Research Note

July 2026

Nokia Deepfield Genome Shield Security

Attacking the network-wide DDoS threat at its head

Authors: Patrick Kelly, Grant Lenahan, Francis Haysom

www.appledoreresearch.com

Appledore RESEARCH

Published by Appledore Research LLC • 44 Summer Street Dover, NH. 03820

Tel: +1 603 969 2125 • Email: info@appledorerg.com• www.appledoreresearch.com

Figures and projections contained in this report are based on publicly available information only and are produced by the Research Division of Appledore Research LLC independently of any client-specific work within Appledore Research LLC. The opinions expressed are those of the stated authors only.

Publish date: 29-Jul-26

Cover image by Patrick Kelly

EXECUTIVE SUMMARY

Telecom service providers face a fundamental shift in the DDoS threat landscape. Attack traffic is no longer dominated by large, easily identifiable volumetric events originating *outside* the network. Instead, increasingly sophisticated botnets leverage millions of compromised residential and IoT devices to generate highly distributed attacks that are more difficult to detect and mitigate using traditional scrubbing-center architectures. As attacks become faster, more distributed, and harder to distinguish from legitimate traffic, network and IT operations teams must move beyond reactive detection toward automated, infrastructure-native protection that operates at carrier scale.

Nokia Deepfield Genome Shield addresses this challenge by extending network-wide visibility with automated security orchestration that enables mitigation directly within the IP infrastructure. Rather than relying solely on centralized detection and traffic diversion, the solution combines network intelligence with closed-loop automation to identify malicious traffic, distribute mitigation policies, and enforce protection at line rate across deployed routers. This architecture reduces operational complexity, accelerates response times, and minimizes the impact on legitimate customer traffic while allowing operators to leverage existing network investments instead of deploying additional mitigation infrastructure.

For telecom operations and IT decision-makers, our take is that Genome Shield represents more than an incremental enhancement to DDoS defense—it reflects a broader architectural transition toward distributed, automated cybersecurity integrated into the network fabric itself.

As service providers seek to improve resilience, reduce operational overhead, and protect increasingly critical digital infrastructure, security capabilities that combine real-time visibility, intelligent policy automation, and network-native enforcement will become strategic differentiators.

Appledore Research believes Nokia's approach aligns well with the operational direction of modern service provider networks, where security, automation, and IP infrastructure operate as a unified platform rather than as isolated functions.

GENOME SHIELD: PROACTIVE AUTOMATION FOR A RESHAPED DDOS LANDSCAPE

Nokia Deepfield has introduced **Genome Shield,** a new security automation and orchestration capability augmenting its Deepfield Defender DDoS platform. Genome Shield adds a layer of security information aggregation along with the capability to drive dynamic, intelligent actions through Deepfield Defender and ultimately to be terminated by intelligent routers in your network. Ahead of the public launch, Appledore Research received a detailed briefing from Nokia and was impressed by the company's clear articulation of the evolving threat landscape, its pragmatic approach to innovation, and its focus on deploying technologies that address real operational challenges today rather than future aspirations.

Genome Shield is not positioned as another incremental enhancement to traditional DDoS mitigation architectures. Instead, Nokia presents it as a response to a fundamental shift in cyber threats. Both Nokia and Appledore assess that the DDoS threat environment has undergone more change during the past twelve months than at any point in the previous twenty-five years. The rise of massive botnets, increasingly distributed attack vectors, and the exploitation of compromised consumer devices have exposed limitations in legacy mitigation approaches built around detection, signaling, and traffic diversion.

In fact, Deepfield has always been positioned very differently than other DDoS systems. It has always had two distinguishing features that make it fundamentally unique:

1. The secure Genome, which discovers and understands network traffic flows in detail, as source-destination pairs, and can categorize them, critically as various security risk types (or also importantly, not)

2. It has long worked closely with Nokia's line of FP-series routers to deliver closed-loop, semi-autonomous remediation – and if desired, FP4 and FP5 routers can do so, at full capacity/rate, in line with the data – no backhaul required to scrubbing centers.

For those with more interest we refer you to earlier coverage specifically of these capabilities, available here and here. Nokia claims that this architecture reduces overall scale costs significantly – and is less disruptive to real, legitimate, live traffic. Appledore's study of the Bell Labs papers concurs with this finding.

The central premise behind Genome Shield is that the industry bottleneck is no longer attack detection but the speed and scale of automated response. They further believe that recent attack types are becoming harder to distinguish from real traffic, as the most sophisticated threats attack the network – many points at once. This is at the same time harder to spot and a more fundamental threat to CSPs' ongoing network operations and business. Nokia estimates that more than 200 million compromised residential devices operating behind home gateways, firewalls, and NAT environments can now be leveraged to launch attacks from within service provider networks. These attacks frequently appear as short duration, multi-terabit bursts or highly distributed carpet-bombing campaigns targeting thousands of destinations simultaneously. Under such conditions,

traditional detect-then-divert architectures struggle to respond quickly enough or economically enough to provide effective protection.

Genome Shield addresses this challenge by shifting enforcement closer to the network infrastructure itself, building on the capabilities linked above and the unique closed loop and scrubbing capabilities already in Defender. Rather than relying on centralized scrubbing workflows, the platform enables pre-positioned mitigation policies that can be continuously enforced at line rate on routers already deployed throughout the network. The result is a more distributed and automated defense model designed to reduce reaction times and improve scalability while minimizing operational complexity.

For Nokia, Genome Shield also represents an important commercial milestone. According to the company, Deepfield has achieved a reported 90–95% win rate in competitive proof-of-concept evaluations against established DDoS vendors and is growing at approximately four times the overall market rate. Recent customer wins include NL-ix, which operates one of Europe's largest Internet exchange-based anti-DDoS deployments, as well as hosting providers and Tier 1 service providers across North America, Europe, and Asia-Pacific. Genome Shield expands Nokia's addressable opportunity beyond traditional inbound DDoS protection into outbound attack prevention and infrastructure defense scenarios that Nokia believes remain underserved by existing commercial solutions.

From Appledore's perspective, Genome Shield reflects a broader industry transition toward distributed, automated, and infrastructure-native security architectures. As attack velocity, scale, and complexity continue to increase, the ability to automate mitigation directly within the network may become a key differentiator for service providers seeking to protect critical infrastructure while reducing operational overhead.

THE RESIDENTIAL PROXY BOTNET SHIFT: WHY NETWORKS THEMSELVES ARE NOW THE THREAT

For approximately 25 years, the DDoS threat profile was, in the words of Nokia Deepfield Head of Technology Craig Labovitz (co-founder of Deepfield and former Chief Architect at Arbor Networks), remarkably stable. Attacks were predominantly spoofed, originated from roughly fifty bulletproof-hosting locations in Eastern Europe, were either amplified through DNS or NTP reflectors or bounced off open resolvers, and targeted servers occasionally a small range — generally at sub-terabit scale. The defensive architecture matched this profile: detect anomalies on the peering edge, divert suspect traffic to a specialized mitigation appliance (often priced at roughly $3,000–$5,000 per gigabit of capacity), scrub, return. Operators provisioned this defense for 10-20% of their network — typically the most critical infrastructure and best customers.

The Botnet Shift

In 2023–2024, the source of attack traffic shifted decisively from spoofed Eastern European origins to US enterprise IoT — exposed DVRs and home- and small-office routers, reaching on the order of a million active bots on a typical day. Defense was harder because the traffic was no longer spoofed: it

came from real Linux stacks behind real public IPs, with no obvious header anomalies to filter on. But it was still ultimately a problem of compromised endpoints outside the operator's own subscriber network.

The change in the past 24 months is qualitatively different. Attack traffic has shifted from US enterprise endpoints to US (and global) residential subscriber endpoints — the home routers, smart TVs, IP cameras and IoT devices behind every consumer broadband connection. Nokia estimates the global population of compromised residential nodes at approximately 200 million, the bulk of them hosted under the largest US fixed and mobile operators. The Aisuru botnet and its Kimwolf successor, first detected in August 2024, was the signal event: it reached at least 700,000 active bots, drove individual DDoS attacks (exceeding 30Tbps at its peak) and produced multiple multi-terabit outages at Tier-1 US carriers in 2025. A coordinated takedown effort in early 2025, involving the FBI, DOJ, three-letter agencies and roughly forty other organizations, fragmented Aisuru into a group of smaller botnets — but the underlying 200-million-device latent threat remains, and Krebs on Security, the Wall Street Journal and multiple security researchers have documented Aisuru's mid-2025 strategic pivot from DDoS to residential proxy services, weaponizing the same infected estate for credential stuffing, AI-scraping anonymization, ad fraud, and an underground residential-proxy market that has grown from tens of millions to a multi-billion-dollar market.

Follow the Money

The economic engine driving this shift is, in Nokia's analysis, AI. A residential IP in Russia or Ukraine is worth a fraction of a US cent because it will be blocked everywhere; a residential IP behind a US Tier-1 ISP is operationally valuable for committing cybercrime, scraping content, evading rate-limits and laundering automated traffic. Two related dynamics are widening the compromise surface in parallel. First, SDK providers pay app and game developers to embed proxy-node code in otherwise legitimate consumer apps, monetizing the home connection without the consumer's knowledge. Second, low-cost consumer hardware — TV streaming devices, IP cameras — is reaching market with back-doored firmware factory-installed, subsidized by residential-proxy operators in exchange for the device joining the proxy network at first boot. Major smart-TV vendors are publicly reported to be paying AI-scraping companies to include their SDKs in shipping devices.

A Final Shift: Attacking the Network Fabric (and your lifeblood)

The latest shift is not where attacks are launched *from*, but what they are launched *at*. DDoS traditionally targeted an enterprise or server cluster—in any event some specific target that could then be ransomed. Or maybe it was a political or retaliatory attack in which the goal was not ransom but the damage itself. The latest pattern however is targeting myriad points within a network—potentially yours. This accomplishes two things for the bad actor; it makes the target less obvious and therefore more likely to go unnoticed; second, it can take down an entire network or network segment. The sinister effectiveness of this approach for the attacker is that flows that go from many places to many other places look like normal network traffic. The only way to know there is something malicious about these is if you understand each "to" and "from" flow, along with its normal characteristics. From knowing normal, we can infer *ab*-normal. To a large degree this is

what Deepfield's Genome has always done but this application is incredibly valuable and needed, so long as complex and rapid responses can be created, orchestrated, and controlled.

The operational consequences for service providers are no longer theoretical. Multiple Tier-1 US ISPs face potential malicious aggregate bandwidth from residential proxy nodes within their own networks exceeding 100 Tb/s — larger than the entire national backbone bandwidth of most countries. Operators have seen outages where the issue was not server endpoints under attack, but portions of the operator's own infrastructure failing — aggregation edges and PoPp edges saturated by upstream traffic from infected residential endpoints they themselves serve. The economic effect reaches the subscriber too: subscriber IP risk scores at affected operators hit 100, with customers seeing constant CAPTCHAs, fraud-flagged transactions, and Reddit threads complaining about why their broadband connection seems to break online commerce.

THE THREE PROBLEMS GENOME SHIELD ADDRESSES

Genome Shield is explicit about the structural problems it sets out to solve. Each is, in Nokia's framing, a class of problem that the existing commercial DDoS architecture was not designed for and cannot be retro-fitted to handle at scale.

Problem	Genome Shield response
Slow, reactive mitigation	Proactive, network-wide protection: pre-positioned, continuously enforced defense that responds to sub-minute bursts that defeat detect-then-divert pipelines
Infrastructure protection gap	Outbound and subscriber threat management: addresses compromised devices inside operator subscriber bases attacking outward — a problem class no other commercial DDoS product addresses at scale
Security automation vacuum	Commercial platform for dynamic threat-feed management and automated response: replaces ad hoc scripts and 5–10-person hand-rolled teams maintaining custom security workflows

Slow, reactive mitigation

According to Nokia, the #1 driver bringing customers to Nokia Deepfield from legacy vendors is the speed mismatch between modern attacks and detect-then-divert pipelines. Traditional architectures detect at the peering edge using coarse-grained flow analytics, decide to divert, signal the routers, redirect traffic to a heavyweight DPI scrubbing appliance, and only then begin mitigation. Even at best-in-class incumbents, this pipeline runs in minutes.

The new generation of attacks *lasts* minutes: according to Nokia's 2025 Threat Intelligence Report, 78% of DDoS attacks are *completed* within five minutes, 37% within two. By the time the legacy pipeline engages, the burst has come and gone, the damage is done, and the attacker's automation has cycled the source and destination IP sets.

Infrastructure protection gap

No existing commercial DDoS product, on Nokia's assessment, addresses outbound attacks from compromised subscriber devices at scale. Tier-1 operators with the resources to try, have built ad hoc, manual processes — spreadsheets, in-house teams, unreliable threat feeds that work for a month and then go dark, weekly filter updates — to suppress the worst of their own outbound DDoS traffic. Tier-2 and Tier-3 operators have generally not built anything at all. Below the Tier-1 ceiling and inside the long tail of hosting providers and enterprises, the infrastructure protection gap is, in effect, total.

Security automation vacuum

The operators that have built something have built it as a science project. Nokia describes major service providers running five-to-ten-person teams maintaining custom security workflows, hand-rolled scripts, and brittle integrations against feeds that change without warning. The operational cost is high, the resulting protection is partial, the institutional knowledge walks out the door when a key engineer leaves, and the threat surface evolves faster than the team can keep up with. There is, in short, no commercial, scalable automation platform for this work — until, in Nokia's argument, Genome Shield.

ARCHITECTURE: FOUR PILLARS POWERED BY SIX INTELLIGENCE SOURCES

Genome Shield's architecture decouples intelligence aggregation, policy compilation and network-wide enforcement. A Shield compiler ingests threat intelligence from six continuously updated sources, compiles them into automated security policies, and pushes those policies into the data plane of routers that the operator already runs — Nokia 7750 SR (FP4/FP5 silicon), 7730 SXR (FPcx), 7250 IXR, third-party Cisco or Juniper routers, or the Nokia 7750 DMS dedicated scrubber. Enforcement uses three protocols selected by use case: NETCONF for highly granular filter management, FlowSpec for interoperability, and BGP RTBH for bulk traffic discard. Policies can also be pushed to other firm's routers capable of receiving them. There are, however, limitations for most routers due to chip architecture limitations that the FP-series was specifically designed to overcome (covered in the previous notes linked above). More on the intention, architecture and capabilities of the FP-series can be read here.

The four pillars of proactive automation, on Nokia's architecture diagram, are:

1. Disrupt botnet C2: Continuously updated rules block command-and-control traffic from all major botnets before attacks start; Nokia estimates this blocks over 99% of DDoS C2 malicious traffic. Disrupting the command channel leaves devices infected but mute — they stop receiving the instructions to launch DDoS, scrape, or perform other malicious activity.

2. Predictive protection: Always-on, pre-positioned rate limiters at line speed suppress amplification and DDoS bursts before any detection trigger is required.

3. Custom policies: A user-defined rule framework lets operators block scanning, AI crawlers, malware sites and operator-specific threats through static lists or the Defender UI/API.

4. Observability: Dashboards over compromised devices, botnet endpoints, residential-proxy nodes, mining traffic and security trends turn the assurance estate into a security observability platform.

Underneath the four pillars sit six intelligence sources, three of them Nokia-proprietary, three drawn from community and commercial channels:

Intelligence source	What it provides
Cloud Genome	Internet-scale traffic classification — mapping applications, content providers and infrastructure at hourly cadence
Secure Genome	DDoS detection rules and threat signatures derived from analysis of global attack patterns; 5bn+ tracked IPv4/IPv6 endpoints; 100+ AI/ML classifiers; hourly updates
Global DDoS Threat Alliance (GDTA)	Real-time global DDoS threat telemetry aggregated from opt-in Deepfield Defender network deployments
DeepRange	Nokia cyber range — infiltration of botnet C2 networks; reverse-engineering of malware samples; ~98% coverage of all major botnets
Community data	Open-source threat-intelligence feeds and community-shared indicators of compromise
Licensed data	Commercial threat-intelligence and IP-address-reputation feeds from third-party providers

The proprietary trio is the more interesting half. Cloud Genome maps the internet at hourly cadence — what is connecting to what, what types of devices are involved, and how traffic is classified — which gives Genome Shield the context to judge whether a residential gateway, a particular brand of IP camera or a smart-TV model should be behaving the way it currently is. Secure Genome turns that map into DDoS detection rules and signatures, tracking more than five billion IPv4 and IPv6 endpoints with hourly updates and 100-plus AI/ML classifiers. DeepRange is Nokia's cyber range: a research environment that has been used to infiltrate the command-and-control infrastructure of all major botnets, giving Nokia, on its own account, close to 98% coverage of active botnet C2. It is this infiltration capability that lets Genome Shield see attack commands typically thirty seconds before the corresponding DDoS bursts hit the network and proactively pre-position filters to absorb them.

NOKIA'S ARCHITECTURAL DIFFERENTIATION: WHY LEGACY INCUMBENTS CANNOT EASILY FOLLOW

Nokia's differentiation against Arbor (NetScout), Radware and the rest of the legacy DDoS cohort is structural rather than cosmetic. Three architectural choices are particularly important.

First, Nokia separated detection from mitigation. Where Arbor and its peers historically combined coarse-grained flow analytics for detection with the same heavyweight DPI hardware doing mitigation, Nokia built a lightweight, multi-telemetry detection layer (consuming flow, DNS, BGP and other data feeds) and pushed mitigation into routing silicon that the operator was already paying for. This collapses detection time from several minutes to under thirty seconds, and removes the per-gigabit hardware tax that, at the legacy generation's $3,000–$5,000 a gigabit, made it economically impossible to protect more than 10-20% of the network. Genome Shield extends the same logic upstream into proactive policy injection, eliminating the diversion latency entirely.

Second, Nokia's mitigation runs natively on FP5 (and FP4) silicon in Nokia routers and on third-party Cisco and Juniper routers as well, so that the same architecture can be deployed in mixed-vendor environments — increasingly the operational reality at every Tier-1 — without forcing a hardware migration. The Nokia 7750 DMS dedicated scrubber, introduced in 2024, sits alongside this as a dedicated mitigation system providing up to 2.8 Tb/s per chassis (2.4 Tb/s with the Advanced Countermeasures Engine for application-layer countermeasures), roughly three-and-a-half to four times the filter scale of a typical legacy scrubber. Operationally, Genome Shield also replaces the protocol-by-protocol manual threshold tuning that legacy systems required — work that took new engineers two-to-three months to learn and walked out the door six months later — with intelligence-driven automation that just works.

Third, Nokia tackled the outbound problem directly. Most legacy DDoS products were architected around the assumption that the threat was outside the network and the defended assets were inside; Genome Shield turns that assumption on its head by treating the operator's own subscriber base as a source of attack traffic and using continuously updated C2-disruption rules — typically 500 to 1,000 ACLs at any moment, fully automated — to cut off the head of botnets active inside the network. The illustrative case Nokia cites is a Latin American operator that had a roughly one-terabit-per-second outbound DDoS problem consuming most of its international transit capacity. After deploying Genome Shield, the outbound DDoS traffic disappeared in seconds, not because the hundreds of thousands of infected residential nodes were cleaned (they remained infected) but because they stopped receiving C2 instructions. The action is surgical — Nokia is not blocking subscriber internet access — but the effect is large.

The defensible moat, on Appledore's read, is the combination of DeepRange-driven C2 visibility, the Cloud Genome–Secure Genome data infrastructure and the silicon-native mitigation path. Each is hard for an incumbent to replicate quickly: DeepRange because it depends on multi-year research-and-infiltration work; the Genome data layer because of its breadth (five billion-plus tracked endpoints, hourly updates); and the silicon path because it requires control of the routing data plane, which the pure-software DDoS specialists do not have.

CUSTOMER FOOTPRINT AND GO-TO-MARKET INFLECTION

Nokia Deepfield is no longer competing only at the Tier-1 service provider segment. The customer base has widened across the value chain to encompass Tier-2 and Tier-3 ISPs; internet exchange points; hosting providers; sovereign and onshore security mandates; mission-critical networks across government, healthcare, and research and education; and large digital enterprises. Genome Shield extends the addressable footprint further by adding outbound and infrastructure-defense capability to environments — particularly IXPs and hosting providers — where assurance had historically been the most that operators thought they needed.

Named recent wins include NL-ix, where Nokia Deepfield Defender now powers what the two companies describe as the largest IXP-based anti-DDoS deployment in Europe, with the underlying Defender platform tested in production for nearly three years. Nokia has separately referenced wins at additional internet exchanges and at multiple hosting providers, and reports replacing legacy incumbents in head-to-head deals while remaining deployed alongside them in many accounts to address use cases — outbound, residential-proxy, carpet-bomb — that the incumbents cannot. Joint research with the Comcast Threat Research Lab, presented at NANOG 97 in the talk “The Kimwolf Aftershock: Residential Proxy Botnets One Year Later,” provided independent validation of Nokia’s threat data and made the company a primary public voice on the residential-proxy threat.

Geographic dynamics differ by region. In APAC and Europe, demand acceleration over the last twelve to eighteen months has been geopolitically driven, with operators reading the threat as a national-resilience issue rather than a per-customer service. In Latin America, the driver is more commercial — competitive attacks on commerce platforms — combined with higher attack intensity. In North America, the immediate driver is the outbound, residential-proxy traffic from infected endpoints inside the largest networks, including the Tier-1 US carriers facing the 100 Tb/s aggregate malicious-bandwidth ceiling. Salt Typhoon and Volt Typhoon have separately raised demand for the kind of network-wide observability — including automated, on-demand pcap from compromised devices for lateral-movement analysis — that Genome Shield and Defender enable.

Commercially, Nokia reports a 90–95% PoC close rate, growth at approximately four times the broader DDoS market growth rate, and meaningful pull-through into IP routing sales because the same FP5 silicon that runs Genome Shield filters is the silicon Nokia wants to ship. The company is candid that it remains an engineering-led business with comparatively modest security-industry brand recognition — a gap it is now deliberately working to close through analyst engagement, the NANOG talk, the Wall Street Journal coverage of Aisuru and a public GitHub repository documenting Nokia’s botnet research.

APPLEDORE ANALYSIS

Nokia Deepfield's launch of Genome Shield is, in Appledore's view, the most architecturally consequential DDoS-defense announcement in recent memory, because the problem it solves is qualitatively different from the problem the legacy DDoS architecture was built around. Three observations are central.

The Outbound Problem Is the Real Story

The headline framing of Genome Shield — proactive automation versus reactive mitigation — is accurate **but understates the architectural break**. The genuinely new capability is treating the operator's own subscriber base as a source of attack traffic and providing a commercial, automated platform to address it. No legacy DDoS product was built for this, because for twenty-five years it was not the problem. With approximately 200 million residential nodes compromised and a two-to-three-billion-dollar economy now incentivizing further compromise, the outbound, infrastructure-defense problem is not going away. Genome Shield's ability to identify and continuously disrupt 500–1,000 C2 endpoints at a time — without blocking subscriber traffic and without requiring the impossible task of cleaning the endpoints themselves — is a structurally novel capability.

For operators, the implication is that outbound DDoS protection is rapidly migrating from optional differentiator to table-stakes infrastructure resilience. Network-internal botnet traffic is now plausibly the largest single threat to network reliability, particularly as inference workloads at the edge raise the stakes for any unpredictable consumption of network capacity. Operators that cannot manage their own infected estate will see customer-experience consequences — slow speeds, captchas, fraud blocks, eroded NPS — before they see infrastructure outages.

Architectural Decoupling Is a Defensible Moat

The decision to decouple detection from mitigation, push mitigation into routing silicon, and base detection on Genome and DeepRange intelligence creates a structural advantage that legacy incumbents cannot quickly close. DeepRange in particular — the cyber-range infiltration of all major botnets with claimed 98% coverage — is multi-year intellectual property, not a roadmap item. Cloud Genome and Secure Genome (five billion-plus tracked endpoints, 100-plus AI/ML classifiers, hourly updates) are similarly hard to replicate without sustained investment.

NetScout's recent pivot to smart data — an abstraction layer over Infinistream passive monitoring exposed as an AI-sensor and data API — is the most thoughtful incumbent response visible today and is worth watching as a competing architecture for agentic-era assurance, but it does not directly address the outbound DDoS problem Genome Shield is built for. Cloud-based DDoS services (Cloudflare, Akamai) operate in a different topology and remain complementary rather than competitive for the network-internal, outbound use cases.

Genome Shield Is a Platform, Not a Product Refresh

The naming, the architecture and the choice of intelligence-source disclosure all point at platform intent. Genome Shield is less a new SKU than a control plane over which a much wider set of security automation use cases — scanning suppression, AI-crawler control, malware-site blocking, residential-proxy disruption, customer-care integration, predictive mitigation against in-flight C2 commands seen ahead of attack launch — can be progressively deployed. Nokia has telegraphed that observability data will be exposed by API and MCP for customer-care use cases, and that agentic and AI capabilities are in active development across observability and security. The strategic question for Nokia is whether Genome Shield becomes the security control plane through which operators run a much broader set of network-resilience and integrity decisions, in which case the addressable market is considerably larger than today's DDoS-defense TAM.

Watch Points for the Balance of 2026

Four things to track over the next few quarters:

1. **Marketing and brand-building cadence:** Nokia's biggest weakness in security is brand presence, not technology.
2. **Botnet evolution** after the early-2025 takedowns: the fragmentation of Aisuru into a family of smaller botnets has reduced peak bandwidth but not the latent threat (the 200-million-device infected base is intact, and the underlying SDK and back-door supply chains have not been disrupted). Re-consolidation, the emergence of new families, or a step-up in attacker AI-automation could change the threat profile again quickly.
3. **Conversion of incumbents:** Nokia reports a 90–95% PoC close rate. The pace at which 2025-outage-shaken operators flip from displacement-and-overlay to full replacement is the most direct revenue-validation.
4. **Customer-care and endpoint-quality monetization:** Genome Shield's observability data is a natural input to customer-care, IP-reputation and endpoint-quality use cases. If Nokia exposes that data through APIs and MCP at the cadence the market now expects from agentic-era operations stacks, Genome Shield could become a revenue source for operators rather than only a cost-avoidance tool — a more durable commercial position.

The final take-away is that CSPs looking to source commercial solutions on new attack vectors coming from endpoints need to have Nokia Deepfield Genome Shield on their shortlist.

Insight and analysis for telecom transformation.

@AppledoreVision

Appledore Research

www.appledoreresearch.com

info@appledorerg.com

+1 603 969 2125

44 Summer Street Dover, NH. 03820, USA

Appledore RESEARCH