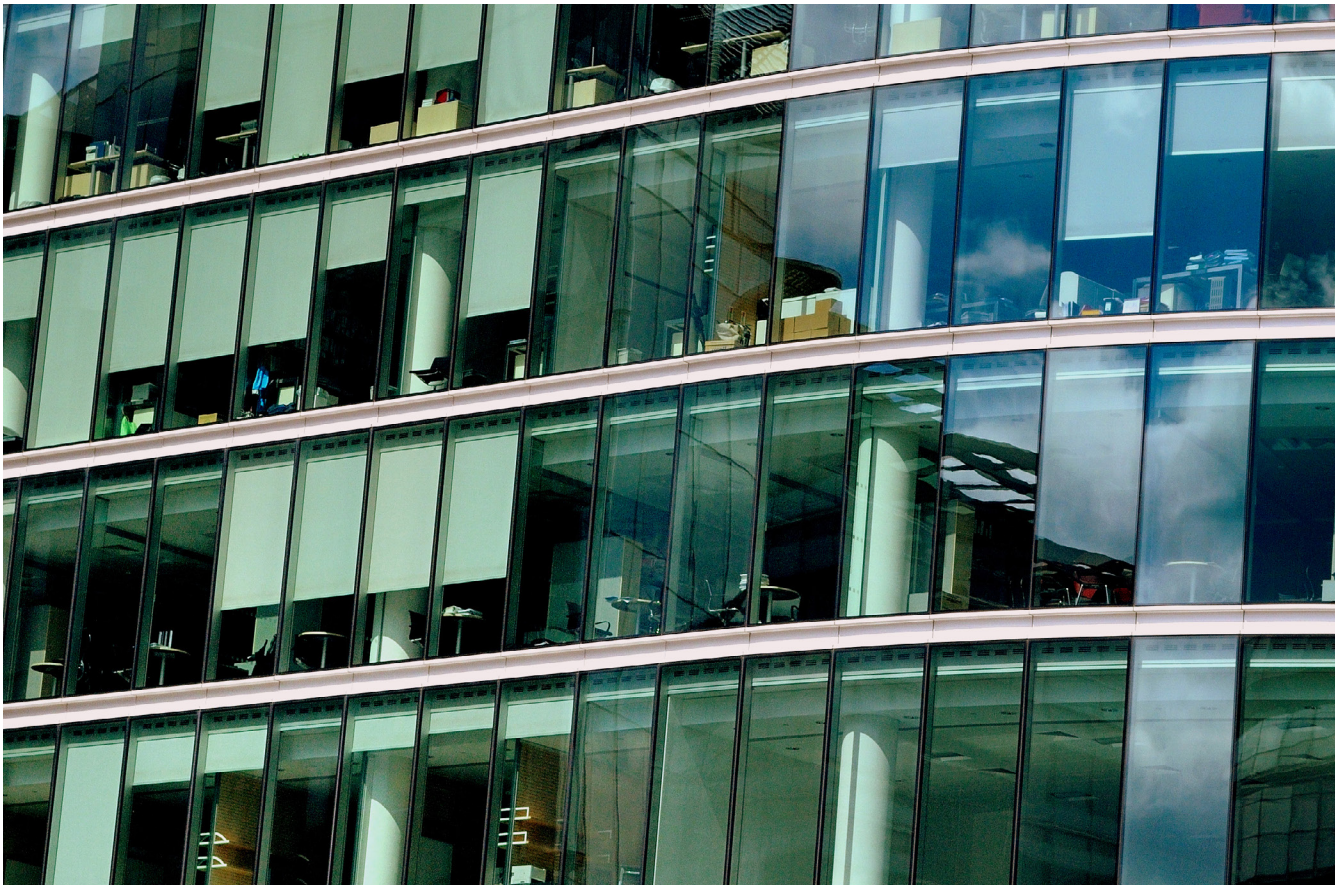
NOKIA



Security cloud for large enterprises

Use case

Provide security and compliance, evolve in sync with the fastest moving environment, and reduce total cost of ownership (TCO) by at least 25 percent.

Are you worried that your exposure surface (the areas that hackers can attack) is facing geometric increases as multiple cloud management systems, virtualization and container environments, and open source software packages are adopted? Are you concerned that hacker attacks are becoming increasingly professional and motivated by financial or political gain? Are you caught between the imperative for security and the infeasibility of providing it with legacy approaches?

Let Nokia show you how to secure your environment from end-to-end starting at the data center switch or virtual switch all the way to the remote branch. And, the Nokia enterprise private cloud can provide a TCO cost savings of at least 25 percent compared to a legacy environment that was upgraded to a cloud. This Nokia use case describes how our cloud approach builds security into every component to combine rigorous security with cost-effective automation and compliance capabilities—without the disruption of rip and replace.

Challenges

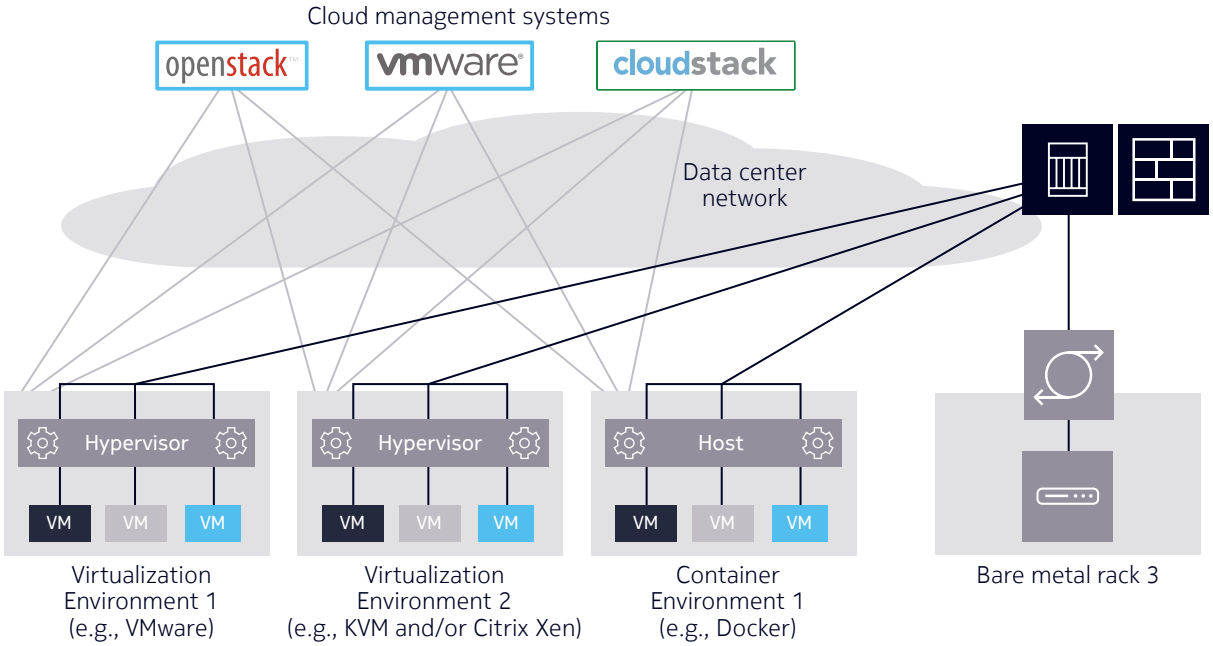
The scope of this use case is limited to the discrete networking challenges within the data center, the network connecting data centers and supporting applications, and the overall cloud environment.

Data center

As computing defenses evolve hackers refine their attacks to hit weak or unprotected spots in the overall exposure surface (see Figure 1). When cloud management (e.g., OpenStack), virtualization, and container systems are added to the environment, the following exposures become critical:

- **East-west network traffic inter-rack communications exposures:** As these communications are not typically secured, they are a prime way for a hacker to gain or widen access.
- **Exposures in virtualized and containerized intra-environment communications:** Communications within the virtualization hypervisor or the container host are not secured by default. That means a compromised virtual machine (VM) can provide access to all other VMs on the same hypervisor.
- **Security gaps for bare metal applications intra-rack communications:** For performance, racks typically contain a switch utilized by all servers on the rack.

Figure 1. Heterogeneous virtualized environment leads to a geometric increase in security exposure surface within the data center.

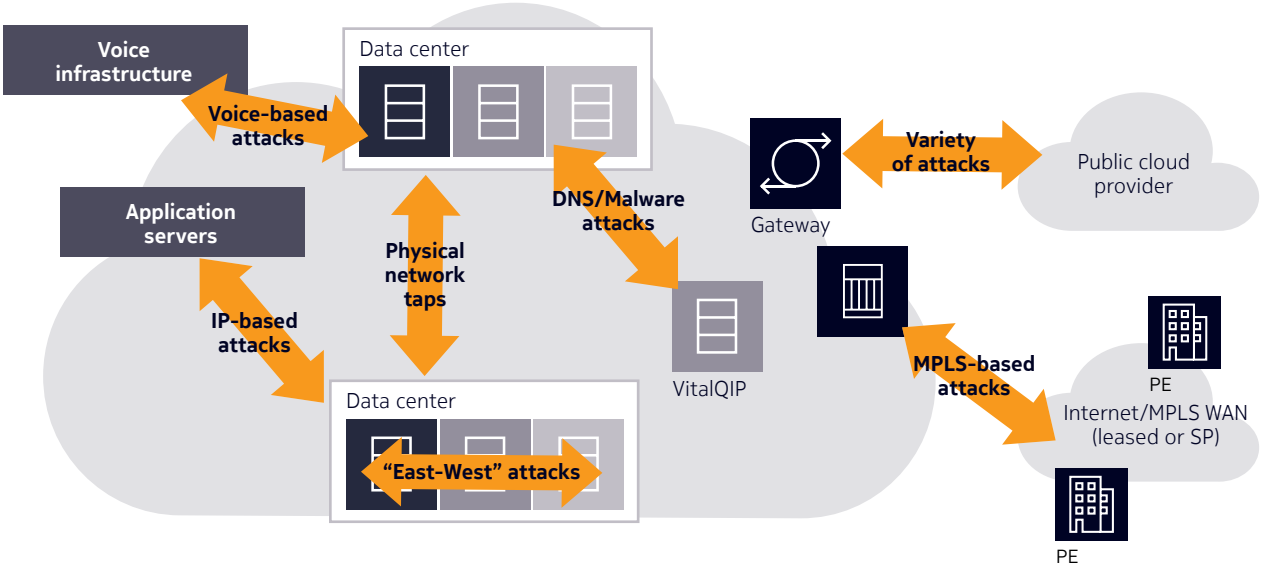


Network and application

As illustrated in Figure 2, a variety of security challenges arise in the network, starting at the physical layer and persisting all the way to the application layer:

- **Physical security/network taps:** Even optical networks can be tapped without disrupting the signal.
- **Exposures within each layer and at layer boundaries:** Each major subsystem has its own security exposure surface and each boundary presents opportunities that hackers can exploit.
- **Application security gaps:** As each application developer is often required to build-in security, the lack of a comprehensive approach is both expensive and risky.

Figure 2. Both legacy and cloud environments have exposures to a variety of attacks.



Throughout the cloud

As Figure 2 illustrates, throughout the cloud (from the data center through the network and to the WAN and public clouds as well as from data to voice), several overarching security concerns arise:

- **Exposures because of manual errors:** The majority of security breaches are because of manual errors that were exploited by hackers. For example, over several years the annual Ponemon security study has shown that approximately 60 to 85 percent of all security breaches with data loss were made possible by a manual error.
- **Risks due to the complexity of multi-tier applications:** Multi-tier applications increase the security workload geometrically by requiring multiple network connections be secured (e.g., web server to application server to database server).
- **Gaps within and among architectures:** Each major component (e.g., data center, WAN, public cloud, and voice) has its own security approach that often does not perfectly align with other approaches. Even if dovetailed, many security measures such as voice often are not cloud-ready. As a result, workload and security risk increase.

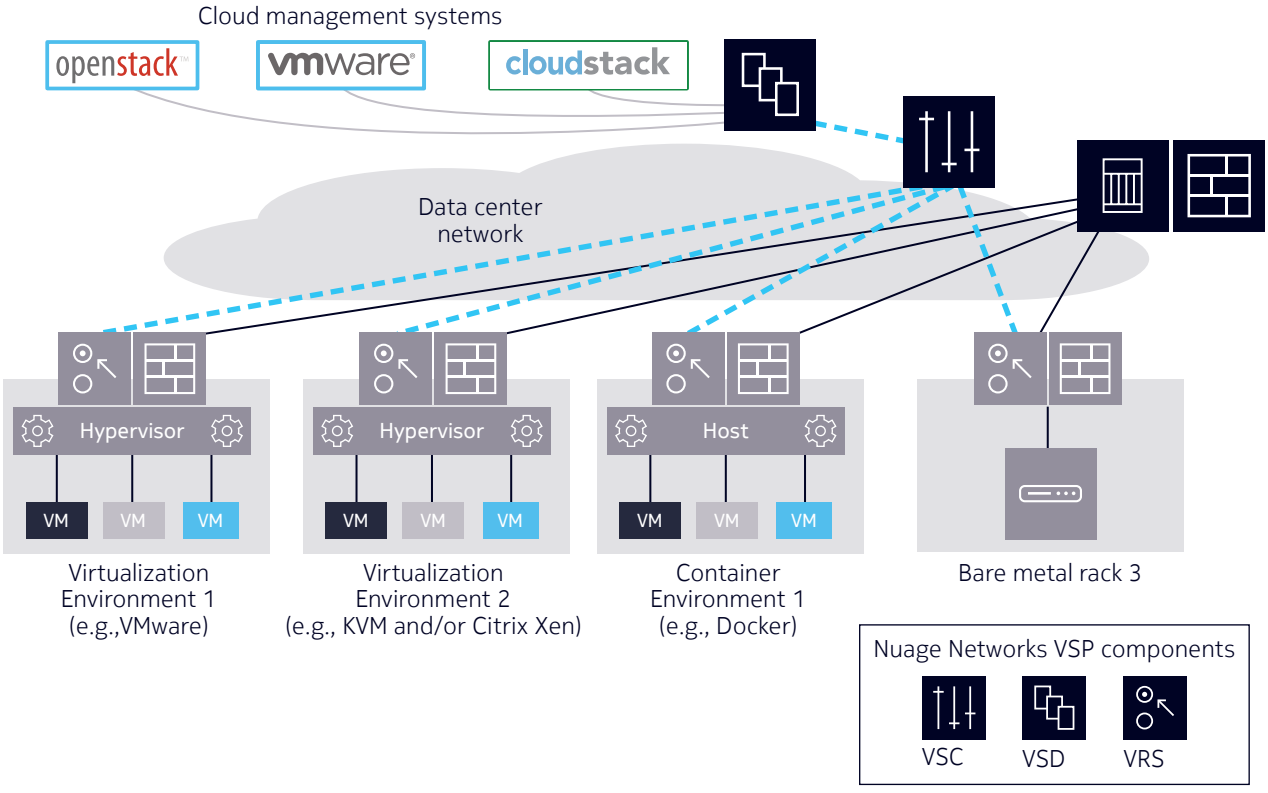
How we help you

Nokia combines multilayered security with cutting-edge networking technology to deliver a cloud infrastructure that provides mission-critical communications and operations while reducing costs. Each security component is entirely cloud-ready in terms of handling the complex multilayer and multisite needs of modern webscale applications and of handling extremely high and variable scalability. All major aspects of the infrastructure—from within the hypervisor throughout the data center and out to the furthest reaches of the WAN and from data to voice—are protected. Furthermore, Nokia can create a highly secure environment for even the most complex enterprise configuration without requiring forklift upgrades.

Shown in Figure 3, this capability revolves around the Nuage Networks (a subsidiary of Nokia) product portfolio. The Nuage Networks Virtualized Services Platform (VSP) provides software defined networking (SDN) capabilities that automate and secure the data center network. Nuage Networks VSP overlays the existing environment to upgrade it, without requiring forklift upgrades, transforming the environment to a best practices cloud. Cloud management system commands from any or all of OpenStack, CloudStack, and VMware vCenter are relayed to components of Nuage Networks VSP.

Within the virtualization hypervisor or container host, VMs and containers are secured and isolated starting at their initial connection to the network. Leveraging microsegmentation, each network stream is isolated.

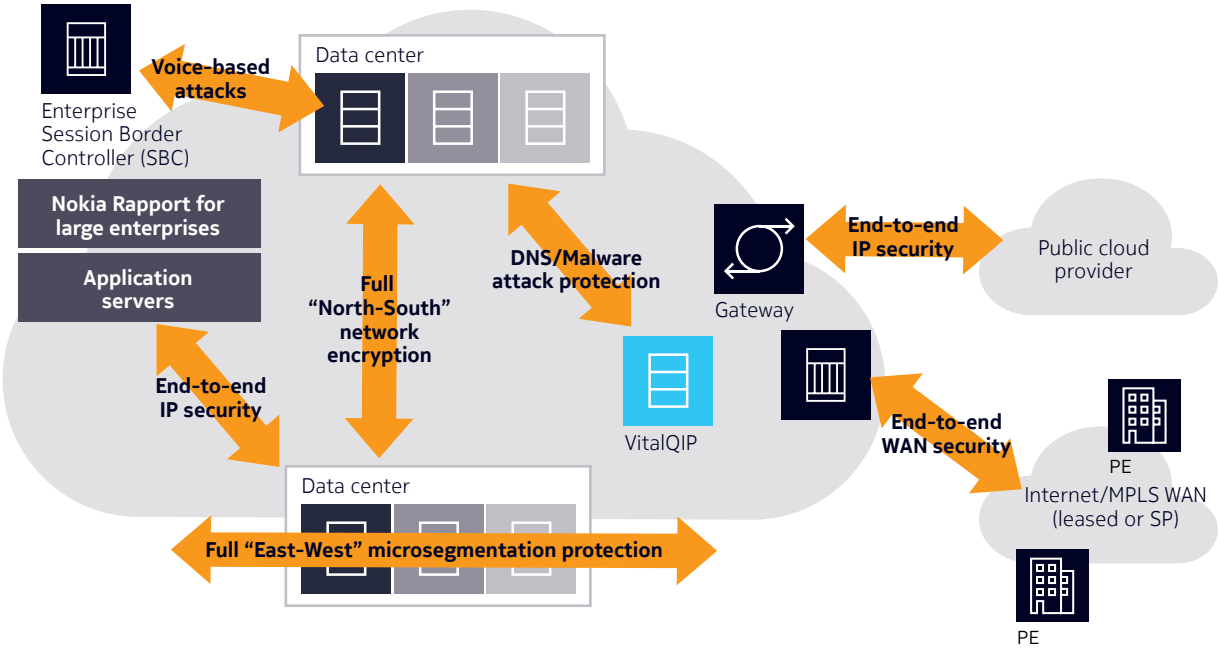
Figure 3. Multilayer controls protect from the initial network connection through the connections to the external network(s).



Using a top-of-rack switch with gateway capabilities, even bare metal servers are virtualized and secured. Existing security approaches such as firewalls are fully leveraged. And, network inspection capabilities down to the packet level enable one or more emerging security approaches to be incorporated. Because a single approach provides the security framework, the entire data center exposure surface is minimized while security is consistent and automated.

Rather than a bolt-on afterthought, security is built into each layer and each interface between layers of the Nokia cloud. Figure 4 shows how the Nokia optical networking infrastructure includes Layer 1 encryption to protect north-south against physical taps. By leveraging intelligent declarative policies that are interpreted dynamically at the end point, even the most complex IP environment can be secured effectively and efficiently. Further, by creating a unified and secured WAN over any combination of IP and MPLS networks, the entire WAN environment is highly secure as well as managed by the same system as IP and the data center. Core network services such as DNS are protected against malware and other attacks using the Nokia VitalQIP platform. And, even voice communications are protected by the Enterprise Session Border Controller. Lastly, powerful APIs including REST enable a wide variety of specialized security appliances to be seamlessly incorporated.

Figure 4. Security is built into every cloud component to minimize the overall exposure surface.



NOKIA

How our approach changes the game

This end-to-end security approach minimizes the overall security exposure surface by protecting key components such as VMs and containers starting at the initial network connection. Perhaps most importantly, each layer of security—from data center to WAN and from data to voice—is completely cloud-ready. Capabilities include:

- **Microsegmentation within the hypervisor and container host:** Communications among VMs within the hypervisor and communications between containers within the container host are fully secured.
- **Virtualized and secured networking for bare metal applications:** Intra-rack communications as well as data center networking are fully secured starting at the initial network connection.
- **Secure east-west network traffic (inter-rack communications):** These critical communications are fully secured.
- **Layer 1 encryption:** At the physical layer, encryption built into Nokia's optical products provides defense against physical taps.
- **Voice communications:** The Nokia Enterprise Session Border Controller (SBC) provides a next-generation, cloud-ready layer of protection for voice communications. The SBC protects against a wide range of exposures such as calls transferred from outside the organization all the way to distributed denial of services (DDoS) attacks.
- **Automated declarative policies:** Manual errors can be minimized if not eliminated by providing intelligent declarative policies that are interpreted at each endpoint.
- **Application templates:** With Nuage Networks VSP, network administrators can define application templates with embedded security definitions that handle the complexity of the network environment automatically. Furthermore, as applications and workloads are migrated around the environment, changes to application code are not needed.
- **Service chaining:** Application templates provide step-by-step definitions for multi-tier applications using service chaining. For example, a service chain of declarative policies would define that web server A can talk to application server B using firewall B and application server B can talk to database server C using firewall C. This approach removes the complexity of the application environment from the application developer's task list. Additionally, manual intervention is not required when applications and workloads are migrated within or among data centers.
- **Universal approach:** The same approach works within the data center, across the IP network, and throughout the WAN. This minimizes security risk and operations costs.
- **Compliance tracking:** Each policy interpretation is logged and stored in a central big data store for compliance analysis and reporting.
- **Hard cost savings:** The Nokia enterprise private cloud reduces total cost of ownership by a minimum of 25 percent as compared to the original legacy environment that was transformed to cloud.

NOKIA

Why our approach is different

- **Comprehensive:** Starting with physical (Layer 1) encryption and extending up to application (Layer 7) with application templates, the Nokia approach comprehensively combines built-in safeguards with best-of-breed security practices at every layer.
- **Full and consistent coverage across virtualized and container environments:** This is one of the few, if not the only approach that provides full coverage across multiple virtualization and container environments.
- **Open:** While Nokia provides the end-to-end infrastructure, APIs allow existing (e.g., firewalls) and specialized (e.g., application monitors) infrastructure to be fully leveraged.

How you benefit

- **Minimizes risk of a breach:** A consistent and automated approach minimizes the overall exposure surface and minimizes breaches due to manual error.
- **Operationalizes in-house compliance testing and reporting:** By automatically collecting and storing all policy interpretations into a single big data store, compliance verification and testing is finally feasible as part of daily operations rather than relying on periodic audits by outside consultants.
- **Supports the latest application architectures:** Unlike legacy architectures, the Nokia cloud approach provides the protection required by distributed, multi-tiered cloud applications.

For more information on our solutions for large and webscale enterprises, visit https://networks.nokia.com/large-enterprises.

About Nokia

We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry's most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in virtual reality and digital health, we are shaping the future of technology to transform the human experience.

Connect with our sales team

Europe and Asia Pacific: +44 203 582 5650 (M-F 08:00 – 16:00 GMT)

United States and Canada: +1 866 231 0264 (M-F 08:00 – 17:00 EST)

Nokia Oyj
Karaportti 3
FI-02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Product code: SR1706012153EN (September)