ERICSSON



Rethink security in the age of rApps

Security in SMO platforms

ericsson.com/RANahead

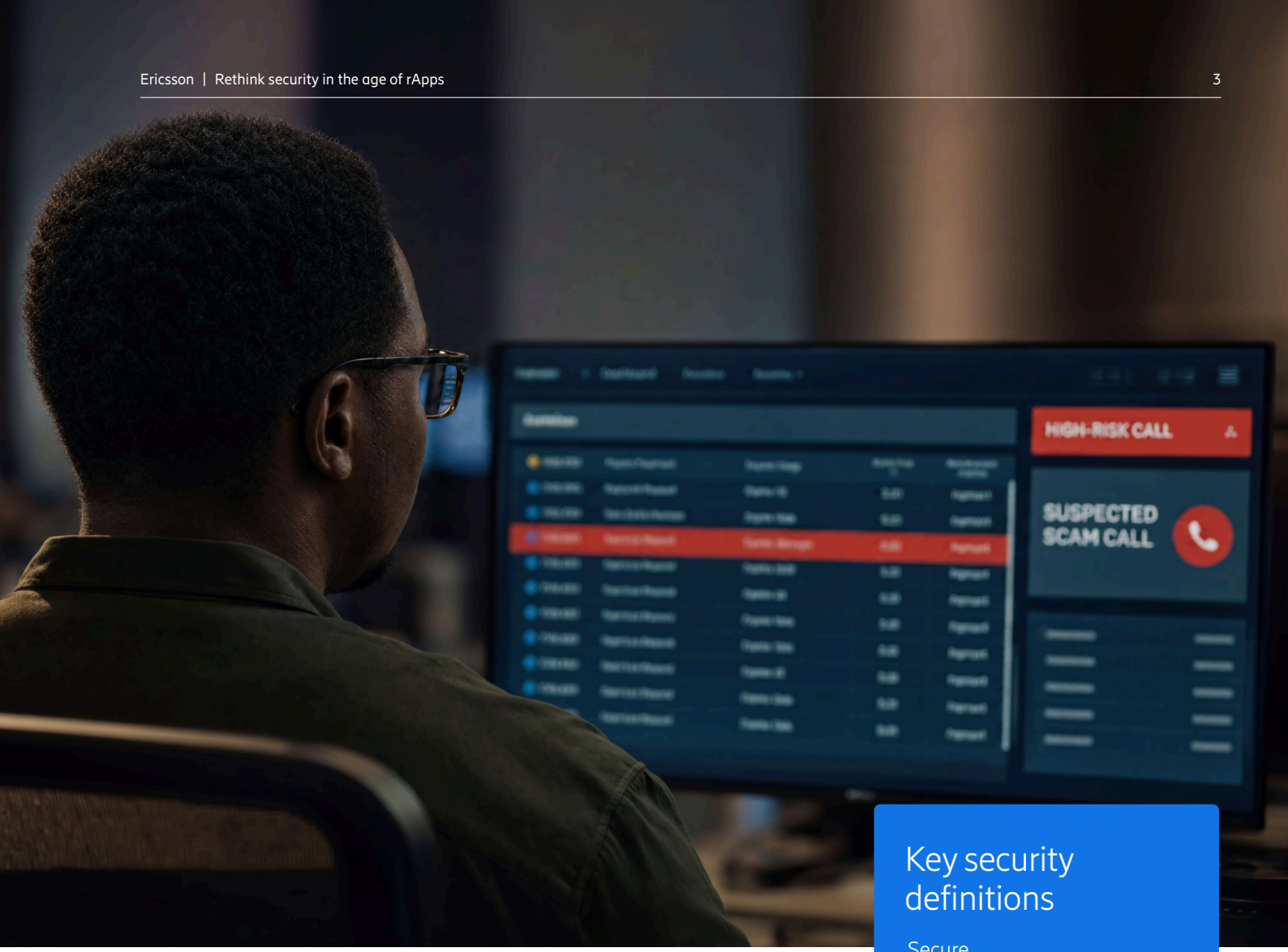
Introduction

Responding to new threats

The evolving threat landscape places even greater importance on securing the platforms that sit at the center of network automation and operations.

As networks evolve toward open and cloud-based networks incorporating AI-driven automation, the role of the Service Management and Orchestration (SMO) platform is crucial. Serving as the control point for configuration, optimization, and assurance for the RAN and Core, the SMO is a vital asset that must be secure.

At the same time, multi-vendor integration, cloud technologies, third-party software supply chains, AI, and an increased number of open interfaces are expanding the attack surface. Traditional security approaches are no longer sufficient. To overcome tomorrow's challenges, operators must adopt a secure-by-design security model that ensures strong data security, identity, controlled access, logging, and traceability across all interactions, with the goal of a Zero Trust Architecture (ZTA) to protect against external and internal threats.



Attacking and defending with AI
The rapid adoption of generative and agentic AI is reshaping the cybersecurity landscape. Industry observations show a growing number of vulnerabilities and exposures being discovered and published on public vulnerability databases such as the NIST:NVD and EU VD. As software ecosystems become larger and more dynamic, the effort required to remediate vulnerabilities and detect exploitation continues to increase significantly. Agentic AI in telecom networks introduces threats that must be mitigated, including agents with elevated privileges, unsecure communications between agents, untrusted third-party tools, weak APIs, and compromised AI supply chains.

To keep pace with this evolution, vendors and operators are expected to leverage AI and automation in their security operations to enable automatic detection and response when security events occur.

Security from the ground up
This evolving threat landscape places even greater importance on securing platforms that sit at the center of network automation and operations. As the control point for management, orchestration, and AI-driven decision-making, the SMO becomes a critical component in maintaining the security, cyber-resilience, and trustworthiness of modern networks.

This guide highlights why securing the SMO is foundational to building trusted and resilient networks able to operate through cyberattacks. It outlines key security practices, the role of zero trust, and the need to prepare for future challenges such as AI-driven threats and evolving cryptographic standards. We are addressing these challenges through a secure-by-design approach to the Ericsson Intelligent Automation Platform (EIAP). By designing with a zero trust architecture (ZTA) mindset, embedding security across the platform lifecycle, and enabling a controlled application ecosystem, we're creating a world where innovations can be made with confidence, without compromising security.

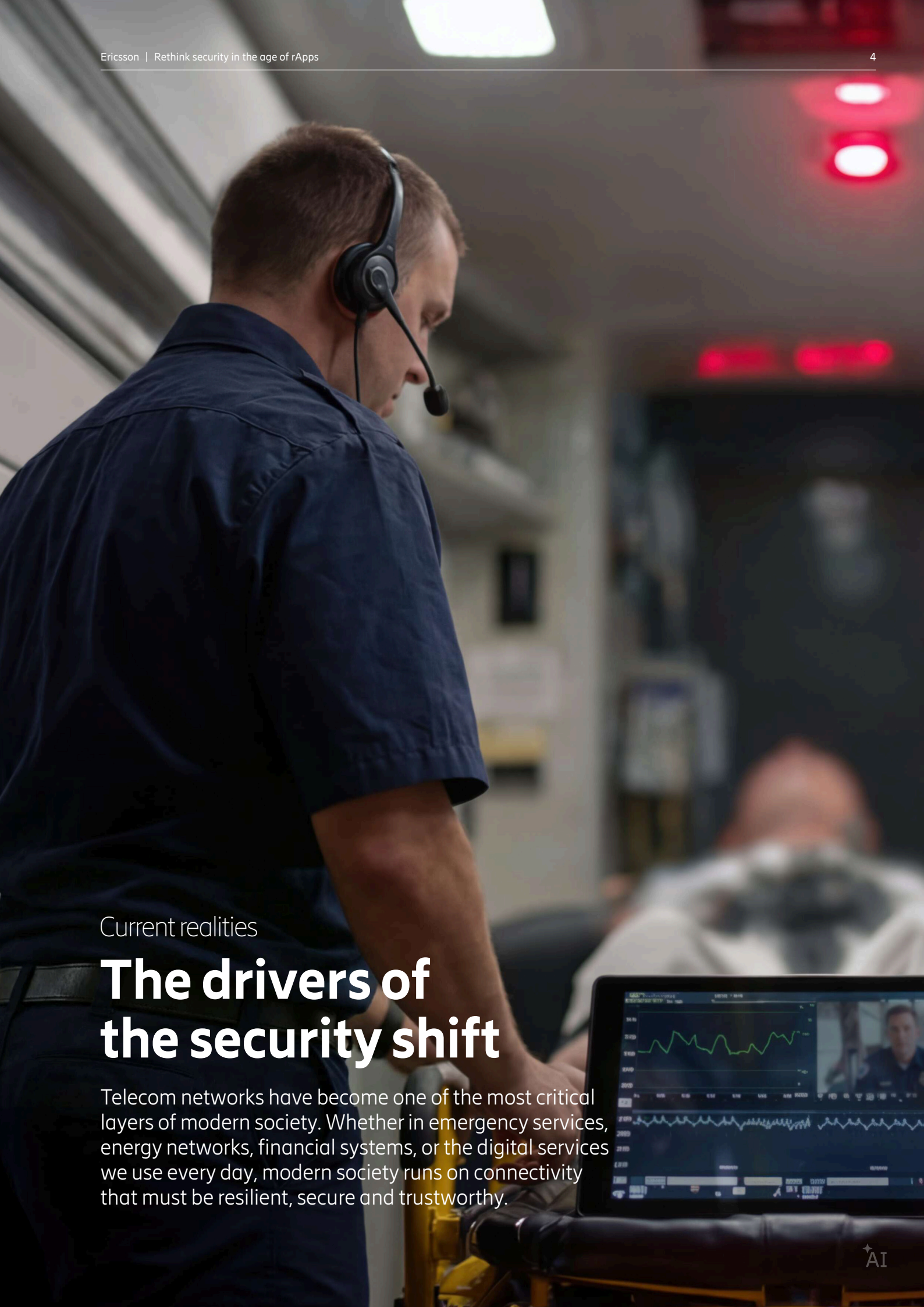
Key security definitions

Secure
Concrete security controls and practices (confidentiality, integrity, availability, authentication, authorization, hardening, vulnerability remediation, and security monitoring) to mitigate risks of intrusions and attacks.

Resilient
Ability to withstand and recover required capabilities and service levels when disruption or attacks occur.

Trustworthy
Composite property of a system, attained from security, resilience, identity management, privacy, and assurance, providing justified confidence in the system's behavior.

Trusted
The status granted by a regulator to a supplier that possesses autonomy to fulfil contractual obligations towards the procurer and obligations towards domestic regulation. This includes, but is not limited to, properties of trustworthiness.



Current realities

The drivers of the security shift

Telecom networks have become one of the most critical layers of modern society. Whether in emergency services, energy networks, financial systems, or the digital services we use every day, modern society runs on connectivity that must be resilient, secure and trustworthy.

This shift has elevated telecom networks to critical pieces of national infrastructure, making them highly attractive targets for nation-state actors and organized cyber-criminals.

Facing new threats
At the same time, the nature of the network itself is changing. Cloud-native designs and open interfaces have made networks more flexible and faster to evolve, but also increased their exposure to potential threats. Functions that were tightly controlled within proprietary hardware appliances are now distributed across virtual and cloud platforms, exposed through APIs, and integrated across multi-vendor environments.

Compounding this is the rise of advanced persistent threats (APTs). These attackers are no longer focused solely on disrupting services—they aim to infiltrate, persist, and move laterally across systems over extended periods. Platforms that provide centralized visibility and control over networks, such as the SMO, become particularly high-value targets in such scenarios.

Adapting to AI
The introduction of AI-driven automation also creates opportunities and risks. Automation platforms can optimize resources and detect anomalies, but they also introduce new dependencies on data, models, and external components.

Security can no longer be treated as a static control layer—it must evolve alongside increasingly autonomous systems.

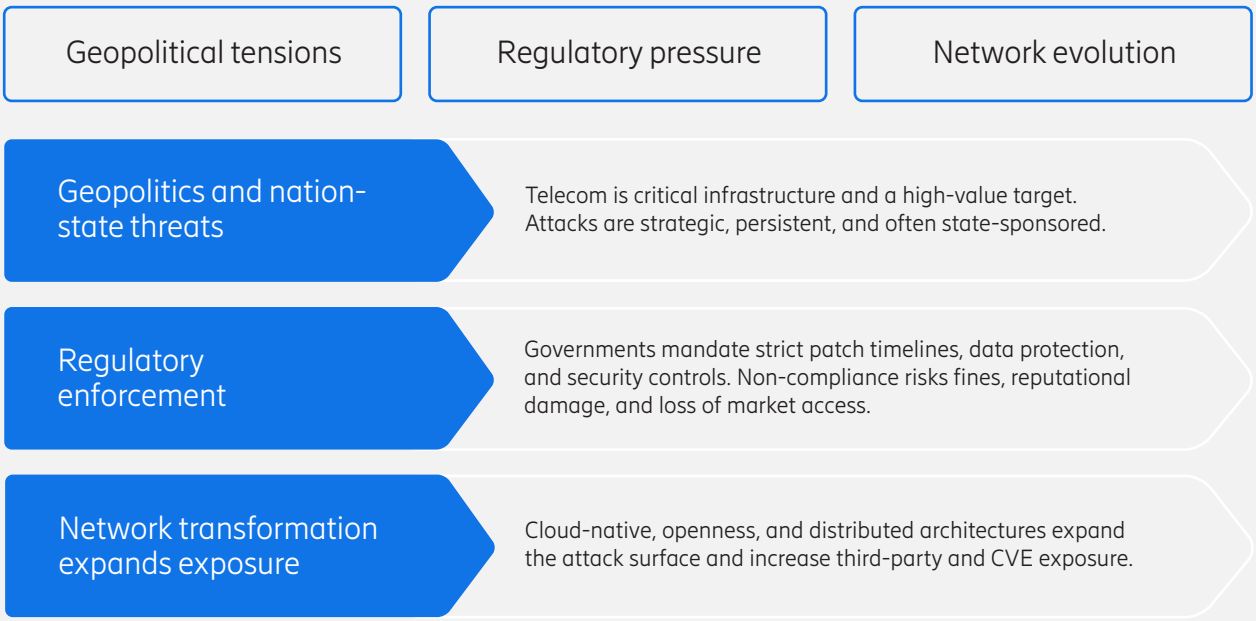
New regulatory pressures
Additionally, regulation is accelerating the urgency. Frameworks such as the EU NIS2 Directive and Cyber Resilience Act, together with guidance from NIST, DHS CISA, and other national telecom authorities, are raising the bar for security, vulnerability management, and data sovereignty.

Operators are now expected not only to protect their networks, but to demonstrate compliance, transparency, and continuous risk management across the entire lifecycle. As a result, security has moved firmly into the boardroom. Operators are increasing investments, redefining risk and vulnerability management strategies, and placing greater emphasis on securing not just individual network functions but also platforms that manage and automate them.

In this changing environment, securing telecom infrastructure is crucial to maintaining trust, cyber-resilience, and operational integrity.

Figure 1.

Security is now a business and regulatory imperative



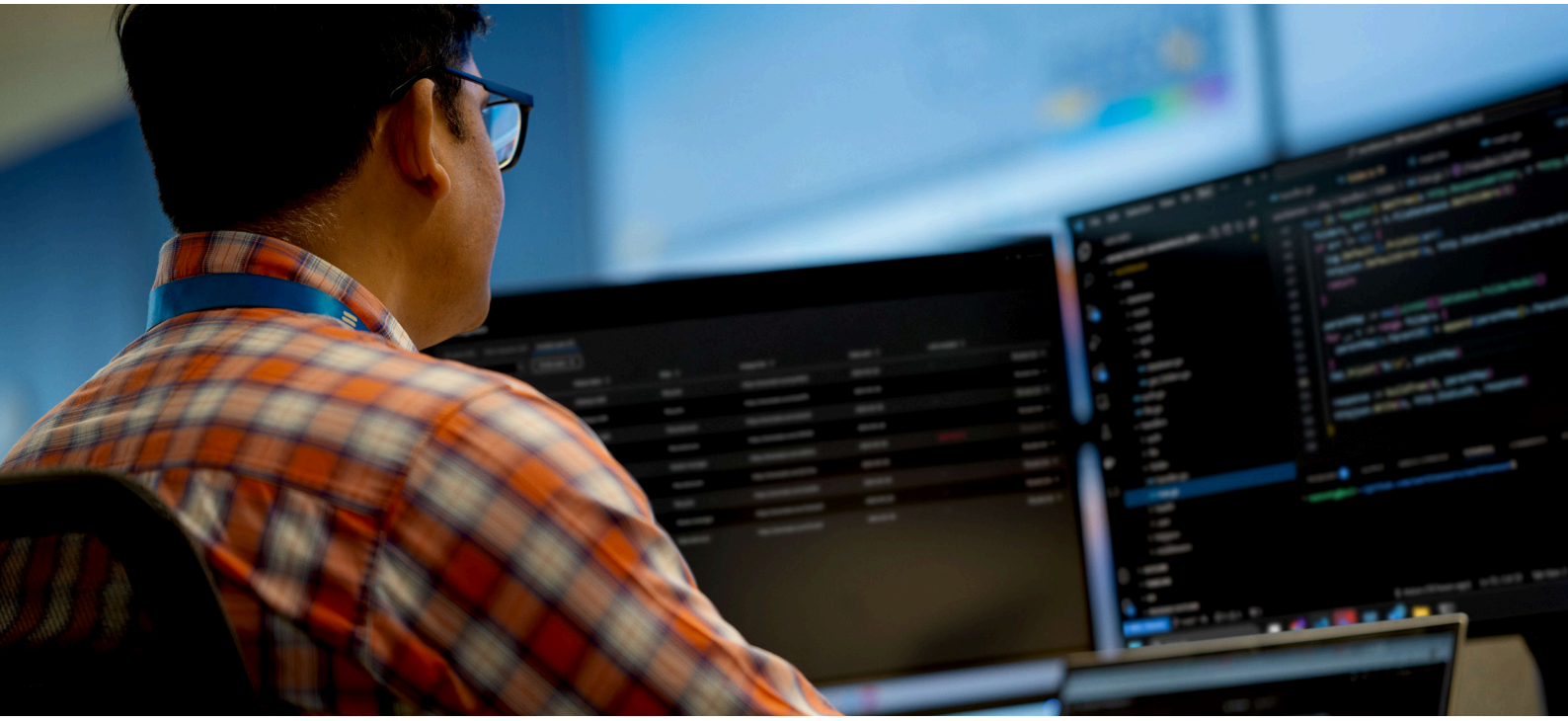
Particular attention must be given to solutions that provide management, automation, and control across the telco network.

With the accelerating adoption of open/cloud RAN, cloud-native technologies, and AI-driven operations, the SMO's role in enforcing security and enabling trusted automation across multi-vendor environments becomes increasingly important.

Adapting to openness

Why SMO security is key in open RAN

The SMO serves as the centralized platform for managing physical, cloud, and open RANs, providing control over configuration, automation, optimization, and assurance.



As networks become more software-driven and distributed, the SMO effectively acts as the brain of the RAN, and soon core, making decisions that directly impact network behavior at scale. This is what makes the SMO such an attractive target.

An adversary who gains control of the SMO would have visibility across the network and the authority to act on it. Through standardized interfaces such as O1, O2, and R1, the SMO interacts with network functions, cloud infrastructure, and rApps. These interfaces are essential for openness and innovation, but they also introduce data exposure if not properly secured.

Improperly configured authentication and authorization across these interfaces creates potential pathways for lateral movement, allowing an attacker who gains access through one component to move across the system via the SMO.

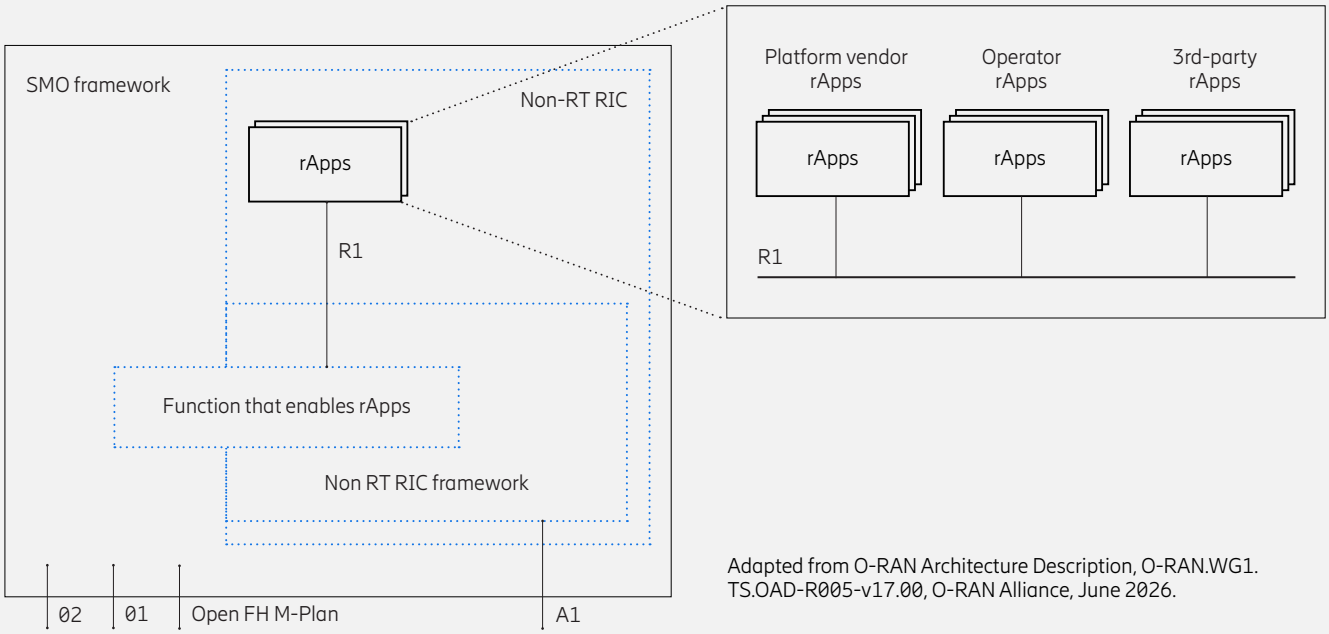
Open networks bring new challenges

In a multi-vendor open RAN environment, the challenge becomes even more complex. The SMO is responsible for integrating and coordinating software components from multiple suppliers, each with its own lifecycle, security posture, and deployment model. This introduces supply chain risks that must be managed with secure onboarding and run-time security.

The growing ecosystem of third-party (3PP) rApps further raises the stakes. For example, Ericsson's rApp ecosystem alone is made up of over 100 rApps from just as many developers and companies. These numbers multiply when considering similar ecosystems being nurtured by other SMO vendors.

rApps have powerful automation and optimization capabilities, but they also require controlled access to SMO data and conflict management features, and some level of security certification to establish trust. Without strong governance, identity management, audit logging, and isolation, this openness could introduce unintended risks. Establishing trust between the SMO platform and 3PP rApps is therefore essential.

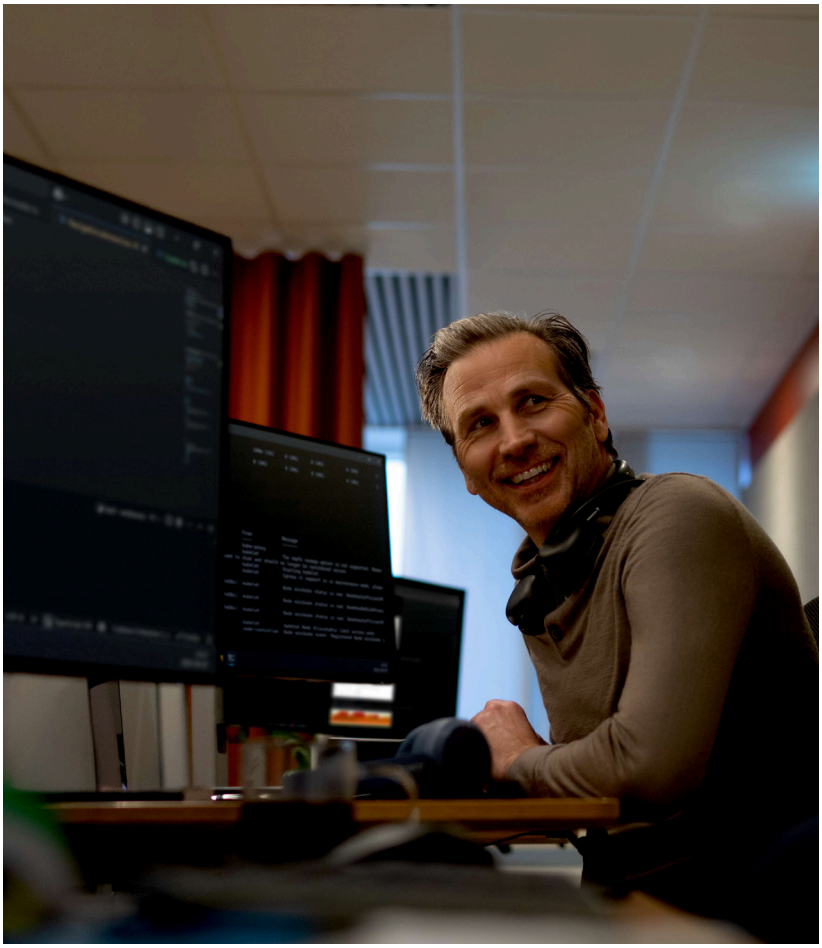
Figure 2.
SMO architecture



Adapted from O-RAN Architecture Description, O-RAN.WG1. TS.OAD-R005-v17.00, O-RAN Alliance, June 2026.

A foundational requirement
Ultimately, the SMO is no longer just a management system. It is a strategic control point for the entire RAN domain. Securing it means protecting not only individual interfaces or components, but the integrity of the platform as a whole.

As operators embrace openness and automation, SMO security becomes a foundational requirement to ensure that innovation does not come at the expense of control and security.

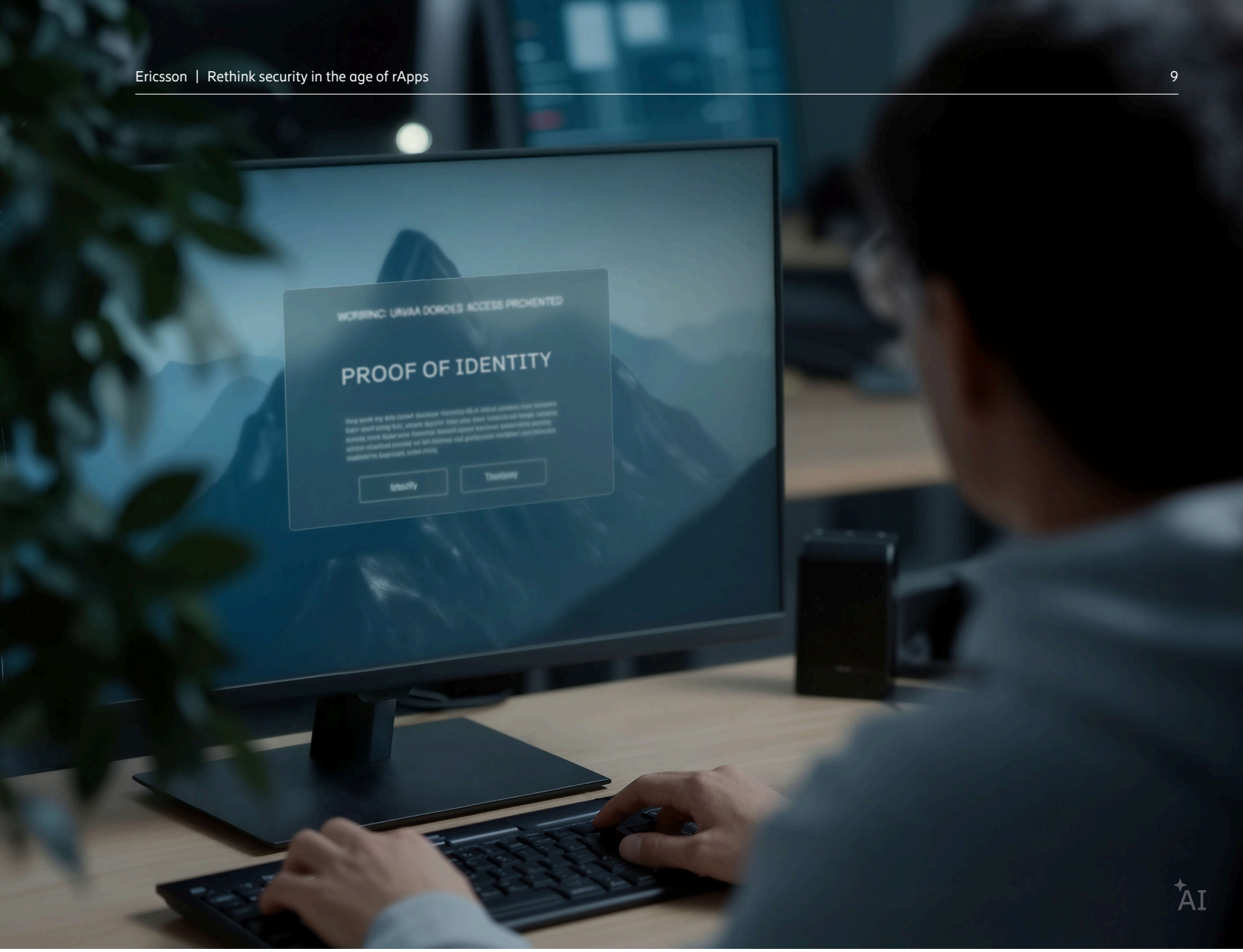




Taking new measures

Best practices for SMO security

Securing the SMO requires a comprehensive approach that spans identity and access management, data confidentiality, logging, supply chain integrity, and software signing. As the central platform for automation and control, it must be protected not just at the perimeter, but across its entire lifecycle.



Industry guidelines and security specifications from the O-RAN Alliance Working Group 11 (WG11) provide a strong foundation and interoperable security controls across multi-vendor RAN deployments, including SMO and rApps.

Tight access management
A key starting point is enforcing least privilege access. Every user, system, and application interacting with the SMO should have only the permissions strictly required for its role. Combined with role-based access control (RBAC) and target-based access control (TBAC), this helps reduce the risk of misuse.

Strong identity and access management (IdAM) is equally critical. This includes support for modern authentication standards like OpenID Connect over OAuth 2.0 and multi-factor authentication. Because the SMO integrates with multiple domains and 3PP applications, establishing clear, verifiable identities is essential to maintaining trust across the ecosystem.

Robust authentication and encryption
All communication with the SMO must be protected through robust authentication and encryption mechanisms. Certificate-based authentication and protocols such as TLS and mutual TLS (mTLS) ensure that both ends of a connection can be trusted and that data-in-transit remains confidental and integrity protected. This is critical for O1, O2, A1, and R1 interfaces between O-RAN architecture elements, applications, and SMO services, and is especially important for external interfaces outside the O-RAN domain on systems that consume or produce data.

Software and supply chain integrity
Another critical area is software integrity and supply chain security. With frequent updates, CI/CD pipelines, and 3PP components, all software artifacts must be trusted and verifiable. Practices such as maintaining a software bill of materials (SBOM), using signed images, and securing the development pipeline help prevent the introduction of compromised or vulnerable components.

Continuous logging
Finally, continuous logging contributes to observability that is key for detecting and responding to threats. The SMO should provide full visibility into user activity, system behavior, and interface interactions. Combined with external security incident event management (SIEM) systems for log analytics and automated alerting, this enables identification of suspicious patterns early and response before they escalate.

Tightening network security

Zero trust for SMO

Zero trust architecture (ZTA) translates the principles of zero trust into an implementable framework for telecom networks.

As the SMO evolves into a cloud-native, service-based platform, ZTA protects against internal presence and lateral movement by enforcing security controls within the network, complementing the traditional perimeter-based approach.

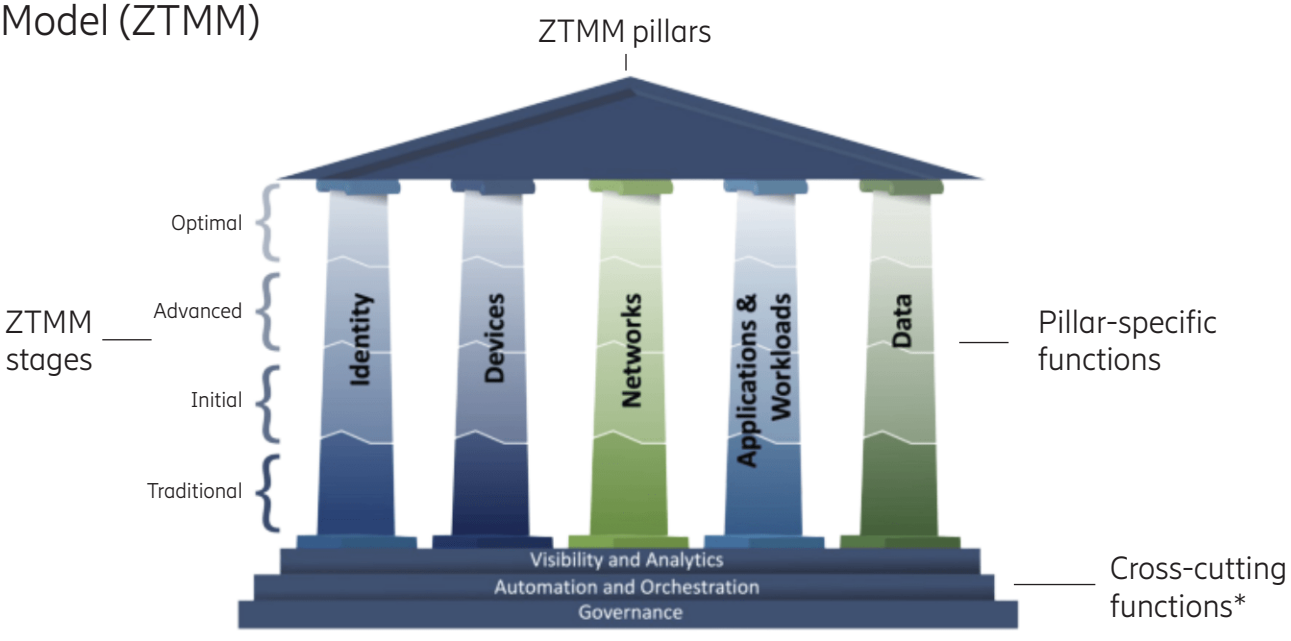
Securing critical infrastructures
Internal security controls are implemented under the assumption that the adversary is already inside the network, as demonstrated by recent nation-state advanced persistent threats (APTs) that successfully performed lateral movement once inside. Adversaries use APTs for reconnaissance, data exfiltration, or compromising system behavior.

The maturity model

The implementation of a ZTA is supported by the US DHA CISA Zero Trust Maturity Model (ZTMM), which outlines four basic implementation stages to move from traditional perimeter-based security to optimal AI-driven security that is automated and dynamic:

- Each network function is a resource secured as a micro-perimeter.
- Confidentiality and integrity protection are provided for data in-transit on external and internal interfaces, data-at-rest, and data-in-use.
- Authentication and authorization are enforced on a per-session basis for external and internal subjects.
- Continuous monitoring, logging, and alerting is implemented to detect and respond to security events.

Figure 3.
CISA Zero Trust Maturity Model (ZTMM)



Source: Zero Trust Maturity Model Version 2.0, US DHS CISA, April 2023.

*Cross-cutting functions follow the 4 stages of ZTMM: Traditional->Initial->Advanced->Optimal



Across-the-board security
In practice, this means ZTA must be implemented in the cloud stack, across workloads, and across pods. Workloads should run with minimal privileges, for example, by enforcing containers to run as non-root and restricting unnecessary capabilities.

At the infrastructure level, microsegmentation helps isolate microservices and limit communication paths, reducing the risk of lateral movement within the SMO environment.

Security must also extend to how workloads are built and executed. Enforcing read-only root file systems, validating images, and securing the software supply chain all contribute to stronger runtime protection. At the same time, secure pod-to-pod communication, based on mutual TLS, ensures that internal traffic is protected.

Together, these measures turn zero trust into something tangible—creating a platform where every workload, every connection, and every action is explicitly controlled and continuously validated.

This internal and external approach to the system is key to maintaining a secure SMO in an open, automated and multi-vendor environment.

Meeting tomorrow's challenges

Future-proofing SMO security

As the SMO continues to evolve, security must keep pace with both technological change and an increasingly complex threat landscape.

Future-proofing the platform means going beyond a reactive approach to risk and instead building the right foundations to anticipate threats before they create major problems.

A new security paradigm
One area gaining attention is post-quantum cryptography. While large-scale quantum threats may still be some years away, decisions made today around cryptographic agility and key management will determine how easily SMO platforms can adapt in the future. Preparing early helps avoid costly redesigns later in the lifecycle.

At the same time, AI is starting to play a dual role in security. On one hand, it introduces new risks, such as automation platforms that rely more on data, models, and autonomous decision-making. On the other hand, it enables more advanced defense mechanisms. AI-driven analytics can help detect anomalies, identify unusual user behavior patterns, and enable faster, more informed responses to potential threats.

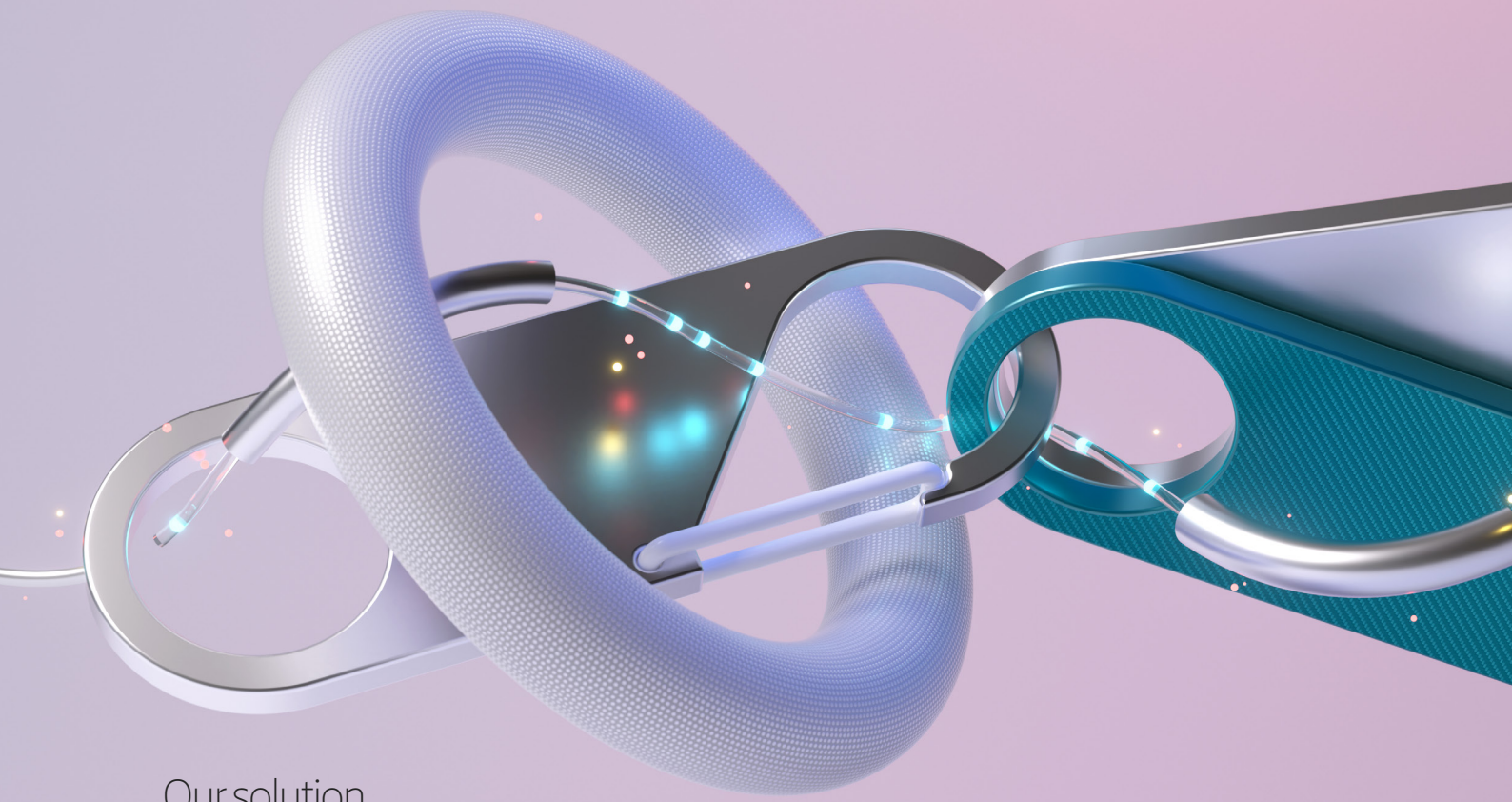
Another important dimension is the evolution of the SMO application ecosystem. As 3PP applications become more common, ensuring secure onboarding and lifecycles becomes critical. This includes clear policy enforcement, isolation, and security controls for rApp access to data and platform capabilities.

The impact of AI
The rapid adoption of frontier AI is introducing even more new security and governance challenges for SMO platforms and network operations. AI copilots, agents, and automation tools are rapidly being integrated into operational workflows and may gain access to highly sensitive systems, operational data, and automation capabilities.



As AI systems begin to operate with privileges comparable to trusted users, strong identity controls, policy enforcement, auditability, and data governance become increasingly important. Additionally, AI-assisted software development and vulnerability research are accelerating the discovery of security exposures, increasing pressure on operators and vendors to analyze, prioritize, and remediate vulnerabilities faster across complex cloud-native environments.

Build for adaptability
Looking ahead, the goal is to build an SMO platform that is not only secure today but adaptable to tomorrow's developments in cryptographic standards, autonomous operations, and expanding rApp ecosystems. By embedding flexibility, visibility, and control into the platform from the start, operators can move forward with confidence as both technology and threats continue to evolve.



Our solution

Embedding security in EIAP

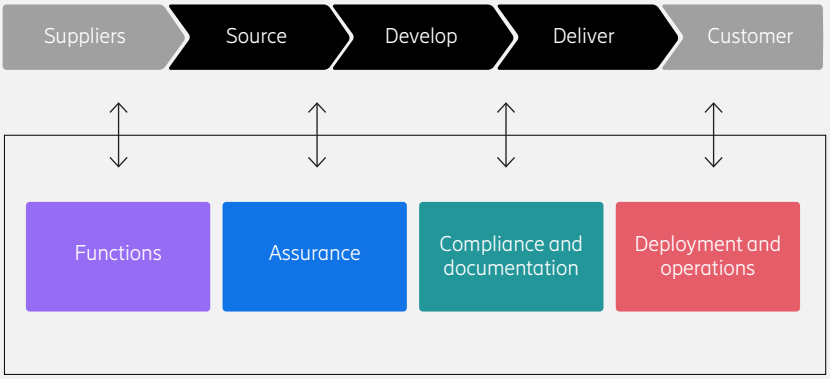
EIAP (Ericsson Intelligent Automation Platform) is designed with security as a foundational principle, recognizing the critical role that SMO plays as the control point for the RAN. EIAP embeds security across the platform lifecycle, from design and development to deployment and operations.

Security by design
Built in alignment with the Ericsson Security Reliability Model (SRM), O-RAN principles, and industry best practices, EIAP provides a secure-by-design platform that supports openness without compromising control.

Ericsson Security Reliability Model (SRM)

The SRM establishes a structured and risk-based approach to integrating security and privacy across the entire platform lifecycle, from development and sourcing to deployment and operations. Core security capabilities, such as identity and access management, confidentiality of data, audit logging, hardening, and secure supply chain practices, are integrated into the solution to help ensure that every interaction, internal and external, is authenticated, authorized, and traceable.

Figure 4.
Security Reliability Model (SRM)



EIAP also addresses the operational realities of telecom networks. With advanced security assurance and regular vulnerability reporting, operators gain visibility into their security posture and the ability to respond quickly to emerging risks. This is essential in environments where software updates, third-party components, and evolving threats are part of daily operations.

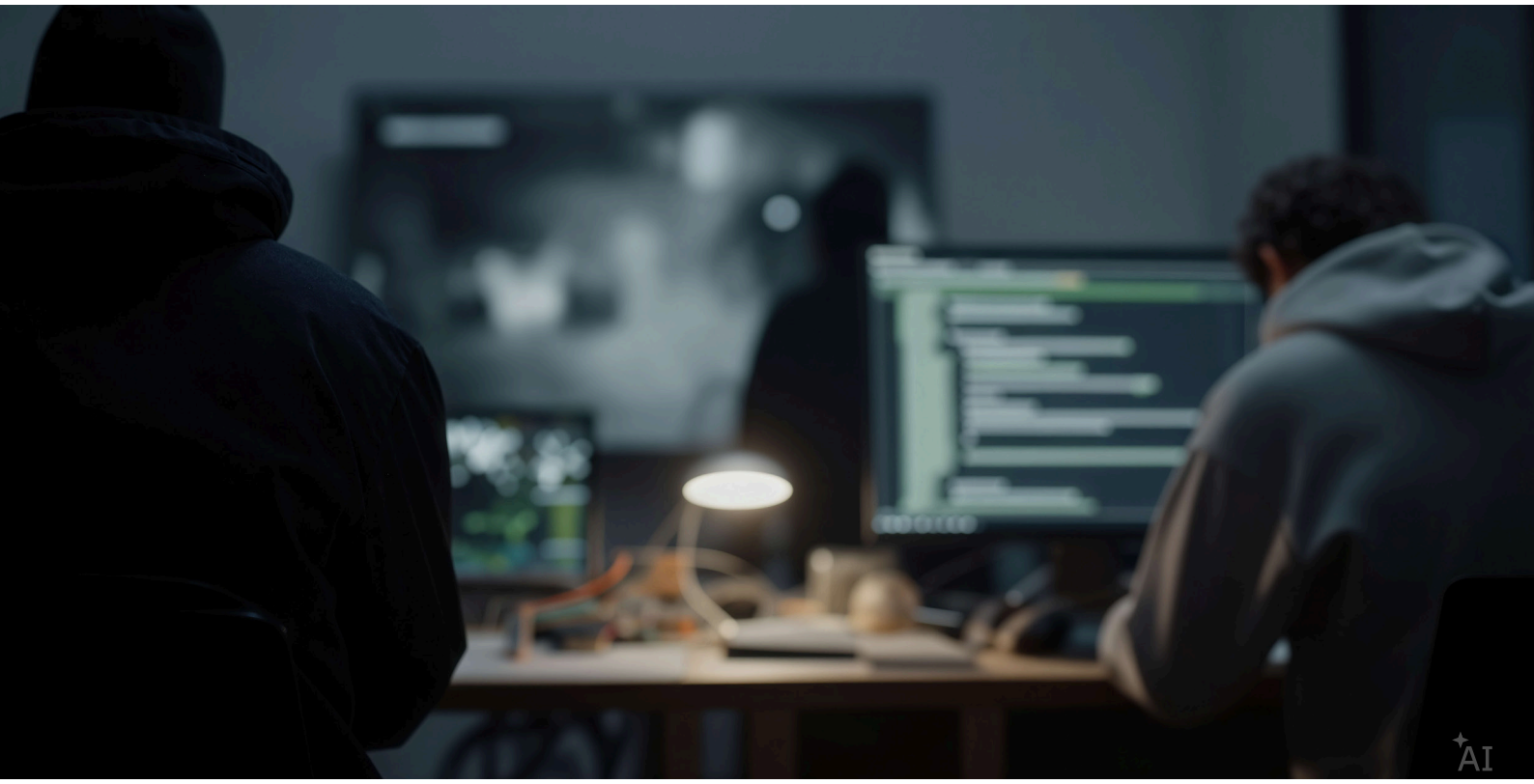
Ultimately, EIAP provides a trusted foundation for SMO, combining openness, automation, and security. It enables operators to innovate safely, with the knowledge that security is consistently enforced across users, workloads, interfaces, and applications.



Enabling secure innovation

Building a secure 3PP rApp ecosystem

Ericsson's rApp ecosystem ensures 3PP rApps are secure from the start. This is achieved through a combination of standards-based controls, a hardened SMO platform (EIAP), secure onboarding, and a formal certification service.



Certified security

The certification service is the formal gate for third-party rApps, extending beyond security compliance validation to include interoperability and integration testing with EIAP. It is designed to ensure all rApps are securely designed, use the R1 interface in compliance with O-RAN specifications, and are validated for EIAP readiness before deployment.

rApps that make the grade are marked in Ericsson's rApps directory with a certification badge, creating transparency and peace of mind.

For developers, the certification process provides a clear security goal, and for operators, it gives confidence that all certified rApps are secure, interoperable, and ready for production.

Alongside the certification service, EIAP includes a design and onboarding environment and runtime catalog to validate, onboard, configure, and monitor rApps before they can operate on production networks. Only rApps that conform to the open, standardized R1 interface and pass interoperability and security checks are accepted.

Through a structured, tool-driven process, Ericsson ensures that each rApp complies with Ericsson security, data privacy and platform interoperability requirements. This allows operators to benefit from innovation while maintaining strict governance over how rApps interact with the platform and underlying network.

Expanding the toolbox

AI-driven defense for autonomous networks

When networks become intent-driven and autonomous, cross-domain security orchestration must be in place to ensure autonomy and AI are implemented safely, with full observability, and closed-loop verification according to ZTA principles.

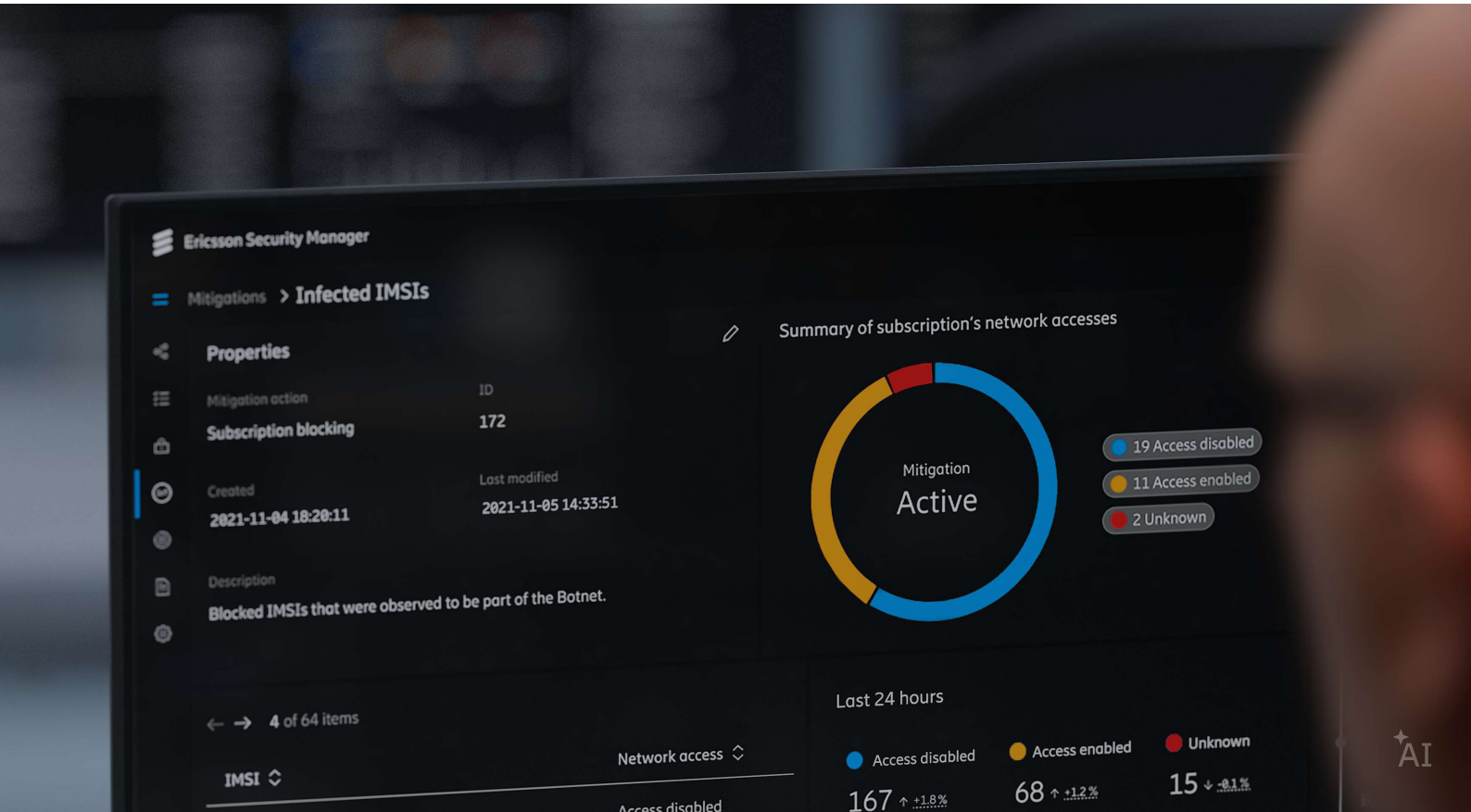
As business intents are usually set on very high level, they need to be translated into expected security outcomes and actionable security policies that are aligned across the autonomous domains and compliant with security objectives and regulatory requirements.

Keeping agents on track
AI agents in the SMO, rApps, and the autonomous domains require guardrails on what they are allowed to perform and what data they can access and change, as well as continuous monitoring. This becomes particularly important in multi-vendor environments with agentic third-party rApps.

Ericsson Security Manager (ESM) is our cyber defense solution for autonomous networks. Today, its policy automation engine supports human-in-the-loop, closed-loop automation that meets TM Forum Level 3 autonomy standards. In the future, AI-native end-to-end security intent management will be added to reach Level 4 autonomy, enabling the translation of intents into policies and guardrails, with continuous verification, agent trustworthiness monitoring, and automated remediation across domains. This will give the network the ZTMM required for Level 4 autonomy.

Mapping threats autonomously
ESM also brings the AI-driven unified telemetry fabric and analytics required for automated threat detection and response. It ensures continuous visibility over threats, risks, and software vulnerabilities across the SMO, rApps, network functions, and infrastructure, enabling autonomous networks that are safe and trustworthy.

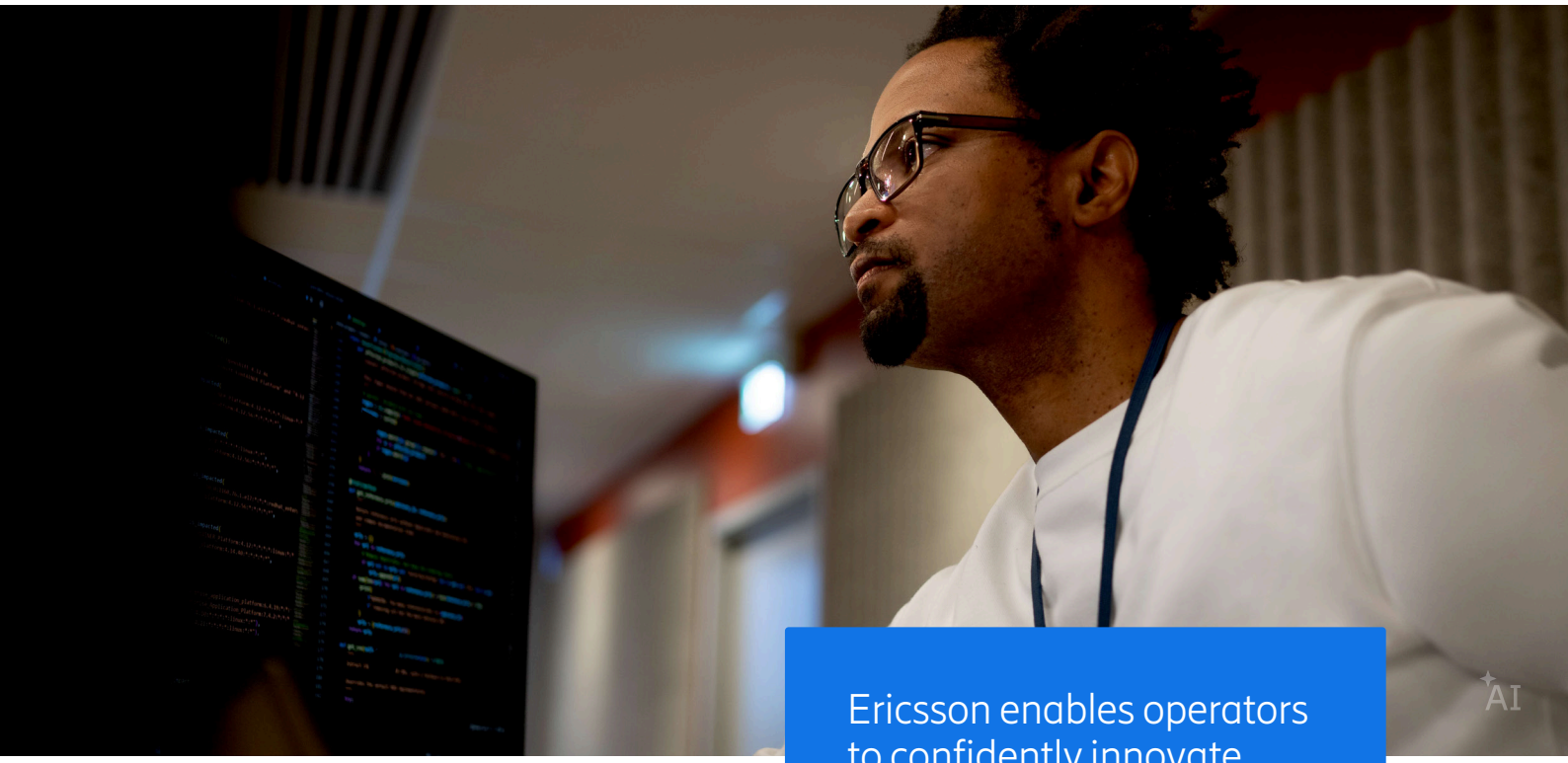
Combined with security features and telemetry data from applications and infrastructure, it is a holistic cyber defense solution for autonomous network protection, threat detection, and response.



Looking ahead

Creating a secure SMO

As operators move toward Open/Cloud RAN and AI-driven automation, securing the SMO means going beyond standalone controls and shifting toward a platform built with security in mind from the start.



Ericsson enables operators to confidently innovate without compromising trustworthiness.

By combining deep telecom expertise with a secure-by-design approach, the EIAP is a truly trusted SMO platform that benefits from lifecycle-wide security integration and alignment with the Ericsson Security Reliability Model (SRM), O-RAN principles, and industry best practices.

By supplying built-in security controls, continuous vulnerability management, and support for a secure application ecosystem of third-party rApps, Ericsson enables operators to confidently innovate in a way that doesn't compromise trustworthiness.

About Ericsson

Ericsson's high-performing networks provide connectivity for billions of people every day. For nearly 150 years, we've been pioneers in creating technology for communication. We offer mobile communication and connectivity solutions for service providers and enterprises. Together with our customers and partners, we make the digital world of tomorrow a reality.

ericsson.com

The content of this document is subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document

© Ericsson AB 2026