Nokia Deepfield Genome Shield

Network security automation and orchestration for Deepfield Defender
Release 26.7

Nokia Deepfield Genome Shield is a foundation for proactive security automation and orchestration that facilitates continuously updated, always-on, network-wide protection against modern distributed denial-of-service (DDoS) attacks and broader security threats.

Genome Shield is designed to help network security teams (NetOps and SecOps) keep pace with fundamental shifts in the DDoS threat landscape. Attacks now originate from within telecommunication provider networks through remotely controlled residential proxy botnets made up of approximately 200 million compromised subscriber devices. Once instructed by botmasters through command-and-control (C2) communication, these devices deliver DDoS attacks in many forms, from DDoS tsunamis (1–10+ Tb/s bursts that arrive within minutes) to persistent, continuous sub-50 Gb/s attacks that can disrupt critical communications. These attacks have unprecedented levels of sophistication and dynamism and are at times driven by AI. Their attack tactics, techniques and procedures (TTPs) employ fast-changing vectors; with AI-enabled tools, attackers are able to monitor the efficiency of their attacks and adjust their TTPs in real time.

Traditional detect-then-divert mitigation was built for spoofed, multi-hour attacks from outside the network. It is structurally too slow for sub-minute bursts and cannot address outbound DDoS attacks by compromised devices within the network.

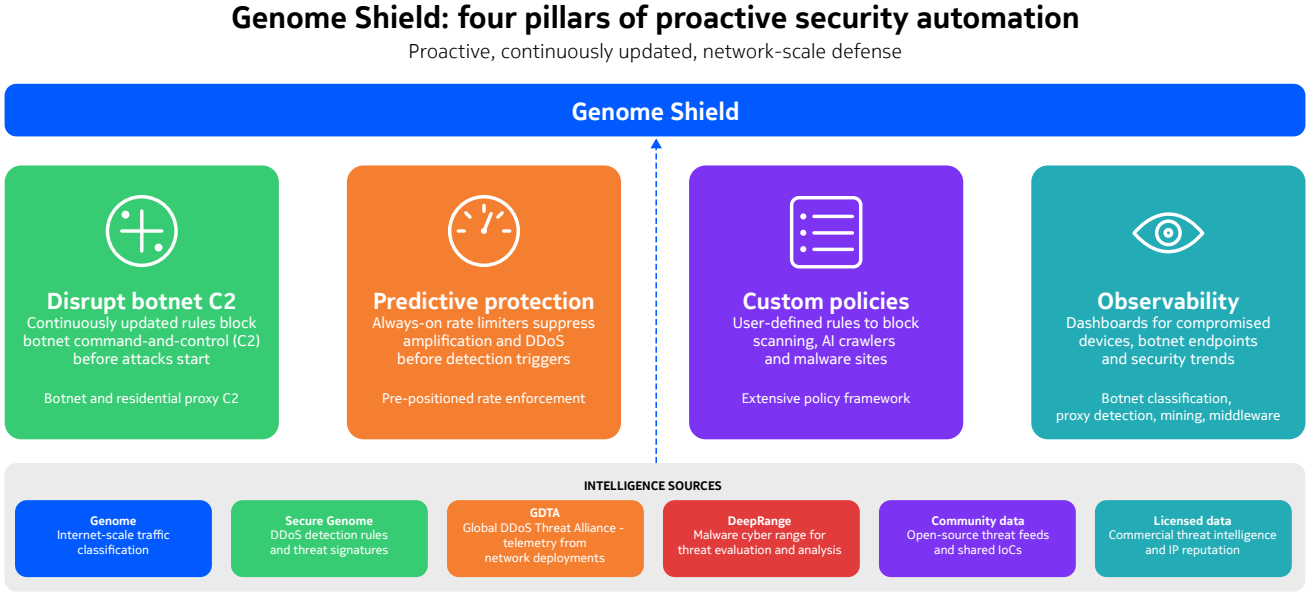

Figure 1. Genome Shield's four pillars of proactive security automation, powered by six intelligence sources

Genome Shield extends **Deepfield Defender**'s capabilities to close this mitigation gap. It aggregates threat intelligence from **six continuously updated sources**, compiles it into **automated security policies**, and enforces them in the data plane of operators' existing routers. There are no diversions, no detours and no added latency. These capabilities turn the network into a self-defending protection mechanism against both inbound and outbound threats.

Genome Shield enables Deepfield Defender to address new types of security use cases, such as outbound DDoS. Legacy approaches face many challenges with detection and mitigation of outbound DDoS; at their best, they are only partially effective and introduce a high percentage of false positives and false negatives.

Features

- **Proactive protection:**
  Always active, continuously enforced defense with no reactive diversion delay.
- **Proactive security orchestration:**
  Automated coordination of network-wide security countermeasures into a unified, proactively enforced posture.
- **Dynamic threat feed management:**
  Aggregates and combines threat intelligence from multiple sources, and makes it available to Defender to be enforced at high scale.
- **Infrastructure defense:**
  Threat management for compromised subscriber devices that attack outward.

Benefits

- Eliminates the diversion mitigation gap with proactive enforcement that responds to bursty, sub-minute attacks that defeat reactive detect-then-divert models.
- Provides real-time protection against thousands of dynamically changing malicious IP addresses at line speed, solving the filter-scale problem that defies modern botnet defenses.
- Replaces in-house developed scripts and ad hoc security automation with a commercial, scalable platform.
- Protects against inbound DDoS attacks and outbound threats from compromised subscriber devices.
- Transforms Deepfield DDoS defense solution into a network security intelligence platform with expanding observability use cases.
- Offers flexible deployment options compatible with router-based edge mitigation (Nokia and third-party routers) and Nokia 7750 Defender Mitigation System (DMS).

Why deploy Genome Shield?

The DDoS threat landscape has undergone a structural transformation. For 25 years, attacks were predominantly spoofed. They originated from external sources and were mitigated through scrubber-based diversion. The rise of residential proxy botnets—networks of close to 200 million compromised devices operating within subscriber networks—has invalidated the assumptions underlying the development of an entire generation of DDoS defense products.

Modern DDoS attacks are non-spoofed and use real IP addresses. They can show up as multi-terabit hyper-volumetric attacks that last seconds rather than hours. They can also come in the form of attack vectors that dynamically and rapidly change source IP addresses, originate from behind home firewalls and network address translation (NAT) systems, and target multiple systems at once.

As of June 2026, potential malicious aggregate bandwidth from residential proxy botnets exceeds 100 Tb/s for each of several Tier-1 US operators, and is bigger than overall traffic level for most countries worldwide.

Genome Shield addresses this structural shift. While legacy approaches treat detection as the core problem, Genome Shield recognizes that the binding constraint has shifted toward proactive security automation and orchestration. It delivers pre-positioned, proactive protection that does not depend on diversion latency, manual intervention or static rule sets.

Genome Shield within the Nokia Deepfield DDoS security solution

Genome Shield adds a proactive automation and orchestration layer to the comprehensive Nokia Deepfield DDoS security solution. It feeds its continuously updated threat intelligence to Deepfield Defender for fast and accurate detection and agile mitigation orchestration.

Genome Shield helps leverage the network's own enforcement points, including Nokia routers —7750 Service Routers with FP4/FP5 silicon, 7730 Service Interconnect Routers with FPcx silicon, and 7250 Interconnect Routers, third-party routers (e.g., Cisco, Juniper) for edge mitigation, and the 7750 DMS, a dedicated mitigation system. When deployed with Nokia routers or 7750 DMS, Genome Shield and Deepfield Defender provide highly accurate, scalable, network-based and network-optimized mitigation that maximizes the benefits of advanced IP technology for network security.

As an advanced security orchestration platform, Genome Shield introduces proactive protection for security use cases that reactive mitigation cannot address, coordinating volumetric, stateful and application-layer countermeasures into a unified, proactively enforced posture. Rather than selecting and configuring individual countermeasures reactively, Genome Shield maintains a comprehensive, continuously enforced defense that dynamically adapts as threat intelligence evolves.

Three problems Genome Shield addresses

Problem	Shield response
Slow, reactive mitigation	**Proactive network-wide protection:** Traditional detect-then-mitigate approaches cannot respond to bursty, sub-minute attacks, and cloud diversion ramp-up times exceed attack duration. Genome Shield provides a pre-positioned, continuously enforced defense.
Infrastructure protection gap	**Outbound and subscriber threat management:** Compromised devices within telecommunication provider subscriber bases attack outward—a problem class that no existing commercial DDoS product addresses at scale. Genome Shield manages inbound and outbound threat vectors.
Security automation vacuum	**A commercial platform for dynamic threat feed management and automated response:** Major telecommunication providers are currently building ad hoc scripts and dedicating 5–10-person teams to maintain custom security workflows. Genome Shield provides a scalable, commercial alternative.

Key capabilities of Genome Shield

Disrupt botnet C2

Continuously updated rules block C2 traffic from all major botnets; our estimate is that we block over 99% of all DDoS C2 malicious traffic. Genome Shield neutralizes attacks at the source to prevent C2 traffic from reaching compromised subscriber devices. Named rule families include C2 disruptors for specific botnet families. Each family is maintained through intelligence from DeepRange, Secure Genome and community data. More rule families are added through ongoing Secure Genome updates.

Dynamic threat feed management

Genome Shield maintains and enforces massive, continuously updated IP threat feeds at network scale. Threat feeds are sourced from Secure Genome, which tracks more than 5 billion IPv4/IPv6 endpoints with hourly updates and 100-plus AI/ML classifiers and also from provider-contributed intelligence. When attacks involve thousands of dynamically changing, real IP addresses, Genome Shield's dynamic threat feed infrastructure ensures that security enforcement keeps pace. In doing so, it addresses the defining operational challenge of residential proxy botnet defense.

Proactive automated enforcement

Unlike reactive mitigation workflows that require detection, decision and diversion before protection begins, Genome Shield operates in a continuously enforced mode. Rules are pre-positioned across network enforcement points. Automated rule injection responds to Secure Genome updates and real-time telemetry without manual intervention.

Outbound infrastructure defense

Genome Shield addresses a problem class that legacy DDoS products were never designed for: protecting the network from its own compromised subscribers. With millions of residential proxy nodes operating behind home firewalls and NATs, Genome Shield provides the outbound threat management capabilities that telecommunication and hosting providers urgently require.

Six intelligence sources

Genome Shield aggregates threat intelligence from six continuously updated sources, combining proprietary research by Nokia with community and commercial data:

- **Deepfield Cloud Genome®:** Internet-scale traffic classification that maps applications, content providers and infrastructure.
- **Deepfield Secure Genome:** DDoS detection rules and threat signatures from analysis of global attack patterns.
- **Global DDoS Threat Alliance (GDTA):** Real-time global DDoS threat telemetry aggregated from Deepfield Defender network deployments (opt-in).
- **DeepRange:** Nokia cybersecurity range that allows infiltration into botnet C2 networks and facilitates secure download and reverse engineering of malware samples.
- **Community data:** Open-source threat intelligence feeds and community-shared indicators of compromise.
- **Licensed data:** Commercial threat intelligence and IP address reputation data from third-party providers.

Network integration

Genome Shield operates through a pipeline that includes three phases: intelligence aggregation, policy compilation and network enforcement. The Shield Compiler/Automation layer generates policies from aggregated intelligence and pushes them to the network through three enforcement protocols: NETCONF for highly granular filter management, FlowSpec for interoperability, and BGP RTBH for bulk traffic discard.

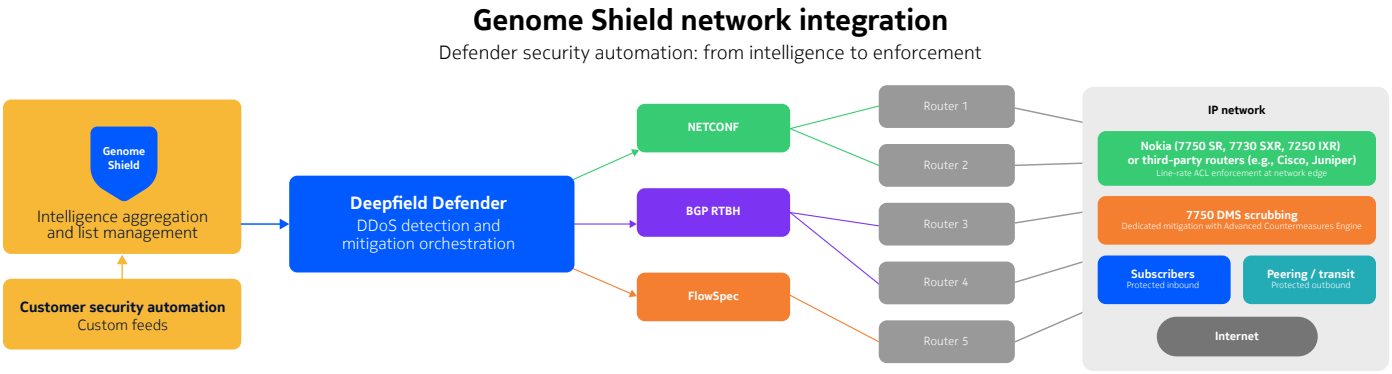

Figure 2. Genome Shield network integration: from intelligence aggregation through policy compilation to network-wide enforcement

Typical deployment scenarios

- Telecommunications providers with millions of compromised subscriber devices that require inbound DDoS protection and outbound C2 disruption from their own subscriber base.
- Hosting providers that require bidirectional protection at scale because they are simultaneously among the most attacked targets globally and source networks for attack traffic.
- Transit providers and internet exchange points (IXPs) that need to protect their infrastructure and customers and lack a tailored commercial security automation solution.
- Network operators replacing ad hoc security tooling because they are currently maintaining custom scripts and dedicated teams to inject filter rules, disrupt C2 infrastructure and manage botnet intelligence manually.
- Service providers with sovereign and on-shore security mandates that require domestic security infrastructure but cannot accept cloud-based security solutions.
- Managed security service providers (MSSPs) and managed DDoS service providers seeking to monetize DDoS protection as a premium, revenue-generating service using Genome Shield-enabled Defender's automated workflows.

Technical specifications

Table 1. Genome Shield specifications

Genome Shield	
Product type	Software platform for security automation and orchestration
Deployment model	On-premises, cloud-based or hybrid
Countermeasure scope	Proactive coordination of security countermeasures into a unified, network-wide enforcement posture
Protection mode	Proactive (continuously enforced); reactive mode also supported
Protection direction	Outbound DDoS C2 disruption and infrastructure defense
Intelligence sources	Genome, Secure Genome, GDTA, DeepRange, community data, licensed data
Enforcement protocols	NETCONF, BGP RTBH, FlowSpec
Threat feed management	Dynamic, automated, Genome-sourced and provider-contributed threat feeds
Management interface	Deepfield Defender GUI, REST API

Table 2. Genome Shield countermeasure families

Countermeasure families	
Botnet C2	Continuously updated rules block botnet C2 communications before attacks start
Residential Proxy C2	Disruption of residential proxy C2 infrastructure
Custom policies	User-defined rules via static lists and the Deepfield Defender UI or API for operator-specific threat identification

Table 3. Compatible enforcement infrastructure

Enforcement points	
Edge mitigation	Provided by line-rate filter enforcement at the network edge using Nokia routers (7750 SR family based on FP4/FP5 silicon; 7730 SXR family based on FPcx; 7250 IXR family) or third-party routers (e.g., Juniper, Cisco)
Dedicated scrubbing	Provided by Nokia 7750 DMS-1-24D, which supports up to 2.8 Tb/s of mitigation capacity per system, or up to 2.4 Tb/s with Advanced Countermeasures Engine (ACE), for application-layer countermeasures
Architecture	Genome Shield helps Deepfield Defender orchestrate proactive mitigation across edge (Nokia or third-party routers), 7750 DMS, third-party scrubbing systems or a combination of these, depending on operator requirements and network topology

Genome Shield is uniquely positioned to help telecommunication providers, AI and cloud providers, hosting companies, IXPs, research and education networks, and large digital enterprises defend against emerging and future threats by shifting from reactive mitigation to proactive protection against DDoS and other types of attacks.

About Nokia

Nokia is a global leader in connectivity for the AI era. With expertise across fixed, mobile, and transport networks, powered by the innovation of Nokia Bell Labs, we're advancing connectivity to secure a brighter world.

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

Document code: CID215420 (July)