Unlock the value of your network

Three keys to digital trust:
Integrated operations, tools and intelligence
Cybersecurity in 5G with NetGuard XDR Security Operations
Contents

Page 3 How do you secure an open ecosystem?
Page 4 New risks from new sources
Page 5 Integrated security operations
Page 6 Integrated security tools
Page 7 Integrated threat intelligence
Page 8 Integrated everything with extended detection and response
Page 9 Integrate your security capabilities with XDR-based solutions from Nokia
Page 12 Trust Nokia to help you build a comprehensive, integrated 5G security posture
How do you secure an open ecosystem?

To capitalize on the 5G opportunity, communications service providers (CSPs) need to build digital trust with their enterprise customers. Everyone in the emerging 5G ecosystem needs to know their mission-critical data and applications will be safe.

But protecting a 5G network can be as challenging as building one. The openness of 5G networks and the complexity of 5G services — and the shift from bounded, self-contained networks to hybrid cloud environments with no definite perimeter — are exposing CSPs to new and different risks.

To overcome these risks and build digital trust, CSPs must move from the fragmented security posture they have built up over the years toward one that is integrated across three key areas:
New risks from new sources

With 5G more open and complex than any previous network generation, CSPs must anticipate and prepare to mitigate a number of external and internal threats:

- **Cyber threats**
  Software vulnerabilities from open-source software and microservices have created numerous attack vectors that can be exploited by malicious actors.

- **Human error**
  Because 5G is so new, there's a greater risk of human error when configuring or maintaining the software that runs the network's components, inadvertently making CSPs vulnerable to attack.

- **Growing complexity**
  There are too many disjointed security tools to manage (and not enough people to manage them), leading to more alarms and more false positives that eat up valuable security analyst time.
Integrated security operations

Unite endpoints, the network and the cloud for a single view of security. The more you can see at once, the easier it is to stop threats before they affect your customers.

Endpoints, the network and the cloud all make up their own complex environments to manage, each requiring unique security infrastructures. But most tools available to security analysts can attend to just one of these environments at a time.

As networks grow in size and complexity, that fragmented view becomes more of a liability: analysts can lose track of threats and incidents as they shift their attention from one part of their operating environment to another.

For total visibility from endpoints through the network and into the cloud, CSPs need to integrate all aspects of their security operations into one unified management interface. This makes it possible to constantly monitor and quickly react to anomalous traffic patterns and attacks no matter where they’re coming from — while also easily managing complex operations such as network slice provisioning.
Integrated **security tools**

When you streamline the number of security tools in your kit, orchestration is easier and you can confidently expand your network without compromising its integrity.

Addressing increasingly complex cyberthreats requires equally complex security defenses. Every new application and component brought into the network is a potential vulnerability that has to be secured.

Up to now, the usual solution has been to deploy more point products to address the issues. Many CSPs run 30 to 50 discrete security tools, many overlapping in their functionality and each sending their own alerts when something's not right. This makes security controls disjointed, hard to manage and prone to false alarms. And at a certain point, deploying new security tools on top of existing ones becomes difficult due to lack of interoperability across the set.

CSPs that can integrate their many security tools into a single platform are better able to keep their networks secure, even as they add new services and customers to the mix.
Integrated threat intelligence

A complete picture of the cyberthreat landscape is essential to assuring the integrity of your network and reducing the burden on your security teams.

CSPs receive and analyze threat data from many sources: their own on-premises systems, cloud applications and endpoints, as well as open source and commercial threat intelligence services. Combined, this data helps give a better understanding of the cyberthreat landscape to prepare defenses and response actions.

But with 5G making the network more complex — and with the entire telco industry faced with a shortage of specialized cybersecurity personnel — security analysts are getting overwhelmed by the sheer volume of incoming data. It is becoming increasingly difficult to make sense of it all and generate actionable threat intelligence.

If CSPs can bring together all of their internal and external threat intelligence into a single system, security teams will be more easily able to distinguish between false positives, anomalies and legitimate threats — so they can then prioritize and act on the real risks.
Integrated **everything** with extended detection and response

**Extended detection and response (XDR)** enables all three areas of integration. It takes security orchestration, automation and response (SOAR) to even greater heights through a cloud-native architecture built to accommodate the ever-growing and increasingly complex volumes of data coursing through 5G networks.

XDR-based security operations are anchored by a robust data pipeline. That makes it possible for CSPs to collect more data from more sources, all processed and analyzed through one cohesive security management system — so they can act on threats faster and more effectively than ever before.

**Figure 1. The key capabilities of XDR**

That pipeline also allows XDR to provide overarching security lifecycle management, orchestrating and automating all aspects of risk and threat prediction, detection and response. CSPs can more easily integrate disparate threat intelligence data that is tailored to their unique requirement, model specific threats and attacks to their networks, and automatically apply the most appropriate preventative controls.

The result: XDR solutions have been shown to **improve the effectiveness of security operations by as much as 70%**.

**The managed services opportunity with XDR**

CSPs don’t need to operate an XDR solution themselves to get the benefits. With managed detection and response (MDR), XDR capabilities are delivered as a managed service by a highly experienced service provider. MDR is an increasingly popular option for CSPs who lack the in-house skills to detect and respond to increasingly complex cyber threats, or are looking to ease the burden on their overwhelmed security operations teams.
Integrate your security capabilities with XDR-based solutions from Nokia

Nokia NetGuard XDR Security Operations platform is a cloud-native XDR security platform that lets CSPs integrate their disparate security capabilities into a single platform — so they can respond to evolving threats more efficiently and accurately.

• **Integrated security operations:** CSPs get end-to-end visibility across networks, clouds and endpoints through a “single pane of glass” management interface — allowing security teams to quickly pinpoint the exact source of any potential breach.

• **Integrated security tools:** NetGuard XDR Security Operations helps CSPs manage and administer disparate point products in a coherent and consistent way, providing a library of interfaces and connectors that bring a range of end-to-end infrastructure components and multi-vendor security tools under a single security management platform.

• **Integrated threat intelligence:** Cognitive threat detection analyzes network sessions for malware or anomalous device behavior, and interprets the global threat landscape in a consistent, actionable way. Automated alert prioritization and classification eliminate the need for security teams to investigate redundant or lower-priority notifications so they can focus on blocking legitimate attacks.
The security functions at the heart of a trusted 5G network

NetGuard XDR Security Operations is the industry’s most comprehensive XDR security solution, offering integrated privileged access management, audit compliance, certificate management and network-based malware detection:

**NetGuard Identity Access Manager**

The 5G ecosystem will involve many partners, customers and end users, all requiring different access privileges for network services, devices and equipment. NetGuard XDR Security Operations gives security teams a way to automatically handle privileged access management — for example, by ensuring vendors of various network elements can access only their own equipment.

**NetGuard Certificate Lifecycle Manager**

Different network elements have different digital “identities” — along with certificates that verify those identities and give them the “right” to connect to the network. With NetGuard XDR Security Operations, security teams can manage the lifecycles of all certificates (including renewing or revoking them, as needed) in a streamlined, automated way.

**NetGuard Endpoint Security**

Malware and attack activity need to be detected, investigated and stopped before they become costly breaches. NetGuard XDR Security Operations’ network-based sensors and cognitive threat detection, powered by machine learning and artificial intelligence, analyze all network sessions in real time to differentiate abnormal traffic from legitimate access.

**NetGuard Audit Compliance Manager**

Attackers that get past endpoint security devices will likely try to manipulate network configurations to install malware, upload keyloggers or open backdoors into the core domain. NetGuard XDR Security Operations helps prevent that by constantly monitoring established configurations for any deviations — and raising alarms when anomalous activity is detected.

**NetGuard Security Management Center**

CSPs need analytics and reporting capabilities that can aggregate security data from many different sources. Through NetGuard XDR Security Operations’ single command-and-control portal, they can monitor and manage multi-vendor security systems to develop a more complete risk profile, improve their situational awareness and automate the orchestration of complex threat-response workflows.
XDR Security Operations

- Slice security
- Cloud security
- Network security
- Endpoint security

Data Enrichment
Anomaly Detection
Automated Playbooks
CxO Dashboard
Workflow Orchestration
Compliance Reports
Threat Intelligence

Digital Identity
Trust Nokia to help you build a comprehensive, integrated 5G security posture

With an integrated security infrastructure protecting their 5G networks, CSPs can establish the digital trust with their enterprise customers that will be critical to driving future growth.

Nokia NetGuard XDR Security Operations with XDR gives CSPs the advantages they will need in the 5G era through:

- **Automation**: Prioritize risks and automate security operations according to specific attack surfaces and business operations, reducing the cost of labor for repetitive actions.
- **Speed**: Take advantage of machine learning, multi-dimensional network analytics and threat intelligence to analyze and respond to cyberthreats rapidly, greatly reducing hackers’ dwell time.
- **Adaptation**: Adapt to changing attacks in real time with intelligent analytics that identify patterns and provide continuously updated detection algorithms, reducing the likelihood of costly data breaches.
- **Integration**: Gain a stronger security posture with comprehensive interfaces for infrastructure components and multivendor security tools that simplify security operations while maximizing operational efficiency.

Visit our website or contact us to learn more about Nokia NetGuard XDR Security Operations with XDR today.
About Nokia
We create the critical networks and technologies to bring together the world's intelligence, across businesses, cities, supply chains and societies.

With our commitment to innovation and technology leadership, driven by the award-winning Nokia Bell Labs, we deliver networks at the limits of science across mobile, infrastructure, cloud, and enabling technologies.

Adhering to the highest standards of integrity and security, we help build the capabilities we need for a more productive, sustainable and inclusive world.

For our latest updates, please visit us online www.nokia.com and follow us on Twitter @nokia.

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.

© 2021 Nokia