Nokia Deepfield Defender

DDoS detection and mitigation

Nokia Deepfield Defender provides service providers (cable providers, cloud providers and Telcos) as well as large enterprises with real-time distributed denial-of-service (DDoS) detection and mitigation, to stop threats before they stop your IP network.

Deepfield Defender is a software application that detects attacks down to the Internet of Things (IoT) device or cloud server, dramatically reducing false positives; this allows for surgical mitigation of even the largest attacks.

Defender is one component of the Deepfield solution, which consists of:

- Nokia Deepfield Core Platform: Big data engine/software platform that is the basis for the Deepfield applications
- Nokia Deepfield Cloud Genome: Patented map of the global service supply chain that adds visibility to all applications built onto Core Platform
- Three applications
  - Nokia Deepfield Cloud Intelligence: Analytics application that provides end-to-end network visibility and context-aware content engineering
  - Nokia Deepfield Service Intelligence: Analytics application that monitors customer Quality of Experience (QoE) in real time
  - Nokia Deepfield Defender: Security application that performs real-time DDoS detection and mitigation.
Features

- Fastest, most flexible and accurate DDoS product on the market
- Protection out-of-the-box with built-in protection groups
- Intuitive user interface with multi-vector views on each incident
- Router mitigation: Trigger via BGP Flowspec or blackhole routing, or employ hardware to mitigate specifically detected attack traffic

Benefits

- Advanced detection algorithms make baselining a thing of the past
- Unmatched DDoS protection: See down to the source to mitigate attacks in real time
- OPEX savings through better detection and more accurate, streamlined mitigation
- No vendor lock-in

Overview

Today’s DDoS attacks are more complex and seismic than ever before. Attackers are accessing unsecured IoT devices and large-capacity cloud servers to create terabyte-level attacks that have the ability to take down an entire network or data center. These different sources are impossible to accurately and quickly detect with legacy tools. To combat these threats, your defense must be context-aware with visibility into services, content delivery networks (CDNs), sites and the IoT—not just IP addresses.

Defender is the fastest, most flexible and accurate DDoS product on the market. Defender automatically combines many sources of real-time streaming datasets from your network to detect and mitigate DDoS attacks in seconds—not minutes—and minimizes false positives.

This software application coordinates network-wide mitigation countermeasures from a single control point via BGP Flowspec and blackhole routing. Defender also integrates with third-party hardware and virtual mitigation devices, including those from A10, Radware and Verisign.

Figure 1. How Deepfield works
Use cases

The camera on your garage could be involved in the next DDoS attack. This is because an attacker is easily able to infect 100,000 or more IoT devices with a simple botnet. Combine this volumetric traffic with the muscle of 10G traffic from an unsecured cloud server, and attacks quickly escalate to over 1 TB in size.

Defender uses Cloud Genome to see down to the source and continuously models normal network traffic patterns and behaviors. Defender automatically detects and blocks DDoS integration with on-premises and software-based filtering.

User interface

Defender provides an intuitive user interface to manage complex security policies across thousands of DDoS filtering appliances, firewalls, GBP, Flowspec, blackhole routers, load balancers and virtual machines (see Figure 2).

Figure 2. Defender user interface

Detailed features

**Context:** Identify security threats by service/application, domain, hosting provider, CDN, carrier network and country.

**Per-session-flow granularity:** Search sessions across millions of IP addresses and thousands of routers.

**Customized protection:** Customize your security policy by ingesting new data sets.

**Open ecosystem:** No vendor lock-in. Mix and match to use the best hardware and virtual mitigation devices from our partners for total DDoS defense. Partners include A10, Radware and Verisign.

**Third-party threat feeds on demand:** Gain real-time access to dozens of commercial and community-driven databases of evolving threats.

**Deepfield threat feed data source:** The Deepfield threat field data source crawls the internet for threats so you don’t need to.

**Multi-vector views on each incident:** Multi-vector views on each incident let you see all the details without jumping between incidents.
**Dashboard:** View active and past incidents in the context of your network traffic. Look at your traffic as a whole or by protection group. View and export network-wide summary reports of the whole network or the backbone.

**Incident details:** Every attack and incident has a dedicated page with a multi-vector view of the attack’s signature details, history and relevant mitigations. If you need to mitigate quickly, start a strategic mitigation directly from this page.

**Mitigations:** View all active and past mitigations from one spot. Troubleshoot which mitigations or policies are causing more trouble for good traffic. Create policies for long-term network problems.

**Configurations:** Configure your DDoS-related devices from the Connectors page for fast, easy mitigation. Set up BGP Flowspec and blackhole sessions in advance of attacks.

**Defender users**

ISPs, cable operators and large enterprises can use Defender for network engineering/operations, business development and marketing.