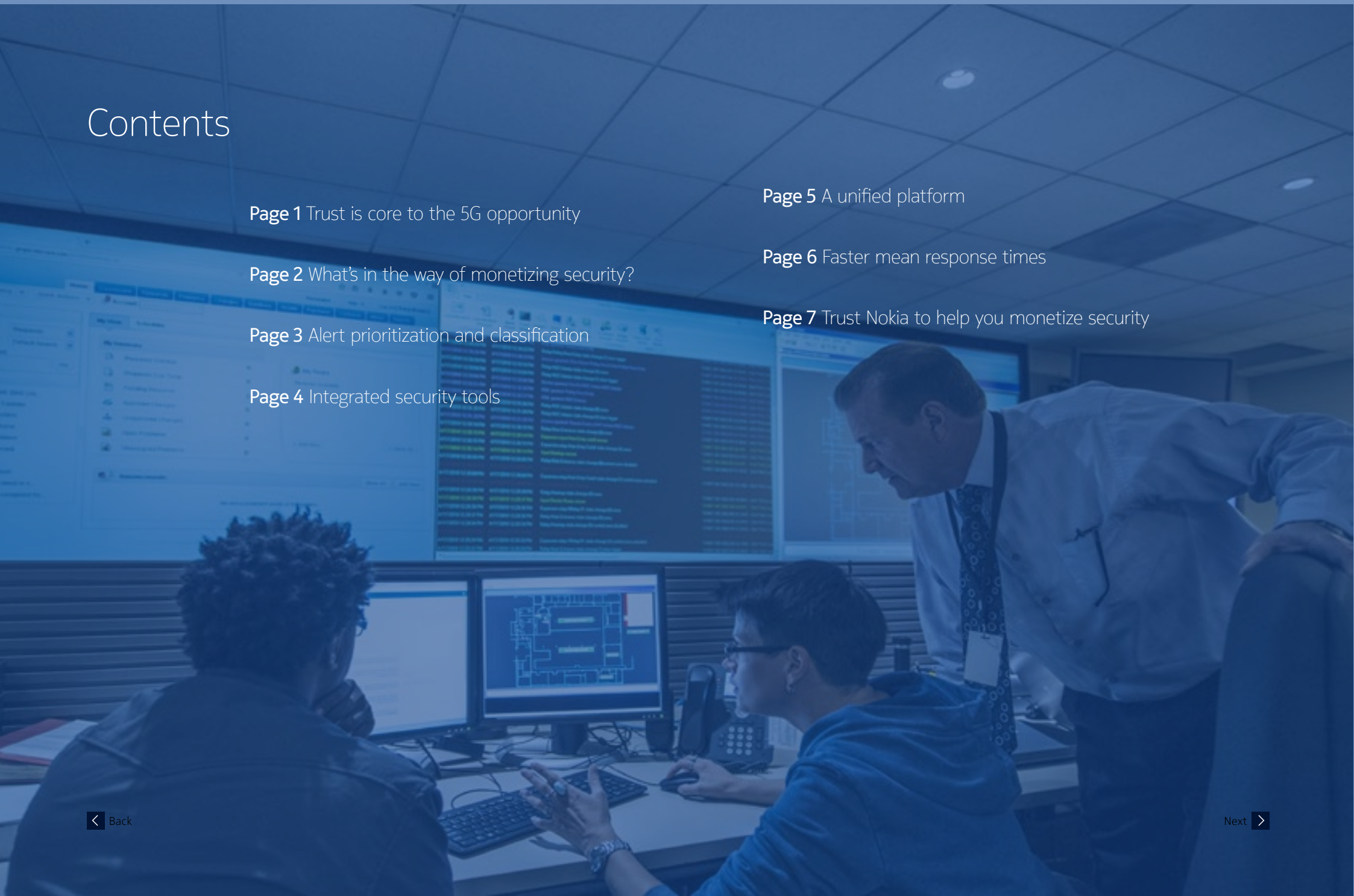
Unlock the value of your network

Cyber security in 5G with NetGuard XDR Security Operations

Five must-haves to monetize 5G security

Next

Contents



Trust is core to the 5G opportunity

The openness of 5G environments and the complexity of 5G services requires communications service providers (CSPs) to invest more time, money and resources in security — and in building "digital trust" with their customers — than ever before.

That's prompted many to seek ways of converting security from an operating cost into a revenue generator. And by making smart use of automation, machine learning, artificial intelligence (AI) and standardization, they can.

With the right combination of tools and technologies, CSPs can make security a value-add of their slice-based 5G services for enterprises or even offer managed security as a service beyond connectivity itself. But first they have to overcome the challenges of a fragmented and inefficient security environment.

Your 5G trust-building toolset

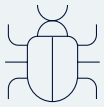
NetGuard XDR Security Operations is a cloud-native security platform that makes it possible to respond to evolving threats efficiently and accurately — using automated tools, extended analytics and integrated threat intelligence.

NetGuard XDR Security Operations uses extended detection and response (XDR), which natively integrates multiple security products into a cohesive security operations system.

XDR provides overarching security lifecycle management that orchestrates and automates risk and threat prediction, detection and response, with threat intelligence tailored to a CSP's unique requirements. The result: **security operations effectiveness is improved by as much as 70%.**

What's in the way of monetizing security?

The shift from bounded, self-contained networks to hybrid cloud environments with no definite perimeter is exposing CSPs to new and different kinds of risks:



Cyber threats

Software vulnerabilities from open-source software, microservices and functions of unknown provenance create a huge number of attack vectors that can be exploited in highly sophisticated attacks.

Human error

People are often the weakest link in the security chain: they're easily deceived by phishing emails and can be unintentionally negligent when configuring or maintaining software modules that run or manage network components.

Growing complexity

Addressing the new threats demands increasingly complex defenses. But by deploying more and more point products, CSPs' security controls and monitoring tools become increasingly disjointed, overlapping in their functionality and prone to false alarms — and in need of hard-to-find, specialized personnel to configure and maintain them all.

To overcome these risks and capitalize on the security monetization opportunity, CSPs **need five key capabilities:**

Alert prioritization and classification

Integrated threat intelligence

Integrated security tools

A unified platform

Faster mean response times

Back

Next

Alert prioritization and classification

Focus your team's attention on the alerts that really matter — so you can deploy enterprise-ready 5G slices or managed security services knowing you can keep up.

Anomaly or attack?

In many cases, it's hard to know. Most CSPs have secured their infrastructures with a multitude of point solutions, each sending an alert when something's not right. But not every alert is equally important. And with so many coming in from so many different sources, security teams can quickly become overwhelmed trying to correlate and classify them as anomaly, false positive or legitimate attack.

How Nokia helps

NetGuard XDR Security Operations' **alert prioritization and classification** capabilities help security analysts quickly and easily distinguish between false positives and legitimate attacks. They automatically identify and classify alerts by type and severity (e.g., configuration changes, open ports), eliminating the need to investigate redundant or lower-priority notifications. Instead, security teams can focus their efforts on blocking or countering legitimate attacks.

This also helps CSPs deliver against **slice-specific service-level agreements (SLAs)**, which will be critical to unlocking enterprise use cases requiring individual security with multi-tenant capabilities, such as smart cities and utilities.

Back

Next

Integrated threat intelligence

A coherent, actionable picture of the cyberthreat landscape is essential to assuring the integrity (and profitability) of your 5G services and managed security offerings.

What's really going on out there?

CSPs allocate significant resources to analyzing threat data from their on-premises systems, cloud applications and endpoints. They also invest heavily in open source and commercial threat intelligence services that add to their own data so they can better understand the cyberthreat landscape. But that landscape is large, complex and constantly evolving.

With 5G making the network more complex, analysts are struggling to keep up and make sense of all the incoming data — making it increasingly difficult to get the complete picture and generate actionable threat intelligence.

How Nokia helps

The **integrated threat intelligence** capabilities of NetGuard XDR Security Operations interpret the global threat landscape in a consistent, actionable way. Real-time threat intelligence and network-based sensors can detect, identify, investigate and stop threats before they turn into costly breaches. **Cognitive threat detection** analyzes network sessions for malware or anomalous device behavior such as command-and-control traffic, exploit attempts and distributed denial of service activity.

Back

Next

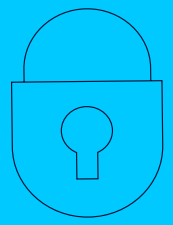
Integrated security tools

Simplify and streamline your security tools for efficient orchestration — controlling costs and boosting the quality of your security offerings.

Too many apps to manage?

As networks have grown in complexity and size, every application and hardware element is a potential vulnerability that needs to be secured — either through its own capabilities or with an additional tool. And those can add up.

It's not uncommon for CSPs to have 30 to 50 discrete security tools, each making the overall system even more challenging to manage. At a certain point, it also becomes increasingly difficult to integrate new tools into the mix, even as threats continue to proliferate and evolve.



How Nokia helps

NetGuard XDR Security Operations' XDR capabilities help manage and administer disparate point products in a coherent and consistent way, integrating tools for audit compliance, privileged access, threat intelligence, network-based malware detection and certificate management in a **single security management** platform. There's also a library of interfaces and connectors for seamless use with a range of CSP infrastructure components and multivendor security tools. The result: an end-to-end security infrastructure that's easy to manage.

A unified platform

Unite endpoint, network and cloud for a single security view. The more you can see at once, the better able you are to guarantee — and charge for — the added value of security.

How much can you see at once?

Endpoints, the network and the cloud all make up their own complex environments to manage, requiring unique security infrastructures. Many CSPs struggle to keep a bird's-eye view of the whole: their security tools only allow them to see into any one environment at once. As threats become more complex, that becomes a growing liability. Greater visibility is needed across every aspect of network and service operations.

How Nokia helps

Built on an open, cloud-native platform, NetGuard XDR provides end-to-end visibility across networks, clouds and endpoints through a **"single pane of glass" management** interface — making it possible to constantly monitor and instantly react to anomalous traffic patterns. CSPs can integrate their disparate security systems into a single platform, letting security teams look across and into any aspect quickly while easily managing complex operations such as network slice provisioning.

Back

Next

Faster mean response times

Protect your operations — and your revenues — by reducing threat dwell time.

Lost time, more risk

The longer a threat dwells in the network undetected, the more opportunities an attacker has to damage systems and steal important data. That makes it critically important to act as quickly as possible on any perceived threat.

Security teams need better ways of knowing when threats are present — along with faster ways of pinpointing and neutralizing them when they strike to minimize the potential losses.

How Nokia helps

With NetGuard XDR Security Operations, CSPs can respond to threats quickly, minimizing costs and disruptions when attacks or breaches occur. **End-to-end visibility** from endpoint through the cloud lets security teams quickly pinpoint the exact source of a potential breach to minimize threat dwell time, while **automated security playbooks** relieve the burden on security teams by continuously augmenting response actions for any kind of threat — distributed denial of service attacks, insider attacks and more.

Back

Next

Trust Nokia to help you monetize security

With all five security capabilities in place, CSPs can be confident in the integrity of their 5G networks and services — and in their ability to manage security as an offering for enterprise customers.

Nokia NetGuard XDR Security Operations with extended detection and response capability helps CSP´s lays the foundation CSPs will need to capitalize on the opportunity to monetize 5G security with:

- **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.

The monetization potential of security as a service

CSPs can turn security into a high-growth revenue-generation opportunity by combining the flexibility and scalability of cloud-native architectures with the intelligence and integration capabilities of XDR. With attackers going after enterprises' mission-critical applications and processes, CSPs that can offer value-added, subscription-based security services — such as 5G slice monitoring, endpoint protection for industrial IoT devices, or identity and access management — will be better positioned to protect their customers and bolster their bottom line at the same time.

Visit our website or contact us to learn more about Nokia NetGuard XDR Security Operations today.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

CID210539

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.

Back