Nokia Deepfield Defender

Leverage the power of AI-driven, petabyte scale big data analytics and combine it with high-performance IP networking technology to protect the entire network from all types of DDoS attacks in an automated manner, with zero-touch operation

Solution sheet

Telecommunications service providers, cloud and AI providers, internet exchange points (IXPs), cloud builders, research and education networks (RENs), and large digital enterprises are equally concerned about security threats originating from outside of their networks and data centers (inbound or ingress DDoS) as well as threats and attacks originating in their networks and data centers, aimed at targets within and outside of their networks (outbound or egress DDoS).

Over the last several years, Distributed Denial of Service (DDoS) attacks have grown significantly in frequency, intensity and sophistication. This growth has been fueled by the rapid expansion of botnet ecosystems — including IoT botnets and residential-proxy-based DDoS networks — alongside the increased availability of bandwidth at the edge and the broader attack surface introduced by 5G, distributed edge architectures and AI-enabled attack tooling. The growth of wireline and wireless networks and rollouts of new technologies such as 5G and distributed edge network architectures have expanded the threat and attack surface. Today, DDoS attacks come from all directions – from outside and inside of networks, and have diverse targets – network infrastructure, business and residential customers.

The Nokia DDoS security solution, centered around Nokia Deepfield Defender, combines the power of AI-driven big data analytics (delivered by Defender) and advanced, programmable IP routers, such as 7750 Service Router (SR) family (based on FP4/FP5 silicon), 7730 Service Interconnect Router (SXR) family (based on FPcx silicon) and 7250 Interconnect Router (IXR) family, and select third-party routers (e.g., Cisco, Juniper), and/or an advanced dedicated mitigation platform, Nokia 7750 Defender Mitigation System, engineered to defend against all types of DDoS — including botnet, carpet-bombing, and L4–L7 DDoS attacks. This combination delivers a next-generation DDoS detection and mitigation solution with significant benefits over legacy (appliance-centric or DPI-centric) solutions, built around 20-year-old approaches: better scalability, improved detection (with lower false positives), more agile and granular, network-based and optimized mitigation – and all this with much-improved cost efficiency.

This solution sheet provides an overview of Nokia Deepfield Defender. It outlines key features and innovation areas that empower it to be a cornerstone of a holistic, 360-degree DDoS security solution or the AI and cloud era.

Contents

Overview	3
Nokia Deepfield approach to DDoS security	4
How Deepfield Defender works	5
The Nokia DDoS security solution	7
Improved security context through Deepfield Secure Genome	8
Big data security analytics	9
AI/ML engine for optimized DDoS mitigation	11
Network-based protection against DDoS attacks	12
Benefits of network-based DDoS protection	13
Capability to stop DDoS attacks at the network edge	14
Improved, efficient and cost-effective DDoS mitigation scaling	14
Investment protection	14
Deploying Deepfield Defender for DDoS mitigation	15
Deploying Deepfield Defender with Nokia IP routers	16
7750 Defender Mitigation System	17
Multi-layer DDoS mitigation	18
Infrastructure protection	19
Auto-mitigation of DDoS	20
Managed security as a service	21
Using Deepfield Defender	22
Intuitive GUI	22
Use case-focused workflows	22
Advanced security policies with customizable filters	22
Reporting	22
DDoS security as a managed service	23
The Nokia Deepfield advantage	24
Abbreviations	25
References	25

Overview

DDoS threats and attacks are becoming more frequent and impactful in the AI and cloud era. The growth of all-IP networks has extended the security perimeter and expanded the threat and attack surface.

Attacks now come from outside and inside of networks owned and operated by telecommunications service providers, cloud and AI providers, internet exchange points (IXPs), cloud builders, research and education networks (RENs), and large digital enterprises. These attacks are aimed at internet hosts and servers, enterprise and residential users, and network infrastructure. Botnet-driven attacks — including those launched from compromised IoT devices and increasingly from residential proxy networks — have become the dominant DDoS vector, now compounded by AI-enabled attack tooling that lowers the barrier to launching sophisticated, multi-vector campaigns.

To minimize the security risks associated with a new generation of DDoS threats and attacks, a new - more intelligent, efficient, and agile approach is required.

The Nokia approach to DDoS security is based on combining the power of AI-driven, big data analytics with the advanced processing capabilities of network routers and next-generation DDoS mitigation systems to achieve efficient, scalable and cost-effective DDoS protection directly at the network edge. Nokia Deepfield Defender is the AI-driven security automation platform at the core of this approach. It unifies real-time, network-wide DDoS analytics with automated, closed-loop mitigation across the entire IP network — turning DDoS defense from a reactive workflow into a continuously adapting, autonomous capability.

Nokia Deepfield Defender provides fast and accurate DDoS detection and facilitates agile mitigation of all types of DDoS attacks.

This software application is a component of the Deepfield portfolio of IP network intelligence, analytics and security applications.

Features

- Global, detailed internet security context obtained through Deepfield Secure Genome® used for DDoS detection and mitigation
- Accurate, knowledge-based DDoS detection which eliminates the need to maintain and tune large sets of thresholds
- Real-time, network-optimized surgical DDoS mitigation
- Multi-layer orchestration of DDoS mitigation
- Intuitive user interface with:
  - Detailed DDoS attack analytics
  - Comprehensive incident reports
  - Forensics
  - Real-time DDoS mitigation feedback
- Zero-touch operation with auto-mitigation
- Flexible and configurable security workflows

Benefits

- Minimal impact on network services and subscribers
- Protection against all types of DDoS (amplification/reflection, flooding, botnet/application)
- Automated protection from evolving and future DDoS threats
- Ability to mitigate hundreds of ongoing DDoS attacks simultaneously
- DDoS security for the whole network, all services and all users
- Excellent cost efficiency with much-reduced TCO compared to legacy solutions.

Nokia Deepfield approach to DDoS security

The Nokia Deepfield approach to DDoS security is based on decoupling the security intelligence from mitigation for better efficiency, scaling and adaptability to evolving network threats.

This approach effectively creates a centralized DDoS security control plane, which drives distributed DDoS mitigation through network-wide security policy enforcement.

In this model, centralized, real-time DDoS knowledge is used by Defender to activate agile and surgical DDoS mitigation on network-distributed sets of routers and other mitigation systems and devices.

Defender can also improve network/security-related cross-organizational workflows by equipping network security and operations teams with detailed information and reports and allowing direct programmatic integration with other security systems via APIs.

In effect, Defender operates as an AI-driven security automation platform: real-time threat intelligence and surgical mitigation are orchestrated continuously, across every layer of the IP network, with zero-touch operation as the default.

How Deepfield Defender works

Deepfield Defender collects information from the IP network:

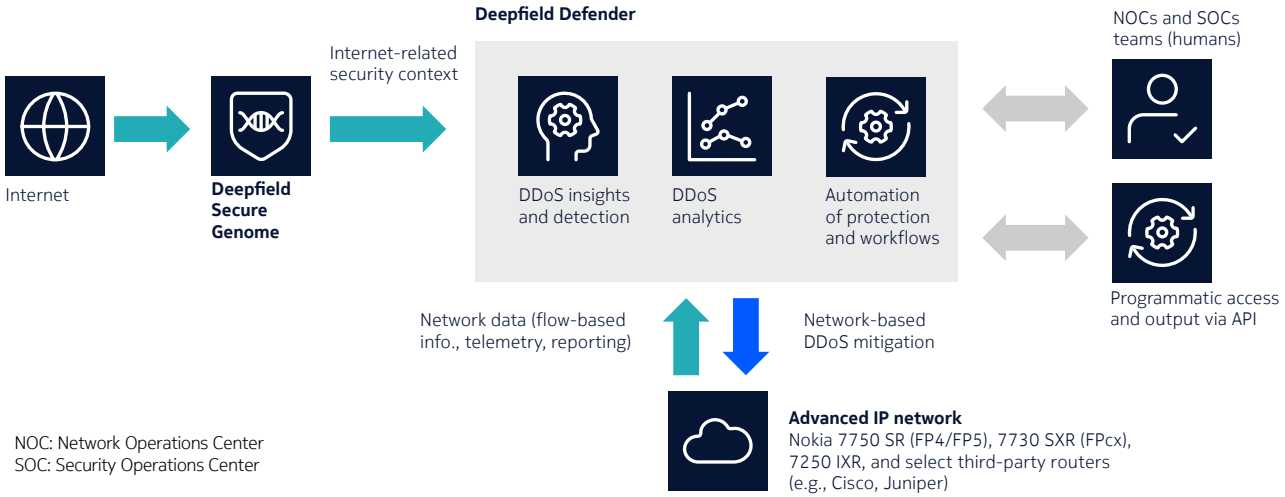
- Real-time IP flow information
- Simple Network Management Protocol (SNMP) data
- Border Gateway Protocol (BGP) data

and uses a big-data analytics engine to process the data and turn it into actionable knowledge.

Deepfield Defender leverages Deepfield Secure Genome® to detect and mitigate DDoS threats across the entire network (see Figure 1). Deepfield Secure Genome is a Nokia-proprietary data feed containing up-to-date information about the global security context of the internet. This security-related data feed is created by cloud-based agents using Nokia's advanced and proprietary technology. Deepfield Secure Genome tracks and maintains the global internet security map, containing information about over 5 billion IPv4 and IPv6 endpoints. This continuously updated correlation — between Secure Genome's internet-wide threat context and live network telemetry, including data from Nokia Deepfield Global DDoS Threat Alliance (GDTA), is what powers the closed-loop intelligence layer that drives both detection accuracy and mitigation efficacy and efficiency.

Defender builds on the Secure Genome data feed, correlating information from Secure Genome with the real-time information obtained from the network - to detect network threats as they occur.

Figure 1. How Deepfield Defender works



Defender monitors traffic flows and network protocols used for DDoS attacks in real time and uses advanced algorithms to track and compare traffic volumes, attack patterns and "signatures" and query/response ratios across the whole network against "peacetime" values when no attacks are occurring.

Using this combined knowledge, and with the help of heuristics and advanced algorithms, Defender can classify DDoS traffic "natively" without requiring operators to manually configure or tune tens or hundreds of threshold-based triggers — a procedure largely used in legacy DDoS systems.

Defender's ability to classify and identify DDoS traffic "out-of-the-box" results in more accurate real-time detection of DDoS threats and attacks with minimal false positive and false negative rates and allows Defender to activate the most appropriate, optimized and agile DDoS mitigation.

While DDoS detection and optimized DDoS mitigation are automated, sophisticated controls allow users to adjust and tailor configuration options.

Big-data analytics is the foundation for our effective, future-ready approach, turning Defender into the most comprehensive multi-layer security framework to protect against DDoS attacks of any type, coming from any origin and across any network edge —and aimed at any network target or victim.

Defender is a foundation for a full and comprehensive DDoS security framework that can orchestrate and coordinate various and multiple mitigation options: from network-based mitigation using routers to dedicated mitigation systems and scrubbing centers.

The Nokia DDoS security solution

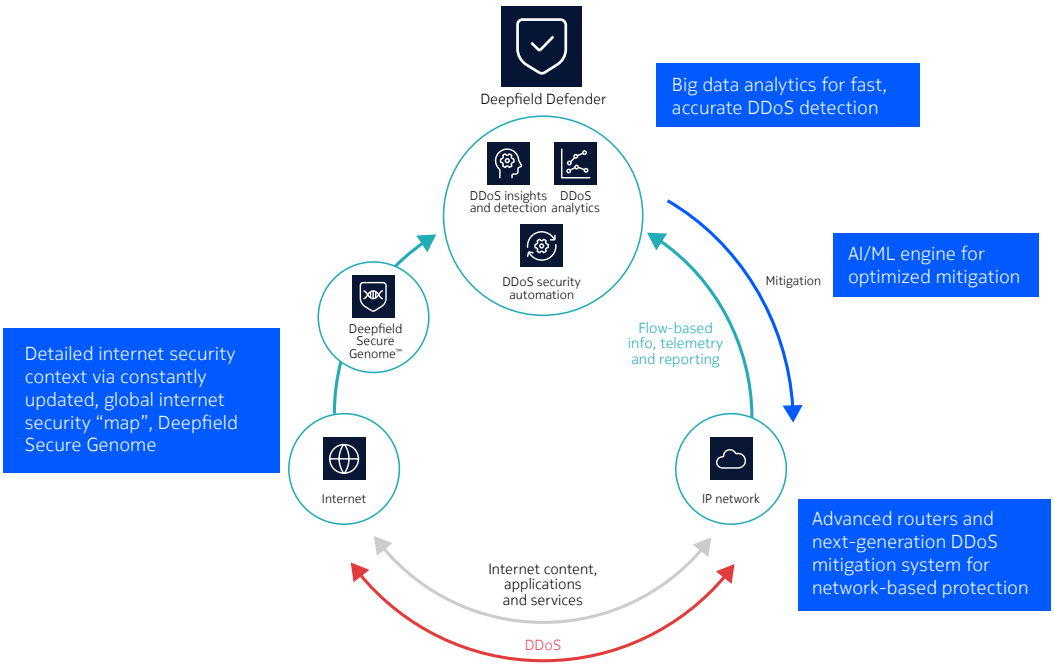
The Nokia DDoS security solution combines the power of Nokia Deepfield petabyte-scale big-data IP analytics with high-performance IP routers to protect the whole network from all DDoS attacks at a high scale with zero-touch automation.

The Nokia DDoS security solution is composed of the following:

- Deepfield Defender: Highly scalable software system which uses big data-driven analytics for real-time DDoS detection, detailed reporting and agile DDoS mitigation
- Deepfield Secure Genome®: Up-to-date, detailed, internet-related security data feed for improved DDoS detection accuracy
- An advanced, high-performance IP network — including the Nokia 7750 Service Router (SR) family (FP4/FP5), the Nokia 7730 Service Interconnect Router (SXR) family (FPcx), the Nokia 7250 Interconnect Router (IXR) family (merchant silicon), and select third-party routers (e.g., Cisco, Juniper).
- Nokia 7750 Defender Mitigation System — an advanced dedicated mitigation platform engineered to defend against all types of DDoS, including botnet, carpet-bombing and L4–L7 DDoS attacks.

The Nokia DDoS solution provides 360-degree protection for your whole network, all services and all users. The solution equips telecommunications service providers, cloud and AI providers, internet exchange points (IXPs), cloud builders, research and education networks (RENs), and large digital enterprises and other large digital network operators with advanced security capabilities to minimize the threats and impact of DDoS attacks.

Figure 2. The Nokia DDoS security solution



The solution brings significant innovation in several key areas:

- Better internet security context – for better and more informed decisions about threats and attacks;
- Big data analytics – for real-time, network-wide, accurate DDoS detection;
- AI/ML engine for optimized DDoS mitigation;
- Advanced routers and next-generation DDoS mitigation systems for agile, scalable and granular network-based protection.

Improved security context through Deepfield Secure Genome

Deepfield Defender delivers more accurate DDoS detection for the threats occurring anywhere in the network and aimed at any target.

This unprecedented level of DDoS detection accuracy is achieved through Deepfield's unique ability to have a detailed, global and up-to-date security context from the internet using the Deepfield Genome patented and proprietary data feeds - Secure Genome and Cloud Genome, collectively called Deepfield Genome.

Deepfield Secure Genome is a Nokia proprietary, cloud-based data feed that continuously tracks billions of IPv4 and IPv6 addresses on the internet, maps them to DNS names, and employs advanced AI/ML rules to further tag the addresses into security-related types and categories.

Like Deepfield Cloud Genome, Secure Genome is based on Nokia Deepfield's patented technology and is constructed by cloud-based agents run from the Nokia Deepfield cloud infrastructure. These agents continuously probe and map the internet, scanning hundreds of millions of IP addresses daily, and further analyze, identify and categorize data across many security dimensions.

The resulting Secure Genome data feed is made available to our customers and their Deepfield deployments in real time through continuous updates.

Through Deepfield Cloud Genome and Deepfield Secure Genome, we track, categorize and map security-related information for billions of IP hosts and traffic flows to provide an up-to-date security-related data feed to Defender. Because Secure Genome provides a holistic security-related perspective of all internet applications and services,

it gives Deepfield Defender a complete, real-time view of the internet-related DDoS security context.

Secure Genome empowers Defender with full visibility into many customizable, security-related categories, including allow lists, block lists, known DDoS amplifiers such as misconfigured DNS resolvers, DDoS bots, and repeated malicious threats.

This detailed, security-related insight enables Defender's superior DDoS detection with :

- **Detailed internet security context:** Identify security threats by involvement in prior DDoS attacks, misconfigured or vulnerable service/application, and network topology knowledge of spoofed traffic sources.
- **Improved DDoS detection accuracy:** Monitor and inspect the most relevant IP sessions with per-flow granularity.
- **Third-party and on-demand threat data:** Flexibility to add access to third-party databases of evolving threats.

Big data security analytics

Two main challenges with big data analytics in any area are the availability of relevant big data sets and the quality of human intelligence (HI) applied for initial analysis. Only then can further Artificial Intelligence (AI) and Machine Learning (ML) algorithms and techniques be applied to enhance and automate the output.

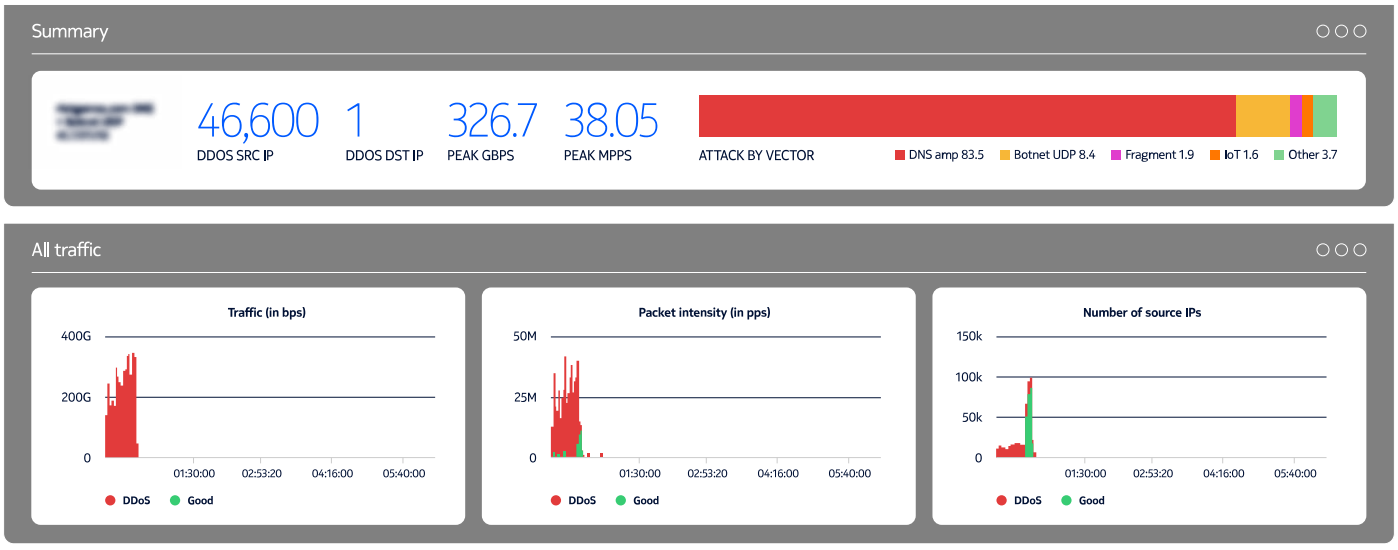
Over the last two years, Nokia Deepfield has compiled one of the industry's largest libraries of real-world DDoS attacks.

Our Deepfield DDoS Library includes thousands of geographically, topologically, and commercially diverse attacks for every known DDoS vector, including amplification/reflection, volumetric flooding, botnet/application-layer attacks, residential proxy DDoS, carpet-bombing and L4–L7 attacks. The Deepfield DDoS Library includes samples from all operative commercial booter/stresser websites and anonymized daily samples from collaborating network operator customers; these samples range from low-volume HTTPS application attacks to multi-terabit botnet and amplification floods.

The information from our Deepfield DDoS Library is used to:

- Dissect and analyze DDoS attacks and devise best strategies and tactics for dealing with an individual or multiple concurrent attacks;
- Test best DDoS mitigation scenarios and implement the countermeasures in Deepfield Defender;
- Teach our AI/ML algorithms to detect and auto-mitigate DDoS threats and attacks;
- Estimate the false positive rate for the DDoS mitigation countermeasures applied for a specific attack.

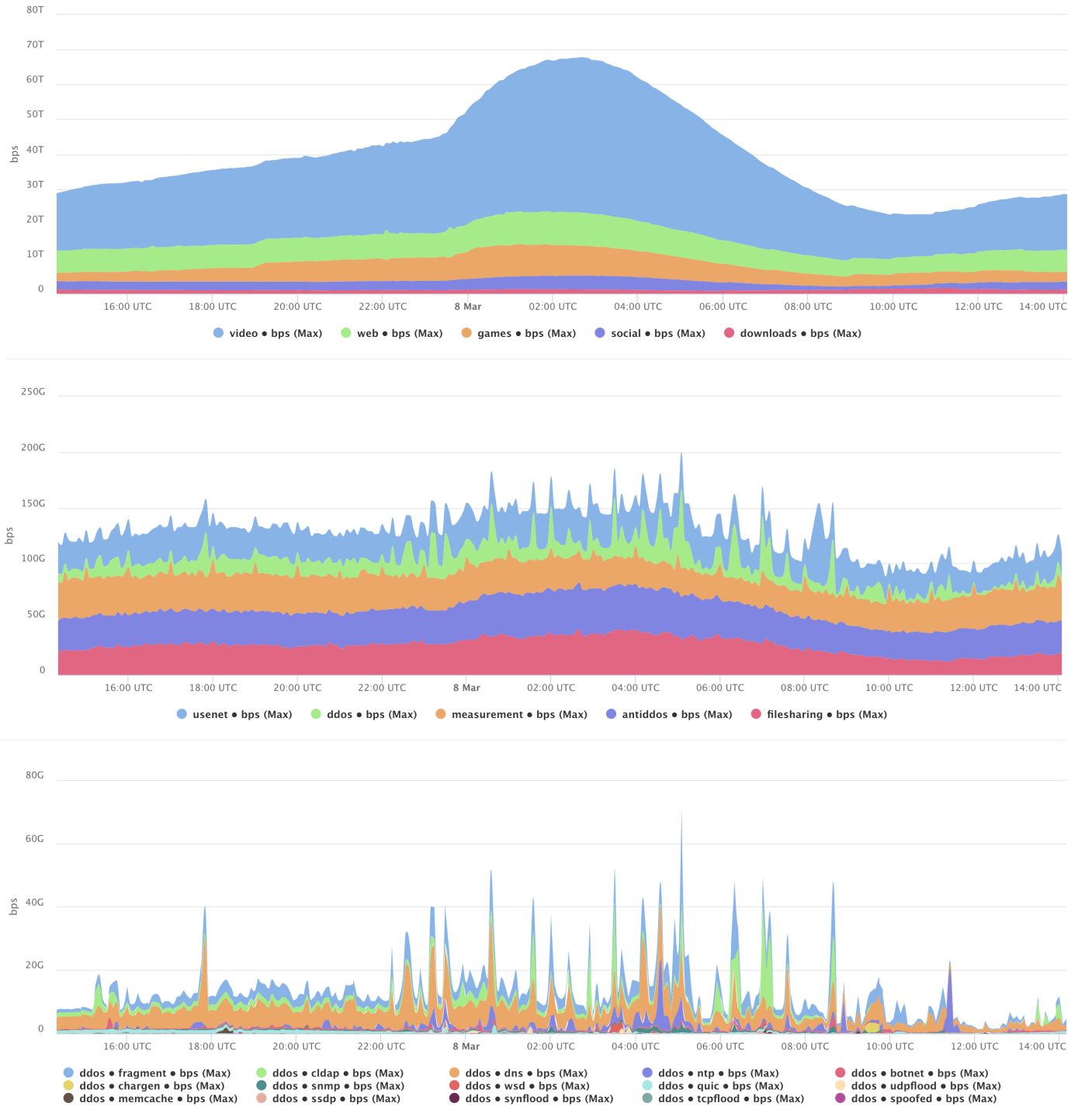
Figure 3. Using Deepfield DDoS Library to analyze attacks and create the most optimal countermeasures



Defender's ability to see DDoS as just another network traffic type greatly helps to monitor DDoS traffic in real time and zoom in on it at many different levels, as seen in Figure 5:

- Looking at all network traffic and DDoS as another traffic type
- Zooming in only on DDoS
- Zooming in on individual DDoS vectors.

Figure 4. Defender's unique ability to monitor and zoom in on DDoS traffic in real time



AI/ML engine for optimized DDoS mitigation

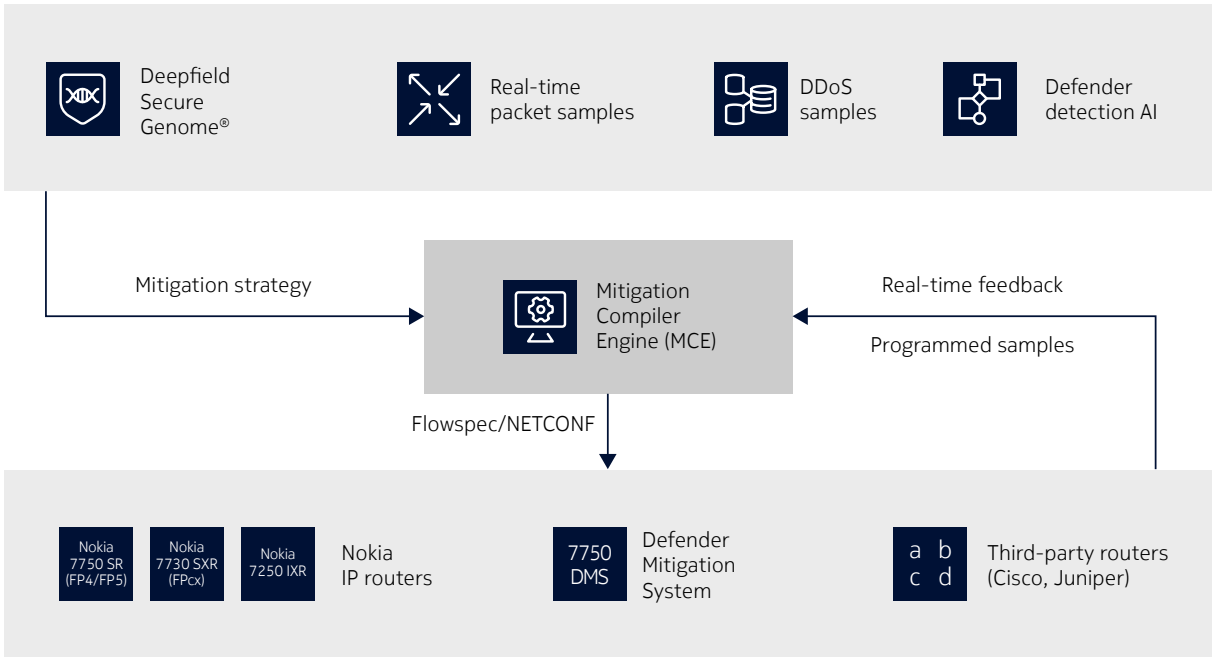
Using advanced AI/ML algorithms, Deepfield Defender calculates the optimal mitigation strategy for a DDoS attack (or multiple concurrent attacks) and immediately instructs routers to apply these filters and neutralize DDoS attacks.

Optimizing DDoS mitigation is quite a different problem than DDoS detection; it is a problem that needs to consider the actual network and its mitigation capabilities and provide an optimal solution that will satisfy the constraints and deliver high-performance mitigation with minimal false positives and false negatives. This must be done in real time to facilitate agile response to ongoing threats.

Defender's Mitigation Compiler Engine (MCE) takes into consideration the number of ACLs/filters that are available for security-related tasks, API type (Flowspec/NETCONF), router vendor model and OS version, service provider's commercial model (i.e., which systems/customers need protection) as well as threat model and details about the actual DDoS mitigation architecture and DDoS mitigation capabilities.

The output from the MCE is an optimized set of mitigation actions for a particular DDoS attack – in the form of a dynamic set of network filters that are updated throughout the duration of an attack and applied across the network to facilitate agile, scalable and granular, network-based mitigation of DDoS traffic. Defender's network-wide, holistic visibility of all DDoS threats and attacks, coupled with MCE's agility and dynamism, results in the ability to handle hundreds of simultaneous DDoS mitigations.

Figure 5. Using AI/ML to create optimized DDoS mitigation (countermeasures)



Network-based protection against DDoS attacks

The power of the advanced packet processing capabilities of a modern IP network is leveraged through Deepfield Defender's ability to establish a secure, closed-loop automation mode with IP routers and use them to efficiently remove all DDoS attacks at the network edge in the most efficient manner.

Defender enables much improved, network-based filtering through tight integration and closed-loop operation with advanced IP routers such as the Nokia 7750 SR (FP4/FP5), 7730 SXR (FPcx), and 7250 IXR families, with additional support for select third-party routers (e.g., Cisco, Juniper) via standards-based protocols such as BGP Flowspec, IPFIX315, NETCONF and RTBH.

Leveraging its accurate DDoS detection capabilities, Defender can instruct routers in real time to allow or rate-limit certain types of traffic or remove/block malicious DDoS traffic completely.

Using NETCONF or BGP Flowspec, Defender can install temporary or permanent Layer 3/Layer 4 access control list (ACL) filters on routers. This allows the routers to surgically remove the most impactful and damaging DDoS traffic, resulting in the most efficient protection against DDoS attacks, large-scale state exhaustion attacks (e.g., TCP SYN/ACK attacks), or other amplification, reflection, flooding and botnet-driven DDoS attacks.

In a world where DDoS attacks happen with increased frequency, intensity, dynamism and the ability to morph and obfuscate, new levels of agility for DDoS detection and mitigation are required — including the most dynamic installation of super-large sets of filter rules on routers.

This is an area where Defender, combined with the latest generation of routers, can bring significant advantages in the fight against DDoS and achieve new levels of network efficiency and overall security while maximizing the return on the existing network investment.

Defender can further enhance its security knowledge base and improve DDoS mitigation by obtaining additional security-related data directly from routers:

- Additional streaming telemetry data, e.g., via generalized Remote Procedure Call (gRPC) telemetry for filter counters, to provide real-time DDoS mitigation feedback
- Mirrored data samples
- Other information that advanced routing elements can produce.

Benefits of network-based DDoS protection

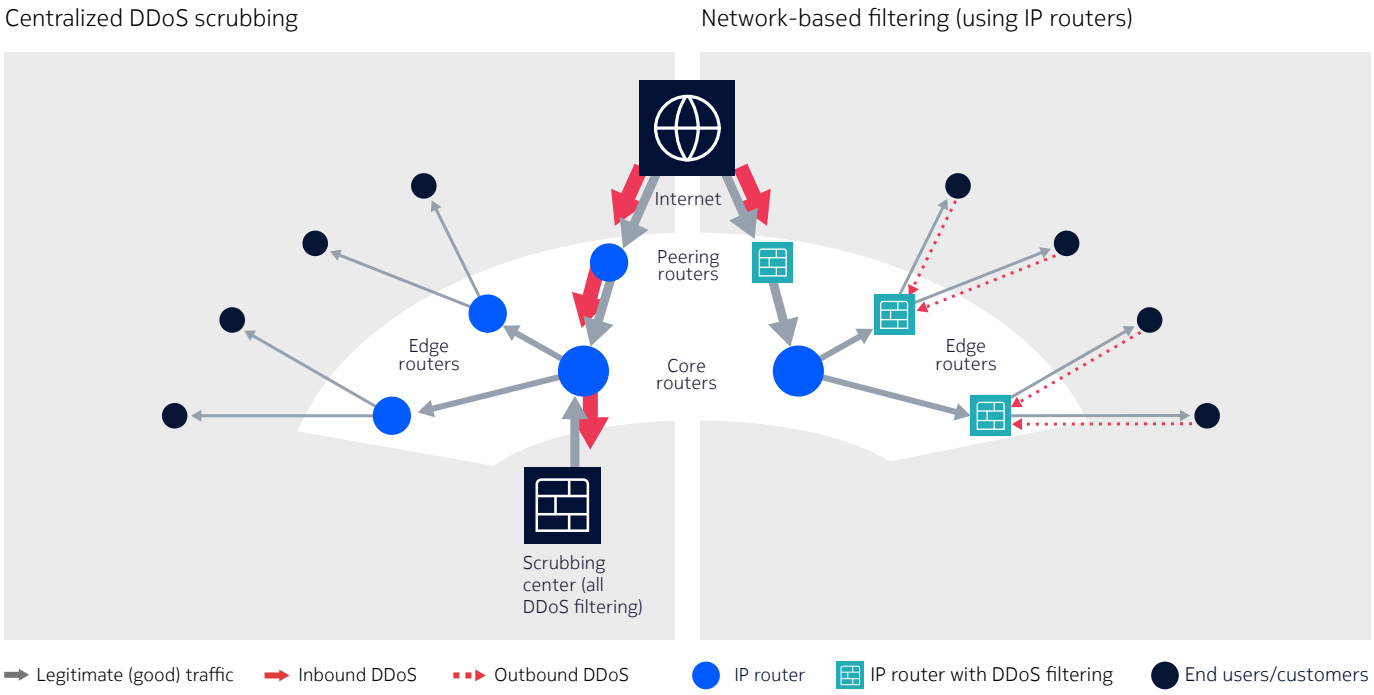
The rationale for network-based DDoS mitigation is driven by a business and technology imperative to mitigate DDoS attacks using the most efficient (lowest number of false positives and false negatives) and most cost-effective (lowest cost per bit) approach.

This approach is efficient because:

- Attacks saturating the internet pipe need to be blocked upstream as much as possible (by the upstream service provider or cloud providers)
- Network-based mitigation of DDoS traffic at the edge of the network leads to the most efficient TCO (by using the routers that are already in the network).

Network-based filtering offers significant benefits over the centralized scrubbing approach. Figure 6 shows these two approaches.

Figure 6. Router-based DDoS filtering versus centralized DDoS scrubbing



The main benefits of our Defender-enabled DDoS protection with network-based filtering are:

- Capability to stop DDoS attacks at the network edge
- Improved, efficient and cost-effective scaling
- Investment protection.

Capability to stop DDoS attacks at the network edge

Defender-enabled DDoS protection stops damaging DDoS attacks at the network edge using the advanced capabilities of the latest generation of routers.

Improved, efficient and cost-effective DDoS mitigation scaling

Defender enables much more efficient and cost-efficient scaling of DDoS mitigation than can be achieved with centralized scrubbing centers, which require massive amounts of network traffic diverted to them and backhauled to the network.

Using NETCONF or BGP Flowspec, Defender-enabled Deepfield DDoS protection can orchestrate many network routers and instantiate network filters efficiently, concurrently and dynamically, allowing protection for tens or hundreds of concurrent DDoS attacks.

Investment protection

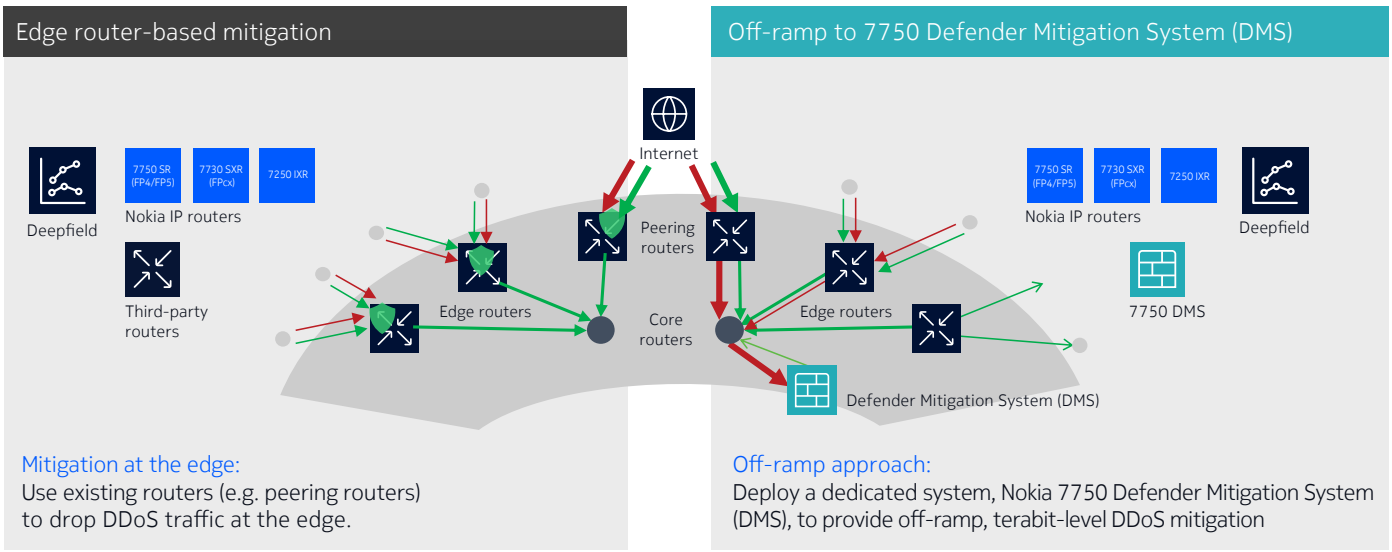
Deepfield-enabled DDoS protection offers significant cost savings on backhaul and security appliances. With our distributed, network-based DDoS filtering, service providers can realize cost savings of 65 to 85 percent compared to legacy approaches.

Deploying Deepfield Defender for DDoS mitigation

Deepfield Defender delivers the most robust and comprehensive distributed denial of service (DDoS) protection scheme against all types of DDoS traffic, combining its advanced DDoS detection capabilities with sophisticated packet processing features of high-performance routing elements, such as the Nokia 7750 SR, 7730 SXR and 7250 IXR families, plus select third-party routers (e.g., Cisco, Juniper).

Generally, there are two deployment approaches for driving DDoS mitigation with Deepfield Defender: using security filtering on edge routers that perform other network functions such as peering or using a dedicated mitigation system, 7750 Defender Mitigation System (DMS). These two options are shown below, and practical deployments may involve a combination of these.

Figure 7. DDoS mitigation options using edge routers and 7750 Defender Mitigation System (DMS)



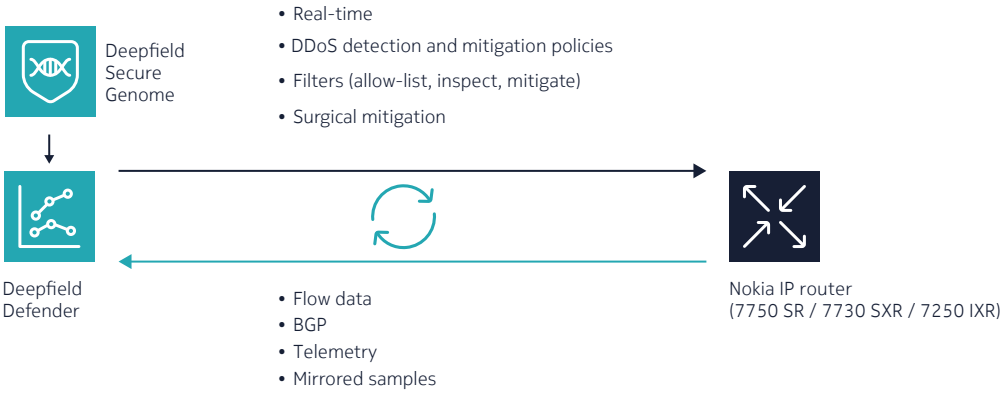
Mitigation at the edge:
Use existing routers (e.g. peering routers) to drop DDoS traffic at the edge.

Off-ramp approach:
Deploy a dedicated system, Nokia 7750 Defender Mitigation System (DMS), to provide off-ramp, terabit-level DDoS mitigation

Deploying Deepfield Defender with Nokia IP routers

Deepfield Defender can be deployed in closed-loop automated mode with the latest generation of Nokia IP routers, such as the Nokia 7750 SR, 7730 SXR and 7250 IXR families (see Figure 8).

Figure 8. Network-based protection with Deepfield Defender and Nokia IP routers



This solution enables agile DDoS mitigation with large-scale, granular ACL filtering of DDoS traffic. Network filters are installed by Defender on routers in real time using NETCONF or BGP Flowspec.

When deployed with Nokia IP routers for network-based mitigation, Defender leverages its broad DDoS security knowledge based on the following:

- Flow-based data
- BGP
- SNMP
- Telemetry (feedback from dropped/passed traffic)
- Mirrored samples
- Other security-related information.

With this knowledge, Defender can instantiate complex security policies and drive network-based, real-time surgical DDoS mitigation with advanced features such as auto-mitigation. This solution enables granular implementation of DDoS policies while allowing network-wide scaling and full, 360-degree network-wide protection with deterministic performance.

7750 Defender Mitigation System

Nokia 7750 Defender Mitigation System (DMS) is an advanced dedicated mitigation platform engineered to defend against all types of DDoS — including botnet, carpet-bombing and application-layer DDoS attacks. It can be deployed with Deepfield Defender when:

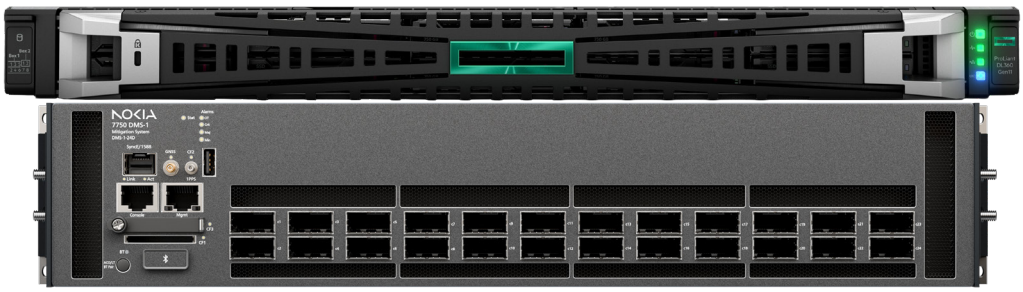
- Third-party routers (with limited security filtering scale) are deployed;
- There is a preference by security teams toward a separate and dedicated security enforcement platform;
- There is a need to replace a legacy scrubbing solution with a higher-throughput, more cost-efficient platform purpose-built for the modern DDoS threat landscape.

7750 Defender Mitigation System provides superior DDoS protection with much-improved cost-efficiency.

The current platform, 7750 DMS-1-24D, is a 3RU (including the Advanced Countermeasures Engine, ACE) dedicated mitigation system with up to 2.4 Tb/s of DDoS mitigation capacity and can be co-located with the network edge or located separately.

For more details, please check the 7750 DMS-1-24D datasheet.

Figure 9. 7750 Defender Mitigation System 7750 DMS-1-24D



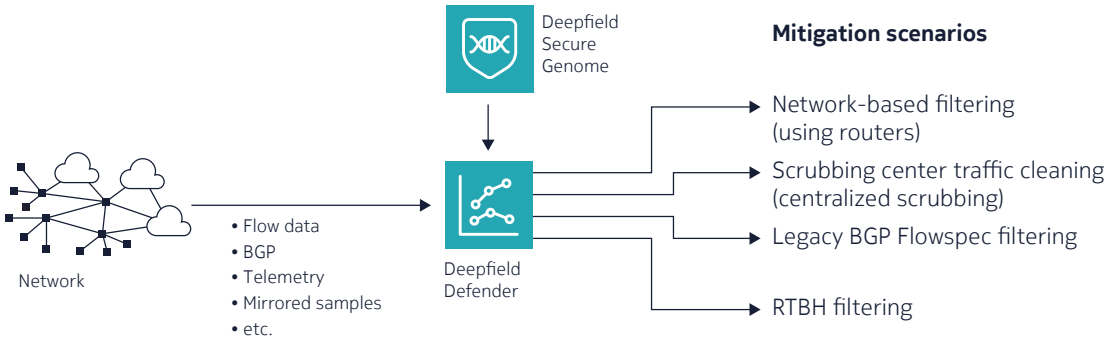
Multi-layer DDoS mitigation

In addition to performing network-based mitigation, Defender can also be deployed as a central point for orchestrating multi-layer DDoS mitigation strategies. Additional DDoS mitigation options are available, from RTBH and BGP Flowspec filtering to integration with major third-party hardware and virtual mitigation devices.

In a multi-layer mitigation scenario (see Figure 9), Defender coordinates network-wide mitigation countermeasures from a single security control point and can drive all types of DDoS mitigation options, which can include any combination of:

- Network-based filtering (using routers)
- Scrubbing center-based filtering
- Legacy BGP Flowspec filtering
- RTBH filtering.

Figure 10. Comprehensive, multi-layer DDoS mitigation orchestration using Defender



Infrastructure protection

DDoS attacks do not only target internet servers and hosts. Increasingly, DDoS attacks are launched against the telecommunications network infrastructure, targeting network elements, systems and processes.

As a result, service providers must extend DDoS protection capabilities to cover their networking infrastructure across a combination of technologies.

Deepfield Defender allows monitoring of network infrastructure within the entire network, including peering and service edge, as well as centralized and distributed data centers.

Defender comes with advanced DDoS detection capabilities “out-of-the-box.”

Service providers can have a full view of DDoS threats and attacks in the network without the need for granular and continuous tuning of DDoS detection algorithms and mitigation parameters. This allows providers to define security policies to protect their infrastructure and customers.

In addition to pre-loaded, automated DDoS detection rules and optimized mitigation strategies, Defender allows granular control to customize DDoS detection and mitigation parameters.

For example, different security policies can be used to protect different parts of a provider’s network and different groups of customers:

- Connectivity (service edge protection)
  - Fixed residential broadband: DSL, cable, fiber-to-the-anything (FTTx)
  - Business access: DSL, cable, FTTx, dedicated internet
  - Mobile core and access: 5G core, mobile transport, Wi-Fi hotspots
- Cloud and AI infrastructure
  - Public cloud and hyperscale services
  - AI training and inference clusters
  - Hosting and colocation
- Internet exchange points (IXPs) and peering fabrics
- Research and education networks (RENs)
- Data center and ISP services (DNS, mail, cloud storage, IPTV)
- Managed security service offerings (MSSP)

Operators can customize security policies based on desired levels of protection and severity of potential impact on customer categories, types or groups. Defender provides automated updates using new and updated security-related information as it becomes available.

Auto-mitigation of DDoS

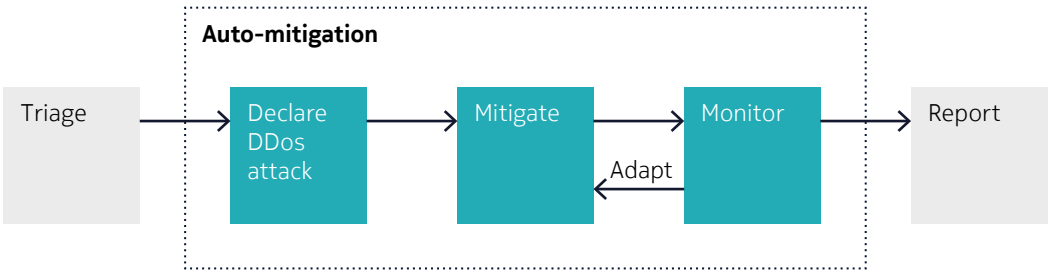
Historically, router-based DDoS mitigation workflows have entailed many manual steps to activate mitigation. Also, DDoS mitigation techniques have been limited, often restricted to performing auto-divert of traffic to scrubbers.

A typical DDoS security workflow includes detection, triage, mitigation, monitoring and reporting stages (see Figure 11).

1. During the DDoS detection phase, the attack event is identified.
2. During the triage phase, actions that need to be initiated are evaluated.
3. As a result, an appropriate DDoS mitigation is created and activated.
4. The DDoS mitigation is monitored for efficiency and outcome and is adapted, stopped or restarted accordingly.
5. Finally, detailed reporting on incidents and ongoing and completed DDoS mitigation is required. These reports may be passed to customers to optimize and improve their defense.

Even with rapid response, manual DDoS mitigation activation can take significant time. For some DDoS attacks, this can mean that the damage is already done by the time mitigation is put in place.

Figure 11. Auto-mitigation and DDoS workflow phases



Deepfield Defender significantly improves this process with its auto-mitigation feature, which allows very agile activation of DDoS protection.

After the attack vector is identified, router-based DDoS mitigations can be instantiated automatically (without user intervention) while providing network and security operators with full control to monitor or override mitigation settings.

Auto-mitigation significantly improves the agility of mitigations and allows the network to defend itself against impactful DDoS attacks.

Extensive reporting during and after DDos mitigation details the successfully mitigated DDoS attacks and the mitigation efficiency.

Auto-mitigation of DDoS is supported on router-based, scrubber-based and hybrid auto-mitigations.

When using router-based DDoS mitigation, BGP Flowspec, RTBH, NETCONF or a combination are used to configure filter policies.

Auto-mitigation of DDoS improves the overall security workflow and management of mitigation.

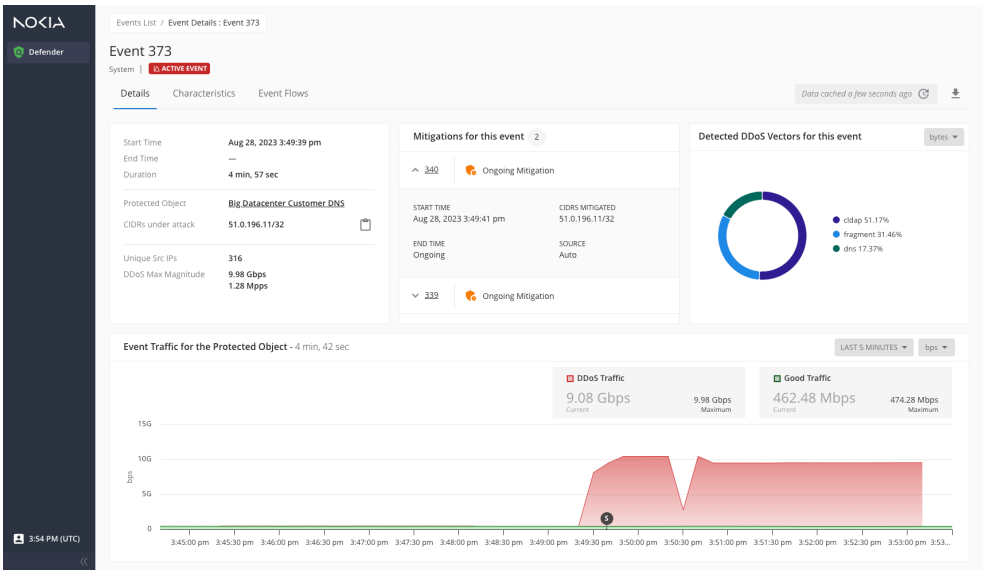
Managed security as a service

As an option to its core functionality, Deepfield Defender provides an extensive set of features that allow service providers to become a managed DDoS security service provider (MSSP) and offer a managed security service to their customers. Deepfield Defender can enable MSSPs to provide great insights to their customers about how they are protected. To this aim, Defender delivers the (optional) MSSP portal functionality, with features like:

- Creation of scheduled PDF reports and delivery over email
- SAML2-based Single Sign On (SSO) into the MSSP portal for service provider-managed security customers
- Granular MSSP permission settings (to allow or restrict the level of detail offered to subscribers)
- MSSP console restrictions
- Enhanced MSSP user workflows
- MSSP portal landing page for events with event details, characteristics, flows
- Protected Object lists page
- Protected Object console and analytics tabs,
- and many others.

An example of an event detail s page is shown below.

Figure 12. MSSP portal: Event details page



Using Deepfield Defender

Deepfield Defender is a software application that can run in the network, on dedicated servers or virtual machines, or deployed in the cloud.

Seamless horizontal and vertical scalability required for the largest deployments is ensured in both deployment modes using a sophisticated, highly resilient and scalable software architecture.

Deepfield Defender can dramatically improve security workflows and further facilitate security automation through its sophisticated features.

Intuitive GUI

Defender uses an intuitive GUI to define, manage and implement complex security policies across a broad and diverse range of DDoS filtering appliances and NETCONF/BGP Flowspec/RTBH routers (see Figure 10).

New DDoS detection and mitigation options can easily be added. Features such as protected objects and auto-mitigation help define and implement comprehensive network security scenarios that maximize the integrity and security of the network.

Use case-focused workflows

The Deepfield approach enables intent-based DDoS mitigations: instead of defining mitigations using large and complicated lists of source and destination IP addresses (and many additional criteria), a mitigation policy can be defined, such as “enable the mitigation countermeasure “UDP Amplification / Reflection” to drop all UDP amplifier and reflection traffic.”

This approach makes it straightforward to define and enforce advanced and customized security policies.

To enable these enhanced filter capabilities, Defender utilizes the Cloud Genome and Secure Genome data feeds to build allow-lists and block-lists.

Manual, semi-automatic and fully automatic workflows are supported for provisioning protected customers and defining custom DDoS detection and mitigation policies.

Advanced security policies with customizable filters

Defender can drive the instantiation of many different network filters on network routers.

Filters installed on routers using NETCONF or BGP Flowspec are fully customizable. For example, some routers can install all these filters, and others just a subset. This flexibility facilitates the creation and dynamic management of current security policies.

Reporting

Using SNMP, IP Flow and streaming network telemetry (gRPC) obtained from routers, Defender generates event and DDoS mitigation reports with detailed incident and mitigation information.

Data such as packets/sec and bits/sec counters used by the mitigation filters on routers is collected, aggregated and processed by Defender to deliver real-time DDoS mitigation feedback and reports that help monitor and optimize mitigations and serve as a basis for customer reports.

Automation

Defender has been designed to continuously improve its DDoS detection capabilities and adapt to the changing nature of network threats and attacks. Defender has been designed to continuously improve its

DDoS detection capabilities and adapt to the changing nature of network threats and attacks.

As an AI-driven security automation platform, Defender treats every detection, every mitigation and every post-incident report as a learning event — closing the loop between intelligence, action and operator workflow. The result is a defense posture that adapts continuously, without continuous manual tuning.

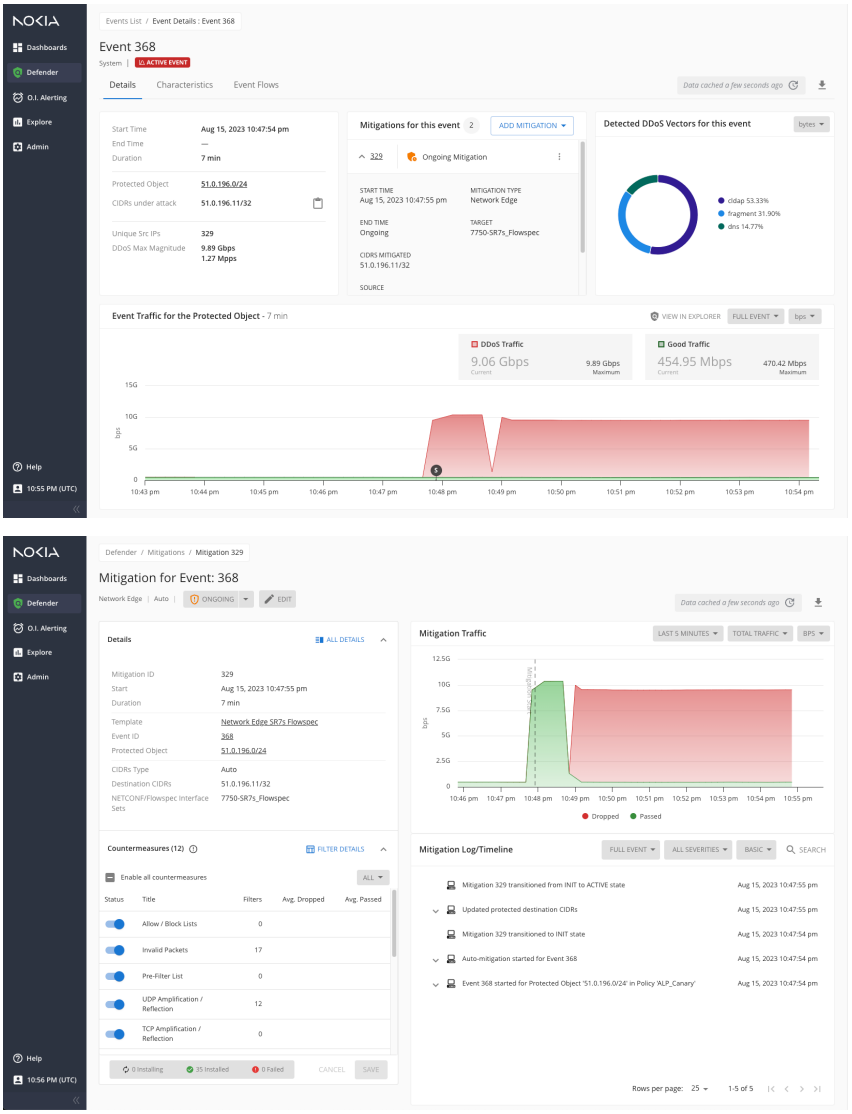
Seamless functional and operational integration with third-party systems and processes, such as API exposure, enables further workflow optimization and security automation.

DDoS security as a managed service

Defender-enabled DDoS protection can be a foundation for creating and offering secure connectivity services to users and customers.

Individual security policies for different security levels can be created and offered to customers and users, as well as various levels of protection based on the use of protected objects.

Figure 13. Defender GUI snapshots related to the detection and mitigation of a DDoS attack



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 telecommunications service providers, cloud and ai providers, internet exchange points (IXPs), cloud builders, research and education networks (RENs), and large 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 multidimensional, 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 is an AI-driven DDoS detection and mitigation platform — engineered as a security automation foundation that leverages 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 for the AI and cloud era.

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

Abbreviations

ACL	access control list
AI	artificial intelligence
API	application programming interface
BGP	Border Gateway Protocol
CDN	content delivery network
DDoS	Distributed Denial of Service
DMS	Defender Mitigation System
DNS	Domain Name System
DSL	digital subscriber line
FTTx	fiber-to-the-anything (x)
gRPC	Remote Procedure Call (RPC) framework
GDTA	Global DDoS Threat All
GUI	graphical user interface
HI	human intelligence
IoT	internet of things
ISP	internet service provider
IXP	internet exchange point
IXR	Interconnect Router
MEC	multi-access edge computing
ML	machine learning
MSSP	managed security service provider
NOC	network operations center
REN	research and education network
RTBH	remotely triggered black hole
SOC	security operations center
SNMP	Simple Network Management Protocol
SXR	Service Interconnect Router
SR	Service Router
SXR	Service Interconnect Router
TCO	total cost of ownership
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

References

1. Nokia Deepfield https://nokia.com/deepfield
2. Nokia Deepfield Defender https://www.nokia.com/networks/ip-networks/deepfield/defender/
3. Deepfield Secure Genome https://www.nokia.com/networks/ip-networks/deepfield/genome/
4. FP Network Processor technology https://www.nokia.com/networks/technologies/fp-network-processor-technology/
5. Nokia 7750 Defender Mitigation System: https://www.nokia.com/ip-networks/deepfield/7750-defender-mitigation-system/
6. 7750 Service Router https://www.nokia.com/ip-networks/7750-service-router/
7. 7730 Service Internconnect Router https://www.nokia.com/ip-networks/7730-sxr/
8. 7250 Interconnect Router https://www.nokia.com/ip-networks/7250-interconnect-router/

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: CID201106 (September)