Nokia Secure Data Center Networking

Fortify, validate and drive trust into data center networking infrastructures

NOKIA

Introduction

In an era dominated by artificial intelligence (AI)-driven workloads, cloud migrations and escalating cyber threats, data center network security stands as a critical pillar for organizational resilience. Data center networks, from leaf-spine topologies in the fabric to various IP and optical interconnection capabilities in the data center gateway, enable high-performance connectivity but also expose critical security vulnerabilities.

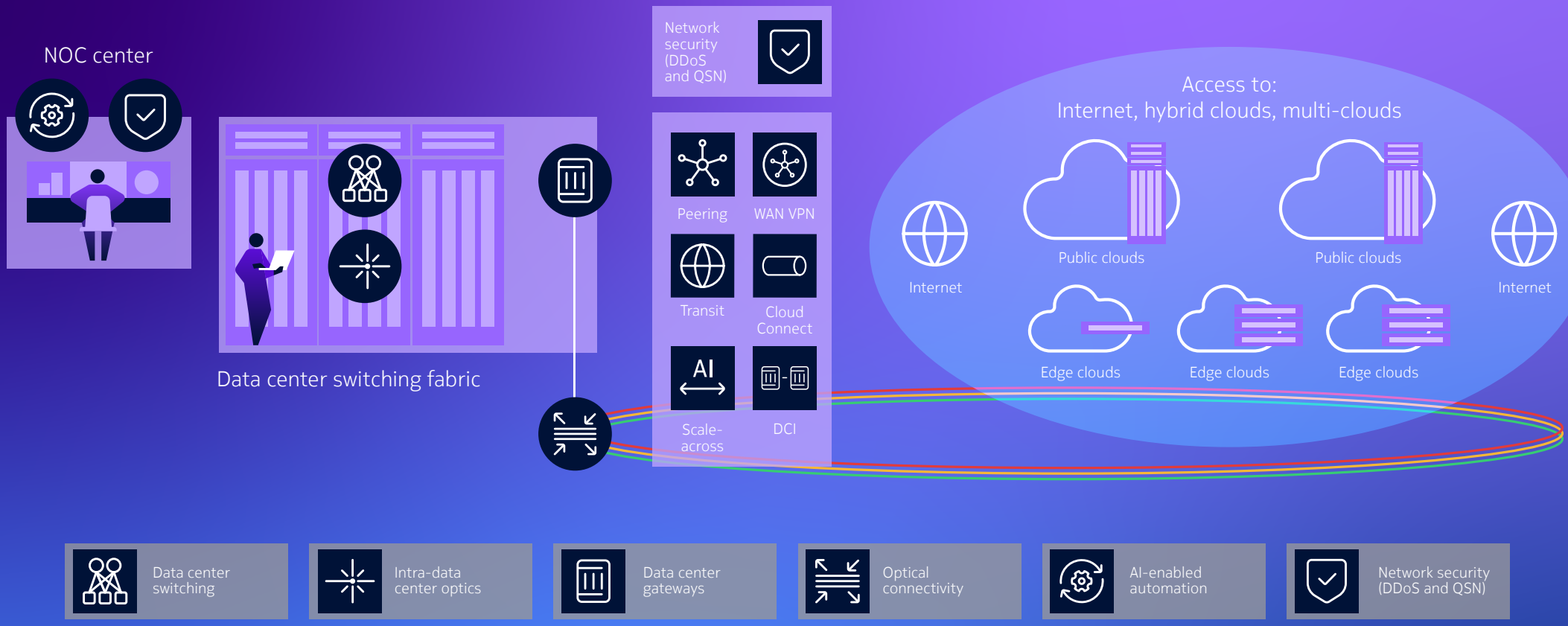
Data center networks face a sophisticated array of threats that exploit their high interconnectivity and scale. Topping the list are advanced persistent threats (APTs), which involve targeted, prolonged attacks that infiltrate networks undetected, often leveraging vulnerabilities in switches or overlays to establish footholds. Ransomware follows closely, encrypting data and disrupting operations. Flattened network structures enable ransomware to spread quickly if they are not segmented properly. Malicious and accidental threats pose internal risks to the network because employees or contractors with access can bypass perimeters.

Migration from older legacy security techniques to keep pace with the new threat landscape is no longer optional. It is a strategic imperative for resilience in an era of pervasive threats, distributed workloads and increasing regulatory scrutiny.

This brochure discusses key threats, best practices and emerging technologies, drawing on industry insights to provide actionable recommendations for keeping data center networks secure. By implementing segmentation, zero-trust models and automated defenses, organizations like yours can fortify their data center networks against breaches to ensure efficiency and compliance. With proactive, integrated strategies and solutions that prioritize security, you can stop threats and avoid catastrophic data loss and operational downtime.

Security challenges in data center networks

- AI, cloud and massive volumes of east–west traffic are reshaping data center networks and exposing new security gaps.
- Attackers now target the network fabric itself, exploiting lateral movement and control plane weaknesses.
- Failures within AI data centers are measured in service outages. They are also measured according to their economic impact, such as cost sunk and wasted GPU processing time and power consumed.
- Edge cloud, hybrid cloud and multi-cloud connectivity expands the attack surface and makes consistent policy enforcement more difficult.
- Perimeter-based security no longer scales, leaving east–west traffic largely unprotected.
- A single data center network breach can have a major business impact by disrupting services, violating compliance and causing lasting financial and brand damage.



Data center switching

Intra-data center optics

Data center gateways

Optical connectivity

AI-enabled automation

Network security (DDoS and QSN)

The new security reality of data center networking

Modern data center networks must be designed as unified, end-to-end systems that have security and trust built in, not bolted on.

Protection must span your entire network continuum, from the high-performance data center switching fabric that carries east–west traffic to the routing and interconnection layers that link data center and clouds though internet connectivity and other WAN technologies.

By embedding security directly into your network and extending consistent policy, segmentation and encryption across hybrid and multi-cloud environments, you can eliminate trust gaps and reduce operational risk. Centralized, cloud-based automation provides end-to-end visibility, policy orchestration and real time analytics. These capabilities ensure that security remains consistent, adaptive and scalable as workloads evolve.

This holistic architecture provides a resilient, automated and intrinsically secure foundation for modern applications, cloud adoption and AI-driven workloads.

The security approach that sets you apart

The shift to cloud-enabled, and AI-driven data center networks presents a unique opportunity to rethink security. By moving beyond perimeter-based models and embedding security directly into the network fabric, you can reduce risk and improve agility and resilience.

To deliver the standout security that data center fabrics need in the cloud and AI era, you need to:

- Fortify your data center fabric with modern security measures that brings together zero-trust microsegmentation, firewalls and trusted systems.
- Validate by proactively adopting automation and real-time visibility so that your security approach can adapt as workloads change—limiting blast radius, closing trust gaps and strengthening defenses against known and emerging threats. The result is a simpler, more resilient and highly secure foundation.
- Drive trust by enabling confidentiality at scale across your data center networking environment. This means protecting internal and external communications and extending this protection across your WAN to the cloud ecosystem.

Fortify the data center fabric

We help you fortify your data center fabrics with comprehensive, embedded security solutions designed to mee the demands of today's complex networks.

Embedded threat mitigation:
We create a zero-trust segmented fabric where microsegmentation handles the dominant east–west traffic with granular, distributed policy enforcement. While firewalls provide north-south flow protection.

Resilient network foundation:
Our solutions ensure the integrity and availability of your vital network infrastructure by safeguarding it against disruptions and maintaining business continuity.

Holistic security ecosystem:
We provide holistic protection by integrating robust security measures across the entire network lifecycle and collaborating with partners for a unified defense.

Trusted compliance and assurance:
We help you meet stringent regulatory requirements and industry standards in ways that build trust and ensure operational integrity.

Key fortification tools

Microsegmentation and firewalls

The Nokia SR Linux network operating system (NOS) implements microsegmentation, a security approach that divides your data center network into fine-grained, policy-controlled segments so that traffic can be explicitly authorized and policies enforced between individual workloads. This enables a true zero-trust fabric, where microsegmentation secures dominant east–west traffic through distributed, line rate policy enforcement, complemented by firewalls for deep inspection of north–south flows.

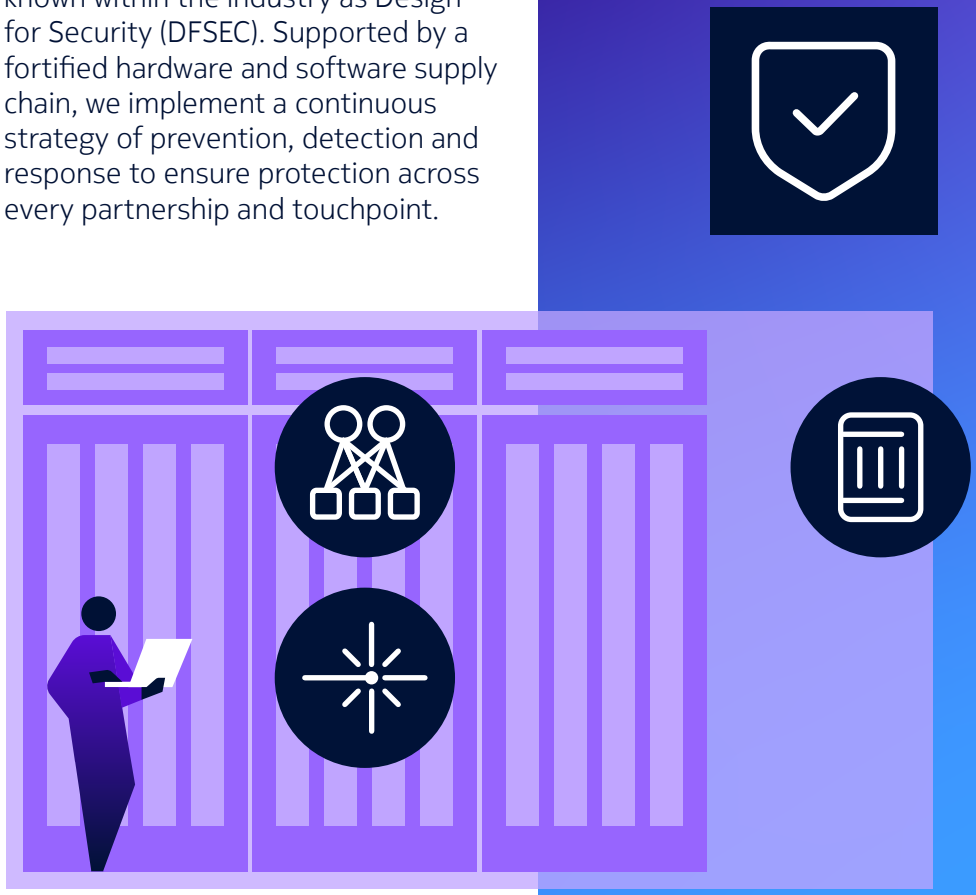
By enforcing policy natively inside your switching fabric, microsegmentation eliminates the need to hairpin internal traffic through centralized firewalls. Together, microsegmentation and firewalls create a complementary security model. The firewalls provide deep visibility and threat prevention at boundaries and chokepoints, while microsegmentation delivers scalable, distributed enforcement across every workload.

This approach limits lateral threat movement, contains ransomware, simplifies regulatory compliance and scales seamlessly across hybrid and cloud environments. Regulations such as General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI-DSS) are easier to meet through verifiable workload isolation and audit-ready controls.

System-level protection

Our IP trusted systems approach includes robust system security that protects management and control planes by preventing unauthorized access and securing routing interfaces. It helps you drive platform trust through advanced system integrity verification and encryption, including secure and measured boot, runtime hardening and application signing alongside Trusted Computing Group (TCG)-compliant TPM 2.0 Keys for reinforced device identity and attestation capabilities.

We support a secure product lifecycle that encompasses proactive and reactive measures in a secure development lifecycle (SDL) approach, known within the industry as Design for Security (DFSEC). Supported by a fortified hardware and software supply chain, we implement a continuous strategy of prevention, detection and response to ensure protection across every partnership and touchpoint.



Validate with a proactive, automated defense

Our AIOps-driven strategy empowers you to neutralize threats before they impact operations. This ensures a robust and resilient digital infrastructure.

From insight to intervention
We help you shift from reactive incident response to proactive threat mitigation by leveraging advanced intelligence to prevent attacks before they materialize.

Comprehensive threat visibility
Our solutions provide a unified view of your entire network. They identify vulnerabilities and emerging threats across all domains, from core to edge.

Automated, adaptive security
You can use our solutions to implement intelligent, automated defense mechanisms that continuously adapt to evolving threat landscapes to minimize manual intervention and response times.

Business continuity and resilience
Our solutions safeguard your critical services and data, ensuring uninterrupted operations and maintaining trust through a highly resilient and secure network environment.

Key validation tools

An open, scalable telemetry framework

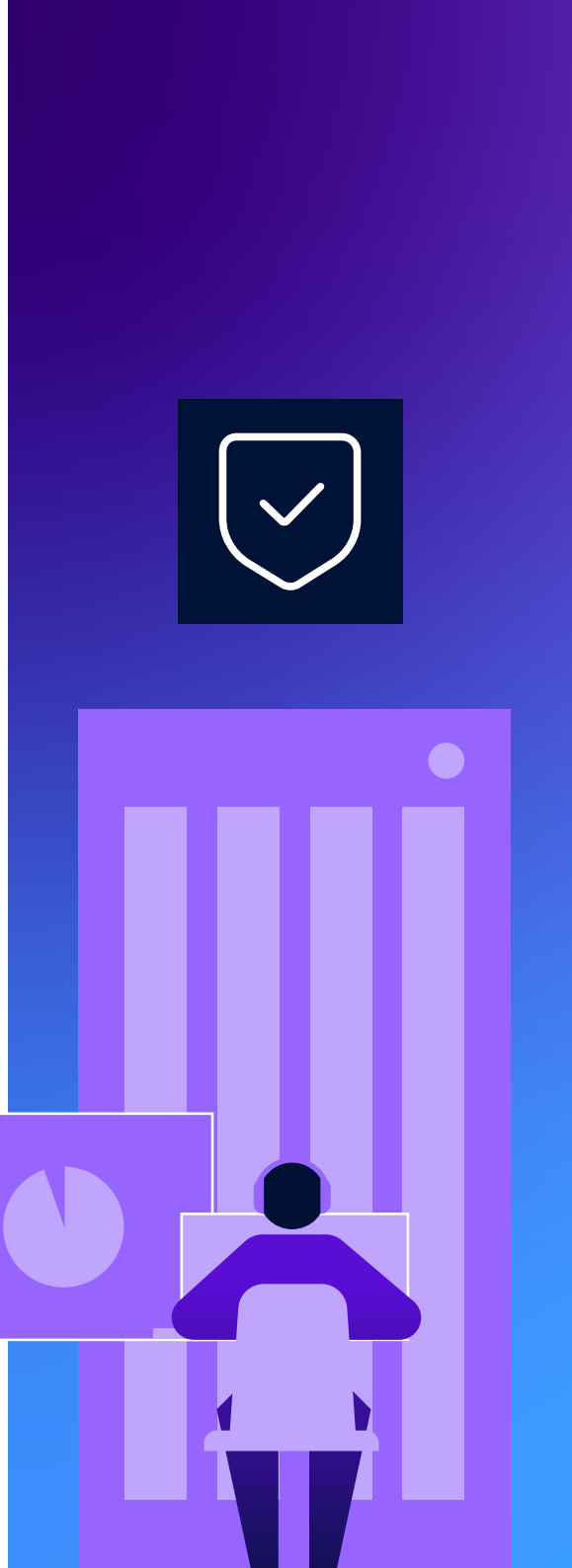
Nokia SR Linux NOS provides an open and scalable telemetry framework that leverages on-change streaming telemetry, including state, to provide new levels of network visibility. The data center fabric acts as a sensor, delivering granular streaming telemetry to provide visibility of security events, anomalies, counters and thresholds, as they happen in near real-time.

Intent-based security automation

Security telemetry can be directly exported to defined security tools or collected by Nokia Event-Driven Automation (EDA) platform. The EDA platform allows for customization to address specific security needs and/or integrate with a rich ecosystem of security tools. It also includes a digital twin that lets you use intent-based security automation to validate policy changes before rolling them out to reduce risk and maximize operational continuity.

Actionable network intelligence and security automation

Nokia Deepfield is an AI-driven, big data software analytics platform purpose-built for the cloud and AI era. It allows you to extend real-time visibility and autonomous security across IP networks.



Drive trust with confidentiality at scale

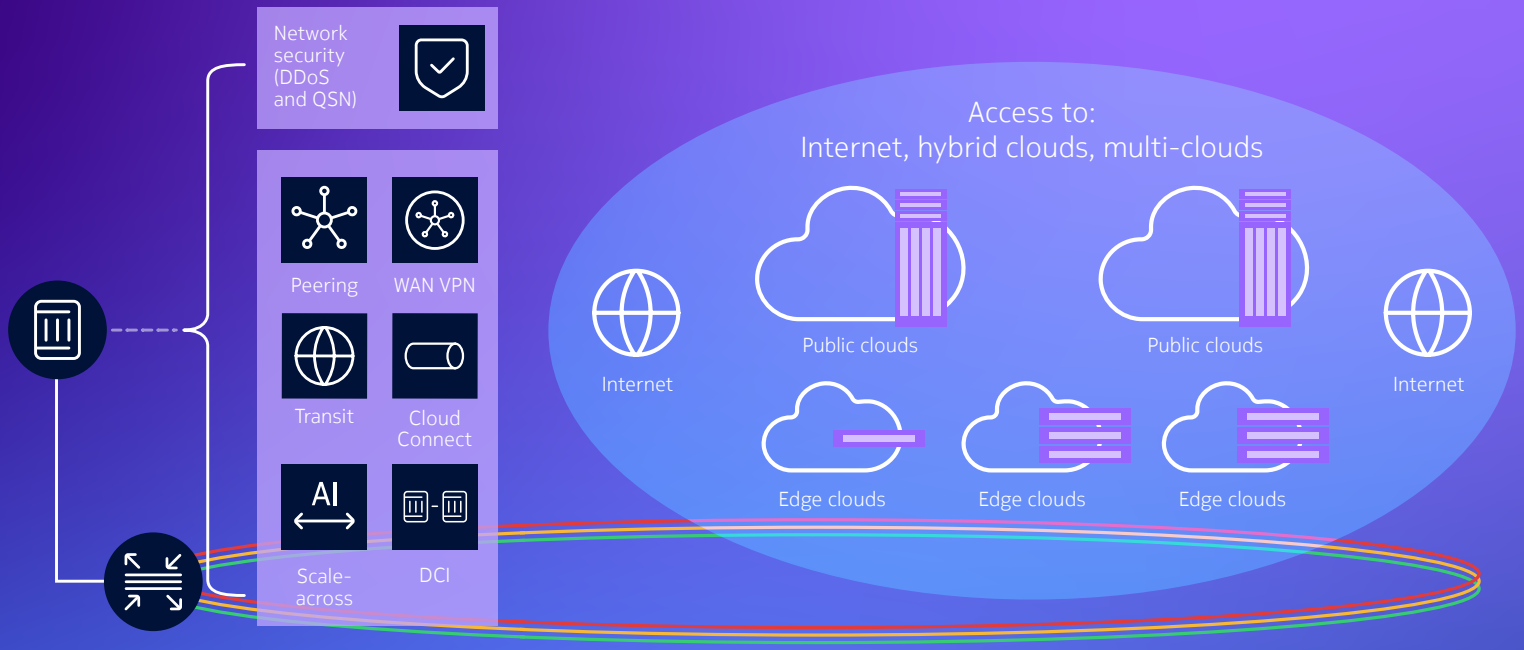
For today's data-intensive and AI-driven applications, ensuring confidentiality at scale is a technical challenge and a strategic imperative for organizations seeking trust and compliance across the fabric, WAN and clouds.

Managing complexity
Our solutions help you maintain data confidentiality, integrity and availability as data volumes grow and your operational environments become increasingly distributed.

Proactive data protection
We help you implement comprehensive, quantum-safe networking and DDoS protection to safeguard the confidentiality and integrity of sensitive data communications between fabric locations.

Trust and compliance
You can rely on our solutions to uphold stringent regulatory requirements and foster customer confidence through demonstrably secure and trusted AI and cloud services.

Strategic investment for future resilience
We help you prioritize investment in advanced confidentiality technologies and methodologies to mitigate risks, ensure business continuity and secure a competitive edge



Key tools for building trust

Data center gateway

Our Data Center Gateway enables you to scale and simplify integration and security between data center fabrics and clouds across the WAN. This includes support for interconnection over IP, MPLS (LDP, RSVP, SR-MPLS) or SRv6 tunnels in the WAN.

The Data Center Gateway also provides seamless interworking for resilient services such as EVPN to IP-VPN/VPLS. and offers the option to encrypt traffic when it exits the data center fabric while preserving the different classes of service.

Quantum-safe networking and DDoS protection

We provide a choice of quantum-safe cryptographic technologies, including OTNSec, MACsec, enhanced MACsec (ANYsec) or IPsec, to meet diverse business and operational requirements.

For IP peering applications, we offer advanced AI-driven DDoS protection from a modular appliance that can be configured inline to the traffic or offline, as with a scrubbing center.

We can consolidate the border leaf and Provider Edge (PE) router into one powerful, trusted, resilient and scalable system that provides a foundation for simpler operations and lower costs.

Realize the potential of a secure data center network you can trust

The evolution of data center networks from isolated, static infrastructures to highly interconnected, cloud-enabled platforms present a critical inflection point for security architecture. Moving beyond legacy models that rely on implicit trust, Nokia Secure Data Center Networking offers a transformative vision for protecting data centers against new and emerging threats.

By integrating security as an intrinsic, distributed and automated capability across the entire data center networking ecosystem—from the fabric to interconnection routing, cloud networking, and management platforms—we enable you to build resilient, adaptive networks that proactively neutralize threats and safeguard critical services.

Our approach, built on the pillars of Fortify, Validate and Trust, delivers comprehensive protection and ensures future resilience. We fortify the data center network with zero-trust segmentation and embedded threat mitigation, while our AIOps-driven strategy empowers proactive defense through enhanced tools and automation, shifting from reactive incident response to intelligent threat mitigation. By prioritizing confidentiality at scale, including quantum-safe end-to-end measures, we help you meet stringent regulatory requirements, build unwavering trust and secure a competitive edge in today's dynamic AI and digital landscape.

Find out more

Your exploration doesn't have to end here. If you want to dive deeper into the innovations shaping the future of data center networks, our **Data Center Networks** resource hub is a great place to start.

If you have questions or would like to explore these capabilities further, our team is here to help.

Connect with your Nokia sales representative to continue the conversation and discover how we can support your data center network evolution.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID: 215426 (July)

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.