Nokia Deepfield Secure Genome

Mapping internet security in the cloud era

Nokia Deepfield Secure Genome maps the global internet to provide unprecedented security insights to service providers, webscale companies and large digital enterprises.

Deepfield Secure Genome is a cloud-based data feed that continuously probes and tracks billions of IPv4 and IPv6 addresses on the internet, maps them to Domain Name Server (DNS) names, and employs advanced machine learning (ML) rules to tag the addresses into security-related types and categories. The result is a global, cloud-based, security-focused data feed about internet applications and services: a dynamic security map of the internet.

Secure Genome data can be combined and correlated with network-related data sets for real-time detection and mitigation of distributed denial of service (DDoS) attacks.

Secure Genome is a component of the Nokia Deepfield Genome, a set of two complementary and proprietary data feeds that employ Nokia patented technology:

• Cloud Genome: Provides full visibility of internet content, applications and services.
• Secure Genome: Provides full visibility of internet security-related data.

Secure Genome is an intrinsic part of the Nokia Deepfield portfolio of IP network intelligence, analytics and DDoS security applications for service providers (cable providers, multiple system operators [MSOs], telecommunications service providers), webscale companies and large digital enterprises.

Deepfield applications ingest data from many sources in your network, then process and correlate the data to provide a real-time, multidimensional view of your network, services and IP flows. Deepfield applications are further enhanced by Deepfield Genome to deliver better network insight and facilitate improved performance and security.

Features

• Maps and tracks more than 4 billion IPv4 and 1 billion IPv6 endpoints
• Feeds the Deepfield DDoS analytics engine information on secure and insecure endpoints and data flows
• Employs more than 100 advanced ML rules for automatic classification and precise allocation of applications and flows into security-related traffic types and categories
• Creates and maintains internet security-related whitelists, blacklists and blocklists.

Benefits

• Improves accuracy of real-time DDoS detection by reducing false positives and false negatives
• Allows full matching of network-based information with the internet security context
• Facilitates advanced DDoS mitigation scenarios and automation.
How Secure Genome works

With the large number of public IPv4 and IPv6 addresses, the internet’s security perimeter has expanded significantly. Security threats and attacks are on the rise, and DDoS attacks are becoming much larger, more frequent and more sophisticated. Online piracy (illegal online redistribution and consumption of copyrighted content) is also on the rise, with companies and individuals engaging in online streaming of pirated content to thousands of users. To combat a new generation of attacks as well as online piracy, a cloud-based approach is becoming central to the security strategies of many organizations.

Legacy approaches, where DDoS analytics are derived from dedicated hardware probes, are no longer effective. Legacy DDoS mitigation approaches such as “blackholing” or selective traffic filtering using Flowspec and traffic diversion to dedicated scrubbing centers are no longer effective for sophisticated and terabit-scale DDoS attacks. Network-related information must be augmented with security-related information from the internet to achieve better, more accurate DDoS detection.

Cloud Genome focuses on mapping billions of IP addresses and millions of cloud applications and services to provide a detailed understanding of the global internet supply chain. Secure Genome complements this information with security-related data.

Like Cloud Genome, Secure Genome continuously crawls the internet, mapping, categorizing and updating its internet-wide and security-focused database. Secure Genome maps billions of IP addresses and millions of cloud applications and services to provide a detailed understanding of global internet security (see Figure 1), including:

- Reflectors – A list of open reflectors on the internet, including:
  - Open DNS resolvers
  - Open/insecure NTP servers
  - Open Memcached servers
  - Open SNMP servers

- Known and trusted endpoints and traffic flows (whitelists)

- Known malicious endpoints and traffic patterns (blacklists)

- Commercial and community shared lists about malicious IP addresses (blocklists)

- Safe browsing information obtained from third parties (e.g., Google Safe Browsing data)

- Online piracy-related blacklists.

Secure Genome relies on a number of distributed, cloud-based, data-mining agents. These agents constantly examine and interact with internet endpoints to learn about the services and the traffic patterns, and then build a powerful security map of the entire internet. This map is used for real-time traffic analysis and DDoS detection to provide a level of DDoS detection accuracy and agility that was previously unattainable.

With Secure Genome, false positives (flagging legitimate traffic as a DDoS) and false negatives (allowing malicious traffic to pass) are significantly reduced, resulting in improved DDoS protection.

Figure 1. Deepfield Genome
Deepfield Secure Genome can help identify insecure endpoints and traffic flows in real time. With this information, you can confidently plan your DDoS protection strategies, network-wide mitigation scenarios or approaches to fight online piracy.

Providing context to the Deepfield DDoS applications

Secure Genome provides context to the following security applications:

- **Nokia Deepfield Defender**: Provides real-time DDoS detection and mitigation.
- **Nokia Deepfield Network Firewall**: Uses advanced IP routing elements to establish a closed-loop automation mode of DDoS protection with the network, to expand real-time detection capabilities and enable network-based protection with auto-mitigation capabilities.

Secure Genome also provides security-related context to the Deepfield analytics applications.

An example of how the Deepfield Genome knowledge enhances legacy flow-based information is shown in Figure 2.

**Figure 2. Enhancing legacy flow-based information with Deepfield Genome knowledge**

<table>
<thead>
<tr>
<th>Ingress interface</th>
<th>Egress interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source address</td>
<td>Destination address</td>
</tr>
<tr>
<td>Server type</td>
<td>Device type</td>
</tr>
<tr>
<td>Reflector type</td>
<td>Destination port</td>
</tr>
<tr>
<td>CDN</td>
<td>Hosting provider</td>
</tr>
<tr>
<td>Protocol</td>
<td></td>
</tr>
<tr>
<td>Source port</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td></td>
</tr>
<tr>
<td>Site/service</td>
<td></td>
</tr>
<tr>
<td>Geographical information</td>
<td>Geographical information</td>
</tr>
<tr>
<td>Fully Qualified Domain Name (FQDN)</td>
<td></td>
</tr>
<tr>
<td>Trusted</td>
<td>Untrusted</td>
</tr>
<tr>
<td>Number of bytes</td>
<td></td>
</tr>
<tr>
<td>Number of packets</td>
<td></td>
</tr>
</tbody>
</table>

| Legacy flow-based information | Enhanced by Cloud Genome | Enhanced by Secure Genome |
Deepfield Defender uses Secure Genome information to improve its real-time DDoS detection and analytics capabilities and to facilitate a variety of DDoS protection scenarios, ranging from Border Gateway Protocol (BGP) blackholing to more advanced approaches using Flowspec or scrubbing centers.

Secure Genome empowers Nokia Deepfield Network Firewall to become a powerful forensics and mitigation platform that can enable network-wide orchestration of security policies. Secure Genome also facilitates Nokia 360-degree DDoS protection using Deepfield Network Firewall and the latest generation of Nokia FP4 processor-based service routers, paving the way for security automation and the self-defending networks of the future.

Protecting against next-generation DDoS attacks requires your defense to be context-aware, with full real-time visibility into traffic traversing your network—both incoming (from the internet) and outgoing (from your subscribers towards the internet). The increasing occurrences of malware-infected systems that can act as botnets and the complexity of a new generation of attacks necessitates the ability to differentiate false positives and false negatives with the highest accuracy, and then alert on only those triggers that require follow-up by security teams.

With Secure Genome, new generations of sophisticated morphing and volumetric attacks can be detected with improved accuracy, and more agile mitigation is possible, resulting in quick action that does not incur traffic loss or service downtime.

The Nokia Deepfield advantage

The real-time cloud and network context provided by the Nokia Deepfield solution enables service providers to extract the actionable intelligence needed to better design their networks, react to performance anomalies and changing traffic patterns, manage security threats, and better package their product offerings to attract and retain subscribers.

Nokia Deepfield enables service providers to understand, in real time, the service delivery path from the internet/cloud through the peering edge and at the customer edge—a path that can span multiple clouds, data centers, CDNs and networks. This visibility is the critical first step to intelligent network automation, which will enable networks to respond immediately to changing conditions with minimal manual or physical intervention, lowering costs and improving performance.

To learn more about the Deepfield DDoS security applications, visit the Deepfield web page.