NOKIA

Your network is the shield

Nokia Deepfield Genome Shield: Proactive, always-on DDoS protection for the AI era





DDoS has flipped. Attacks now come from inside provider networks — roughly 200 million compromised subscriber devices, monetized for AI scraping and weaponized for crime and conflict. Most attacks are over in under five minutes, before reactive defenses even engage.

Nokia Deepfield Genome Shield turns the network into a continuously enforced, self-defending shield.

Pre-positioned defense
Protection is in place before the attacks hit

Stop attacks from within
Protect your subscribers and stop outbound DDoS traffic

No diversion, no detour
Enforced in the routers you already deploy

MEASURED ACROSS 140+ OPERATOR DEPLOYMENTS

The new DDoS, by the numbers

Data collected by the Nokia Deepfield Emergency Response Team (ERT) from global deployments, and from the Nokia Threat Intelligence Report 2025.

77%

of all attacks end within five minutes — before most reactive defenses engage

37%

of all attacks end within two minutes; time-to-peak is typically 1-3 minutes

82%

of all attacks stay below 50 Gb/s — modest individually, lethal collectively

58%

of all attacks are multi-vector, defeating single-signature mitigation

52%

of all attacks are multi-target, carpet-bombing many prefixes at once

200M+

exploitable subscriber devices form today's residential proxy botnets

DDoS at country scale

Marshaled simultaneously, the compromised devices across Tier-1 US carriers could generate aggregate firepower in the hundreds of terabits per second — exceeding 100 Tb/s for each of several Tier-1 US operators, and more than the total traffic of most countries. DDoS is now a national-security concern, not just an operator issue.

Key takeaway: Small, short, swarming and from within: today's attacks are invisible to threshold-based systems and over before detect-then-divert can respond.

DDoS got monetized, weaponized — and moved inside your network

For more than two decades, DDoS followed a predictable playbook: spoofed traffic from shady-but-known hosting environments outside the network, at gigabit scale, mitigated by diverting traffic to scrubbing centers. In 2025, that pattern broke.

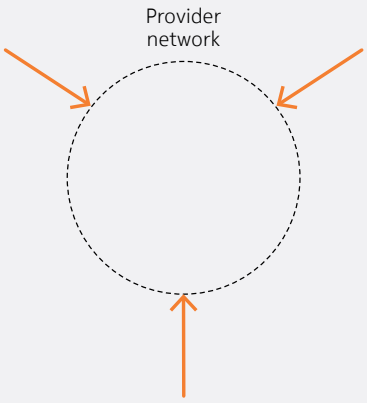
Today, many of the largest threats originate from a provider's own subscribers. Hundreds of thousands of handsets, home gateways and IoT devices inside Tier-1 networks are quietly compromised — weaponized without their owners' knowledge — and marshaled into residential proxy botnets that generate multi-terabit attacks worldwide.

The hidden engine is the residential proxy market: middlemen pay app developers to embed proxy SDKs, and some device makers even ship malware in factory firmware. AI scraping demand has turned this from a niche into a multi-hundred-million-dollar business — in effect, AI has funded the world's largest compromised installed base. The same devices are then sub-leased to criminal organizations and nation-state actors.

The result for operators: degraded RAN, backhaul and peering performance, poisoned IP reputation across the subscriber base, and the collapse of legacy DDoS response timing — most attacks now end before legacy mitigation even engages.

THEN: outside-in

Spoofed, multi-hour, gigabit-scale attacks from external hosts

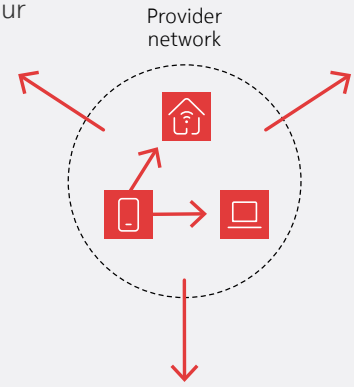


NOW: inside-out

Non-spoofed, sub-5-minute, terabit bursts from your own subscribers

NOW: East-West attacks

Attacks from within your network, on or affecting other subscribers



Key takeaway: The assumptions behind an entire generation of DDoS defense products — spoofed sources, hours-long attacks, time to divert — no longer hold.

Why reactive defense loses the race

Detect-then-divert was engineered for a different era: spoofed, multi-hour attacks from outside the network. Against a DDoS tsunami — a 1-10+ Tb/s burst that ramps in seconds, lasts minutes and recurs in waves — its timing is structurally wrong. By the time alerts escalate and traffic is diverted to scrubbing, the attack is over and the damage is done.

Three problems Genome Shield was built to solve

Reactive mitigation is too slow

Detect-then-mitigate cannot respond to bursty, sub-minute attacks; cloud-diversion ramp-up times exceed attack duration.

The infrastructure protection gap

Compromised devices inside subscriber bases attack outward — a problem class no other commercial DDoS product addresses at scale.

The security automation vacuum

Major telcos are writing ad hoc scripts and dedicating 5-10-person teams to maintain custom security workflows by hand.

Key takeaway: Defense must already be in place when the wave hits — not activated after detection. That shift, from reaction to pre-positioning, is the whole point of Genome Shield.

The impact of outbound DDoS is too high to ignore

Degraded service for other subscribers

Compromised devices flood shared access and aggregation links; innocent subscribers on the same infrastructure see latency spikes, packet loss, and outages.

Wasted and congested peering capacity

Outbound DDoS consumes peering and transit capacity the operator pays for, congesting egress links, degrading interconnection quality, and inviting de-peering or blocklisting by upstream and peer networks.

Regulatory exposure

Regulators can impose high fines and remediation orders that far exceed the cost of prevention.

Key takeaway: Every attack that originates from within your network costs you three times: in subscriber experience, in wasted peering capacity, and in regulatory exposure — making prevention at the source the most effective and cost-effective option.

INTRODUCING

Deepfield Genome Shield

A foundation for proactive security automation and orchestration — continuously updated, always-on, network-wide protection against modern DDoS and broader security threats, delivered as an extension of Deepfield Defender.

Genome Shield inverts the defensive model. Instead of waiting to detect and divert, it aggregates threat intelligence from **six continuously updated sources**, compiles it into **automated security policies**, and enforces those policies in the data plane of the routers operators already run — at line rate, across the whole network.

There are no diversions, no detours and no added latency. The network itself becomes a self-defending protection mechanism against both inbound attacks and the outbound threats generated by compromised subscriber devices — a use case legacy products were never designed to handle.

1 AI-era proactive security

Industry-first proactive, always-on security automation built for the AI era — pre-positioned defense, not reactive mitigation.

2 Intelligent data plane policies

Six continuously updated intelligence sources compiled into automated policies, enforced in the routers service providers already deploy.

3 Network as a shield

Turns the network itself into the shield — no diversion, no detour, no added latency, no new dedicated appliances required.

While legacy approaches treat detection as the core problem, Genome Shield recognizes that the binding constraint has shifted — toward proactive security automation and orchestration.

Key takeaway: Genome Shield turns Deepfield Defender into a unified, always-on shield: protection that is already running when the attack begins.

HOW IT PROTECTS

Four pillars of proactive enforcement

Genome Shield extends Deepfield Defender with four families of continuously enforced countermeasures — pre-positioned across the network so protection runs before, during and after every attack wave.

Disrupt botnet C2

Continuously updated rules block botnet and residential proxy command-and-control (C2) communications before attacks are launched — neutralizing attacks at the source. Named rule families target specific botnet families and are maintained through Secure Genome updates and live DeepRange intelligence.

Nokia estimates Genome Shield blocks over 99% of DDoS C2 malicious traffic.

Predictive protection

Always-on rate limiters suppress amplification and volumetric attack traffic before detection triggers. Enforcement is pre-positioned across the network, so protection runs continuously rather than waiting for a detect-then-mitigate workflow to fire.

Pre-positioned rate enforcement — no diversion delay.

Custom policies

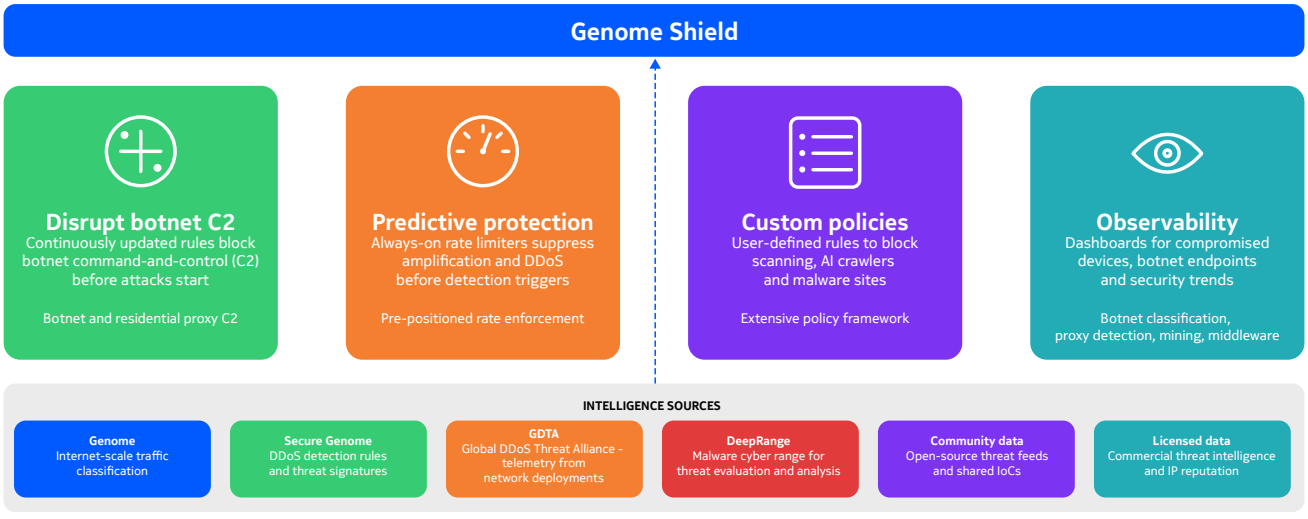
User-defined rules — created via open APIs or the Deepfield Defender UI — block scanning, unwanted AI crawlers and malware sites, and tailor responses to each operator's topology and policy framework.

An extensive, operator-specific policy framework.

Observability

Security-focused dashboards expose compromised devices, botnet endpoints, proxy and mining activity, and emerging threat trends — the visibility teams need to validate automated responses and surface new patterns.

From DDoS defense to a network security intelligence platform.



Key takeaway: C2 disruption stops attacks before they launch; policers absorb what still arrives; custom policies and observability keep the posture tuned to your network.

WHAT FEEDS THE SHIELD

Six continuously updated intelligence sources

Protection is only as fresh as the intelligence behind it. Genome Shield combines Nokia's proprietary research with community and commercial data, compiling all six streams into one enforced policy set.

Cloud Genome

Internet-scale traffic classification mapping applications, content providers and infrastructure.

Secure Genome

DDoS detection rules and threat signatures spanning 5+ billion IPv4/IPv6 endpoints, with hourly updates and 100+ AI/ML classifiers.

Community data

Open-source threat intelligence feeds and community-shared indicators of compromise.

Licensed data

Commercial threat intelligence and IP reputation data from third-party providers.

Global DDoS Threat Alliance

Real-time global DDoS telemetry aggregated from participating Deepfield Defender deployments worldwide (opt-in).

DeepRange

Nokia's cybersecurity range: live insight from botnet C2 infiltration and secure malware reverse engineering.

Herd immunity for the internet

Every Defender deployment that joins the Global DDoS Threat Alliance (GDTA) makes Secure Genome smarter for every other member. Attackers share infrastructure, tooling and intelligence — through GDTA, defenders do too.

The more networks contribute, the faster new botnets, vectors and C2 infrastructure are identified and neutralized for all.

Key takeaway: Six live intelligence streams, one continuously enforced policy set — updated hourly, not at the speed of a maintenance window.

From intelligence to enforcement

Genome Shield operates through a three-phase pipeline: intelligence aggregation, policy compilation and network enforcement. Policies are pushed through standard protocols, so the whole network — Nokia and third-party — becomes the enforcement fabric.

1. Aggregate

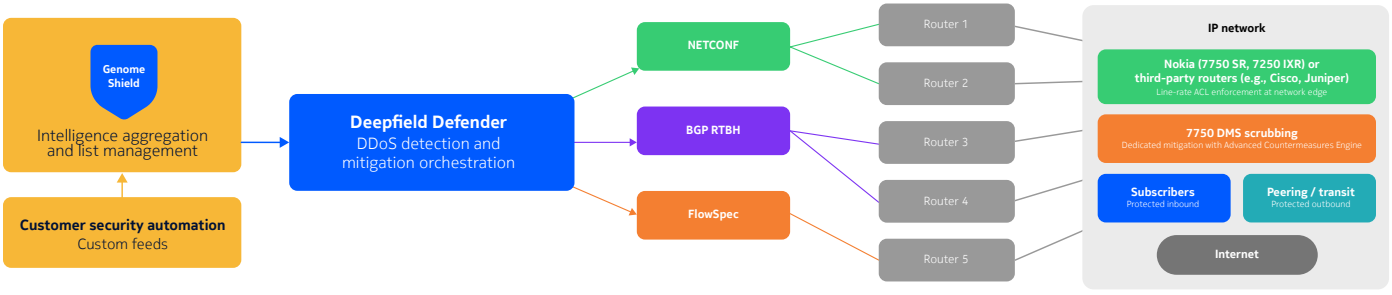
Genome Shield fuses six intelligence sources plus custom operator feeds into managed, deduplicated threat lists.

2. Compile

The Shield compiler and automation layer turns intelligence into enforceable security policies, with Deepfield Defender orchestrating detection and mitigation.

3. Enforce

Policies are pushed to the data plane via NETCONF (granular filters), FlowSpec (interoperability) and BGP RTBH (bulk discard).



The enforcement fabric: the network you already have

Edge mitigation. Line-rate ACL enforcement on Nokia 7750 SR (FP4/FP5 silicon) and 7250 IXR routers — or third-party routers (e.g., Cisco, Juniper).

Dedicated scrubbing. Nokia 7750 Defender Mitigation System (DMS-1-24D): up to 2.4 Tb/s of mitigation capacity per system in 3RU, including the Advanced Countermeasures Engine for L4-L7 protection.

Flexible architecture. Orchestrate proactive mitigation across edge routers, 7750 DMS, third-party scrubbers, or any combination — on-premises, cloud or hybrid.

Bidirectional coverage. Protected inbound (subscribers, services) and protected outbound (peering and transit) — one platform, both directions.

Management

Deepfield Defender GUI and REST API

Deployment

On-premises, cloud or hybrid; requires Deepfield Defender

Licensing

Pay-as-you-grow: start focused, expand as your threat surface grows

Key takeaway: No new appliances, no traffic detours: Genome Shield makes the routers and silicon you already operate do the protecting — at line rate.

WHO IT'S FOR

Where Genome Shield makes an impact

Genome Shield is in use by Deepfield Defender customers today, addressing both inbound DDoS and the outbound threats originating from compromised subscriber devices.

Telecommunications providers

Millions of subscriber devices mean both inbound DDoS exposure and an outbound C2 problem. Genome Shield delivers bidirectional protection at scale from a single automated platform.

Hosting providers

Simultaneously among the most attacked targets globally and source networks for attack traffic — hosting providers need protection that works in both directions at line rate.

AI, cloud and large digital enterprises

High-value compute infrastructure is a prime DDoS target as AI workloads scale. Always-on defense, with no diversion latency, keeps services available.

Transit providers, IXPs, research networks

Infrastructure operators that protect many downstream customers gain a tailored, commercial security automation platform — no more home-grown tooling.

Sovereign and on-shore mandates

Where regulation or policy rules out hyperscaler and cloud-based DDoS services, Genome Shield keeps protection domestic, on infrastructure you control.

MSSPs and managed DDoS providers

Monetize protection as a premium, revenue-generating service built on Genome Shield-enabled Defender's automated workflows.

Key takeaway: One platform replaces ad hoc scripts and 5-10-person manual operations teams — at lower operational cost, with audit-ready policy enforcement.

150+

Deepfield deployments*

70+

Defender deployments*

*as of October 30, 2026

Never face an attack alone

Genome Shield is backed by the people and the community behind Nokia Deepfield's global DDoS research — so automation never means going it alone.

Nokia Deepfield Emergency Response Team (ERT)

Our global team of network security operations engineers researches and disassembles every attack in one of the world's largest DDoS attack libraries — every known method and vector — and works directly with R&D; to turn that research into new protection capabilities, including the Secure Genome and DeepRange intelligence that powers Genome Shield.

With the optional ERT Support (ERTS) service, customers get 24/7 direct access to this team: real-time incident resolution, post-incident analysis, and regular deployment assessments — with a unified team of security and routing experts for customers running Nokia routers or the 7750 DMS.

Global DDoS Threat Alliance (GDTA)

Security is everyone's concern — and so is sharing intelligence about it. GDTA is Nokia Deepfield's opt-in, membership-based alliance through which Defender users share DDoS threat telemetry, improving the Secure Genome feed for every participant. The more we collectively know about attacker methods, the better every member's protection becomes — against current, new and emerging threats.



"We believe the Global DDoS Threat Alliance will go a long way to secure the internet and service providers' networks, and reduce the impact of DDoS threats on participating organizations."

DR. CRAIG LABOVITZ, CTO, NOKIA DEEPFIELD

24/7
Direct ERT support with the ERTS service

DDoS library
One of the world's largest attack collections

Opt-in
GDTA membership, governed by a dedicated privacy policy

Key takeaway: Platform, people and community: automated enforcement, a 24/7 expert bench, and an alliance that makes every member's defense stronger.

NEXT STEPS

Ready to make your network the shield?

Genome Shield is available today. It deploys with Deepfield Defender on your existing Nokia or third-party router edge — optionally with the 7750 DMS — so you can move from reactive mitigation to proactive, always-on protection without re-architecting the network.

Assess your exposure

Explore the new DDoS threat landscape — how attacks moved inside the network and what it means for your P&L.

nokia.com/ip-networks/deepfield/genome-shield/

Go deeper on the platform

Read the Genome Shield data sheet for capabilities, specifications and deployment models.

nokia.com/asset/215420

Join the alliance

Learn how Global DDoS Threat Alliance membership improves protection for every participant.

nokia.com/ip-networks/deepfield/defender/gdta/

Add the expert bench

See what the Deepfield Emergency Response Team Support (ERTS) service includes, from 24/7 incident response to deployment audits.

nokia.com/asset/213594

About Nokia

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

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.

© 2026 Nokia

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

Document code: CID215474 (October)