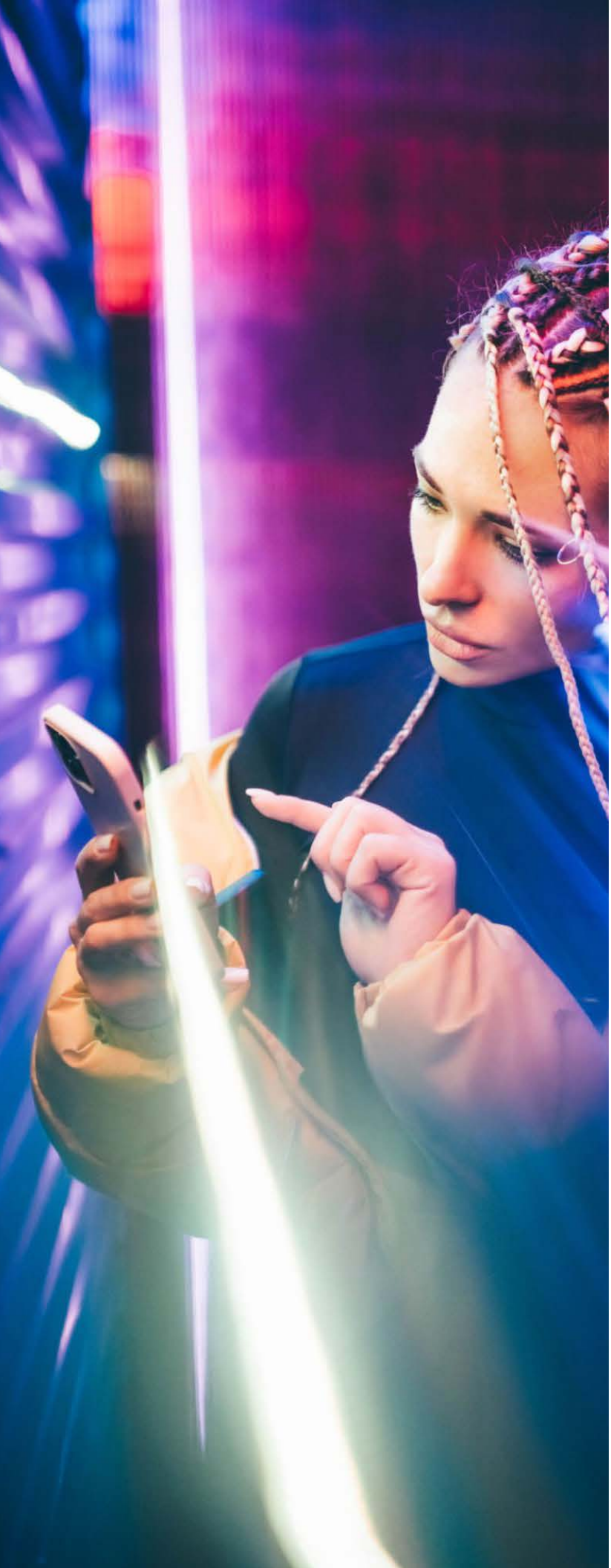
Microsoft and Nokia

Securing autonomous telecom networks with AI-driven defense

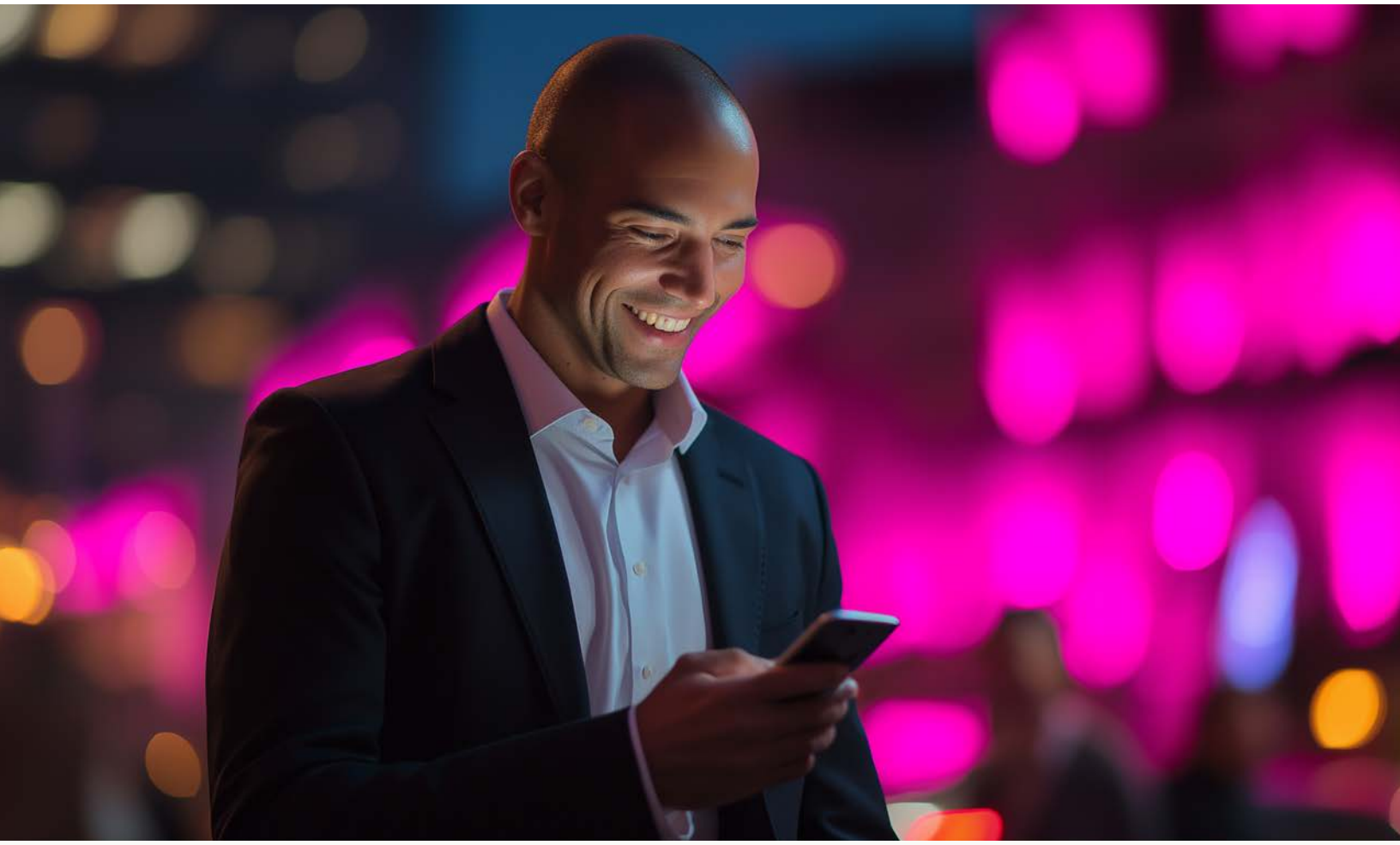


Securing automated telecom networks in a complex security and regulatory environment

Telecommunications networks are rapidly evolving, driven by the rollout of 5G, AI, increased automation, the early commercialization of quantum computing, and the digitalization of critical infrastructure. While enabling new capabilities, these advancements also expand the threat actors and adversarial AI capabilities, making networks more vulnerable to sophisticated, varied, and constant cyber-attacks.

At the same time, providers are facing strict regulatory requirements. The EU's NIS2 Directive, the UK's Telecommunications Security Act, and global standards like ISO 27001 and GDPR impose obligations for risk management, incident response, and data protection.

For telecom security teams, the proliferation of new AI capabilities is simultaneously unleashing a new level of complexity among threat actors as well as the development of tools to combat this ever-changing threat environment. Many operators are finding they need a proactive, scalable, and secure approach to cybersecurity and compliance to address these evolving challenges. Cloud-based SaaS and agentic AI security solutions from partners such as Microsoft and Nokia can help operators address these demands. When used with tools like Microsoft Sentinel, Security Copilot, or Azure OpenAI, these solutions may provide enhanced monitoring, detection, and response capabilities depending on deployment and configuration.



This playbook will:

- Explain why cloud-based solutions are foundational to modern network security
- Highlight advancements in AI-driven automation and agentic technologies
- Present strategies for securing automated and autonomous networks
- Demonstrate how Microsoft and Nokia jointly strengthen network resilience
- Outline support for EU and UK telecom compliance requirements

AI is a new class of threat and response for telecom security teams

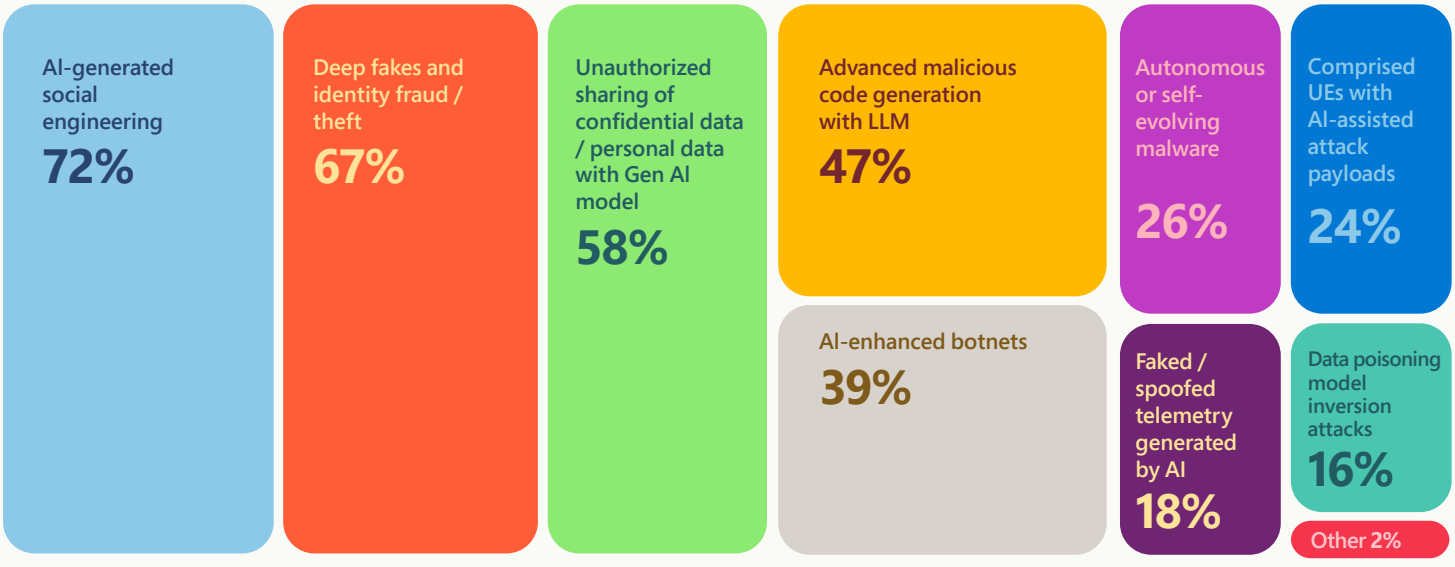
As telecom providers embrace modern network architectures to support the proliferation of new network capabilities and endpoints, including next-generation AI technologies, their critical infrastructure is increasingly exposed to a new wave of sophisticated cyber threats.

Well-resourced and coordinated threat actors are actively exploiting emerging vulnerabilities within 5G environments. Leveraging advanced AI-driven techniques, these adversaries are introducing a new class of security challenges—collectively known as adversarial AI—which encompasses tactics such as social engineering, deepfakes, botnets, and malicious code generated by large language models.

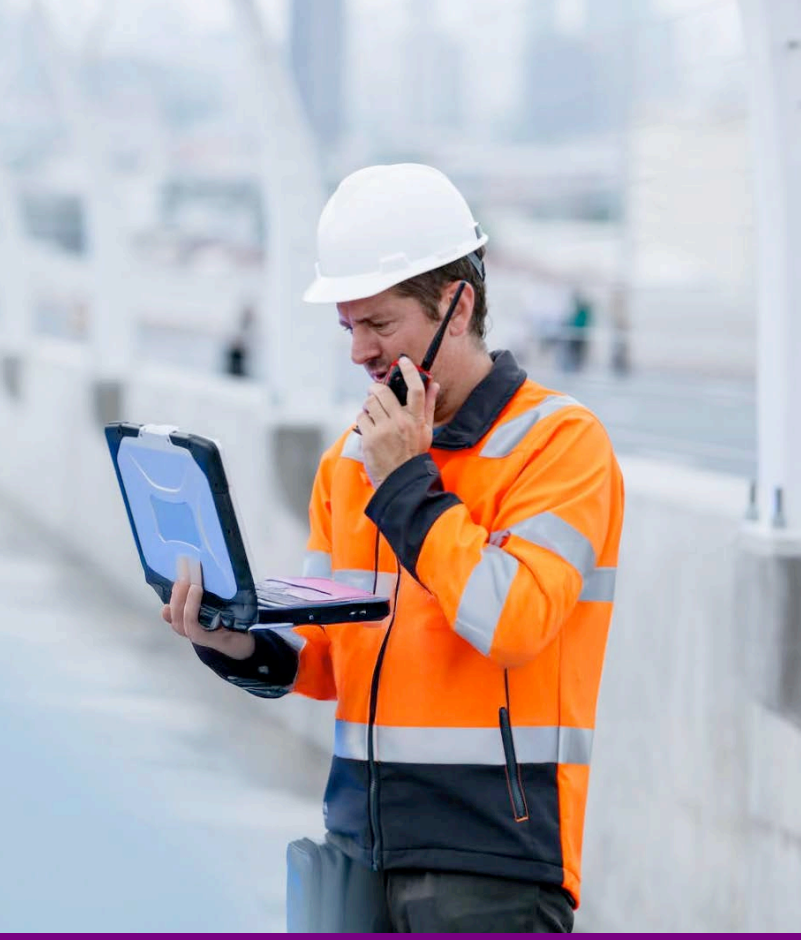
While the sophistication, volume, and velocity of threats increase, the impact of a data breach remains high. According to an IBM report, the average cost of a data breach is $4.4M, making the stakes extremely high for telecoms to meet these new threats head-on (IBM).

The Cybersecurity Ventures Cyber Report 2025 found global cybercrime is on track to increase by 15% in two years and is expected to cost approximately $12 trillion by 2031, up from just $3 trillion a decade ago.

Which attack types do you anticipate becoming significantly more powerful or frequent due to the offensive use of AI technologies (multiple select)?



Attack types on telecoms are expected to become significantly more powerful and frequent due to the offensive use of AI technologies. (ABI)



The question is no longer whether to adopt SaaS solutions but how to do so while maintaining the trust and security stakeholders expect.

As cyberthreats evolve in scale, speed, and sophistication, traditional defenses often struggle to keep pace. Security strategies must adapt—moving beyond static, reactive measures toward AI-driven, autonomous, and adaptive approaches. In this new era, defenders need agentic security capabilities that leverage intelligence, automation, and cloud-scale innovation to stay ahead of adversarial AI.

- Microsoft and Nokia bring expertise in telecom, AI, and cybersecurity to support operators in developing intelligent and automated security approaches. These solutions can complement existing network defenses and support continuous service delivery when deployed appropriately.
- The foundation is a secure, cloud-based architecture that enables visibility, resilience, and scalability.
- Nokia's predictive cybersecurity framework integrates **real-time detection, intelligent correlation, Agentic AI**, and **consolidated threat intelligence** to shift OT security from a reactive to a proactive stance, and respond to threats across complex network environments.

Securing AI innovation starts with a strong cloud foundation

As telecom providers navigate this increasingly complex, and sometimes overwhelming, landscape at the intersection of digital transformation, AI capabilities, heightened security risk environment, and autonomous network operations, some remain hesitant to fully embrace Software-as-a-Service (SaaS) solutions, particularly for critical network operations and management functions. When properly implemented, these solutions may enable automation, enhanced AI services, and operational efficiencies.

However, for many providers, as the industry faces increasing pressure to improve agility, automate OSS/BSS functions, unlock new AI services and agentic capabilities, and reduce costs while maintaining the highest security standards, the question is no longer whether to adopt SaaS solutions but how to do so while maintaining the trust and security stakeholders expect.

Cloud-based SaaS solutions can offer telecom providers several key advantages:

- **Data security:** Cloud providers like Microsoft offer multiple layers of protection,, including in-depth defense, data isolation, comprehensive encryption, and robust backup systems, while maintaining complete transparency about their security controls, that may vary by service and region, and provide detailed audit reports from certifying bodies.
- **Data privacy:** Cloud providers strictly control access to customer data and follow disciplined processes for maintaining accreditations and regulatory compliance across multiple jurisdictions, with specific emphasis on protecting personally identifiable information (PII) through measures like confidential computing and externally managed encryption keys available depending on deployment.
- **Data residency:** Customers can choose where their data is stored and maintain contractual assurances that data will stay within specified national borders while offering hybrid options for situations requiring local processing.
- **Data sovereignty:** Microsoft addresses sovereignty enabling customers to participate in the digital economy securely, independently, and with self-determined controls. The controls are delivered through technical, contractual, and operational measures, aligned to workload sensitivity.

With a secure cloud foundation in place, telecom providers can now leverage this platform to accelerate the next phase of innovation—

autonomous network operations. By combining cloud scalability with AI-driven intelligence, operators can help move beyond traditional automation to create networks that self-manage, self-heal, and continuously optimize performance with minimal human intervention.

Enabling autonomous networks through AI and cloud innovation

The convergence of advanced cloud infrastructure and AI-driven automation is redefining telecom operations, ushering in a new era of autonomous networks. Telecom providers are moving beyond traditional, task-based management toward intelligent, adaptive systems that can self-operate, self-heal, and self-optimize with minimal human intervention.

One of the most innovative components of Nokia's security offerings is its use of Agentic AI. This groundbreaking technology introduces autonomous agents that continuously hunt for threats without human intervention. These agents adapt to emerging attack patterns, learning from each interaction, and proactively defending against new vulnerabilities.

The true power of Agentic AI lies in its ability to carry out complete end-to-end threat hunting workflows—from detection hypothesis, and rule generation to containment and reporting. By automating routine tasks, security teams can refocus their efforts on high-level decision-making such as supervised validations to enhancing the overall cybersecurity resilience.:

Improved network performance:

- Can help deliver faster speeds, lower latency and seamless connectivity
- Can support high network availability and uptime, and low (Mean Time to Repair) MTTR
- Can help optimize resource utilization and efficiency

Enhanced customer experience:

- Can improve quality of service • Can help contribute to complaints and improved brand reputation
- Can help increase customer satisfaction, retention and loyalty

Increased business efficiency:

- Can help reduce operational costs through high automation
- Can contribute to reduced churn and increased Average Revenue Per User (ARPU) due to premium QoS
- Can support competitive differentiation and strong brand identity

Microsoft

AI and Agentic AI: Microsoft's AI stack, including Azure OpenAI and Copilot Studio, enables predictive maintenance, dynamic traffic management, and closed-loop automation.

Cloud-native platforms: Azure Operator Nexus and Microsoft Fabric unify data estates and support real-time telemetry, enabling scalable AI deployments.

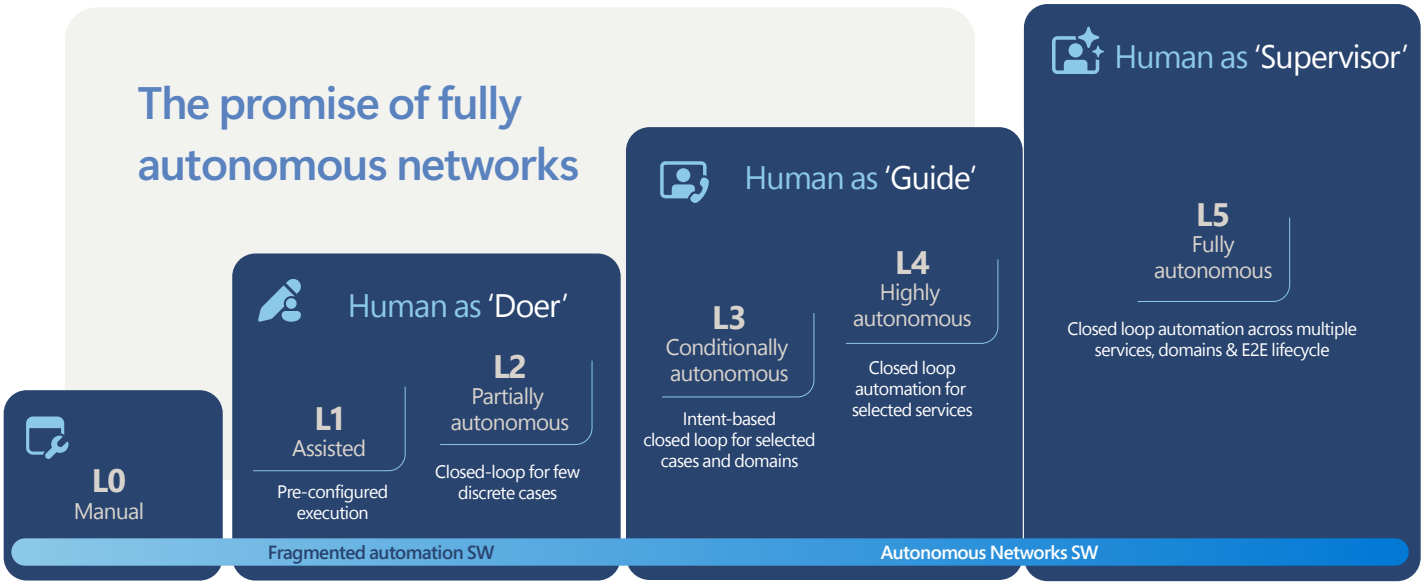
Intent-based orchestration: Operators can define desired outcomes (e.g., QoS targets), and the network autonomously configures itself to meet them.

NOKIA

New AI innovations in security: Nokia uses a telco-trained LLM and Agentic AI to proactively detect threats and rapidly retrieve insights, reducing threat dwell time from days to minutes.

New AI innovations in analytics: Nokia has enhanced subscriber experience analytics for fixed and mobile networks with Generative AI, enabling engineers to use natural language to access insights and reports.

New AI innovations in digital operations: Nokia's Digital Operations Center uses Agentic AI to automate and troubleshoot service orchestration, fulfillment, and assurance.



Telecoms don't need to wait for full autonomy to start reaping the rewards. These innovations are already delivering measurable value:

- Operators have achieved, in certain deployments, approximately **~20% improvement in operational efficiency** and an **~18% reduction in network operation OPEX** through autonomous network initiatives over the past two years (Capgemini Research Institute).
- Around **71% of operators** have been able to cut energy consumption in that period by implementing autonomous network capabilities (Capgemini Research Institute).
- Typical Return on Investment (ROI) for autonomous network programs can range from **1.7x to 3.4x,** with payback periods of **1.5 to 2.9 years** (IBM).
- For many telecoms, anticipated OpEx savings across five years can be in the range of **USD 150 million to USD 300 million** for a single organization (Makman Technology Consulting).

As telecom operators realize tangible ROI from autonomous networks, the next critical step is to ensure that these AI-driven systems are secure. As networks become increasingly automated, adaptive, and reliant on AI, security can no longer be an afterthought. It must be embedded from the outset. Intelligent, automated, and telecom-specific security frameworks are crucial for protecting operations, safeguarding data, and maintaining trust, while helping enable the full potential of autonomous networks.

Protecting autonomous networks with AI-driven security

As telecom networks embrace autonomous operations, robust security frameworks are essential to mitigate evolving threats and meet regulatory demands. Microsoft and Nokia offer a range of security solutions that can help support operators in building secure, AI-enabled autonomous networks. These solutions may incorporate Zero Trust principles, AI-assisted detection, and compliance controls, depending on deployment and configuration.

Disclaimer: Product features, naming, and availability may vary by region and may be subject to change. Some products or features may be in preview or limited release and are not guaranteed to be generally available. Integration between Microsoft and Nokia products is optional and depends on deployment and operational configuration.

Securing autonomous networks with Nokia and Microsoft: AI-driven defense

1. Zero Trust security architecture

Microsoft's approach integrates Zero Trust principles across OSS/BSS and network layers, helping, ensure:

- Supports continuous verification of identities and devices
- Can help enforce least-privilege access
- Designed to support real-time threat detection and response

2. AI-powered threat mitigation

- Security Copilot: can help SOC teams with AI-assisted incident analysis, reverse engineering, and automated remediation.
- Nokia NetGuard Cybersecurity Dome: Unified XDR frameworks such as NetGuard Cybersecurity Dome correlate telemetry across heterogeneous sensors and multi-vendor domains and platforms to create a single, contextualized incident view. By eliminating duplication and noise, security teams gain higher-confidence alerts and a streamlined workflow.

3. Compliance and governance

Autonomous networks must support near-real-time compliance monitoring and policy enforcement with privacy and regulatory standards. Microsoft can help enable:

- Automated policy enforcement
- Capabilities that support audit readiness and data lineage via Microsoft Purview
- Secure AI model deployment with responsible AI frameworks

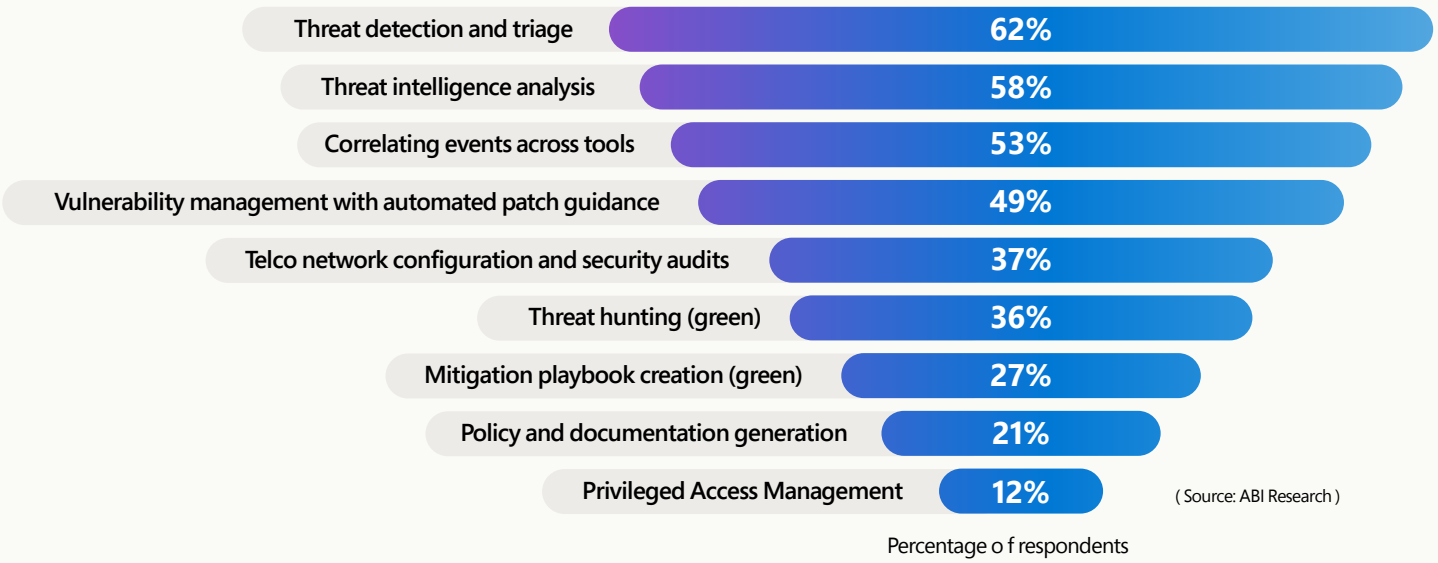
Disclaimer: Product features, naming, and availability may vary by region and may be subject to change. Some products or features may be in preview or limited release and are not guaranteed to be generally available. Integration between Microsoft and Nokia products is optional and depends on deployment and operational configuration.

Nokia NetGuard XDR is a cornerstone of Nokia's "Sense, Think, Act" strategy, providing comprehensive security across the journey to fully autonomous networks. It has been shown, in certain customer deployments, to deliver real-time threat visibility across all network domains, reducing detection times by up to 40%. Leveraging Generative AI, can help rapidly analyze hundreds of thousands of daily threat feeds to adapt detection logic and guide response.

Advanced AI analytics can help identify subtle patterns across more than 200 mission-critical network functions, has been shown to help reduce breach risk and lower analyst workload by approximately 60%.

Purpose-built for telecom networks, NetGuard XDR is designed to provide a level of insight and protection beyond generic IT security solutions, covering the network from core to edge (Nokia AstarLab.)

Areas telecom executives believe Gen AI could have the highest impact on their security operations. (ABI)

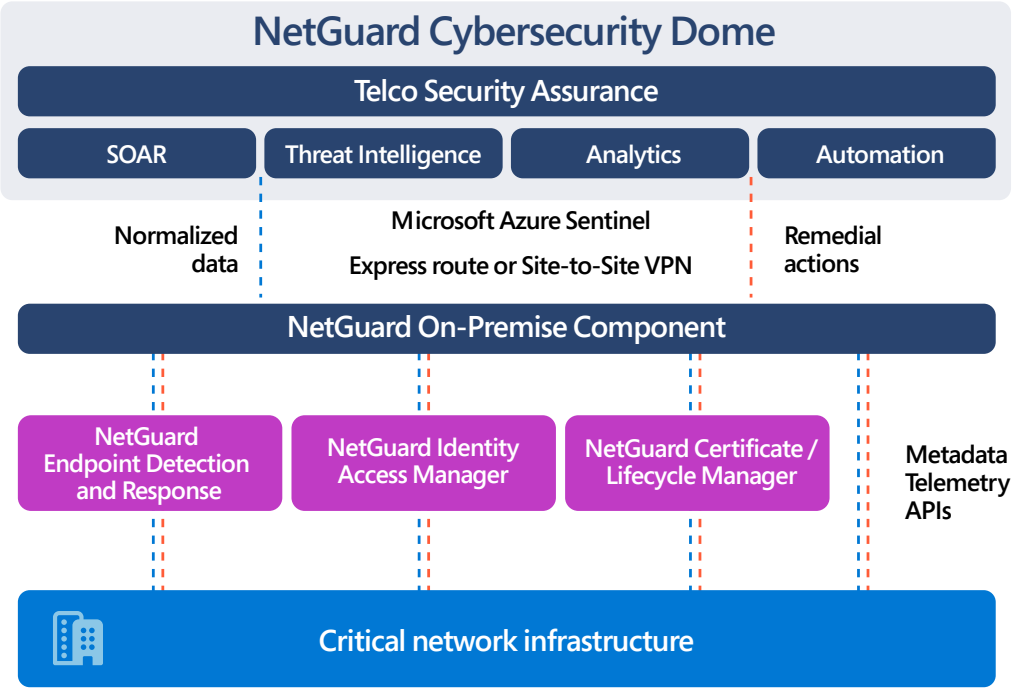


Disclaimer: Product features, naming, and availability may vary by region and may be subject to change. Some products or features may be in preview or limited release and are not guaranteed to be generally available. Integration between Microsoft and Nokia products is optional and depends on deployment and operational configuration.

Integrated network security for the autonomous era

Microsoft and Nokia have forged a powerful alliance to enhance cybersecurity in this new era, leveraging Nokia's NetGuard Cybersecurity Dome and Microsoft Azure capabilities. This comprehensive solution integrates AI and automation and can help protect against the complex threats faced by telecom providers in the UK, EU, and across the globe. Nokia NetGuard Cybersecurity Dome offers a suite of security services to help maintain business continuity by providing cross-layered detection and response across endpoints, networks and cloud. It utilizes AI-powered data correlation and dynamic threat scoring to help security teams quickly identify and prioritize incidents. The combination of Microsoft's cloud capabilities and Nokia's network security solutions is designed to offer scalable and flexible security support, to help operators address evolving telecom security requirements. Actual results depend on configuration, operational practices, and regional availability.

With a secure and scalable cloud foundation in place, telecom operators are now helping position themselves to harness AI-driven network automation, which can help unlock the full potential of autonomous operations and next-generation service innovation.



The Nokia NetGuard Cybersecurity Dome delivers comprehensive 5G security with AI and automation across Core, RAN, and Transport domains. Built on Extended Detection and Response (XDR), it aggregates and analyzes security data with telco context, helping teams assess risk and accelerate incident response.

Nokia NetGuard Cybersecurity Dome on Microsoft Marketplace

Disclaimer: Product features, naming, and availability may vary by region and may be subject to change. Some products or features may be in preview or limited release and are not guaranteed to be generally available. Integration between Microsoft and Nokia products is optional and depends on deployment and operational configuration.

Conclusion

A secure, cloud-based, AI-powered network is not just an answer to today's threats, it is increasingly important for resilient, future-ready telecom operations. By combining advanced AI orchestration, robust security controls, and a proactive compliance strategy, Microsoft and Nokia offer a model for telecom operators aiming to lead in the next era of autonomous connectivity.

Learn more

Microsoft for Telecommunications View here

NCYD video View here

Nokia/MS NetGuard Cybersecurity Dome View here

Frost & Sullivan XDR Frost Radar report View here

Nokia Autonomous Networks ebook View here

Predictive Security Whitepaper View here

Nokia Security Circle event video link View here

Microsoft

Join the conversation on social:

Microsoft

@Microsoft