NOKIA Bell Labs

The Future of Security is End to End

Threats are growing and elusive

The risk of cyber-attacks is continuously increasing with potentially catastrophic consequences, especially for industries that provide mission critical infrastructure and services. Not only is the number of attacks growing but threat vectors are becoming more diverse, and the scale, sophistication, and efficiency of attackers are continuously increasing. Today's cybersecurity solutions have reached their limits, not only in their ability to apply security mechanisms to protect data, but also in their efficacy. Today's security frameworks do not provide a cohesive solution that can parse, group, and evaluate very large volumes of disparate events and alarms, thus requiring significant manual intervention. Meanwhile, the surfaces vulnerable to attacks are increasing both in number and in size – and the potential for catastrophic consequences is growing accordingly.

These concerns are arising as enterprises and industries undergo rapid transformations. New advanced private local area networks are blurring the lines between the LAN and WAN, leading to the convergence of information communications technologies (ICT) and operational technologies (OT). New networking innovations like 5G slicing will use a shared infrastructure to support a myriad of new use cases, each with different requirements for security and quality-of-service. The dangers of security vulnerabilities are particularly acute in the industrial world where formerly proprietary closed systems are becoming more open by using wireless and cloud-based ICT technologies to boost productivity and efficiency. In factories, ports, railways, local governments, utilities, and hospitals, security becomes closely intertwined with safety, amplifying the potential risks.

An end-to-end solution is needed

In order to protect customer networks against these increasingly sophisticated and potentially devastating attacks, today's security solutions must evolve. A new end-to-end security approach must:

- Traverse the entire span of communications from the device, to the radio access network, to the optical and IP transport, to the cloud, and even into industrial automation systems themselves
- Ensure that all products in all networking domains implement the security functionality needed to deliver end-to-end security for 5G, mission-critical, and industrial automation networks
- Include an overarching security solution that generates security-impacting alarms and events across all domains and automatically takes corrective end-to-end actions
- Fully integrate operational intelligence from the field to rapidly develop new security features and deploy them into our products as needed
- Predict new kinds of security attacks and vulnerabilities against which proactive protection is needed as both networks and cyberthreats evolve

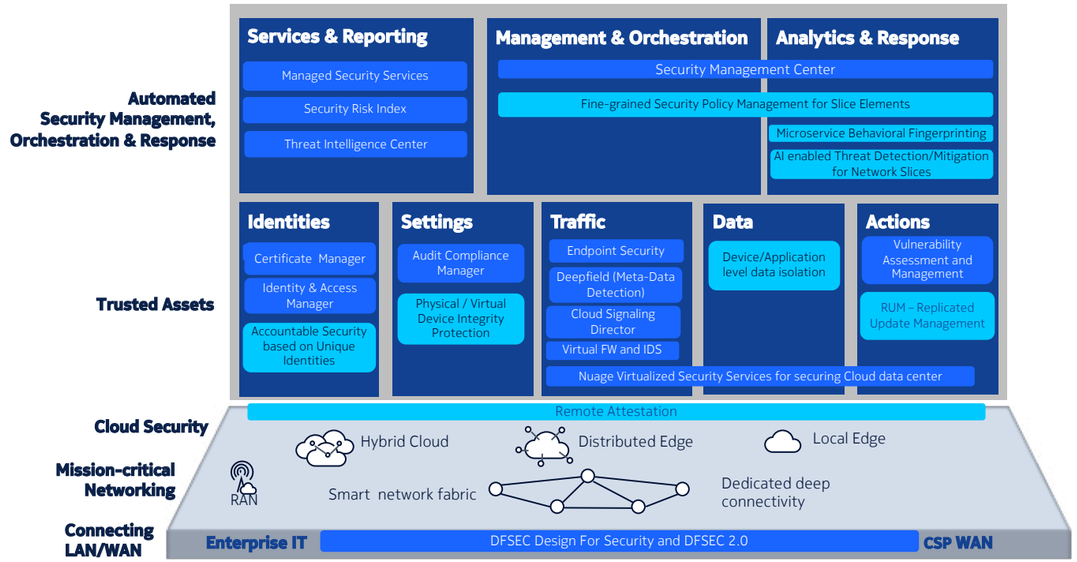
Our portfolio

Nokia has provided the industry leadership to develop end-to-end security for 5G, mission-critical networks, and industrial automation. Through our comprehensive end-to-end networking product portfolio, our holistic security solutions, and our managed security and consulting services business, Nokia has created the security architecture that can not only protect from today's threats but can anticipate future attack vectors and evolve to address future vulnerabilities. Our solution comprises multiple unique elements:

- We have launched Design for Security (DFSEC) 2.0, an enhanced security program that provides the mechanism for systematically ensuring all our products in all networking domains have the necessary baked-in security features to deliver end-to-end security.
- Our holistic telco-centric NetGuard Adaptive Security Operations suite with Security Orchestration, Analytics, and Response (SOAR) with audit compliance, privileged access, threat intelligence, malware detection, and certificate management.
- Our consulting services provide timely operational insights into security issues in customer networks, enabling the rapid development and deployment of necessary additional security features.
- Nokia Managed Security Services (MSS) supports operators on the operational layer with both basic and advanced services.
- We have launched the Future X Security Laboratory (FXSec), a new security end-to-end testing and verification lab at Nokia Bell Labs headquarters in Murray Hill, N.J.

Nokia products are backed by Bell Labs research

Our advanced research initiatives in Nokia Bell Labs are aimed at addressing the critical security needs of the end-to-end mission-critical networks that will define the 5G era. One example of that research work is the use of artificial intelligence to detect and mitigate threats in network slices by utilizing our unique Microservice Behavioral Fingerprinting approach to identify anomalies. Another program centers on physical and virtual entity integrity protection, which provides scalable integrity attestation across hardware, firmware, operating systems, and applications throughout the supply chain. Nokia Bell Labs researchers are pursuing a myriad of other security-related lines of inquiry as they work hand in hand with our product teams to ensure our end-to-end security solution is primed to meet all future threats.



At the same time future networks and solutions are facing significant security challenges as these systems do not operate in a closed world. They will utilize open interfaces and dynamically changing topologies due to SDN, slicing, cloud-native solutions, and all-service-based architectures. They will be connected to billions of potentially vulnerable IoT devices and depend on data stored in the cloud outside of the network operator's control. Nokia aims to provide the best reactive and proactive defenses possible to monitor threats and take mitigating actions to keep live networks secure – using all the techniques at our disposal, including AI. Nokia's end-to-end security design, built-in security features, dedicated security controls portfolio, and managed security services enable operators to proactively protect networks and services and even detect and dynamically mitigate security threats and anomalies due to unknown attacks, unintended misconfigurations and even human errors, which can accidentally invalidate highly sophisticated security architectures. Security is always a co-operative effort among network equipment vendors, operators, and even users, and at Nokia we take our role in building a bulwark against cyber-threats very seriously.

NOKIA Bell Labs

About Nokia Bell Labs

Nokia Bell Labs is the world-renowned industrial research arm of Nokia. Over its 90-year history, Bell Labs has invented many of the foundational technologies that underpin information and communications networks and all digital devices and systems. This research has resulted in nine Nobel Prizes, two Turing Awards, three Japan Prizes, a plethora of National Medals of Science and Engineering, as well as an Oscar, two Grammys and an Emmy award for technical innovation. Nokia Bell Labs continues to conduct disruptive research focused on solving the challenges of the new digital era, defined by the contextual connection and interaction of everything and everyone, as described in the book, The Future X Network: A Bell Labs Perspective.

600 Mountain Avenue, Murray Hill, New Jersey 08904
Phone: (908) 582-3000
E-mail: info@nokia-bell-labs.com
Web : www.bell-labs.com