Online security threats have reached unprecedented levels and are now affecting Internet of Things (IoT) devices, as well as end users. Nokia NetGuard Endpoint Security is a network-based anti-malware solution for fixed, mobile, and IoT devices. The solution detects malware, minimizes the malware’s impact on the subscriber experience, and generates revenue by providing a superior protection service.
Securing networks for IoT and end users
Mobile device infections are on the rise

Data from the latest Nokia Threat Intelligence report 2017 shows constant malware increase in malware command-and-control traffic, exploit attempts, hacking activity and Distributed Denial of Service (DDoS) attacks. Smartphone infections continue to grow, peaked in October 2016 at 1.1% and 50 percent of the threats were high level, such as bots and ransomware. And smartphones accounted for 72 percent of all mobile network infections. In October 2016, the malware infection rate hit an all-time high, when infections struck 1.38 percent of all mobile devices tracked. In addition, devices based on the Android™ operating system were the most targeted mobile platform by far, representing 68.5 percent of all mobile malware infections.

For example, IoT devices have a long life expectancy, which will make timely updates in the field difficult. This issue can lead to outdated security mechanisms, encryption erosion, and anti-malware software that is not supported, which all increase the chances for a security breach. Android continues to be the main mobile platform targeted, but iOS-based devices were also targeted, particularly in the form of Spyphone applications. So, there is a clear trend that cybercriminals are changing their focus from the Windows/PC ecosystem to smartphones and IoT devices.

Today, hackers and criminals target smartphones, computers, and IoT devices directly, or they use these infected devices to attack other systems connected to phone networks or the Internet. Enterprises and service providers must be able to proactively identify infected IoT devices and take steps to mitigate attacks. Therefore, ensuring robust endpoint security – which protects the network when accessed via remote devices – will become increasingly important for network operators.

### IoT represents the latest security challenge

Human lives are increasingly dependent on the availability and integrity of mobile network services for our connected cars, smart cities, health applications, and much more. Further, the Internet of Things is expected to be a $US46 billion industry by 2020. While this trend presents many positive advancements for society, IoT also poses a number of security challenges.

<table>
<thead>
<tr>
<th>Mobile infections peaked October 2016</th>
<th>Smartphone account for most mobile infections</th>
<th>Share of high level threats such as bots and ransomware</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.35%</td>
<td>72%</td>
<td>50%</td>
</tr>
</tbody>
</table>

The number of Android malware samples has soared 80%

### Mobile infections peaked

- **5.1 million** (Jan 2016)
- **8.9 million** (Jul 2016)
- **16 million** (Jul 2017)
Cyber criminals are attracted to smartphones because of their growing use in daily transactions. Today, people not only have a large amount of personal data on one device. They are also using smartphones more often to transfer money. For instance, they may purchase apps, music, and other digital goods; buy physical goods online; or complete mobile banking transactions. This direct or indirect use of credit cards with smartphones is inspiring criminals.

IoT and 5G networks are changing how the world sees data security and privacy. New businesses, value chains, and service delivery models are now being connected to a rapidly growing number of diverse connected devices. In addition, vendors can use topologies such as next-generation cloud architectures to offer a broader variety of services to all types of customers.

Clearly, the programmable world brings substantial benefits to individuals, businesses, and societies. But an equally wide variety of security challenges are now emerging. New technologies open up vulnerabilities and give rise to more sophisticated cyber attacks.

End-users increasingly worry about security
The safety of personal data is a key concern for consumers globally. According to the 2016 Nokia Acquisition and Retention study, 91 percent of consumers are worried about at least one potential security threat. In addition, 39 percent of consumers have been personally affected by malware attacks on their smartphones. Yet, despite this high level of awareness and personal experience, only 43 percent of consumers have anti-virus or anti-malware software on their smartphones. This figure is significantly lower than for laptops and PCs.
IoT threats become reality

Nokia security researchers have long warned that the dramatically increasing number and diversity of IoT devices being connected to the Internet will present enormous security issues. The Nokia Threat Intelligence Lab monitors and detects malware infections in devices and is powered by the Nokia NetGuard Endpoint Security solution, which has been deployed in major fixed and mobile networks around the world — monitoring network traffic from more than 100 million devices.

Pokemon Go
Within hours, Nokia Threat Intelligence Lab found copies of the game that had been injected with malware and made available for download from third-party sites. Samples were found to be infected with a remote access Trojan called “DroidJack,” which allows the attacker to track the mobile phone’s location, record calls, take pictures and steal information and files.

Mirai botnet
First detected by Nokia in October 2016, this malware was responsible for recent massive distributed denial of service (DDOS) attacks, and it is currently assembling an army of a million IoT devices, which could be used to launch future attacks. Mirai spreads by targeting devices that are vulnerable to brute force telnet or ssh password guessing attacks, including a variety of IoT devices, as well as home routers, Wi-Fi and MiFi.

SMSTracker
This spyphone app provides a complete remote phone-tracking and monitoring system for Android phones. It allows the attacker to remotely track and monitor all SMS, Multimedia Messaging Service (MMS), text messages, voice calls, GPS locations, and browser history.

HummingBad
First detected earlier in 2016, this sophisticated malware is an ecosystem of malware components installed using a drive-by download. It establishes a permanent foothold by rooting the device and makes money through ad-click fraud and by installing additional malicious apps.
We are dedicated to safeguarding networks, end users, and devices.
Network-based malware detection in fixed and mobile networks

- **Detect:** Security threats, e.g.
  - Infected subscribers
  - Most active threats
  - Affected devices

- **Monitor:** Correlate traffic patterns from telco networks with
  - Malware intelligence database
  - Self-learned malware patterns
  - Abnormal IoT behavioral profiles

- **NetGuard Endpoint Security**
  - Security insight (dashboard)
  - Action engine (automated actions)
  - Malware intelligence DB
  - Correlation of traffic

- **Migrate:** Minimize impact by applying automated actions, e.g.
  - Inform subscriber
  - Block value added services
  - Trigger firmware update (IoT)

- **Detect: Security threats, e.g.**
  - Infected subscribers
  - Most active threats
  - Affected devices

- **Monitor: Correlate traffic patterns from telco networks with**
  - Malware intelligence database
  - Self-learned malware patterns
  - Abnormal IoT behavioral profiles

- **NetGuard Endpoint Security**
  - Security insight (dashboard)
  - Action engine (automated actions)
  - Malware intelligence DB
  - Correlation of traffic

- **Migrate: Minimize impact by applying automated actions, e.g.**
  - Inform subscriber
  - Block value added services
  - Trigger firmware update (IoT)

- **No SW on end user devices**

- **Smartphones, PCs, IoT**

- **All subscribers, mobile/fixe**

- **Individual subs, remediation**

- **PCs, laptops**

**Nokia NetGuard Endpoint Security**
Nokia NetGuard Endpoint Security protects end users and IoT device owners against fraud, even when there’s no anti-malware software installed on their smartphones or IoT devices.

The solution offers the best available protection against malware by combining network and anti-virus protection. It immediately informs end users and IoT owners when their device is infected — and helps them get rid of the malware. In addition to preventing bill shock, this quick action gives end users peace of mind, because their security is being cared for.

For network operators, Nokia NetGuard Endpoint Security provides information on the security status of their networks, enables proactive support for infected subscribers — and reduces the number of calls to customer support.

Our device-independent solution simplifies usage, while ensuring the same service level for all subscribers. It works by analyzing network traffic patterns from telco services, such as mobile or fixed broadband and SMS. So it can offer earlier malware detection than conventional systems that are based on classic signature mechanisms and other generic methods.

Using an integrated malware intelligence database from our partners, Nokia NetGuard Endpoint Security correlates suspicious network traffic patterns to known threats. This self-learning method detects new malware almost instantly, enabling immediate action to reduce problems for subscribers.

"Operators are in a unique position to protect their networks and their customers' connections and content. By extending its mobile network security portfolio out to the user device, Nokia is taking its portfolio beyond infrastructure based solutions to directly protect subscribers against mobile malware."

Patrick Donegan,
Senior Analyst, Heavy Reading
**Automatic malware containment**
After detecting malware, NetGuard Endpoint Security automatically contains its activities, for example by alerting the subscriber to the contamination or taking actions on the network — such as preventing premium-rate SMS messages from being sent by affected subscribers.

**Dashboards**
Nokia NetGuard Endpoint Security has a customized monitoring dashboard for mobile broadband operators which provides detailed infection data in real time. This information includes the infected subscribers list and several telco-specific statistics, such as the most affected locations or device types. In addition, a “corporate customer” portal allows operators to see the malware infection rates per corporation and take actions to mitigate the problems. This protection, such as for corporate BYOD cases, is an additional differentiator and revenue source for network operators.

**Monitoring and reporting**
Identify and quantify mobile malware security threats

**Subscriber mitigation**
Inform and help subscribers get rid of the malware

**Network mitigation**
Proactive actions on the network to mitigate the risks
Key benefits of Nokia NetGuard Endpoint Security

Reduced time between detection and mitigation. Our network-based solution is device operating system agnostic, allows operators to see the security status of the device on the network, and enables proactive support for infected subscribers. These capabilities result in a “cleaner” network that carries less malware traffic.

Revenue-generating services. With NetGuard Endpoint Security, service providers have the opportunity to increase revenue by selling device security packages and to address new markets, such as mobile payment.

Enhanced customer experience. For subscribers, NetGuard Endpoint Security offers the best available protection against malware, because it combines both network and anti-virus protection in one solution. Providing immediate information when their device is infected, the solution prevents bill shock and gives users peace of mind that their security is being cared for, improving the customer experience.

Brand protection. By immediately detecting and proactively mitigating infected devices, service providers can effectively maintain service quality and limit erosion of their brand due to potential security breaches. These improvements, in turn, can reduce subscriber churn and cut the number of support and customer care calls, resulting in lower operating expenses.
Why Nokia?

Nokia is a proven leader in fixed, mobile, and IoT security. Our portfolio of cyber security solutions takes a holistic approach to securing service providers and protecting end users — from telephone communications to IT-based cloud architectures. We focus on communication infrastructure requirements and continuously optimize our solutions and services to provide specific answers to security threats. Today, we are involved in more than 500 security projects worldwide, offering capabilities that range from design to support. We also lead the industry in securing commercial LTE networks. We leverage our work in security standards forums to design solutions that fully address the security requirements of complex networks.

NetGuard Endpoint Security is available today. Talk to your Nokia representative to learn more about how to protect your customers and connected devices, or visit our website for more information on our Endpoint Security solution.
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: SR1712020264EN (December)

© 2017 Nokia