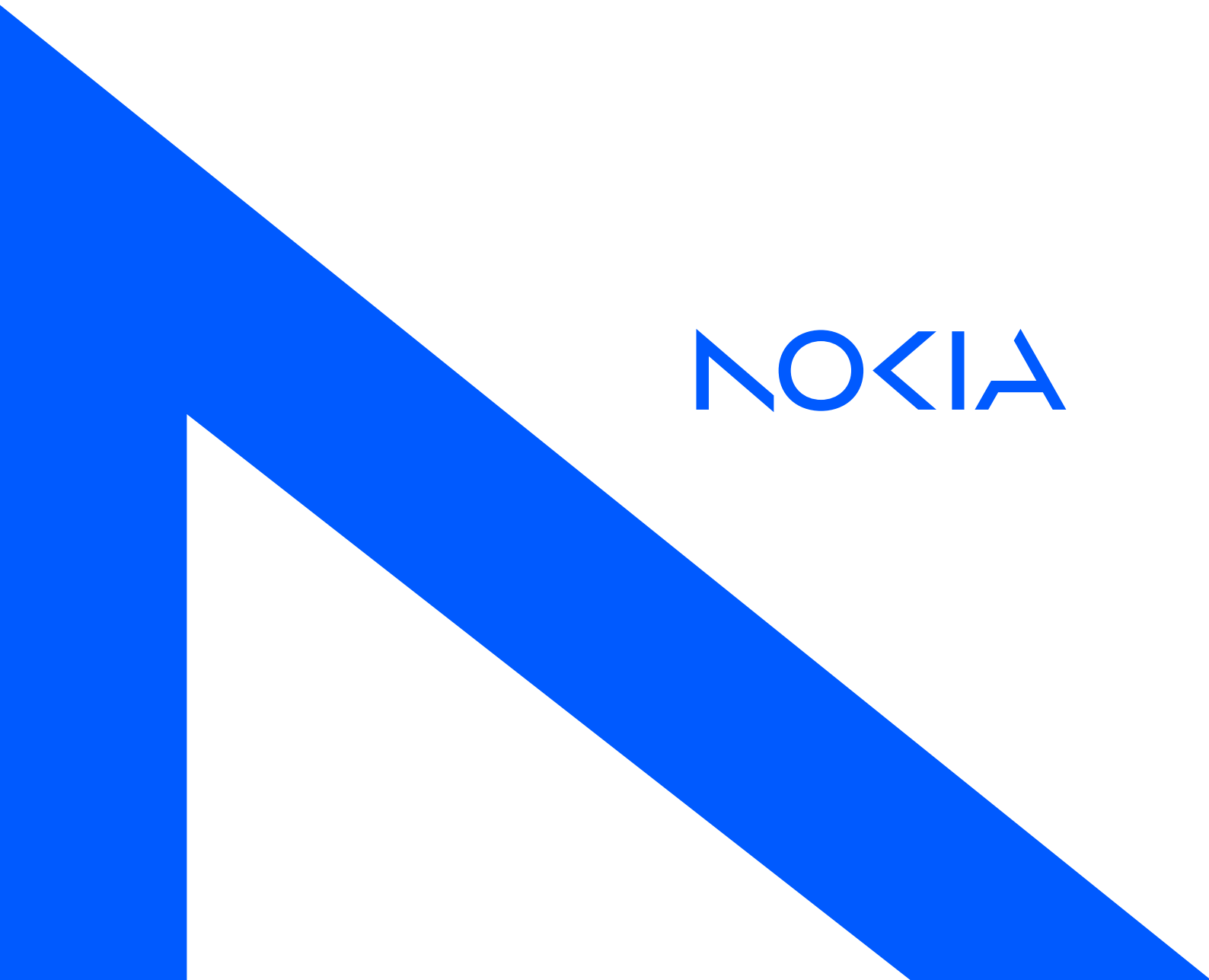
A multilayered, embedded approach to IP network security

A strategy to safeguard business continuity against IP network threats

Application note



Abstract

Networks and data have never been at greater risk. As organizations embrace artificial intelligence (AI) and continued digitalization, they need new IP network security solutions that can stop increasingly sophisticated security threats targeting their networks and data in more ways and more places.

Nokia is addressing this need with a multilayered approach to IP network security. By melding high-performance IP silicon with platform-level security, breakthrough apps and tools within the network operating system (NOS), AI-driven big data security analytics, and quantum-safe cryptography innovation, our approach enables organizations to build scalable, secure and trusted networks that can help you manage risk and mitigate attacks before they impact business continuity.

Contents

Abstract	2
Introduction	4
IP silicon	5
IP trusted systems	6
System security	6
Platform trust	7
Secure product lifecycle	7
Secure supply chain	9
Quantum-safe networks	10
Router NOS applications and tools	12
IPsec Security Gateway	12
Integrated firewalls	13
Enhanced subscriber management	14
AI-driven security analytics and automation	15
From prevention to monetization	16
AI and ML inside Deepfield Defender	17
Summary	19
Abbreviations	20

Introduction

The world is going digital, and petabytes of data traffic now flow across public, private and corporate networks. As organizations apply technologies like AI, cloud, 5G, and quantum computing, IP networks will need to handle even more data.

Technologies such as quantum computing and AI will help unlock the next great innovations. But they will also give threat actors new ways to attack our networks and data. We're already seeing this with AI-powered distributed denial-of-service (DDoS) botnets, emerging quantum computing threats, intricate data breaches, and man-in-the-middle attacks.

Organizations in every industry must prioritize security as they design IP networks for the quantum and AI era. But current security approaches don't offer the scale or functionality you need to tackle bigger, more complex and more frequent threats.

Prioritizing security in the design and support of the many systems the network comprises—especially as the policy and regulatory environment continues to evolve—is at the heart of Nokia's multilayered, embedded approach to IP network security.

Nokia has a deep history in IP networking, security, and technological innovation. We have leveraged this to identify the vector points most fundamental to IP network security. We help organizations prepare for the coming quantum paradigm shift, leveraging in-house Nokia Bell Labs quantum enablement innovation to shield against future threats.

Nokia's IP network security approach yields numerous benefits for IP network operators, including security at scale and enhanced trust in communications systems, along with the security intelligence, analytics and automation to detect and mitigate DDoS attacks in an evolving, AI-driven big data environment.

Figure 1. Our multilayered, embedded approach to IP network security



IP silicon

IP network silicon is vital to IP network security, and the Nokia FP chipset is engineered to safeguard business continuity against the most malicious threats. This is where Nokia's multilayered, embedded approach to IP network security begins, with efficient and high-performance security features prioritized in the IP network infrastructure itself. Integrated line-rate MACsec and enhanced MACsec (ANYsec) network cryptography, secured with AES-256 network encryption, delivers highly scalable, multiterabit, secure and trusted network connectivity.

Figure 2. Integrating security right down to the silicon level



- Line-rate network encryption
- Highly scalable ACL filtering with no performance penalty
- DDoS attack mitigation

Nokia FP silicon provides the filtering scale and performance headroom necessary to be a highly precise attack sensor and mitigation element. Even with the application of hundreds of thousands of ACL filters in FP-based routing platforms, there is no performance impact.

The mitigation aspect of the Nokia DDoS security solution combines packet forwarding capacity and performance with the enhanced packet intelligence and control capabilities of Nokia FP4 and FP5-based routers and an FP5-based dedicated mitigation platform—the 7750 Defender Mitigation System (DMS)—with advanced DDoS countermeasures. Nokia Deepfield Defender acts as a security analytics, detection and mitigation control platform, driving granular, scalable and cost-effective mitigation of all types of DDoS either on the network edge (FP-based routers) or on the 7750 DMS.

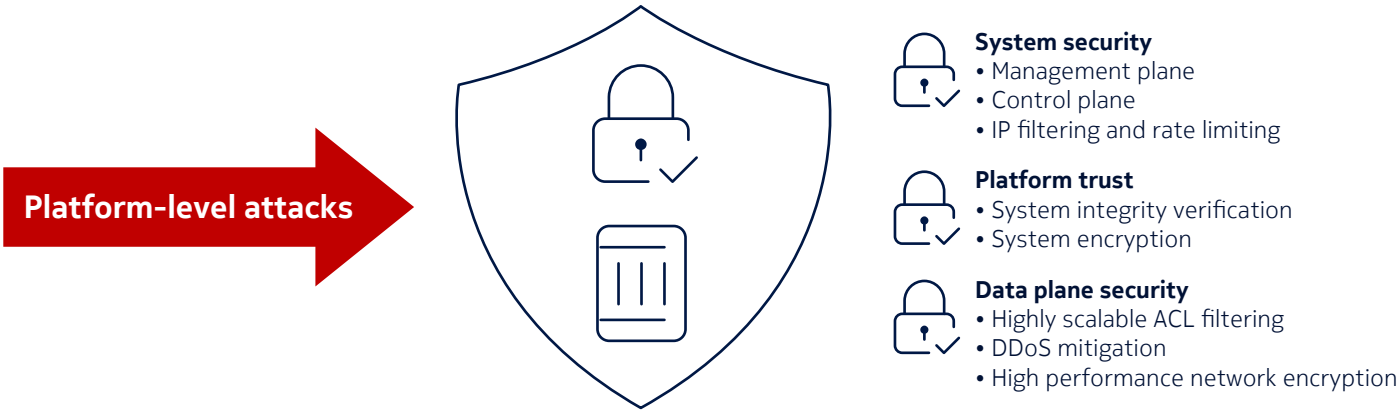
To ensure deterministic network performance and service quality, both mitigation and detection can be used at line rate without impacting the performance of other services running on the same chipset.

IP trusted systems

When an attack strikes at the platform level, Nokia's approach to prioritizing security and trust means that the management, control and data planes are designed with the capabilities and considerations required to both anticipate and withstand these threats.

System security

Figure 3. System security and platform trust



At the management plane, security includes defence against unauthorized access through capabilities such as flexible user authentication, authorization and accounting (AAA); login control; event logging and encrypted management protocols. At the control plane, Nokia implements multiple security controls for routing protocols, such as:

- Authentication (including keys)
- Key chaining
- Database limiting
- Time-to-live (TTL) security
- Prefix limiting
- Origin validation
- Route filtering
- Policies management
- Neighbor disablement

To mitigate a flood of traffic reaching the system control and management planes, Nokia implements multiple levels of queuing, policing and filtering in both distributed and centralized architectures.

Platform trust

Nokia's platform trust is anchored in the pillars of system integrity verification and system encryption.

We implement Secure Boot, which provides a foundation for other platform trust capabilities by ensuring that the software executed by the system originated from Nokia and is trusted.

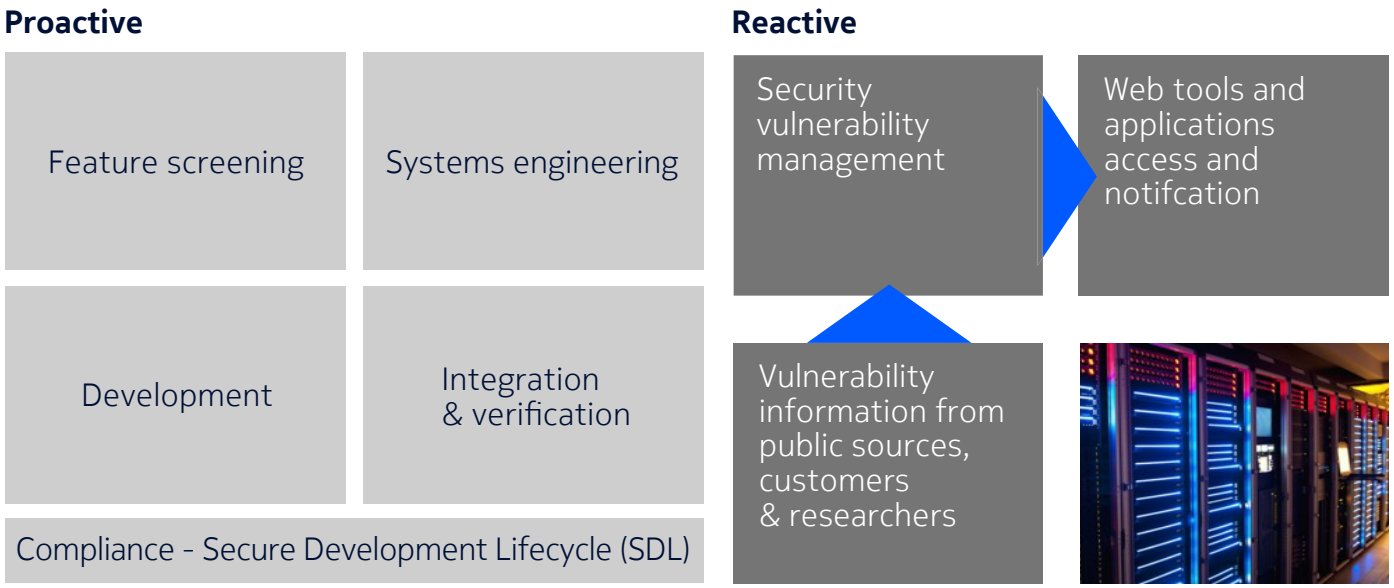
Building on IEEE 802.1AR requirements for device identity keys, the Nokia approach implements Trusted Computing Group (TCG)-compliant Trusted Platform Module (TPM) 2.0 Keys for device identity and attestation. This identity key and certificate are then used in software features to provide cryptographic evidence that the system used by the customer is manufactured by Nokia. One example is secure boot-strapping of the system using secure zero touch provisioning (SZTP), as defined in RFC 8572 and the OpenConfig Bootz protocol.

TPM 2.0 also provides the hardware root of trust for measurement and attestation as well as secure storage for disk cryptographic keys. Measured Boot complements Secure Boot by providing cryptographic evidence that each piece of the system boot chain uses the software version allowed by a customer.

Secure product lifecycle

Nokia approaches planning for security management from both a proactive and reactive point of view. Proactively, Nokia focuses on key elements in the building, coding and testing of our products. Given security events can happen in the field, after products have been deployed in customer environments, the process also reactively identifies and mitigates these risks throughout the secure product lifecycle.

Figure 4. Key components of the security management process



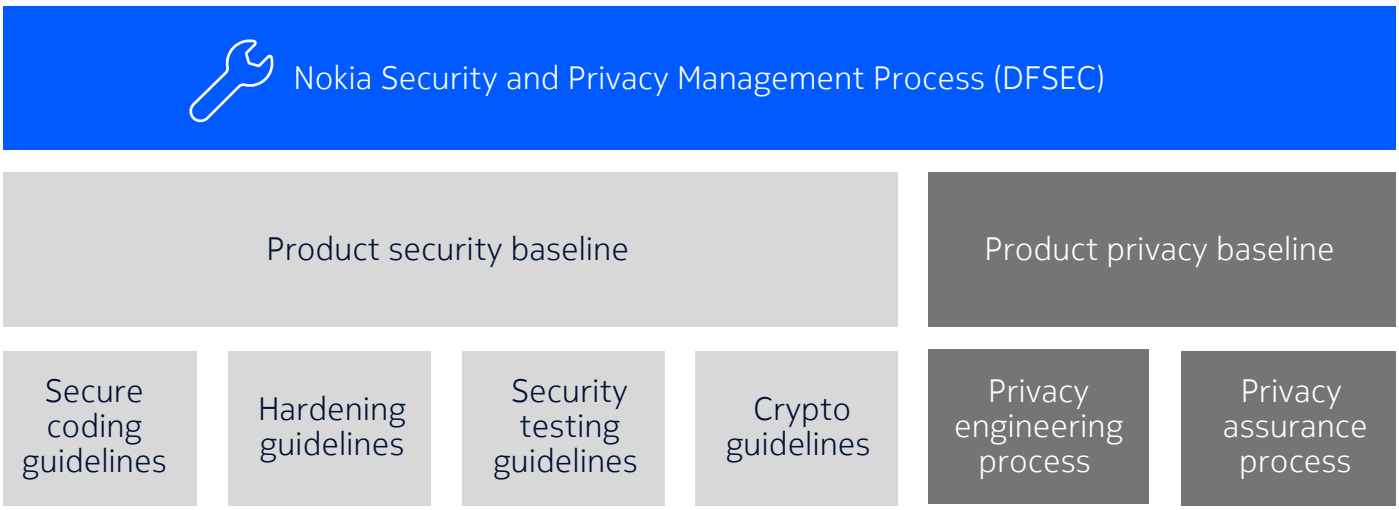
Key components of the security management process

With a focus on the continuous integration and assimilation of industry best practices, standards and regulations, the combination of proactive and reactive Nokia IP network security management involves:

- **Proactive measures:** Feature screening, systems engineering, integration and verification, secure coding and compliance to measure against our secure development lifecycle (SDL) process.
- **Reactive measures:** Vulnerability information from a range of inputs including the computer emergency response team (CERT), assessments and tools, technical alerts, and customer communications.

Nokia's SDL supports the company's security by design culture, continuously assimilating and integrating security best practices, in-house requirements and industry-sourced specifications into both product security and product privacy baselines.

Figure 5. Secure development lifecycle



The product security baseline is tied to process elements and core activities undertaken within the SDL, including:

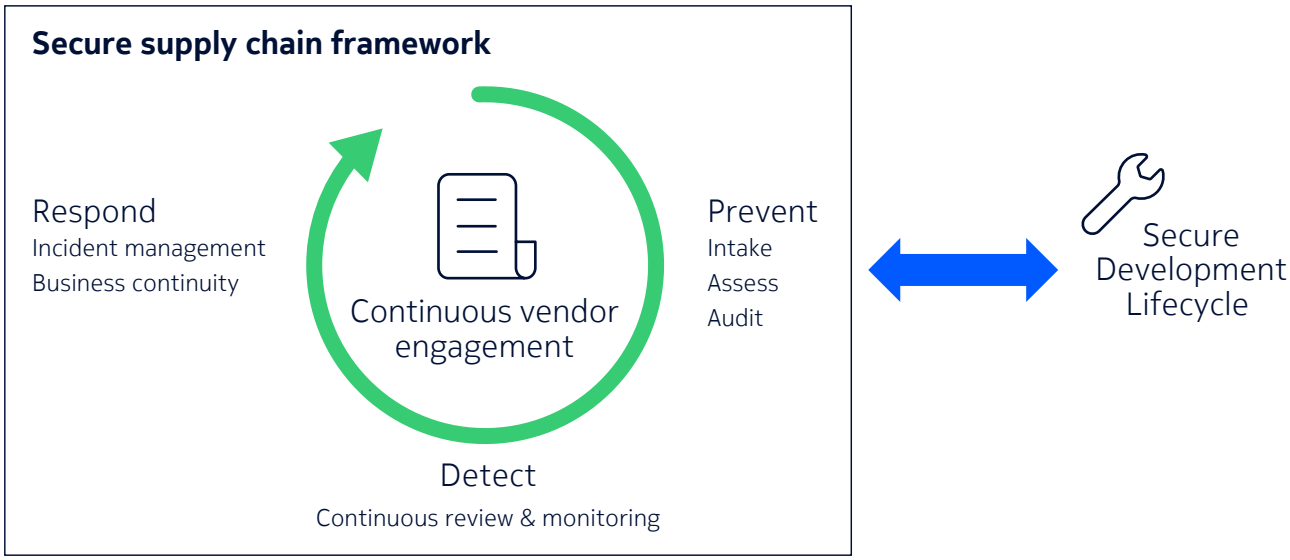
- **Secure coding** guidelines that help developers write secure code in the languages Nokia utilizes in product development
- **Product hardening** to ensure customers do not have to do extra work to make them secure
- **Rigorous security testing** using optimized tools and manual methods to identify product vulnerabilities
- **Crypto guidelines** drawn from industry cybersecurity standards and certifications such as Federal Information Processing Standards (FIPS) and the National Information Assurance Partnership (NIAP)

Nokia's product privacy baseline is founded on the concept that products and software are designed to favor privacy, including securely encrypting collected data.

Secure supply chain

Establishing trusted systems requires that the supply chain from which hardware and software components are sourced is secure as well. Nokia has adopted a strategy of prevention, detection and response to ensure supply chain security is maintained at every point in the relationship.

Figure 6. Secure supply chain framework



Nokia also strictly adheres to a set of oversight and risk management principles. This includes first identifying what needs protection, establishing clear security requirements, understanding supplier security postures and assessing supplier risks.

Security is embedded in the contracting process and upheld by both Nokia and its suppliers.

Raising awareness and training within the supply chain is also critical. New suppliers undergo a comprehensive onboarding process that clearly stipulates Nokia's security requirements around vendor contracts. This is followed by security and privacy vendor risk assessments, along with training on Nokia processes. Once established as a supplier, Nokia conducts regular reviews and continuous monitoring with a focus on ensuring business continuity.

Being prepared to support suppliers during security incidents is crucial as well. An established incident response process is triggered in the event of an issue, with the goal of fast response and resolution.

This structured approach and eye on continuous improvement ensures the company maintains a resilient and trustworthy supply chain, allowing Nokia to build trusted and secure products.

Supplier components are selected for use in our products and further secured through the Nokia SDL and dataflow security (DFSEC) processes.

Quantum-safe networks

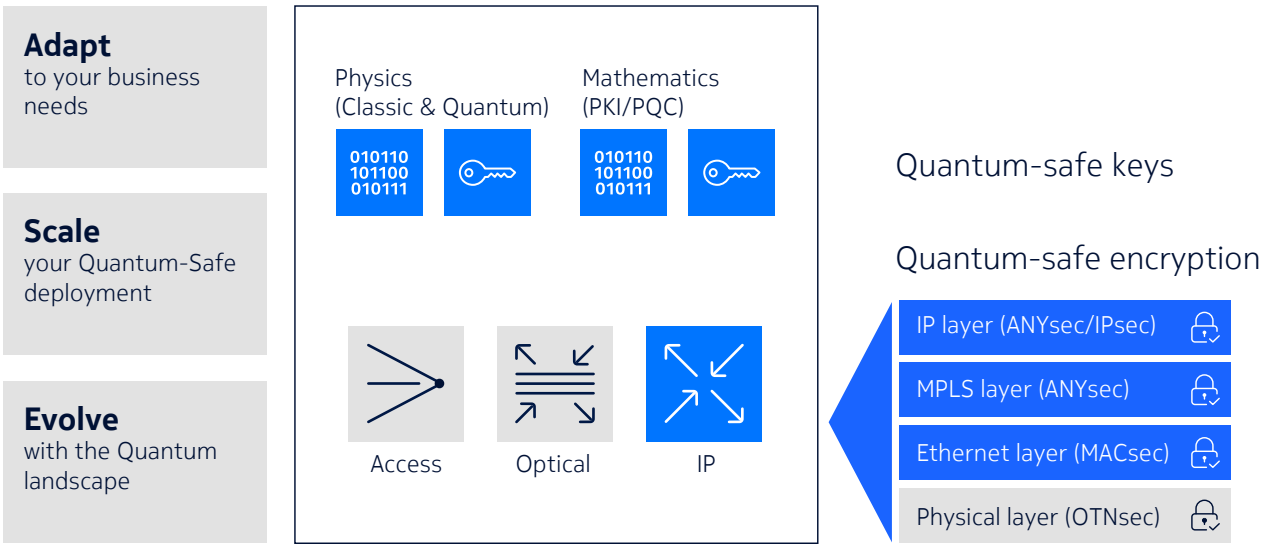
As governments modernize critical infrastructure, enterprises accelerate AI adoption, cloud providers expand global digital platforms and societies become increasingly connected, the network is no longer simply a transport mechanism. It becomes part of the foundation upon which digital trust is established, maintained and protected.

At the same time, a profound technology inflection point is emerging. Advances in quantum computing, artificial intelligence, and cyber threat sophistication are reshaping the security landscape, and it is essential to act now to shield against the quantum migration challenge. While the timeline for a cryptographically relevant quantum computer (CRQC) is uncertain, the cybersecurity migration needed to counter this threat is the largest the information and communication technology (ICT) industry has faced and will require considerable time and effort.

The Nokia IP network security approach is focused on maintaining a digital communications infrastructure that remains secure, reliable and trustworthy.

Called Quantum-Safe Networks (QSN), Nokia's quantum-safe solutions are proven and ready for immediate implementation. At the same time, Nokia Bell Labs is driving continued innovation with key academic and technology partners that will shape the future of quantum-safe network solutions.

Figure 7. Nokia Quantum-Safe Networks

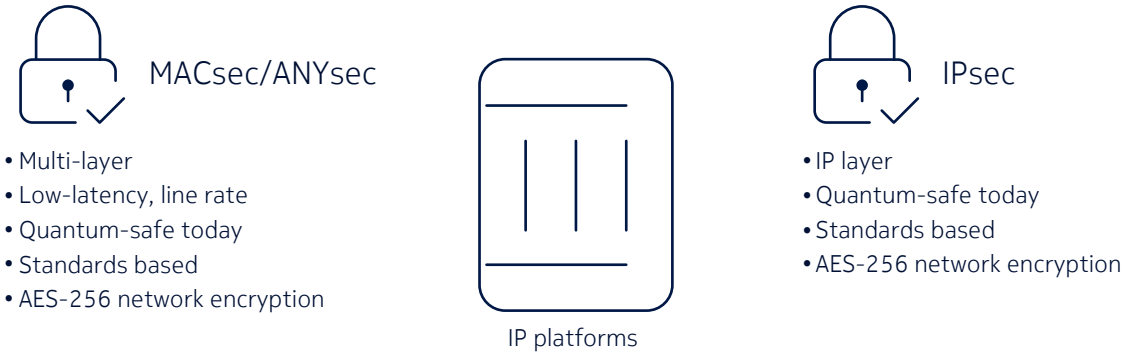


A defence-in-depth approach can deliver quantum-safe security through the appropriate application of quantum-safe IP or optical cryptography. With Nokia QSN, a quantum-safe outcome can be achieved today with the application of one of our quantum-safe IP network cryptography technologies, such as MACsec, enhanced MACsec (ANYsec) or IPsec across a single network layer. If required, a customer may choose to deploy two or more quantum-safe network cryptographic layers in a multilayered approach.

This approach is complementary and helps manage risk in the evolution of application layer cryptography. The approach can be adapted to a customer's business and use case needs, delivers confidence to scale network deployments and supports strategy adjustments as the quantum threat evolves.

By combining crypto-agility and crypto-resiliency in a defence-in-depth approach with advanced quantum-safe cryptography, we create a comprehensive and proactive security posture that can withstand current and future threats, ensuring the security, trust and resilience of our digital infrastructure.

Figure 8. Quantum-safe IP cryptographic technologies



Deployed globally on field-proven IP portfolio

Support for multiple IP cryptographic technologies forms part of our multilayered, defence-in-depth IP cryptography:

- Silicon-based line rate 802.1AE MACsec and 802.1X MACsec Key Agreement (MKA) protocol combined with quantum-safe symmetric cryptographic keys to deliver secure, trusted, quantum-safe Ethernet network connectivity.
- Enhanced 802.1AE/802.1X MKA protocol combined with quantum-safe symmetric cryptographic keys to deliver what Nokia calls ANYsec. Deploy scalable, multilayered security services transparently across existing Ethernet, MPLS, and IP networks with end-to-end or hop-by-hop granularity, speeding the velocity of deployment and delivering quantum-safe network connectivity.
- IPsec capabilities that enable trusted and secure quantum-safe network connectivity, with industry-leading scale, capacity and resiliency to address a range of network and market applications including mobile RAN, core and transport networks, and secure enterprise access and interconnect. Standards-based, Nokia IPsec capabilities include support for transport and tunnel modes along with both public and private services. Quantum-safe today through the support of RFC 8784, the Nokia IPsec cryptographic solution is evolving to incorporate the new post-quantum cryptography (PQC) mathematical algorithms in alignment with the industry.
- Nokia MACsec, enhanced MACsec (ANYsec) and IPsec cryptographic technologies are underpinned by quantum-safe AES-256 block cipher network encryption.

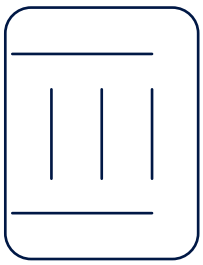
Router NOS applications and tools

As data volumes explode and the number of connected devices proliferates, the urgency around protecting against cyber threats grows. The Nokia IP Network security approach includes several robust options within the Router NOS apps and tools layer that scale and evolve with the threat landscape while safeguarding the high performance and reliability of network infrastructure.

IPsec Security Gateway

Nokia's carrier-grade, router-based IPsec Security Gateway solution inherits the scale, resiliency and security of 7750 SR infrastructure. A single Nokia Secure Gateway can support up to 32,000 macro base stations or 500,000 small cells/femtocells, and up to 3.2 Tbps of encrypted traffic.

Figure 9. IP security gateway



- High throughput
- High scale
- Flexible Resiliency
- System modularity and scalability

7705 SAR
7750 SR
Virtual Service Router

Distributed architecture to deliver industry leading IPsec performance

The solution delivers flexible resiliency, supporting inter-chassis 1:1 or N:M stateful redundancy models and combining system modularity with scalability and a single system IP address to help simplify operational deployment.

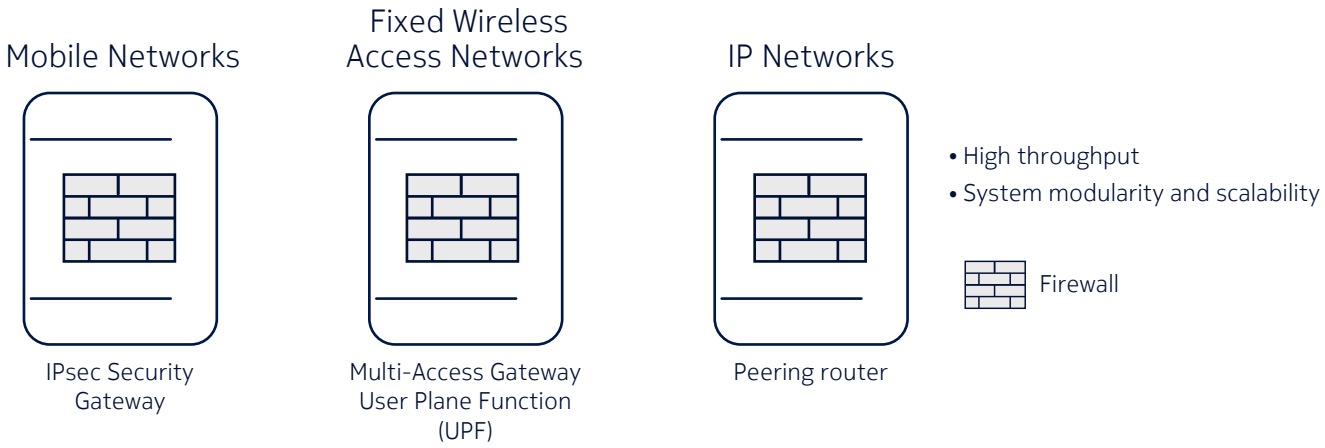
A distributed architecture allows for greater scale, redundancy and flexibility in securing IP networks. The IPsec Security Gateway distributes both the Internet Key Exchange (IKE) control plane traffic and data plane traffic across the system. As well, multicore processors for the IKE process greatly enhance tunnel setup and distribution of data plane traffic across multiple cores, which can increase overall IPsec performance.

The IPsec Security Gateway function can be deployed on the 7750 SR Extended Service Appliance (ESA), 7705 Service Aggregation Router (SAR) and Virtualized Service Router (VSR).

Integrated firewalls

Designed to perform stateful, in-line packet inspection to stop unsolicited traffic from breaching the many secure zones required by today's open, distributed network architectures, Nokia Service Router Operating System (SR OS) firewalls play a central role in Nokia's multilayered IP network defence strategy.

Figure 10. Integrated firewalls



Nokia SR OS-based integrated firewalls sit in-line with traffic and track all sessions flowing into or out of the zone they protect. Flows solicited by legitimate users or applications pass through with rate limiting where required, while traffic not on a firewall's list of solicited flows is blocked. In addition, pinholes can be selectively enabled for trusted unsolicited traffic.

The stateful firewall supports all protocols including Transmission Control Protocol (TCP) and GPRS Tunnelling Protocol (GTP) to discard packets that violate protocol rules and neutralize more complex attacks targeting the control, user, and management planes of network functions and applications.

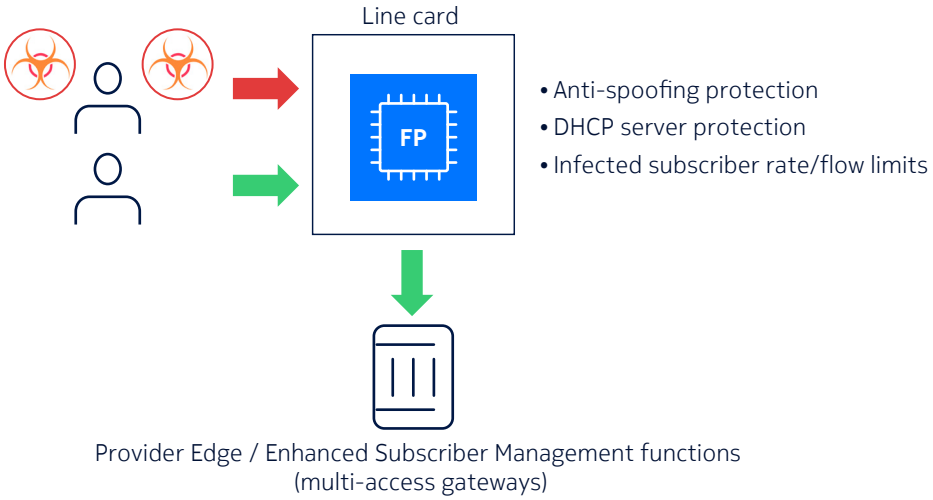
Nokia SR OS firewalls combine high throughput, modularity and scalability, making them well suited to key network locations, including:

- Integrated in the IPsec gateway to perform GTP and Stream Control Transmission Protocol (SCTP) checks and allow operations, administration and maintenance (OAM) traffic
- Integrated with the Multi-Access Gateway user plane function to perform TCP and User Datagram Protocol (UDP) traffic checks
- Integrated with peering routers on partner and roaming links to provide secure zones between a network operator and its partners

The integrated firewall function can be deployed on the 7750 SR ESA and VSR.

Enhanced subscriber management

Figure 11. Enhanced subscriber management



Attacks can also target network-resident services, such as a broadband network gateway (BNG), by pretending to be valid subscribers or users. The Nokia SR OS monitors protocols such as Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) to identify and discard invalid requests that try to bond to the network or that seek to exhaust finite resources such as DHCP sessions.

Integrated unicast reverse path forwarding (uRPF) protection helps mitigate problems caused by the introduction of malformed or forged (spoofed) IP source addresses into the network.

As well, should a provider's subscribers and IoT devices be hijacked and turned against them, FP-equipped routers and gateways have the granularity and power to deflect and control individual subscribers with minimal impact or performance degradation.

AI-driven security analytics and automation

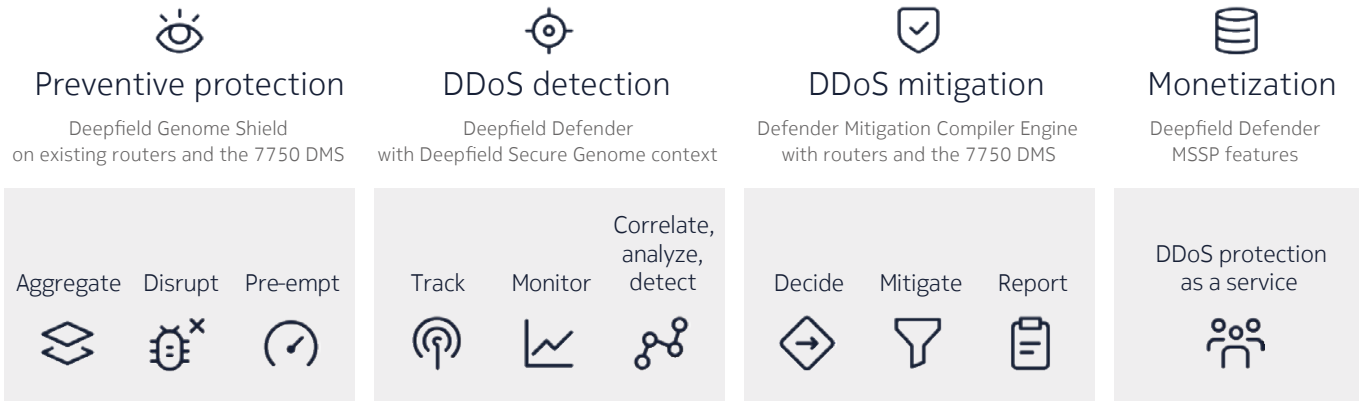
DDoS attacks have become shorter, higher intensity and harder to separate from legitimate traffic. According to the Nokia Threat Intelligence Report 2026, 98% of DDoS attacks end within five minutes, and the median botnet attack lasts only 60 seconds. Residential proxy botnets now draw on an estimated 200 million compromised subscriber devices, so attacks arrive from valid IP addresses, often from inside the provider's own network. Static thresholds, manual response and diversion to distant scrubbing centers cannot keep pace.

Nokia's answer is to make the network itself a shield. The Nokia DDoS security solution combines:

- Nokia Deepfield Defender, an AI/ML-driven platform that detects DDoS attacks, computes the best mitigation strategy and orchestrates it across the network.
- Deepfield Genome Shield, which extends Defender with proactive, always-on and network-wide protection against botnet DDoS.
- Deepfield Secure Genome®, the security map of the internet, which tracks the security context of the internet and is updated hourly.
- Programmable routers as enforcement points, including Nokia 7750 SR and 7250 IXR routers as well as third-party routers (including Juniper and Cisco).
- The FP5-based 7750 Defender Mitigation System (DMS) for the most complex attacks, with up to 2.4 Tbps of mitigation capacity in 3RU.

These components detect all types of DDoS attacks in seconds and mitigate them in-line, with minimal or no impact on legitimate traffic. Operators protect their infrastructure and customers, stop outbound attacks from compromised subscriber devices and turn protection into premium services. The solution is part of the Nokia Deepfield portfolio, with over 160 deployments of Deepfield applications and over 70 deployments of Deepfield Defender.

Figure 12. The Nokia Deepfield DDoS security solution



From prevention to monetization

The Nokia Deepfield DDoS solution covers the attack lifecycle at every stage.

Prevent: proactive protection with Genome Shield

Botnets are built over days and weeks before they attack, and Genome Shield acts in that window. It aggregates threat intelligence from six continuously updated sources, including Secure Genome and the Global DDoS Threat Alliance (GDTA), and transforms it into policies enforced in the data plane of existing routers and the 7750 DMS, with no new appliances. Genome Shield disrupts botnet command-and-control (C2) traffic before attacks launch, pre-positions rate limiting against amplification and volumetric floods, accepts custom policies through open APIs and shows compromised devices and botnet endpoints in observability dashboards.

Detect: big data analytics with internet-wide context

Defender builds peacetime traffic models from flow records, sampled port mirroring (SPM) and Border Gateway Protocol (BGP) and Domain Name System (DNS) data and raises alerts within seconds. Secure Genome adds context for more than five billion IPv4 and IPv6 addresses, updated hourly, so Defender can separate attack traffic from similar-looking legitimate traffic, reducing false positives and false negatives.

Mitigate: the network is the shield

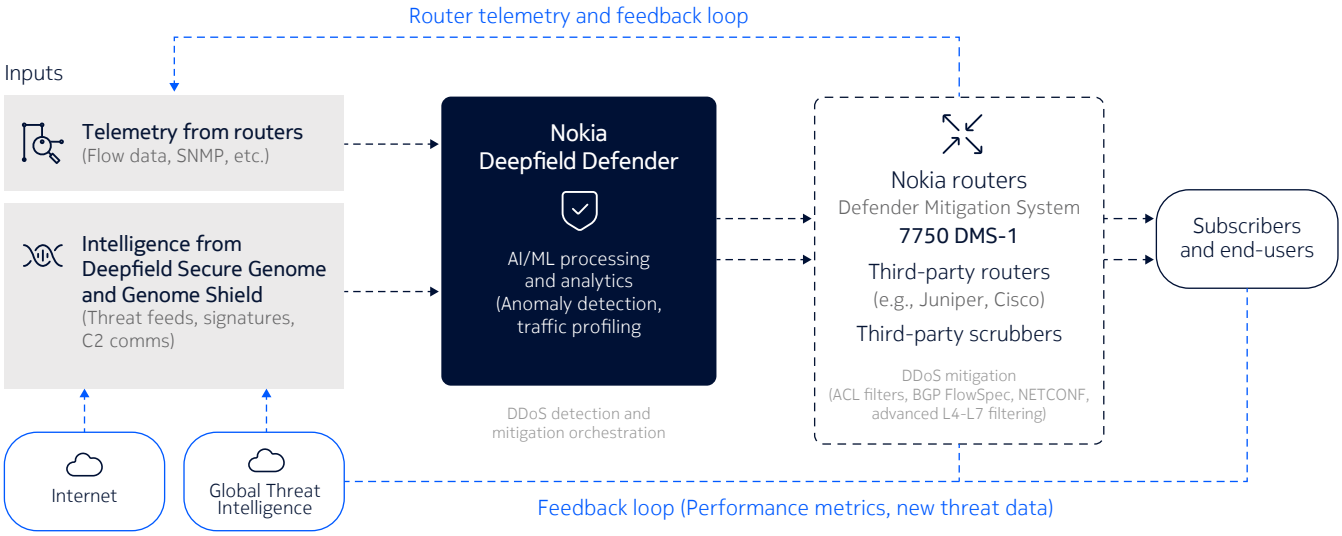
Defender's Mitigation Compiler Engine (MCE) uses AI-based decision trees and deep learning models to com-pute, in seconds, the optimal strategy against one or many concurrent attacks, based on the mitigation re-sources available. It programs countermeasures directly into the network through NETCONF, BGP FlowSpec and remotely triggered black hole (RTBH) filtering. Routers filter volumetric floods at the edge, and the 7750 DMS handles complex botnet and application-layer attacks with L4–L7 stateful inspection. Attack traffic is not back-hauled to an external scrubbing center.

This network-based approach outperforms legacy appliance- and deep packet inspection (DPI)-based defenses on detection accuracy, speed, scale and cost.

Monetize: from cost center to profit center

Because the provider sits upstream of every customer, it can stop attacks before they saturate an access link. Defender's optional managed security service provider (MSSP) features support DDoS protection as a service (DDoS-PaaS), with tiered service levels, a customer portal with attack views and reports, multitenancy, APIs, and automated provisioning.

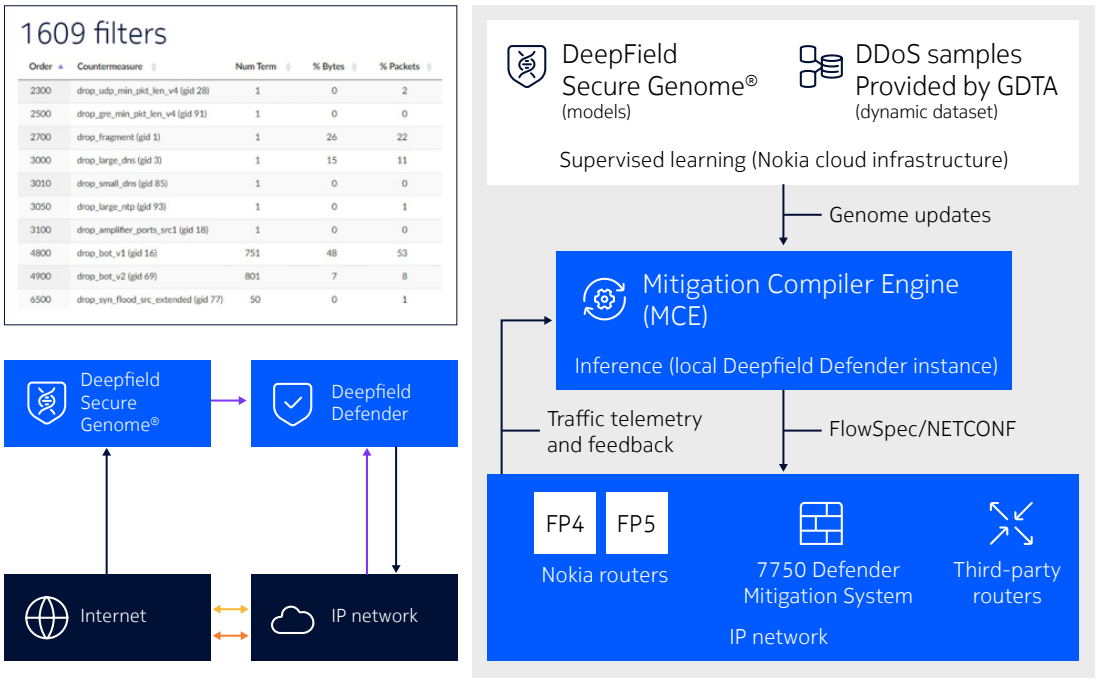
Figure 13. Complete DDoS security: from prevention to monetization



AI and ML inside Deepfield Defender

- **Supervised learning** models trained on the Deepfield DDoS Library of more than 10,000 real-world attack samples detect and classify known attacks in real time.
- **Unsupervised learning** identifies unknown and zero-day attacks by spotting traffic anomalies.
- **Local inference** allows the MCE to run these models inside the operator's own Defender instance.
- **Deepfield Model Language (DML)** defines security policies once and applies them across routers and filter-ing appliances.
- **Secure Genome allow lists and block lists** filter out malicious sources while letting legitimate look-alike traffic pass.

Figure 14. Network-optimized mitigation



Mitigation Compiler Engine (MCE)

- Inference from Deepfield Secure Genome ML models (trained on 10K+ real-world attack samples
- Generates optimized mitigation strategies for complex DDoS attacks
- Effective against know DDoS and emerging vectors

The Nokia Deepfield Emergency Response Team (ERT) supports customers during incidents, and the opt-in GDTA shares threat data that strengthens Secure Genome. Several global service providers, hosting companies and IXPs run the solution in production, including K2 Telecom, Cinia, Hetzner, NL-ix and ESpanix.

Summary

With the world's networks and data more at risk than ever before, a comprehensive strategy is required. Adopting Nokia's multilayered, embedded approach to IP network security can protect both IP network infrastructure and content, ensuring:

- Scalable and efficient protection provided for network systems, customers and data.
- IP trusted systems with system security and trust, with a secure lifecycle to deliver security at scale.
- Quantum-safe IP communications are delivered securely at network scale with high service performance.
- Automated, AI-driven DDoS protection that stops the biggest threats.

By prioritizing security in the design and support of the many systems the network comprises, the Nokia IP network security approach ensures organizations maintain a digital communications infrastructure that is secure, reliable and trustworthy for consumers, enterprises, mission-critical infrastructure builders and telecommunication providers.

Abbreviations

AAA	Authentication, authorization and accounting
ARP	Address Resolution Protocol
AI	Artificial intelligence
BGP	Border Gateway Protocol
BNG	Broadband network gateway
CERT	Computer emergency response team
CRQC	Cryptographically relevant quantum computer
DDoS	Distributed denial of service
DDoS-PaaS	DDoS protection as a service
DML	Deepfield Model Language
DFSEC	Dataflow security
DHCP	Dynamic Host Configuration Protocol
DMS	Defender Mitigation System
DNS	Domain Name System
DPI	Deep packet inspection
ERT	Emergency response team
ESA	Extended Services Appliance
FIPS	Federal Information Processing Standards
GDTA	Global DDoS Threat Alliance
GTP	GPRS Tunnelling Protocol
ICT	Information and communication technology
IS-IS	Intermediate system to intermediate system
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
MSSP	Managed security service provider
MCE	Mitigation Compiler Engine
ML	Machine learning
MKA	MACsec Key Agreement
NIAP	National Information Assurance Partnership
NETCONF	Network Configuration Protocol
NOS	Network operating system
OSPF	Open Shortest Path First

OAM	Operations, administration and maintenance
PQC	Post-quantum cryptography
QSN	Quantum-Safe Networks
RTBH	Remotely triggered black hole
SAR	Service Aggregation Router
SPM	Sampled port mirroring
SDL	Secure development lifecycle
SCTP	Stream Control Transmission Protocol
SZTP	Secure zero trust provisioning
TTL	Time-to-live
TCP	Transmission Control Protocol
TCG	Trusted Computing Group
TPM	Trusted Platform Module
RPF	Reverse path forwarding
uRPF	Unicast reverse path forwarding
UDP	User Datagram Protocol
VSR	Virtualized Service Router

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..

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2026 Nokia

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

Document code: CID214929 (November)