NOKIA

Early detection in mission-critical networks

Designed to work inside live services

When time becomes attacker leverage

Control no longer lives in one place

Control now spans CNFs, APIs, orchestration and operational tooling across suppliers and domains. In open architectures, no single signal is decisive. Compromise can persist inside live systems because detection depends on connecting weak signals without disruption.

AI has moved into operations

AI has moved into live network workflows. Models, training data, pipelines and automation logic are now part of the attack surface.

At the same time, attackers use AI too, moving faster and blending in, so early-stage threats can stay quiet and look like business as usual until it's too late.

Quiet access blends in

In this environment, quiet access becomes the most valuable position inside a telecom network, whether the goal is disruption, monetization, or geopolitical leverage. When attackers move using valid identities and legitimate mechanisms, their activity can look normal to generic security tools.

Thousands of CNFs

Operating continuously across regions and vendors

99.999% uptime

Availability constraints limit containment options

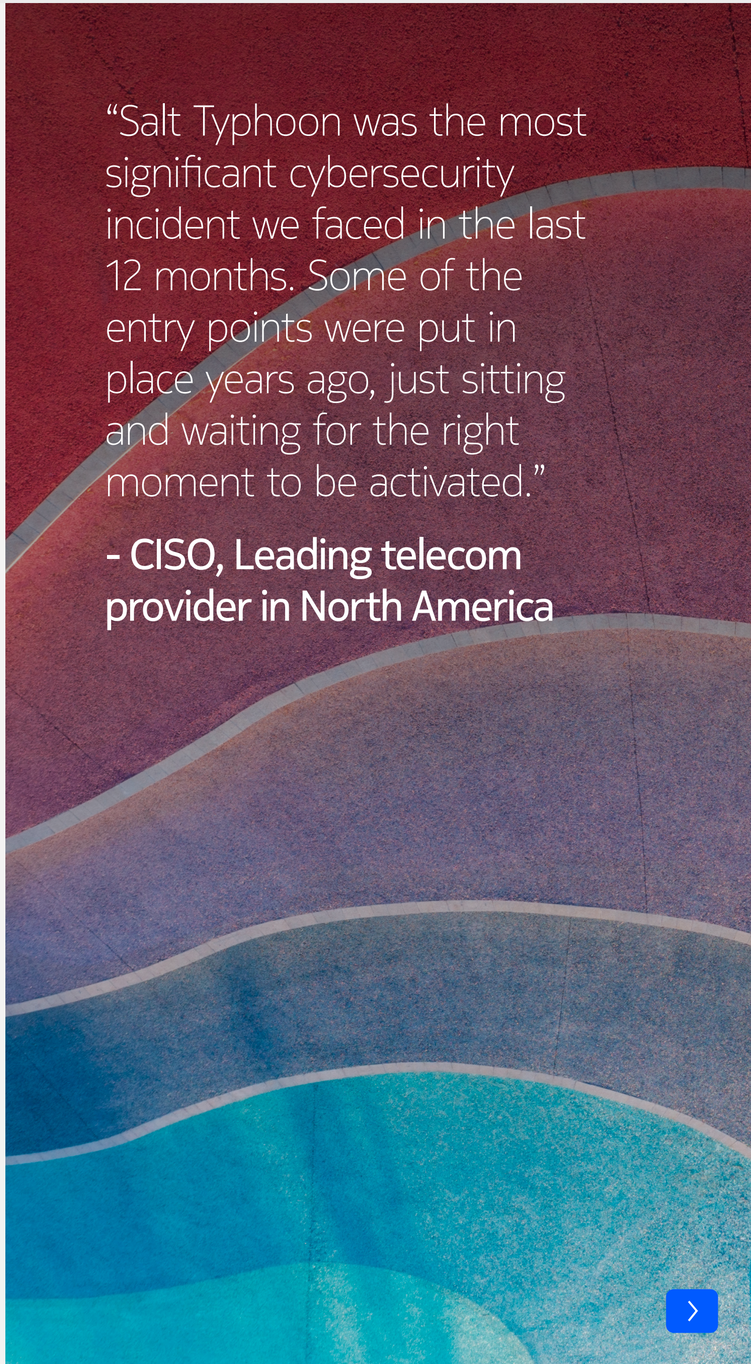
300+ days

Documented dwell time in recent telecom intrusions

20-40% latency impact

Generic probes intercept live NF execution

CNF = Cloud-Native Network Function



What does delayed detection mean in critical networks?

Once time favors the intruder, the cost lands in service risk, assurance burden and external deadlines.

Service risk appears before clarity

In critical networks, delayed detection doesn't always surface as a neat alert stream. In many cases, the first visible signal is service instability. When harmful activity touches service-delivery environments, operators are forced to protect availability while still trying to understand what is happening. Isolation is rarely clean, and the network can't be paused to get the full picture.

Assurance becomes the long tail

Late detection also creates a second, slower cost: proving what can still be trusted across domains that keep changing. Scope, validation and reassurance expand across teams, vendors and environments, even when services remain stable. This is where response runs for months, in parallel with live service and ongoing change.

Regulatory clocks start early

Oversight is moving toward early notification, even before full certainty is available. In the EU, NIS2 mandates an early warning within 24 hours of awareness. In Singapore, telecom providers are expected to report suspected state-linked intrusions within two hours to enable national coordination.

$millions per hour

Delayed isolation escalates into financial impact

11+ months

Multi-agency threat hunting and eviction across four telecom providers

24 hours / 2 hours

Early warning timelines measured in hours

The old assumptions that break in telecom

Assumption 1:

Deep system privileges are acceptable

Security components that require deep system privileges or operate as opaque black boxes are assumed to be safe. In telecom, this risk falls outside the service provider's assurance and trust models.

Assumption 2:

Variable CPU, memory and traffic overhead is tolerable

Enterprise security often treats unpredictable resource consumption as an acceptable trade-off for visibility. In telecom environments, especially under load or attack, this creates instability, disrupts capacity planning, and threatens availability.

Assumption 3:

Kernel-space modification is a viable monitoring strategy

Kernel modules, hooks or OS-level modifications are assumed to provide reliable visibility. In critical infrastructure, these approaches introduce privilege, memory and failure-mode risks that operators cannot accept.

Assumption 4:

Security tools can dictate lifecycle and upgrade timing

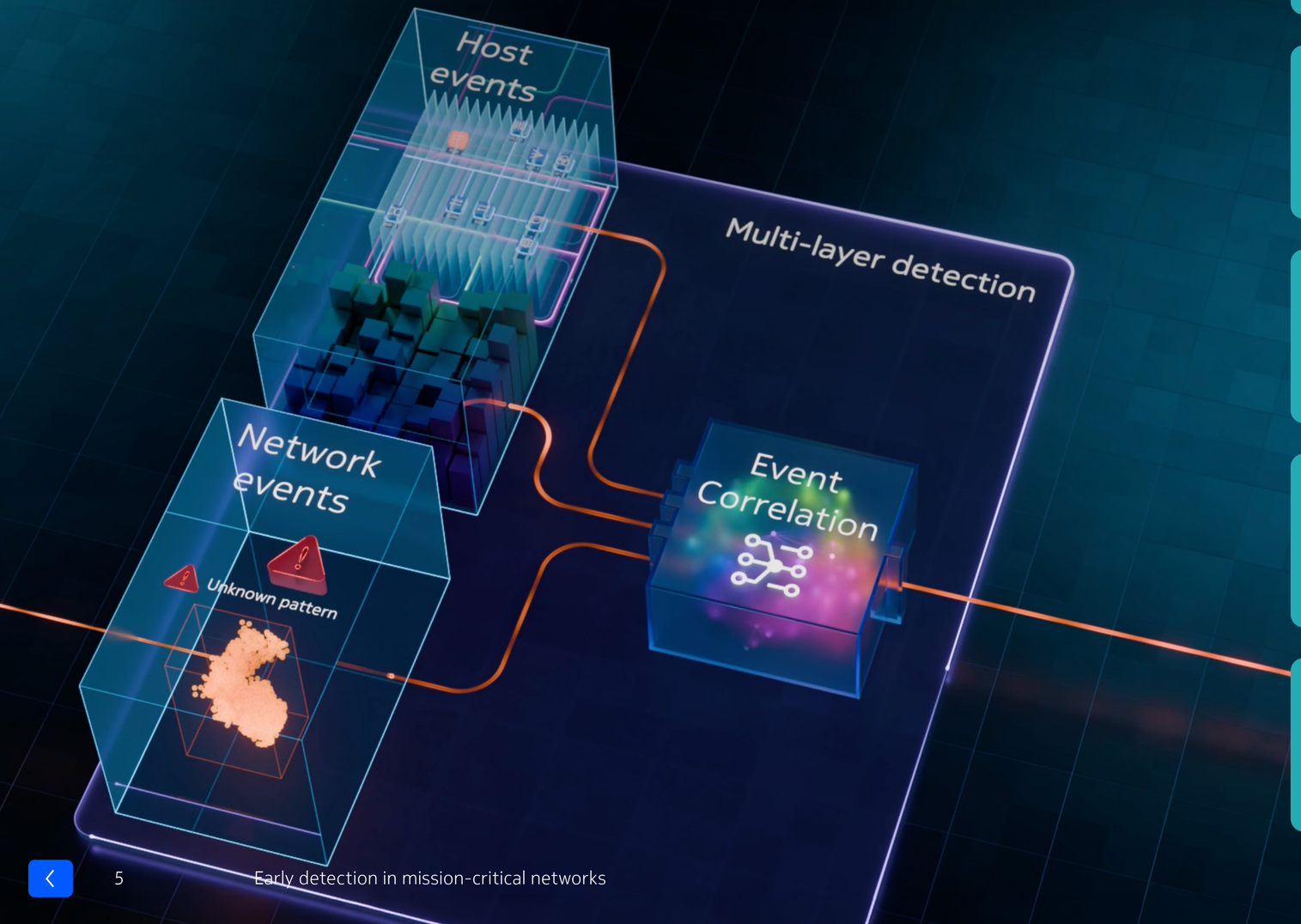
Traditional EDR assumes installation, upgrades and testing can align to security schedules. Telecom systems operate on fixed, validated lifecycles and misalignment adds operational complexity, increases recovery time and drives long-term cost.

Assumption 5:

Security can be layered after the network is designed

Enterprise security is often treated as an overlay. In telecom, all systems must align with customer architectures, regulatory constraints and pre-validated network designs as native elements. Anything that cannot fit cleanly becomes operationally fragile.

Principles of telecom-grade runtime security



Visibility is native, not disruptive:
Security operates inside the runtime of CNFs and management planes without deep system privileges. User-space instrumentation observes behavior alongside live services, preserving service availability.

Resource impact is predictable and minimal:
Detection operates with low CPU and memory overhead. Security doesn't compete with service for resources, even under load or attack.

Lifecycle alignment is built in:
Security tooling follows telecom upgrade, validation and change-management processes. Coverage extends across mixed Linux estates, vendor appliances and legacy systems.

No kernel-space modifications or opaque components:
The architecture avoids kernel-space modules and OS changes. All components are transparent, auditable, and aligned with established assurance and trust models, with contained failure modes.

Security is part of telecom design:
Controls align with network architecture, regulatory constraints and pre-validated designs. Visibility is anchored where behavior forms and change occurs.

NetGuard Endpoint Detection and Response

Designed to work inside live services

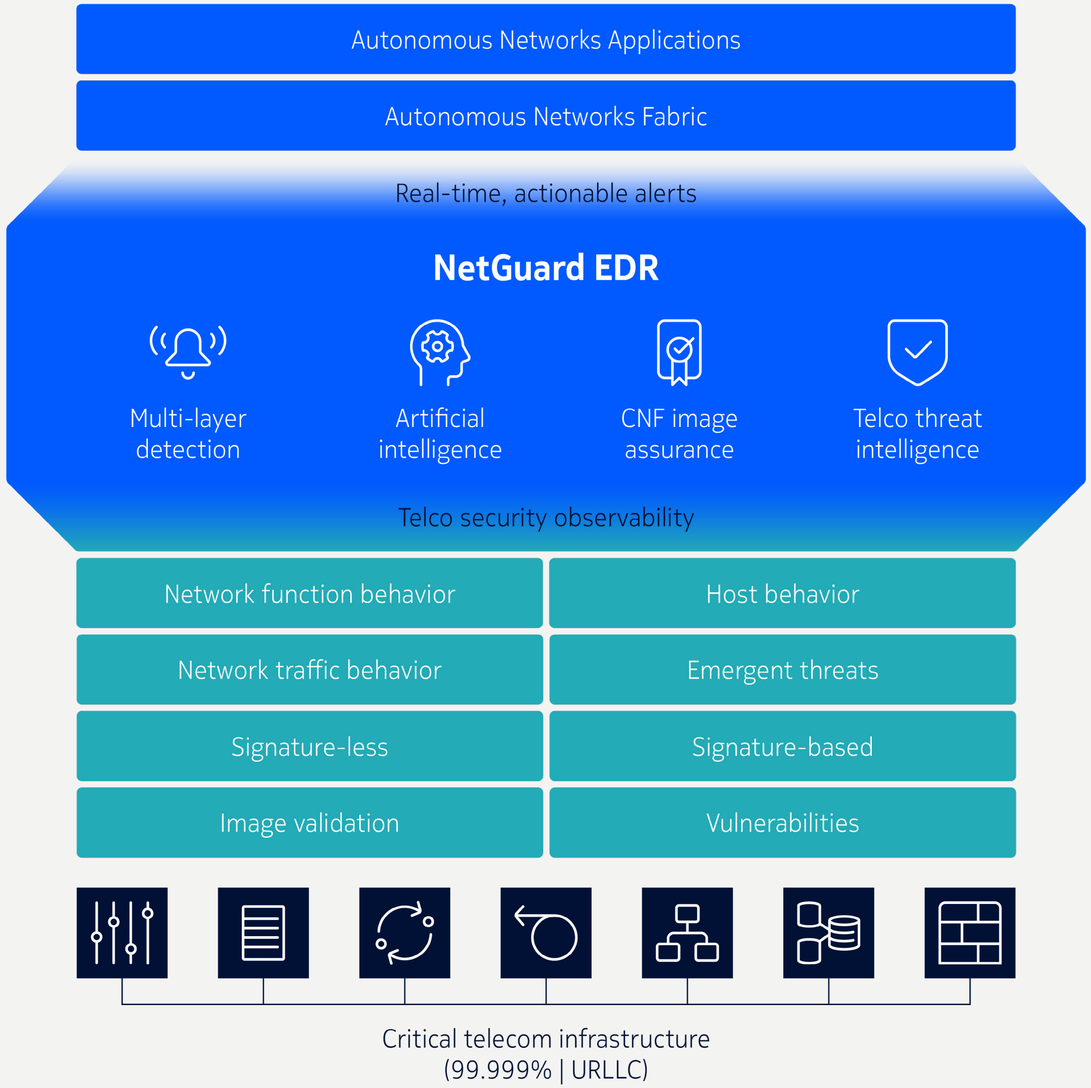
NetGuard Endpoint Detection and Response (EDR) operates inside live telecom environments, observing network, host and traffic behavior as services run.

By correlating signals across these layers, it detects stealthy and multi-stage attacks in real time, without adding latency or disrupting existing security operations.

Security observability
Purpose-built for telecom. Multi-layer detection across network, runtime and behavior, not retrofitted from IT security tools.

No compromise on availability
SLA-safe by design. User-space monitoring across CNFs and VNFs. No kernel modules, no privilege escalation, no latency impact.

Actionable network intelligence
Alerts you can act on instantly. Every alert is backed by evidence, context and mapped attack techniques.



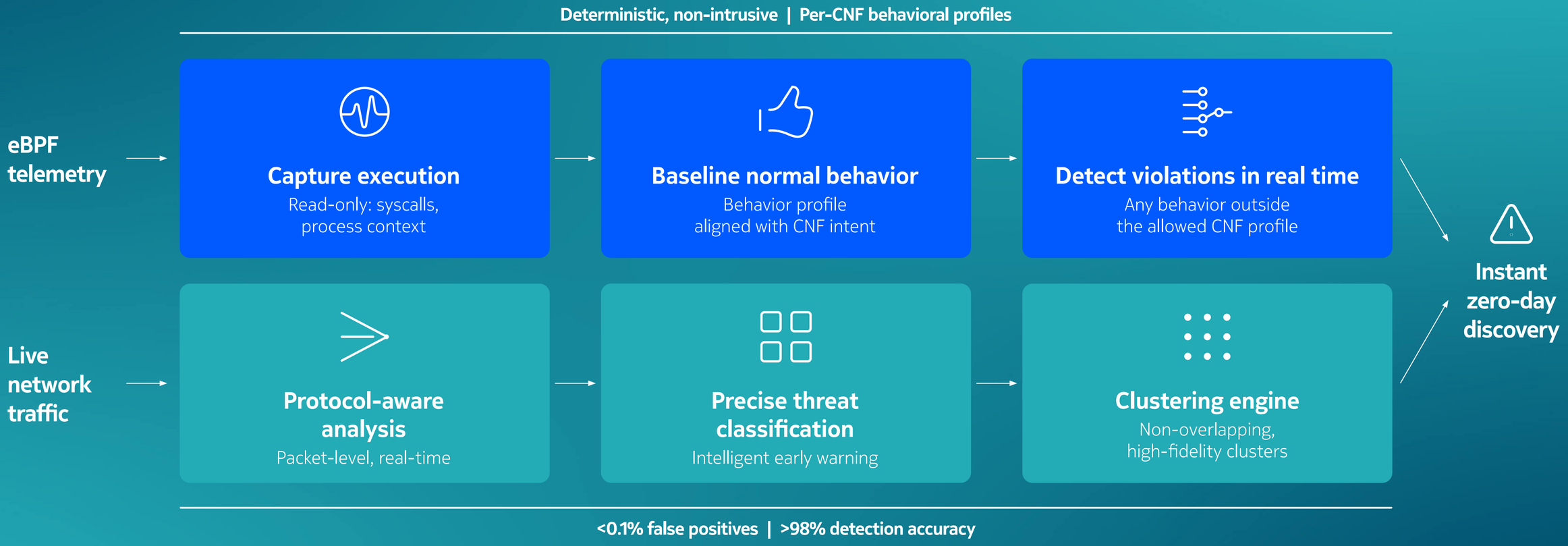
Secure CNFs from supply chain to runtime

NetGuard EDR addresses both prevention and runtime detection in one system. Image assurance and vulnerability scanning reduce what reaches runtime, and that same visibility continues inside live workloads, surfacing advanced activity across the kill chain.

	Image signature verification	Image vulnerability scanner
What	Block untrusted or tampered images before they run	Detect known vulnerabilities in CNF images
How	**Runtime** Validate image signatures on create/update **Periodic** Re-verify running workloads to detect drift	**Periodic** Scheduled background scanning of all images **On-demand** Targeted scans when needed
Why it matters	Prevent supply chain attacks and unauthorized updates Guarantee image authenticity and integrity	Catch vulnerabilities early in the CI/CD pipeline Enforce security posture and regulatory compliance

Detect novel threats inside live services

In NetGuard EDR, AI extends telecom security observability by detecting anomalies in two contexts: deviations from allowed CNF behavior, and the emergence of previously unseen patterns in real-time network traffic – supporting early discovery of novel attacks.



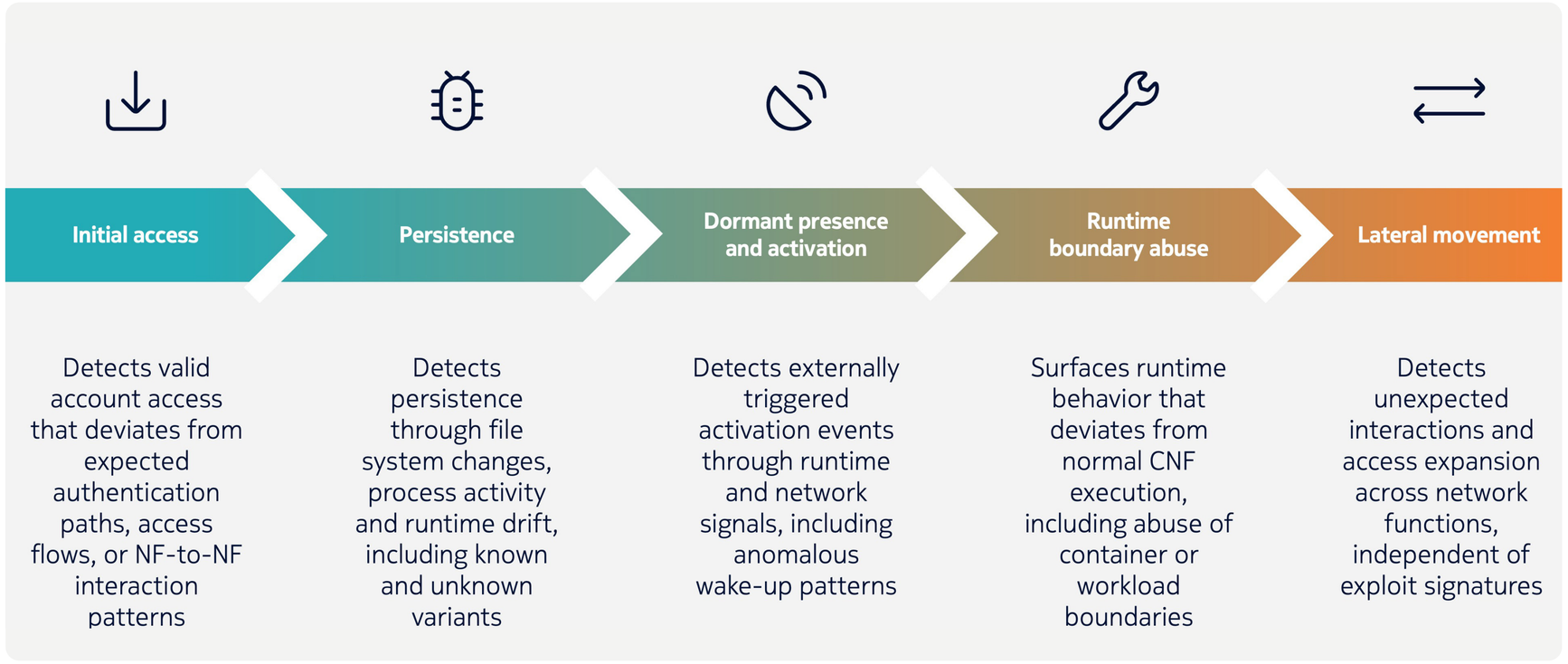
Values from Bell Labs peer-reviewed research

Signals captured from inside live telecom services, spanning network function behavior, runtime activity and real-time network traffic, are correlated with telecom-specific security context and threat intelligence.

In Nokia XDR, this supports AI-driven investigation and autonomous response, where threat hunting accelerates detection and resolution through automatically generated mitigation playbooks.

Use case: Detect stealthy backdoors across the kill chain

NetGuard EDR monitors every step attackers take to establish and hide persistent access in telecom networks.



How NetGuard EDR does it

- Real-time monitoring of endpoint and CNF configuration drift
- Network-aware detection of privilege escalation and lateral movement
- Behavioral analytics for persistence and evasion tactics
- Integration with network operations systems and management-plane telemetry for activation signals
- Expert guidance for handling complex, multi-stage telecom attacks

Telecom-specific threat intelligence

Built on decades of telecom security experience, Nokia turns real operator incidents into detection logic designed for how telecom networks run in production. Rules, signatures, and response guidance reflect live network behavior worldwide.

Nokia Threat Intelligence Lab curates frontline insight from live networks together with trusted research and partner intelligence, filtered and tuned specifically for telecom environments. The result is threat intelligence that feeds directly into detection and response.

Trusted on critical telecom infrastructure

Protecting 35M Colombian subscribers

“With Nokia, we have a telco-specialized approach that helps us significantly. Its integration with the Nokia core allows us to be much more effective in safeguarding infrastructure, protecting customer data and ensuring confidentiality.”

- Iader Maldonado, CTIO at Claro Colombia

Watch the video:

5G Cybersecurity: Claro & Nokia safeguarding Colombia’s largest mobile network - YouTube

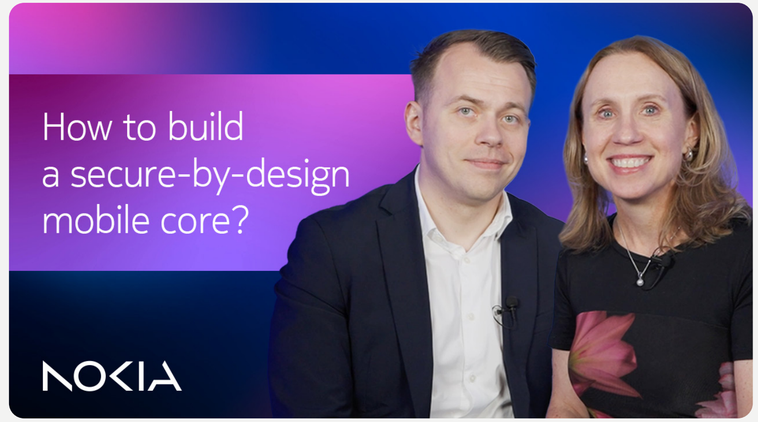
Covering entire subscriber base in India

“We tried and applied the same monitoring mechanism on the telco and we saw the telemetry is sheer and un-handleable. That is when we started looking at purpose-built technologies coming our way like the NetGuard Cybersecurity Dome and NetGuard EDR that Nokia has.”

- Mathan Babu Kasilingam, CTSO & Data Privacy Officer at Vodafone Idea

Watch the webinar:

Securing the telecom core networks - Webinar replay



Telco-grade monitoring in Denmark

“It was quite obvious for us since the beginning that we don’t need just security tools like standard IT security tools. We need telco-grade security tools in order to fulfil all these requirements.”

- Bogdan Hantanu, Senior Operations Director at Norlys

Watch the interview:

Nokia Core Talk: Norlys’ core transformation: Security comes first

Bringing early warning into live services

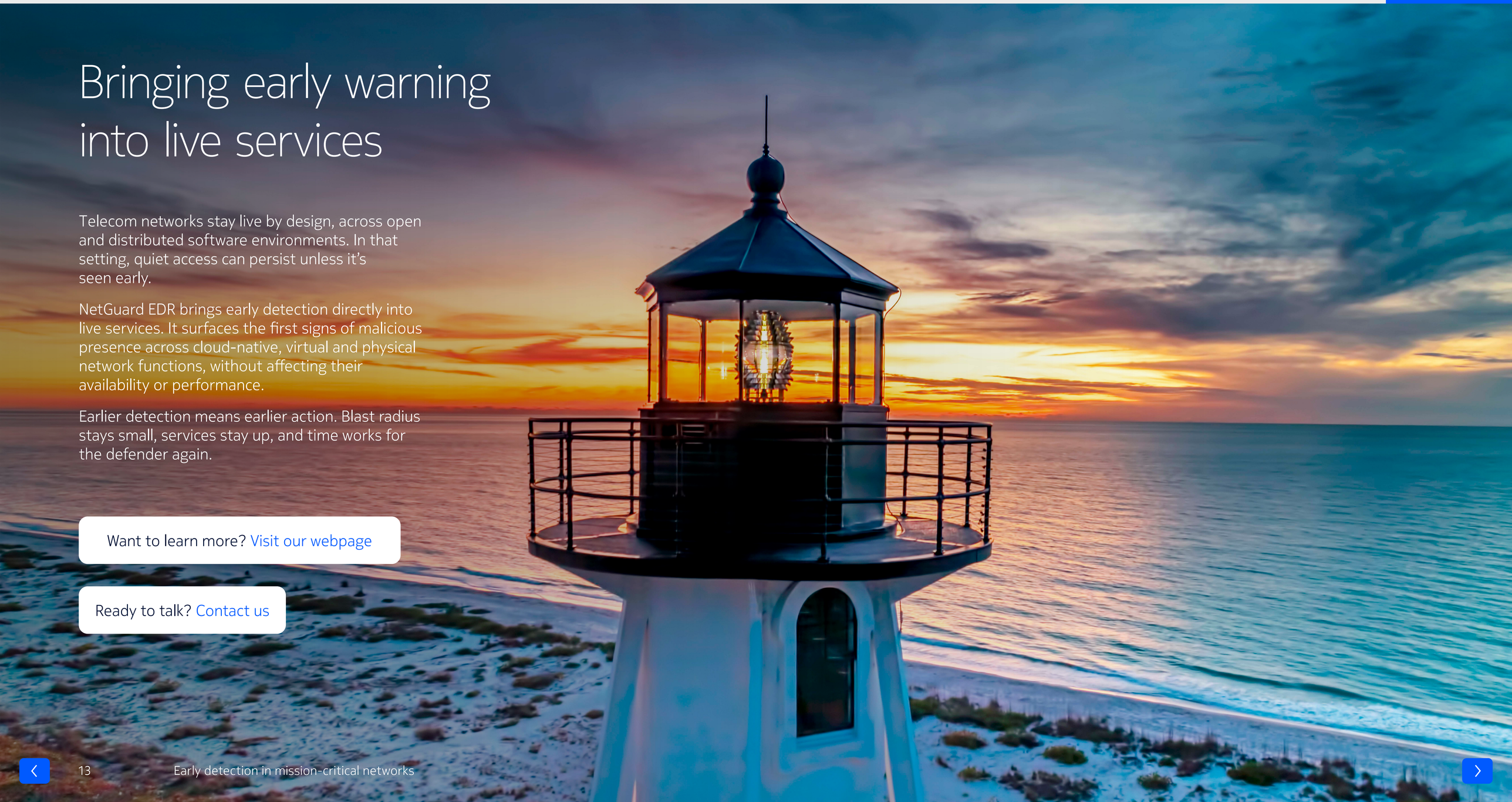
Telecom networks stay live by design, across open and distributed software environments. In that setting, quiet access can persist unless it's seen early.

NetGuard EDR brings early detection directly into live services. It surfaces the first signs of malicious presence across cloud-native, virtual and physical network functions, without affecting their availability or performance.

Earlier detection means earlier action. Blast radius stays small, services stay up, and time works for the defender again.

Want to learn more? Visit our webpage

Ready to talk? Contact us

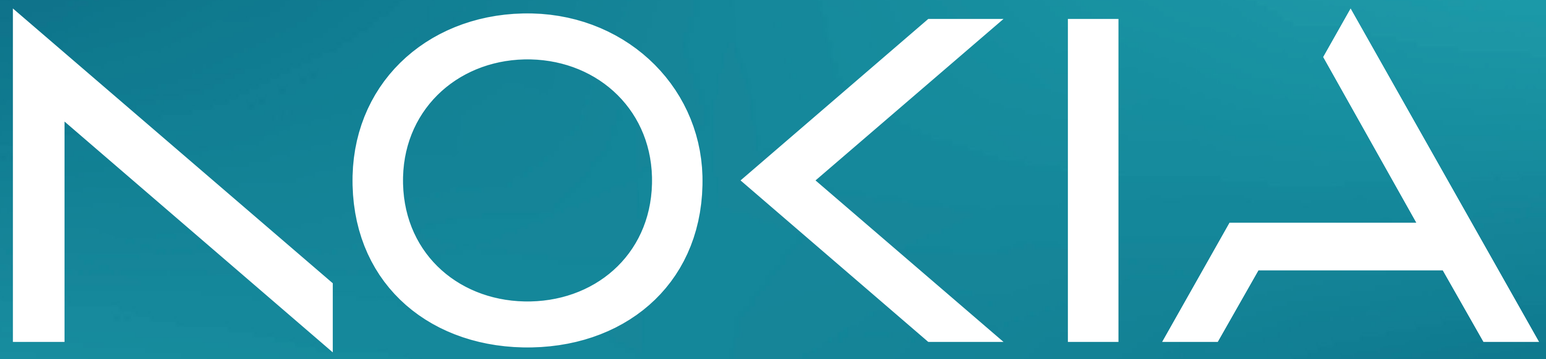


Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID: 213111

nokia.com



About Nokia

Nokia is a global leader in connectivity for the AI era. With expertise across fixed, mobile, and transport networks, we’re advancing connectivity to secure a brighter world.