Nokia NetGuard ACTIVE Security
Dynamic, predictive and automated security operations

The recent increase in sophisticated, targeted security threats such as Advanced Persistent Threats and ransomware by both insiders and external attackers has raised the awareness and urgency from communication service providers for comprehensive security strategies.

NetGuard’s security orchestration analytics and response solutions helps security operations teams streamline and accelerate business processes, reduce costs, and proactively prevent, pinpoint, and address security threats before they result in breaches. To stay ahead of these threats, the right balance between proactive and reactive security best practices are required.

NetGuard ACTIVE security helps security teams identify and limit attack vectors, detect more threats and respond rapidly.
NetGuard ACTIVE Security enables security operations teams become more effective

While cyber criminals are excellently connected, permanently working on how to automate cyber attacks to increase efficiency, the security operation center found that 33 percent of incident response time is spent on manual processes today. Combined with data deluge and alert fatigue, resulting from the fragmented nature of the security market with a myriad of point tools each with its own administration, management, and reporting capabilities, considerable time is wasted on false positives, while real breaches go undetected.

Security teams are also challenged by new threats and increased attack surface due to complex technology and business transformations such as network function virtualization (NFV), software-defined networking (SDN), virtualization, multi-access edge computing (MEC), and 5G.

The NetGuard ACTIVE Security spans physical, virtual, software-defined and traditional networks, seamlessly extends between operational and information technology, and uses automation to enable security operation teams to become more effective.

Today, only

30% of alerts are investigated

54% of legitimate alerts are not remediated.
Cognitive analytics and threat intelligence enable rapid detection and response

Security analytics enable NetGuard ACTIVE Security to detect indicators of compromise, proactively identify harmful actors, help security analysts prioritize risks, and initiate appropriate, rapid response.

By leveraging insights from attack campaigns, threat intelligence data enables real-time predictive response early in the kill chain, and not only after a breach has occurred. Nokia’s industry leading Threat Intelligence Lab analyzes data to determine the communication characteristics of malware. The corresponding detection rules identify infected endpoints. This approach enables threat detection in communication or IoT networks, provided by Nokia’s network-based malware detection product suite.
NetGuard ACTIVE Security provides a contextual view of security posture across the complex, heterogeneous, and diverse operational environments service providers face. It delivers reporting capabilities and real-time monitoring to provide contextual security issues alerts that help to reduce attack surface and time.

NetGuard ACTIVE Security is a fusion of security analytics, threat intelligence, and security orchestration, which consolidates data and extracts actionable insights from a variety of intelligence sources and existing security technologies. This enables security teams to streamline processes, accelerate decision-making and optimize costs while preventing, identifying and addressing security threats before they result in breaches.

Security orchestration and workflow automation are at the heart of the transition from static defense to agile and adaptive response.
The NetGuard Security applications supply rich insights to drive the intelligent, analytics-driven response by the NetGuard Security Management Center.

**NetGuard Identity Access Manager**
A privileged identity access management solution that governs, manages, and monitors user access to network assets, applications, and data.

**NetGuard Audit Compliance Manager**
Providing security configuration auditing of multi-vendor, hybrid heterogeneous networks for incorrect, outdated or vulnerable configurations.

**NetGuard Endpoint Security**
A carrier grade network-based anomaly detection system for IoT, smartphones, and other connected devices.
Critical infrastructure operators are an attractive and growing cyber target as they possess valuable personally identifiable information (PII). They are targeted by politically motivated attacks and nation-state hacking, and they can serve as entry points for malicious actors to launch secondary attacks.

- **Chief Security Officers** need the best methods to assure security compliance and measure risk level.
- **Security analysts** must be able to identify and respond to threats faster.
- **Managed security service providers** must improve customer experience and meet service level agreements.

NetGuard ACTIVE Security gathers and analyzes data, prioritizes threats, and provides contextual risk measurement to stakeholders.
The NetGuard ACTIVE Security architecture leverages the unique capabilities of the NetGuard portfolio including:

**Security Management**
Monitors, controls, and orchestrates to perform proactive actions with machine-learning analytics:
- Security Management Center
- Identity Access Manager
- Audit Compliance Manager

**Network Security**
Pervasive infrastructure protection against external attacks and malicious intrusion:
- Cloud Signaling Director
- Core Network Security
- Virtual Firewall

**Endpoint Security**
Network based malware, botnet and threat detection digital identity authentication of endpoints:
- Endpoint Security
- Certificate Manager

The fusion of these capabilities into a cohesive, modular end-to-end solution which provides open interfaces for multi-vendor integration, delivers market differentiating capabilities, enabling service providers to address the growing threat landscape resulting from mobile broadband expansion, IoT, Cloud and other technology disruptions.
About Nokia
Nokia is a global leader in the technologies that connect people and things. Powered by the innovation of Bell Labs and Nokia Technologies, the company is at the forefront of creating and licensing the technologies that are increasingly at the heart of our connected lives.

With state-of-the-art software, hardware and services for any type of network, Nokia is uniquely positioned to help communication service providers, governments, and large enterprises deliver on the promise of 5G, the Cloud and the Internet of Things. http://nokia.com

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.
Product code: SR1810029424EN (October) CID201314

© 2018 Nokia