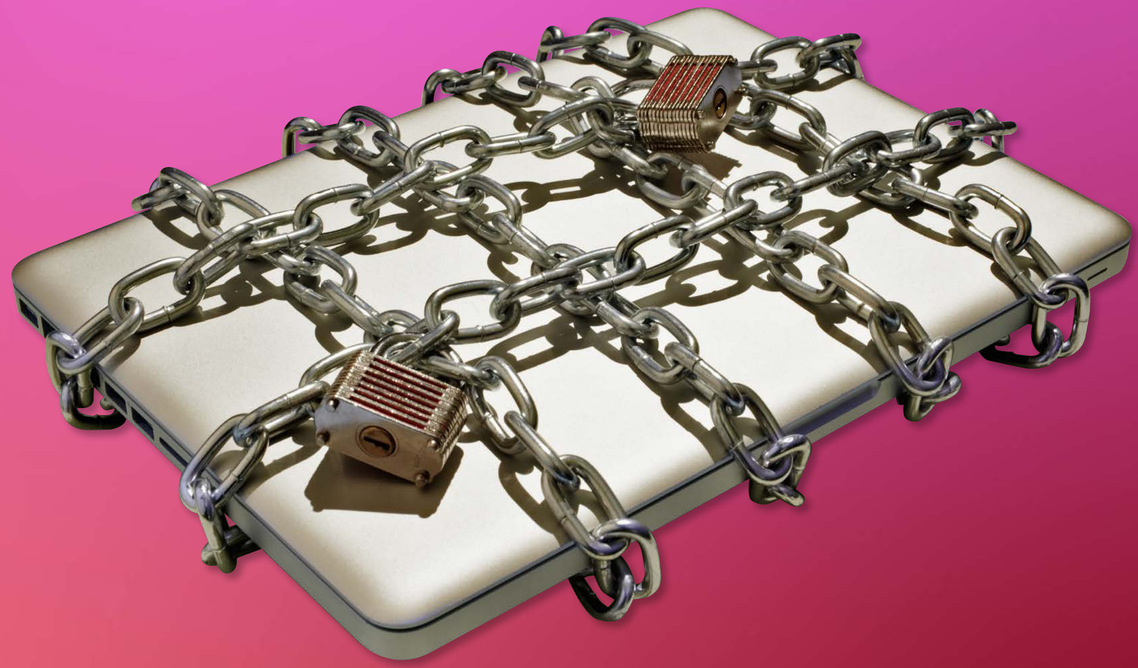
It’s time for a cyber-defense deep dive

NOKIA

Contents



Revamping telco security for a cloud native world

5G and the telco cloud enable exciting new services for customers that can boost communications service provider (CSP) revenue, as well as help to improve their operational efficiency. Yet, virtualized environments and open-source technologies also create new vulnerabilities that cyber criminals will look to exploit.

Nothing less than a transformation of telco security is needed by adopting modern practices like Zero Trust, Defense-in-Depth and DevSecOps.

Why does going cloud-native call for an overhaul of telco security?

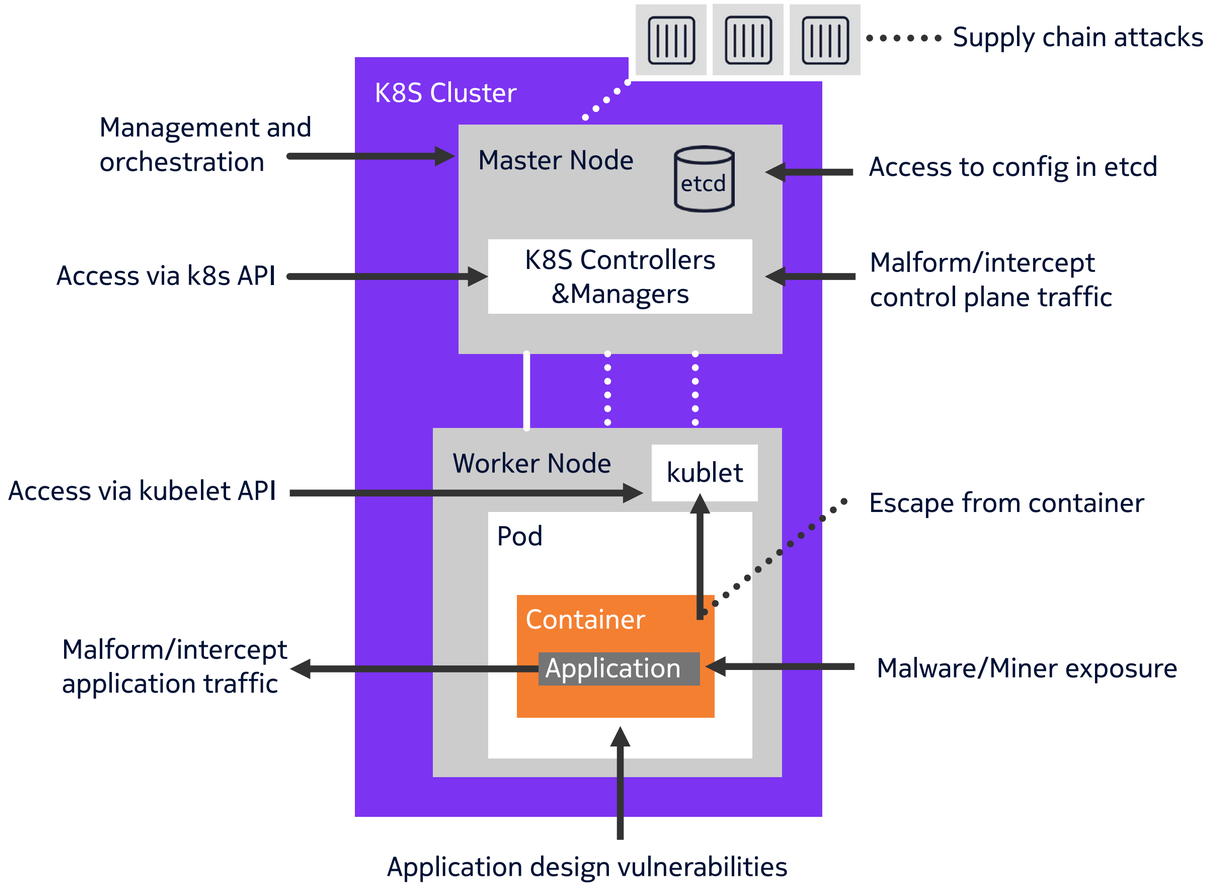
5G is ushering in new approaches. 5G network functions are being virtualized and “cloudified”, making cloud security a major consideration. Telco network functions are deployed in cloud-native environments which are managed differently and use different open-source tools for container and application lifecycle management.

Containerized Network Functions (CNFs) running on generic IT infrastructure and edge compute resources widen the so-called “attack surface”, while the closer convergence of telco and IT networks creates other vulnerabilities.

Why traditional security falls short in a cloud-native world

Relying solely on perimeter protection to keep threats out is no longer valid. That's because the method disregards internal threats, whether from malicious employees, identity spoofing or simple human error. For example, containers can easily be misconfigured, increasing the level of risk. Nor do conventional approaches consider machine-to-machine communication and complex automation, which cannot be trusted by default.

Instead, CSPs can protect their businesses by adopting Zero Trust principles.

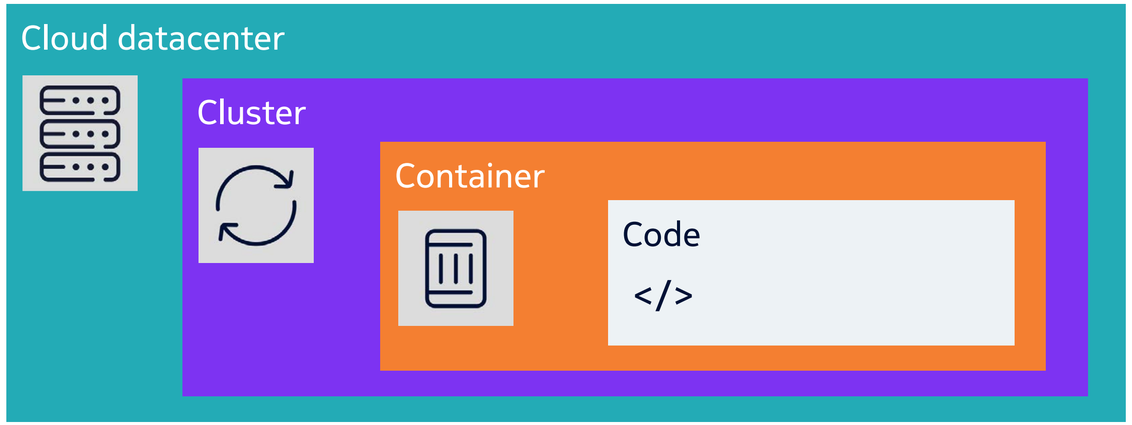


The many vulnerabilities surrounding containerized network function development

A harsh new reality - trust nothing and no one

Zero Trust means there is no such thing as a trust status for anything in the network - traffic, machines, devices and people. Since nothing is trusted, controls must be implemented.

At the heart of Zero Trust is defense-in-depth, which deploys multiple security controls in layers to eliminate or mitigate threats. This is the principle behind cloud-native security which implements security in four main layers:



The four layers of cloud-native security

Cloud data center security which encompasses physical and virtual means to protect a data center

Cluster security which protects customer data as application workloads are run

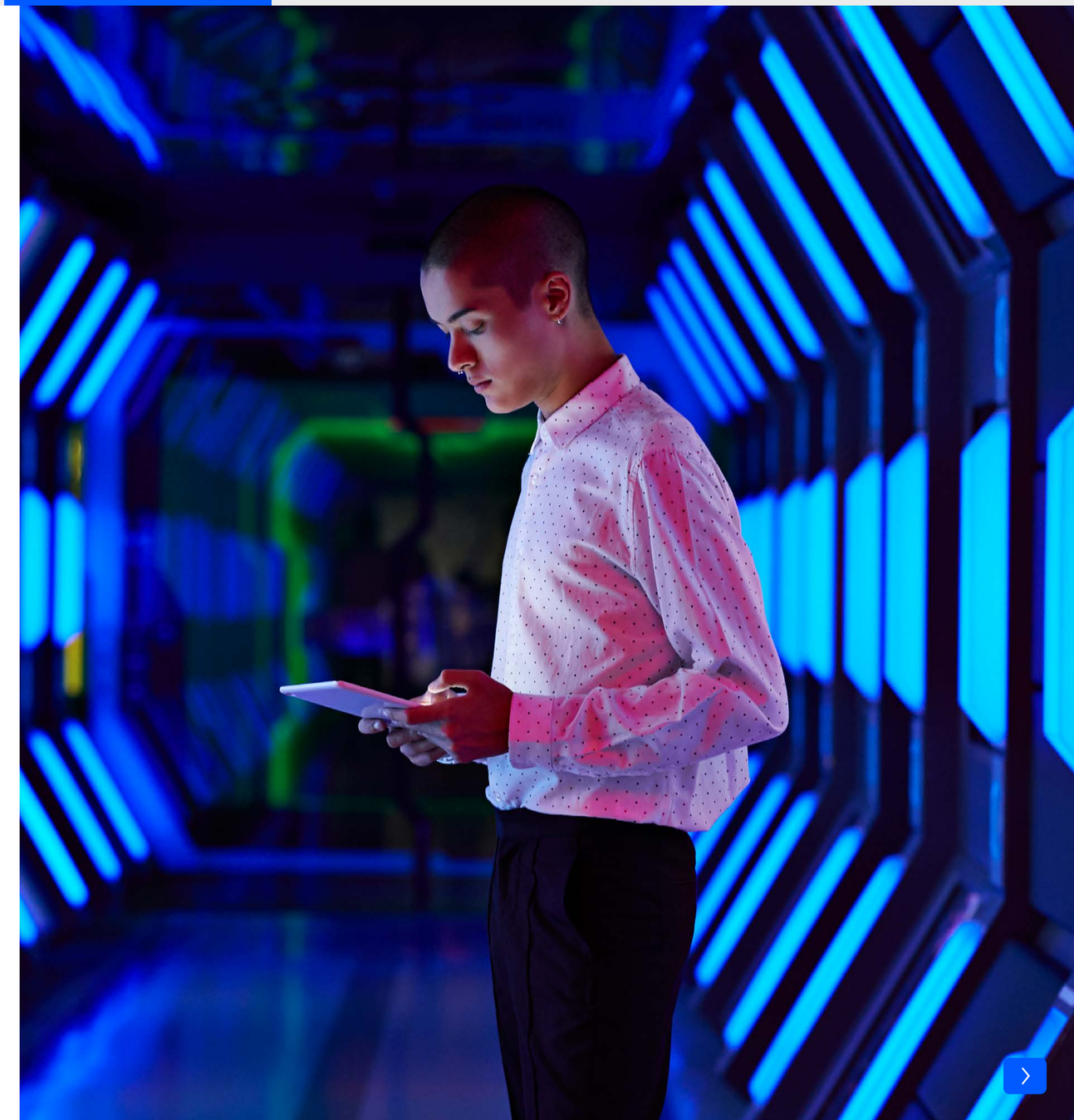
Cluster Node Security which isolates physical or virtual machines from each other to limit any damage caused by a security breach

Container and pod security which isolates and protects groups of containers that share storage and network resources

The shift-left movement embeds security into software development

Nokia is a strong advocate of shifting vulnerability management into the initial stages of the software development life cycle. This shift-left approach to security calls for software development with small but more frequent deliveries achieved through automated processes.

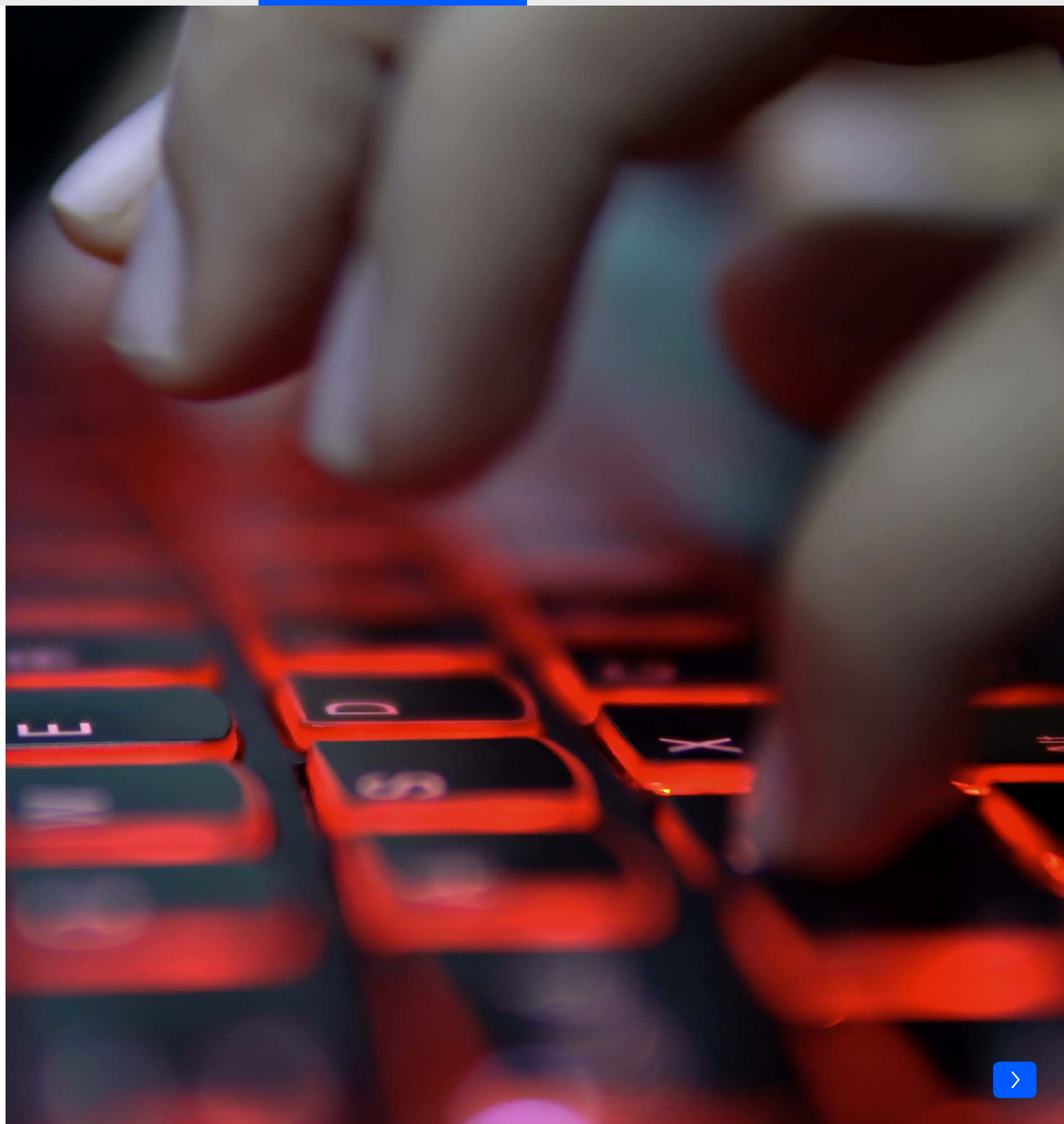
This enables rapid reaction to newly discovered vulnerabilities with DevSecOps helping to mitigate risks across the entire software lifecycle. Security-related tasks, such as automated security tests and code base analysis, become an integral part of the software development process, helping to achieve software integrity and authenticity from development to delivery.



Security by design – how DFSEC protects products

The Nokia Design for Security (DFSEC) process defines security activities for each phase of the product lifecycle to ensure that security is embedded and managed. DFSEC has technical and non-technical elements. Technical aspects include the use of cryptography, firewalling, logical access control, intrusion detection algorithms, threat intelligence and data analytics. Non-technical aspects include security policies, standards, awareness and training.

DFSEC helps to ensure that all components delivered to Nokia customers have a secure configuration by default.



The critical importance of managing vulnerabilities

The Nokia DFSEC process focuses on hardening products to avoid security vulnerabilities. An important part of the process is Security Vulnerability Management (SVM), which assesses the impact of known and newly discovered vulnerabilities and enables appropriate countermeasures, like management of security patching/upgrades.

The SVM process covers not only vulnerabilities found in Nokia products and solutions, but also in third-party software and components such as database or web-server products, protocols, visualization and more.

Find out more about Design for Security. Click here

Want to know more?

Nokia applies industry-leading security approaches to help CSPs confidently protect their 5G networks and businesses. Find out more and help protect the future of 5G.

Click here to read the Cloud Native Network Function security white paper.

To contact us **click here**.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID:212878

nokia.com

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering the future where networks meet cloud to realize the full potential of digital in every industry.

Through networks that sense, think and act, we work with our customers and partners to create the digital services and applications of the future.