Secure endpoints to protect your business: apps, mobility, and the internet of things

NetGuard Endpoint Security compared to other malware detection methods

White paper
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Detection technologies</td>
<td>4</td>
</tr>
<tr>
<td>Signature-based detection</td>
<td>4</td>
</tr>
<tr>
<td>Privacy issues</td>
<td>7</td>
</tr>
<tr>
<td>Other detection methods</td>
<td>7</td>
</tr>
<tr>
<td>Detection technology comparison</td>
<td>9</td>
</tr>
<tr>
<td>Signature development</td>
<td>10</td>
</tr>
<tr>
<td>Measuring coverage</td>
<td>10</td>
</tr>
<tr>
<td>Detection rules development</td>
<td>11</td>
</tr>
<tr>
<td>Weekly rules update process</td>
<td>11</td>
</tr>
<tr>
<td>Next Gen Endpoint Detection and Response when combined with SOAR</td>
<td>12</td>
</tr>
<tr>
<td>Conclusion</td>
<td>13</td>
</tr>
</tbody>
</table>
Introduction

Nokia NetGuard Endpoint Security is an end-to-end, consumer-facing, malware detection, notification and remediation service. It provides service providers with a turnkey solution that allows them to meet or exceed standards and best practices established by governments and industry groups on malware mitigation. It also allows them to offer enhanced security services to their customers, which increases revenue and reduces customer churn.

The system includes:

- Carrier-scale network sensors that detect malware activity in network traffic
- Alert aggregation that automatically maps IP addresses from the alert to the subscriber account
- Automatic customer notification via SMS, smartphone app, e-mail or web interstitial
- Self-serve remediation portal that can also serve in a walled garden environment
- SDK for integration with smartphone app
- White-labeled smartphone app
- Helpdesk portal to assist customer support
- Security analytics portal allowing access to infection details and security forensics.

The system was designed to operate in large-scale broadband and mobile networks hosting millions of subscribers. It uses offline intrusion detection technology that provides better coverage and accuracy than competing technologies, without impacting network performance.

Figure 1. The Nokia Netguard Endpoint Security solution
Figure 1 illustrates the system architecture. Sensors in the carrier network monitor the network traffic between user endpoints and the internet, looking for evidence of malware infection. This includes malware command-and-control (C&C) traffic, exploit attempts, hacking activity, suspicious behavior and DDOS activity. Alerts are sent to a central alert reporting cluster where they are analyzed and stored. Interfaces provide real-time information feeds to SIEM (security information and event management), firewalls and policy enforcement systems. The system also includes a fully automated end-user notification system and a self-serve remediation portal.

This white paper compares the detection technologies that are available and illustrates why signature-based intrusion detection technology provides better coverage and accuracy than the competing technologies. It then goes on to describe how Netguard Endpoint Security maintains the detection rule set, providing coverage for 100 percent of the most active malwares.

### Detection technologies

If you are going to notify a user that they have a malware infection and lead them through a remediation process, you must be very confident that they are actually infected. It is also important to identify the type of malware causing the infection. This lends considerable credibility to the notification and assists in customizing the remediation process. The detection method must:

- Provide indisputable evidence that the user is infected
- Positively identify the malware involved
- Provide coverage for a wide variety of malware.

Signature-based intrusion detection technology that is focused on detecting the C&C exchange between the malware and its controller meets these criteria.

#### Signature-based detection

Netguard Endpoint Security focuses on evidence of infection coming from the user’s computer or mobile device. This provides an accuracy and coverage that is not available from other detection technologies. The key is to focus on the C&C protocols that are used. If we see a consumer device using a known C&C protocol then we know, with great certainty, that it is infected with the specific malware that uses that C&C protocol. The detection rules look for:

- Malware C&C communications
- Backdoor connections
- Attempts to infect others (e.g., exploits)
- Hijacked browsers and spyware activities
- Excessive e-mail
- Denial of service (DoS)
- Hacking activity.

The Snort engine provides a rich language that allows detection rules to be based on IP addresses and ports, packet content, session state, flow direction and event thresholds. It also enables the creation of detection rules that correlate events within a specific flow and across flows.
Effectiveness

There is some confusion between signature-based anti-virus (AV) detection and what Netguard Endpoint Security does. Traditional AV software uses signatures based on file content to identify files that contain malware. The malware creators repackage and modify these malware files at an alarming rate to avoid detection by AV software. AV vendors struggle to keep up with this incredible turnover.

In contrast, Netguard Endpoint Security’s signatures focus on network behavior and C&C protocols. These remain stable over time, unlike the malware files themselves. For example, Netguard Endpoint Security has over 15,000 distinct versions of the ZeroAccess bot in its malware sample database. A single detection rule successfully detects all these variations. The malware creators will often change the packaging, but rarely change the C&C protocol.

Intrusion-detection technology also has a reputation for false positives. This is mostly because IDS devices are usually configured to look for any suspicious activity, including a large number of unsuccessful attacks. The Netguard Endpoint Security detection rules are looking for specific C&C traffic, known exploits, backdoor connections and Trojan activity that are known to be associated with a specific malware infection.

Zero-day attacks

Netguard Endpoint Security generally does not focus on trying to detect zero-day attacks. The detection rules are designed to detect known malware with a very high accuracy rate. There is also a major benefit in being able to positively identify the malware when it comes to the notification and remediation stages.

When a new threat is discovered, the global security research community is very quick to react. We can have a detection rule deployed within a few days of the malware's discovery. As noted above, because we are focused on detecting the C&C protocol, which rarely changes, our detection rules will continue to detect new versions of the malware as it evolves.

In some cases, instead of the C&C, we use specific exploit attempts to detect the malware activity. In these cases, we do have true zero-day detection, as brand-new malware uses old exploits. In this way we had zero-day coverage for Mirai, Wannacry, NotPetya and a host of others.

Blocking malware downloads

The system is not inline and does not block malware downloads. This is not a major issue. Competing technologies such as “next-gen firewalls” claim to be able to detect and block malware downloads, but in practice, it is very difficult to do in an effective way, particularly at the data rates required in a large-scale carrier network. The following issues impact the effectiveness of this technology:

- Almost all malware downloads today are done over encrypted HTTPS connections and the file downloads cannot be detected unless the traffic is decrypted
- When this feature is activated, it greatly reduces the traffic processing capability of the detection device and drives up the cost considerably
- To handle the “polymorphic” malware, the detection device needs millions of signatures, just like anti-virus systems. In addition to making the systems more difficult to keep up to date, this also impacts performance and cost.

It is possible to block known malware sites based on blacklisted IP addresses and domain names, but this does not provide the coverage required and is difficult to apply in the case of smartphone malware, which is often downloaded from otherwise legitimate app stores.
Encrypted traffic

Concern is often raised about the ability of signature-based systems to detect encrypted C&C traffic. Surprisingly, very few malware C&C protocols are encrypted. These include such notables as Zeus, Spyeye, Alureon, Flashback, Rustock, Waledac, Grum, Bredolab, Salty, Bobax, Torpig, Mirai, Satori, Wannacry and NotPetya.

Those that do use encryption can be identified by network traffic characteristics that cannot be encrypted. These include the initial handshake between the malware and its controller, key exchanges, file downloads, traffic patterns, exploit attempts and scanning activity.

Malware that uses customized cryptography is very easy to detect. For example:

- ZeroAccess bot uses the same 16-byte initialization sequence when contacting the C&C server and is trivial to detect; it uses RC4 encryption, but because it always uses the same key, the encrypted data from the initialization is always the same.

- Mazben downloads an encrypted PE file with very specific 8-byte content that is detected; the file signature is unique and provides very strong evidence of infection.

- Cutwail/Pushdo issues a fairly obvious HTTP GET request containing some setup parameters and an encryption key exchange, thus a signature can easily be detected.

- Despite protecting its C&C payloads using encryption, Conficker is detected due to the Netbios exploit it uses to spread through the network.

- Lethic is identified by a combination of packet size and content over a three-packet exchange.

- Mariposa/Palevo is detected through the observation of a characteristic C&C op-code sequences over several packets.

Malware will often use SSL/TLS (HTTPS) to encrypt its traffic. This makes it difficult to distinguish the malware traffic from regular HTTPS exchanges. However, the TLS initial handshake and key exchange is done in clear text and often contains sufficient information to identify malware communications. The following information is available:

- Host name of server
- Digital certificate of the server
- Prioritized list of crypto algorithms to use.

These can be combined using a technique known as TSL fingerprinting to distinguish malware traffic from regular SSL/TLS browser traffic. We use this to build our detection rules.

Despite the fact that the C&C is protected by encryption, the malware often exhibits behavior that cannot be encrypted, such as scanning for vulnerabilities, exploit attempts, brute force attacks and specific DDOS activity. This can be used to create high quality detection rules. When all else fails we can always fall back on information from the packet header and map it to IP and DNS blacklists.

The Nokia Threat Intelligence Labs creates the detection rules for Netguard. We analyze live malware samples in a sandbox environment and create the detection rules based on the traffic generated. We track how often we are unable to create a detection rule because of encryption. It has been steady at less than 1% since 2016, despite the increasing use of encryption.
Privacy issues

There are some concerns about the privacy issues involved in using signature-based detection in the network due to parallels with DPI technology. The signatures that Netguard Endpoint Security uses certainly examine the contents of the packets as they are received at the sensor. However, the packet content is never stored or passed on as part of a security alert. When evidence of malware activity is detected, the ID of the malware that triggered the event, along with information from the packet header, is forwarded to the alert aggregation point. The security event simply indicates that malware activity was detected from an IP address at a specific time. The privacy implications of this are no greater than any other detection technologies that determine that an IP address is infected with malware.

There are also privacy concerns with respect to the management of the security alert information. This must be managed in a secure and sensitive manner. The Netguard Endpoint Security service provides the ISP with various options to ensure that they can meet privacy requirements. Options are provided to only store security events for users that have opted into the service. In addition, options are provided to conceal the IP addresses and other PII using a one-way hash that cannot be traced to the original value or to zero the field entirely.

Other detection methods

There are other detection techniques, some of which can be combined with the signature-based technique described above. The pros and cons of these are discussed below.

Blacklists

A lot of the research effort in malware detection is devoted to finding the malware C&C sites. A common technique is to capture a sample of the malware in a honeypot and watch what it does. Inevitably, it will try to connect to its C&C server and the researcher will now be able to add that IP address or domain name to one of the many blacklists that are available. These blacklists can be deployed in firewalls or DNS servers to prevent users from accessing malicious sites.

So surely a user connecting to one of these blacklisted IP addresses or domains must be part of a malware botnet? Unfortunately, this is not always the case.

• Many malware C&C sites are actually hosted on servers that also host legitimate services, which is especially true of malware that uses web protocols for C&C
• Some are hosted on legitimate sites that were compromised and subsequently fixed, however, they have not been removed from the blacklist
• Some use fast-flux DNS rallying techniques to vary the IP address faster than the blacklists can keep up.

Because of these issues, blacklists provide far too many false positives. Netguard Endpoint Security verified this in a number of network trials using both IP and domain-name blacklists. In one test, over 60 percent of the user population visited sites on a Zeus blacklist in a one-week period. In reality, the actual Zeus infection rate (based on signatures) was less than one percent. The problem was that a couple of the blacklisted IP addresses pointed to popular sites that may have been compromised at some point in the past. Visiting one of these sites did not mean that the user was infected with Zeus. Note that it is easy to know when to add an IP address to a blacklist, but it is very difficult to determine when it should be removed.

Blacklist accuracy can be improved when combined with other detection techniques. The Netguard Endpoint Security system combines blacklists with content-based signatures to improve accuracy.
DNS-based detection

DNS-based malware detection systems use blacklists of known malware domain names to prevent users from visiting those sites. This can be implemented in the DNS server itself, or in a specialized DNS security server deployed in front of the DNS server. The names on the blacklist can be generated by honeypot malware analysis or through traffic analysis techniques. The latter detects the characteristic “fast flux” patterns in the DNS traffic that malware uses when trying to locate their C&C sites. This detection technique provides limited coverage because it is only applicable to malware that use “fast-flux” rallying techniques.

DNS-based solutions are cheap to install and provide some degree of protection, but they have three major weaknesses. First, not all malware uses DNS and, thus, it is completely invisible to this detection technique, including:

- IOT bots such as Mirai, Hakimi and Satori
- Ransomware such as Wannacry and NotPetya,
- Peer-to-peer botnets such as ZeroAccess, TDSS and Alureon
- Banking trojans such as Zeus and SpyEye.

Second, it is relatively easy for malware to bypass the carrier’s DNS-based system and go directly to DNS systems on the internet. Since this is a legitimate usage, they cannot be blocked by the carrier without breaking a number of legitimate applications. The solution is to deploy an additional DNS security server on the internet connection to intercept these requests. Finally, blacklists are prone to false positives, for the reasons outlined in the previous section.

Firewalls

Firewalls provide a rich suite of malware detection and prevention options. Unfortunately, the activation of these features has a huge impact on the traffic processing capabilities of the firewall. A firewall that can handle 10G of traffic with basic application-aware blocking can be reduced to 1G when malware detection features are turned on. This can make the technology prohibitively expensive to deploy in-line in large carrier networks.

Most firewalls have intrusion detection and prevention features that are similar to those used in Netguard Endpoint Security, but the Layer-seven packet inspection required to support these features is very expensive to do in-line, where latency and packet loss cannot be tolerated.

At first glance, one of the most attractive features offered by firewalls is their ability to detect and block malware downloads. This is even more expensive to turn on than the intrusion detection feature. In practice, it is of very little value, since most downloads today are via HTTPS, thus encrypted. For the most part, the firewall is completely unaware that a download is taking place.

Blocking access to known malware download sites is certainly doable from a performance perspective, but it is not practical in the smartphone malware eco-system. Most smartphone malware is embedded in trojanized applications that are downloaded from “app stores”. The Apple and Google app stores are relatively malware free, although periodically malware varieties manage to sneak through their defenses. However, in the Android eco-system there are thousands of third-party app stores that are not as well protected and are being used for malware distribution. It is a difficult decision to block access to an entire app store because it is an occasional source of malware.
Honeypots
Honeypot computers and networks can be set up to attract infection. The idea is that malware scanning the network for victims will find these vulnerable systems and attack them. This is very strong evidence that the attacker is infected or operated by a hacker. The main problem is that honeypots are only effective at detecting malware that spreads through network vulnerabilities. These days, this is a relatively small percentage of the malware ecosystem.

Sinkholing
ISPs can use DNS sinkholing techniques to redirect traffic that was intended for known malware C&C locations to a honeynet server. Anyone who visits the server is likely infected by the malware. The main advantage over the simple blacklist is that the honeynet server can verify that the visitor is using the malware’s C&C protocol. This is an excellent detection methodology since it provides accurate detection and can identify the specific malware, however, it can be quite labor intensive (and costly) to maintain.

Scanning
It has been suggested that scanning for vulnerable systems could be useful in malware detection. While it could be of value to inform the user that their computer is vulnerable, this certainly does not provide any level of confidence that the user is infected with malware. Scanners that identify the backdoors used by specific bots can give the required accuracy. However, there are significant legal and technical issues associated with scanning consumers’ devices.

Traffic-flow analysis
There is considerable research into the use of network flow statistics to detect malware infection. No doubt, the increased network activity associated with DDoS attacks and sending spam can be easily identified in the network and attributed to malware activity. This technique can also be used, in some cases, to identify characteristic C&C activity. It is very useful for identifying that an incident is occurring, but does not usually provide the information required to determine what malware is responsible. It does not meet the criteria for low false positives and positively identifying the malware.

Spam
If a user is sending spam, they are probably infected with malware. Often the e-mail content can be used to identify the specific spam-bot that is being used. In those cases, it does meet the criteria of being able to positively identify the malware with a very low false positive rate. The only problem with using spam and the detection criteria is that it misses the bots that are specifically associated with identity theft and DDoS attacks (though some are multipurpose). The Netguard Endpoint Security system has some signatures that detect excessive e-mail.

Another technique is to use a spam-trap to detect IP addresses that are sending spam and build blacklists based on that. These not only focus on the e-mail volume but also on the content. There are many spam blacklists available. These blacklists can be combined with signatures for greater accuracy.

Detection technology comparison
The table below summarizes the comparison of various detection technologies. The signature-based “intrusion detection” technology used by Netguard Endpoint Security provides better coverage and accuracy than competitive techniques and also identifies the malware. The upkeep is relatively easy since it is handled by the Nokia Threat Intelligence Lab. Most importantly the system can support the traffic scale required for carrier network deployments.
The next table shows how the various detection techniques stack up against various malware types.

<table>
<thead>
<tr>
<th>Malware type</th>
<th>Traffic anomaly behavioral</th>
<th>DNS Behaviour</th>
<th>Blacklists (IP &amp; DNS)</th>
<th>Netguard Endpoint Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exploit Kits</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Rootkit Bots</td>
<td>No</td>
<td>Partial</td>
<td>Partial</td>
<td>Yes</td>
</tr>
<tr>
<td>HTTP Bots</td>
<td>No</td>
<td>Partial</td>
<td>Partial</td>
<td>Yes</td>
</tr>
<tr>
<td>Fake Av</td>
<td>No</td>
<td>Partial</td>
<td>Partial</td>
<td>Partial</td>
</tr>
<tr>
<td>Ad Click Bots</td>
<td>Yes</td>
<td>Yes</td>
<td>Partial</td>
<td>Yes</td>
</tr>
<tr>
<td>DNS Reconfig</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Banking trojans</td>
<td>No</td>
<td>No</td>
<td>Partial</td>
<td>Yes</td>
</tr>
<tr>
<td>p2p Bots</td>
<td>Yes</td>
<td>Partial</td>
<td>Partial</td>
<td>Yes</td>
</tr>
<tr>
<td>RAT</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Backdoors</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>DDOS</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Worm Exploits</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Fast Flux IP</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Fast Flux DNS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Encrypted C&amp;C</td>
<td>Partial</td>
<td>Partial</td>
<td>Partial</td>
<td>Partial</td>
</tr>
<tr>
<td>Zero Day</td>
<td>Partial</td>
<td>Partial</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

The Nokia Threat Intelligence Lab is responsible for ensuring that the detection rule set is up to date and provides coverage for all known active malwares. This is done through an aggressive malware analysis and rules development process, leveraging both internal threat analysis and security expertise, and relevant resources and intelligence from the global security community.

**Measuring coverage**

There are three independent activities that ensure coverage.

1. We actively collect over 200,000 malware samples per day, and have over 100 Terabytes of active malware samples in our Virus Vault. The malware samples are classified, prioritized and run in a sandbox environment to generate network traffic samples. The traffic samples are run against the current rule set to verify that it is detecting the latest version of the malware as seen on the internet. Any samples that fail to trigger are prioritized for further analysis and signature development.
2. As a participant in the internet security community, we have access to threat intelligence from major anti-virus vendors and security labs. This information is used to maintain a list of the top 100 currently active bots. This is correlated with the detection rules and samples databases. Any entries in the top 100 list that are not covered by an active signature are prioritized for immediate action. The latest malware samples are retrieved from the database for detailed analysis and signature development. This ensures 100 percent coverage of the top 100 list.

3. Aggregated malware infection statistics are collected on a daily basis from Netguard Endpoint Security sensors deployed in the field. These show infection trends for specific instances and are used to measure continued coverage. If a specific malware is trending down, we will look for fresh samples to see if the C&C protocol has changed.

Once a malware sample is selected for signature development, it typically takes a few hours to develop and test the signature.

**Detection rules development**

We leverage detection rules from the security community and from a number of third-party sources. The Netguard Endpoint Security rules development team is responsible for filling any coverage gaps and is responsible for about 60 percent of the rule set. Detection rules are developed in a sandbox environment with live samples of the malware. Traffic from the malware is captured and examined for characteristic network behavior that can be used to identify the malware. The rule is then tested with captured and live traffic from the sample. Additional samples for the same malware are then used to confirm the rule.

**Weekly rules update process**

By default the detection rules are updated and pushed out to the field on a weekly basis. If the need arises, for instance, in case of an emergency, a new rule can be pushed out in a few hours. The regular weekly process is as follows:

1. Available rules are collected from a number of sources:
   a. Nokia Threat Intelligence Lab
   b. Emerging Threats Pro
   c. Blacklist updates from Shadowserver, ZeusTracker, SpyeyeTracker, etc.

2. The new rules are selected for inclusion in the rule set if they meet the following criteria:
   a. Detect traffic that indicates malware infection
   b. Positively identify the malware
   c. Provide accurate detection that will not create false positives

3. The selected rules are run through quality analysis scripts to ensure they conform to standards and rate them for accuracy

4. They are then manually reviewed by the rules development team and added to the update list if they pass the review

5. The new rule set is then generated in “passive” mode, which means that they will be active in the sensors but will not generate any customer-facing activity, only going to “active” mode when actual alerts from a new rule have been verified from the field
6. The rule set is then sent to the QA department for tests, including:
   a. Ensuring the rules are functioning against known malware traffic
   b. Measuring whether the rules have introduced any performance issues
   c. Detecting false positives when tested against clean traffic.

At the conclusion of the testing, and any modifications it requires, the rules are finally pushed to the Alert Reporting Cluster in each NetGuard Endpoint Security customer’s data center. From there, each NIDS sensor automatically pulls a fresh version of the rules. They are installed on the sensor without disrupting the operation of the detection engine. There is no system downtime to deploy the new rules.

### Next Gen Endpoint Detection and Response when combined with SOAR

When combined with a next generation security orchestration, analytics and response (SOAR) system NetGuard Endpoint Security is part of a next generation endpoint detection and response solution any connected endpoint including smartphones and IoT devices,

Nokia’s SOAR solution is NetGuard Security Management Center (SMC). NetGuard SMC aggregates, analyses, and correlates security data from a variety of sources, including NetGuard Endpoint Security. Identified threats can be rapidly addressed using Cyber playbooks to drive automated responses in a closed-loop fully or semi-automated process.

#### Figure 2. Nokia NetGuard SOAR suite

The signature-based detection technology used in NetGuard Endpoint Security NIDS sensors provides indisputable evidence that the user is infected, identifies the malware involved and provides coverage for a wide variety of bots and malware. It leverages the best features of a number of detection technologies to provide accuracy and coverage that individual techniques cannot provide on their own.
This insight can trigger NetGuard SMC to execute appropriate responses cyber playbooks to mitigate the effects of these threats. For instance, firewall rules and policies can be dynamically updated to block malware command and control traffic from infected endpoints.

Figure 3. AI-based malware detection and automated mitigation response

Conclusion

The signature-based detection technology used in Netguard Endpoint Security NIDS sensors provides indisputable evidence that the user is infected, identifies the malware involved and provides coverage for a wide variety of bots and malware. It leverages the best features of a number of detection technologies to provide accuracy and coverage that individual techniques cannot provide on their own. The Nokia Netguard Endpoint Security solution is based on proven intrusion detection technology that combines analysis of the packet headers and content, flow state, traffic thresholds, IP address and DNS blacklists to positively identify the C&C traffic associated with malware activity. In summary, this provides the service provider with the best malware detection technology available.