strategy to combat new, sophisticated threats

Telecom networks are very different from traditional IT environments: more complex, bound by stricter rules, and at the core of how people and businesses stay connected. Protecting them requires more than generic cybersecurity solutions. It demands deep, domain-specific expertise, tools built for telecom protocols and architectures, and a security strategy that aligns with the unique performance, availability, and regulatory requirements of CSPs.

At Nokia, our approach is built around those exact needs: a telco-native, multi-layered defense architecture — from secure subscriber data management and zero trust access controls to telecom-specific threat intelligence and AI-driven detection and response. Recent breaches have shown how attackers can move undetected for months, reaching into subscriber systems, metadata pipelines, and even lawful intercept functions.

With trust on the line, telecom security demands the precision, multi-layer visibility and defense mechanisms needed to counter increasingly sophisticated telecom threats, and only specialized solutions can deliver it.

Defense-in-depth



About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

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

Document code: SRxxxxxxEN (Month)

CID 214941