# Nokia Deepfield Secure Genome

## Mapping internet security in the cloud and IoT era

### Nokia Deepfield Secure Genome maintains the “DDoS security map” of the internet to provide unprecedented insights into threats related to Distributed Denial of Service (DDoS)

Deepfield Secure Genome® is a global, cloud-based, DDoS security-focused data feed about internet applications and services: a dynamic security map of the internet. It is a result of Nokia’s patented technology that continuously scans, probes and tracks IPv4 and IPv6 addresses on the internet. IP addresses are tagged into different types and categories using Domain Name Server (DNS) names and advanced machine learning (ML) rules.

Nokia Deepfield Defender combines Deepfield Secure Genome data and correlates it with network-related information (obtained from network routers and other data sources) 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:

- Deepfield Cloud Genome®: Provides full visibility of internet content, applications and services.
- Deepfield 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, internet exchange points (IXPs) and large digital enterprises.

## Features

- Maps and tracks security-related information for over 5 billion IPv4 and IPv6 endpoints
- Feeds Deepfield Defender with information on insecure, potentially dangerous and malicious IP endpoints and threatening DDoS activity
- Employs more than 100 advanced ML rules for automatic classification and precise allocation of the malicious activity of IP addresses and flows into DDoS security-related information
- Creates and maintains DDoS security-related lists of malicious and potentially dangerous IP addresses (blocklists)
- Hourly updates.

## Benefits

- Improves accuracy of Deepfield Defender’s real-time DDoS detection and reduces false positives and false negatives
- Allows real-time correlation of network-based information with the larger internet security context
- Through Deepfield Defender, it facilitates advanced DDoS mitigation scenarios and automation.

# How Secure Genome works

With the increasing number of devices and systems using public IPv4 and IPv6 addresses, the internet's security perimeter has expanded significantly. Security threats and attacks are rising, and DDoS attacks are becoming larger, more frequent and more sophisticated. New DDoS attacks and techniques are on the rise, such as those employing bots – insecure IoT devices that can be exploited and remotely controlled by "botmasters" to launch devastating DDoS attacks on customers and network infrastructure. To combat a new generation of attacks, including botnet DDoS, new, innovative and cost-efficient approaches are becoming central to many organizations' security strategies.

Legacy approaches, where DDoS analytics are derived from dedicated hardware probes, are no longer effective. A new generation of DDoS threats requires a better understanding of the wider internet context and prior history of malicious activity. Also, legacy DDoS mitigation approaches such as "blackholing" or selective traffic filtering and traffic diversion to dedicated scrubbing centers are no longer effective for quickly changing, sophisticated, and terabit-scale DDoS attacks. For more effective mitigation of the latest generation of DDoS, network-related information must be correlated with security-related information from the internet to achieve better, more accurate DDoS detection.

Deepfield Cloud Genome tracks cloud applications and services and maps IP addresses to provide a rich and detailed understanding of the global internet services supply chain. Deepfield Secure Genome complements this information with security-related data.

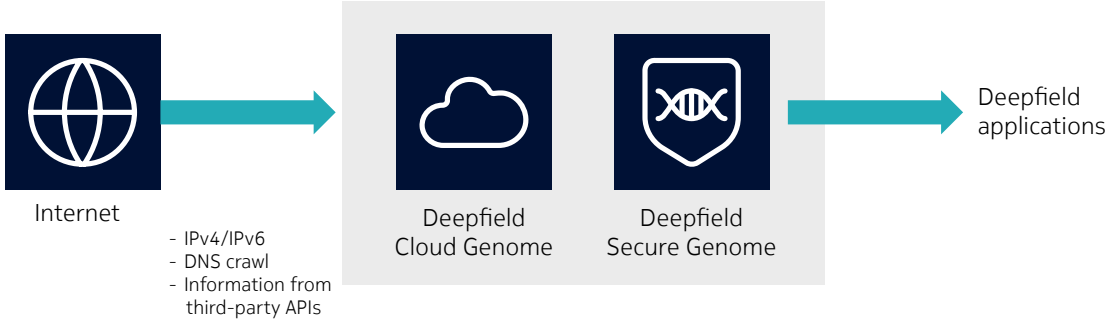
Like Cloud Genome, Secure Genome continuously crawls the internet, mapping, categorizing and updating its internet-wide, security-focused database. Secure Genome maps IP addresses to provide a detailed understanding of global internet security (see Figure 1), including:

- 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
- Known malicious endpoints and traffic patterns
- Commercial and community-shared lists about malicious IP addresses
- Safe browsing information obtained from third parties (e.g., Google Safe Browsing data)
- Online piracy-related blocklists.

Secure Genome relies on a network of distributed, cloud-based, data-mining agents. These agents constantly crawl and probe internet endpoints to learn about the services and the traffic patterns, effectively creating a powerful security map of the entire internet. This map is used for real-time traffic analysis and DDoS detection by Deepfield Defender to provide a level of DDoS detection accuracy and mitigation agility previously unattainable.

Thanks to up-to-date information in Secure Genome, false positives (flagging legitimate traffic as a DDoS) and false negatives (allowing malicious traffic to pass) can be significantly reduced, resulting in improved DDoS detection.

Figure 1. Deepfield Genome



# Providing context to the Deepfield Defender

Deepfield Secure Genome provides DDoS security-related context to Deepfield Defender. This context is used to improve the accuracy of real-time DDoS detection. An example of how the Deepfield Genome knowledge enhances legacy flow-based information is shown in Figure 2.

Figure 2. Automatic tagging of IP addresses into DDoS-related security categories (safe, insecure, potentially malicious, DDoS) by Deepfield Secure Genome

| Src IP | Peer | Genome | % Bytes | % Flows |
|---|---|---|---|---|
| [redacted] | 3462 | [redacted] | 0.23 | 0.22 |
| [redacted] | 4657 | [redacted] | 0.15 | 0.15 |
| [redacted] | 3462 | [redacted] | 0.14 | 0.14 |
| [redacted] | 3462 | [redacted] | 0.14 | 0.13 |
| [redacted] | 4637 | [redacted] | 0.14 | 0.14 |
| [redacted] | 9002 | [redacted] | 0.13 | 0.15 |
| [redacted] | 9002 | [redacted] | 0.13 | 0.12 |
| [redacted] | 9002 | [redacted] | 0.13 | 0.13 |
| [redacted] | 9002 | [redacted] | 0.13 | 0.13 |
| [redacted] | 3462 | [redacted] | 0.12 | 0.12 |
| [redacted] | 4637 | [redacted] | 0.12 | 0.15 |
| [redacted] | 6939 | [redacted] | 0.11 | 0.11 |

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 and more advanced approaches using Flowspec or scrubbing centers to using network-based protection with DDoS mitigation performed by advanced IP routers or a next-generation dedicated DDoS mitigation system.

With the information provided by Secure Genome, Deepfield Defender is further empowered as a powerful forensics and DDoS mitigation platform that can enable network-wide orchestration of security policies.

Deepfield Defender can be deployed with the latest generation of advanced IP routers, such as Nokia FP4, FP5, or FPcx-based IP routers, for network-based protection against DDoS, paving the way for security automation and the self-defending network of the future.

Protecting against next-generation DDoS attacks, such as botnet-based DDoS, requires network defense to be context-aware, with real-time visibility into the traffic traversing the network—both incoming (from the internet) and outgoing (from subscribers towards the internet).

The increasing occurrences of insecure IoT and malware-infected systems that can act as DDoS originators, along with the complexity of a new generation of attacks, necessitate the ability to differentiate between safe and insecure traffic with the highest accuracy while automating large-scale and granular defense that can mitigate DDoS with minimal impact on all other network services and applications.

With Secure Genome, botnet-based and other types of DDoS, including sophisticated morphing, carpet bombing and volumetric attacks, can be detected with improved accuracy. This, in turn, paves the way for Deepfield Defender to drive more agile and automated DDoS mitigation, resulting in increased DDoS protection of customers, services and infrastructure.

## The Nokia Deepfield advantage

Nokia Deepfield is a software suite of network analytics and DDoS security applications for large-scale IP networks. These applications optimize networks and services, enhance customer experience, improve network security and increase operational agility.

Deepfield applications are deployed globally in many networks, including fixed and mobile service providers, cable companies, cloud companies, and digital enterprises.

Deepfield's approach uses big data IP analytics, combining network data (telemetry, DNS, BGP etc.) with Nokia's patented Deepfield Genome technology (live feed that tracks internet content, applications and services and provides DDoS security context). As a result, the Deepfield applications offer multi-dimensional, real-time insights about IP-based services and applications running across the entire IP network - from content-originating domains and CDNs, across the peering and backbone to the customer edge.

Regarding DDoS security, Deepfield Defender represents a foundation for a next-generation DDoS detection and mitigation solution, leveraging rich telemetry and programmability of the IP network itself. Deepfield Defender offers significant benefits over legacy (appliance-based or DPI-based) approaches: better scalability, improved accuracy of DDoS detection (with lower false positives) and more efficient and rapid mitigation in the most cost-efficient manner, delivering holistic, 360-degree DDoS security required for 5G, cloud, and IoT era.

To learn more about the Deepfield solution, visit the Deepfield web page.



Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: CID206727 (September)