Securing the telco future, today

A comprehensive guide to explore the unique characteristics and differences between telco network security and conventional IT security

NOKIA

Safeguarding your customer's sensitive data within the telecommunication network

Security operations teams at telecom companies are under significant pressure to protect customer data and defend against costly cyber attacks that can lead to reputational damage and customer loss.

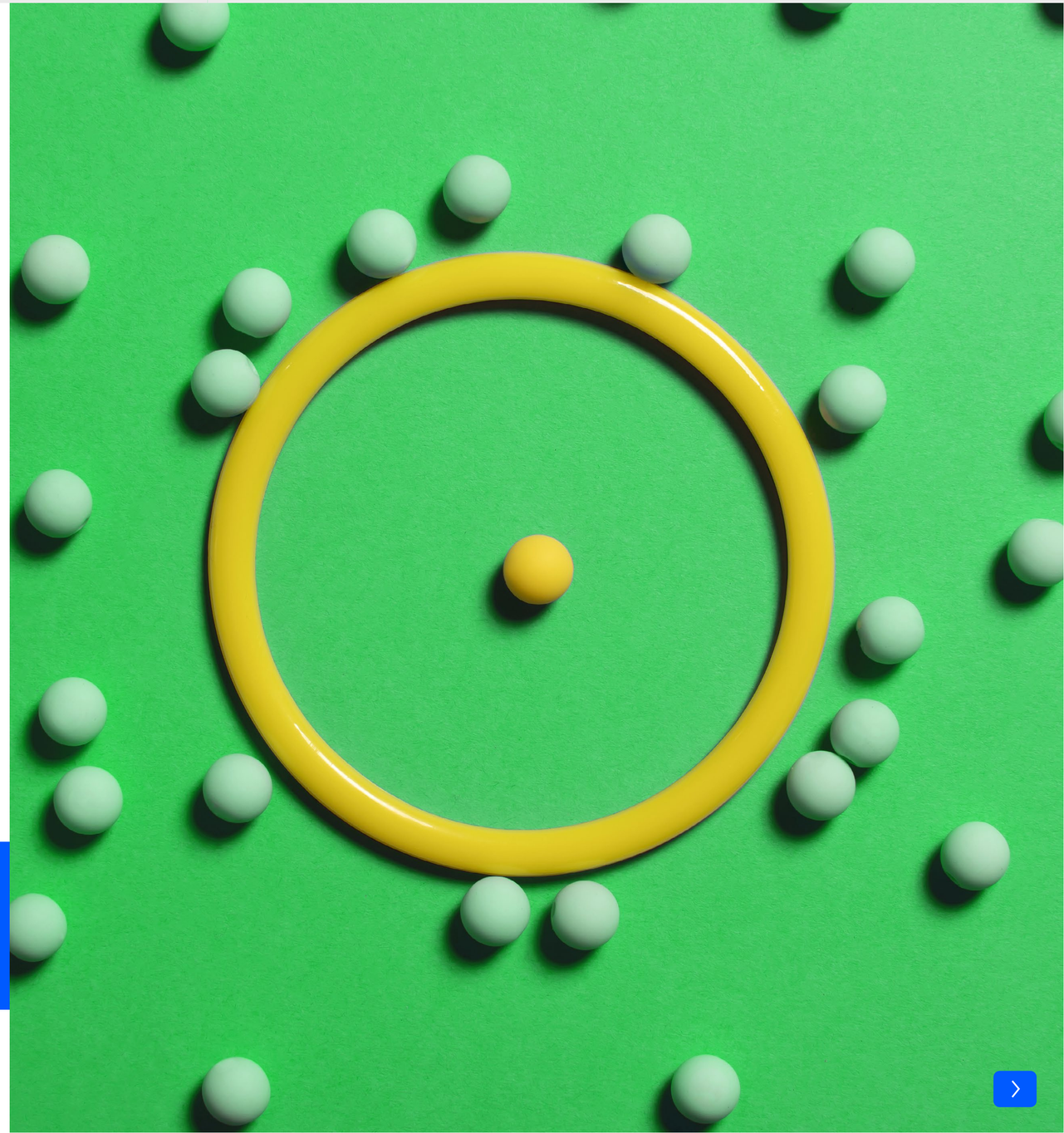
When it comes to cybersecurity, there are two worlds – conventional IT security and telco network security. Each differs significantly in its scope, focus, features, and challenges. Traditional IT security primarily prioritizes its efforts on protecting data, devices, and applications within an enterprise's network. What's top of mind for leaders in IT security is how to avoid data thefts including PII and how to combat ransomware attacks.

Whereas telco network security safeguards the entire telecommunications infrastructure and their goal is to do so without uninterrupted service availability. The top priority for telco network security is to protect the operational continuity of voice/data networks in addition to sensitive customer data and defend against large-scale DDoS attacks.

While traditional IT security is more generalized and focuses on a broader range of digital assets, telco network security requires specialized expertise and solutions as it demands compliance with strict regulatory standards that vary from country to country and are specific to the telecommunications industry.

56% of CSP respondents report that they need to greatly improve their capabilities for telecom-specific attacks.*

* Nokia commissioned GlobalData report, 2022



Navigating the security divide of IT vs. telecom network security

Within the realm of communication service providers (CSPs), there is a need for both IT and telecom network security, but they often converge under a single leadership umbrella. When it comes to protecting your network and understanding your security needs and priorities, it's crucial to recognize the unique characteristics that set these domains apart including components, infrastructure and protocols, skill sets, tools, and regulatory landscape.

In 2023, TM Forum conducted a survey that included respondents from 40 telco operators around the world at the director level or above. 71% of respondents said their organization has a single CISO or CSO across both enterprise IT and network domains.

IT Security	Telecom Network Security
Components	
Industry agnostics such as laptops, Mobile Devices, Intra-net, IT applications and data center	Purpose-built networks such as Core, RAN, Transport, Ac-cess Network, OSS/ BSS
Infrastructure and protocols	
Standard protocols like TCP/IP and TLS	Multi-vendor legacy technologies mixed with the latest cloud-based SBA and telco protocols like SS7, Diameter, GTP
Skill sets	
Skills in endpoint security [mobile, desktop servers], app security, firewalls, and secure gateways.	Expertise in telco network topology, communication proto-cols, attack scenarios for SBA, NE integrations to collect telemetry data and take actions.
Tools and technology	
Homogenous security tools like IT SIEM, IAM, EDR, and laptop antivirus.	Specialized tools like telco XDR, mission-critical EDR, telco PAM, cloud-native architecture
Regulatory landscape	
Governed by standards like HIPAA, PCI, and GDPR	Abides by 3GPP, GSMA, and country-specific regulations such as TSA in the UK, NIS2 in Europe

Uncovering the anatomy of breaches in IT and telco network security

Understanding the nuances of security vulnerabilities and their potential repercussions is crucial when it comes to distinct incidents and the severity of attacks. It's essential to discern these differences and possess the right expertise and partnerships to address your network adequately.

When exploring generic IT security vendors, there are various incidents from common threats like phishing and weak passwords to more severe issues such as data theft, compromised databases, and banking trojans. These attacks can lead to service disruptions and the exposure of user data including PII and credit card information.

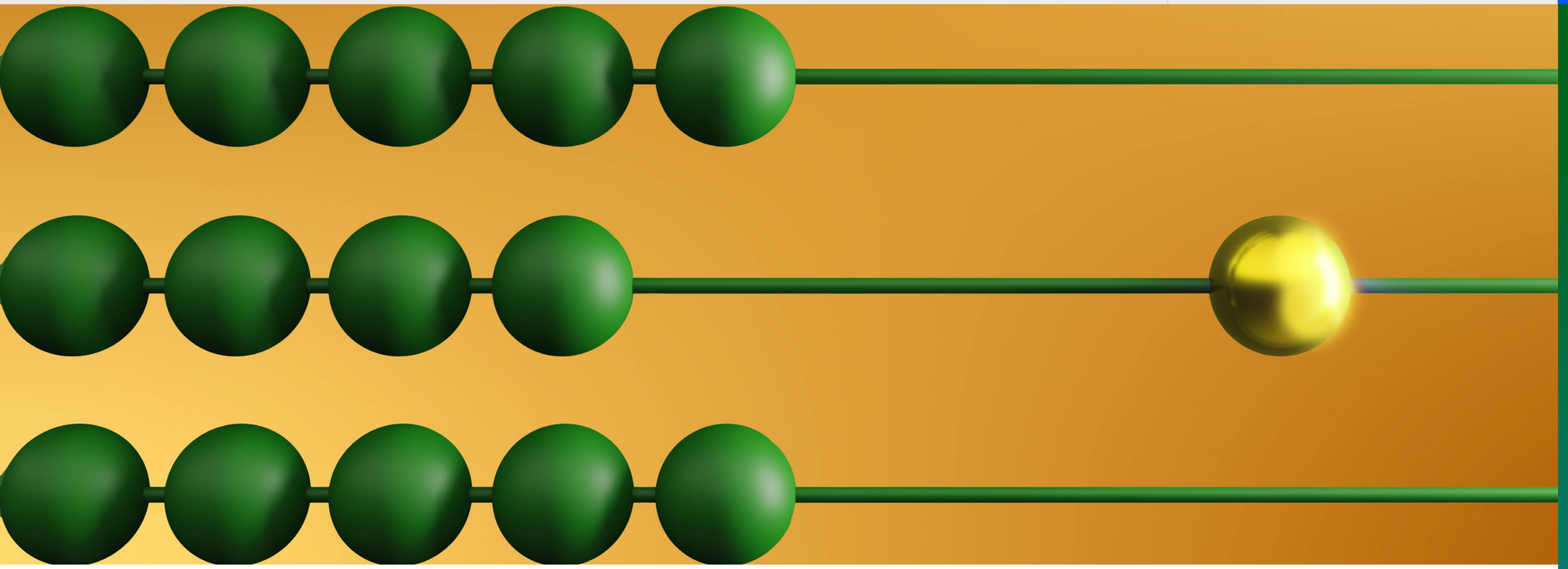
As we dive into the specialized domain of telco security vendors, the incidents are more severe with heavy consequences for end customers. These include eavesdropping on subscriber data/network data, signaling storm towards RAN/Core to cross technology attacks on roaming interface (SS7/ GTP), and compromised telco workloads/ network functions. The fallout of these attacks can lead to network failures and country-wide communication outages. This loss of connectivity can hinder access to emergency services and financial transactions.

It's a stark contrast between IT security attacks which typically involve data theft and service disruptions, and telco network security breaches which can have the potential for life-and-death impact.

One solution offers two distinct approaches to addressing security

Security tools often lead to confusion, with many CSPs unaware of the distinctions between telco-specific and generic security solutions. Despite sharing similar names, these solutions have fundamentally different approaches to network security.

Consider an Endpoint Detection and Response (EDR) solution as an example. Generic EDR systems are tailored for enterprise environments, protecting workstations, end-user devices, and IT data centers. An example is installing anti-virus software on laptops. On the other hand, a telco-specific EDR system has agents running on a critical infrastructure to protect against telco-specific attacks while maintaining the functionality of network elements. The minimal impact on the workloads assures network performance is not affected.



The leader in telco network security

Nokia's real-world knowledge of telecommunications service providers and their critical infrastructure makes us trusted experts to elevate your E2E 5G security operations.

With over 500 global security projects in the last 15+ years, our footprint in shaping security standards and best practices is undeniable, evidenced by our active roles in over five key standardization bodies.

With solutions that are focused on telecommunications service providers and critical telecommunications infrastructure, deliver better business outcomes by prioritizing your security needs. Empowering you to counter cyber threats, uncover new revenue streams, and adhere to compliance demands.

Nokia Cybersecurity Operations

Seamless end-to-end 5G security solutions

Discover more

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID: 213747 (December)

nokia.com

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.