Nokia Deepfield Defender

Unrivaled DDoS detection and versatile mitigation for IP networks

Nokia Deepfield Defender arms service providers, webscale companies and large digital enterprises with accurate, real-time detection and flexible mitigation of distributed denial-of-service (DDoS) threats and attacks—before they impact the network and services.

Deepfield Defender is a software application that detects and mitigates DDoS threats and attacks for service providers, webscale companies and large digital enterprises.

DDoS threats and attacks are becoming common and more impactful in the era of the cloud, 5G and the Internet of Things (IoT). The growth of all-IP networks has extended the security perimeter and expanded the threat and attack surface. Clearly, a more agile, precise and intelligent approach is required to thwart and minimize the security risks associated with DDoS threats and attacks.

Defender relies on big data-driven network intelligence to detect DDoS threats and attacks and can be deployed in a wide range of mitigation scenarios to minimize or neutralize the impact on your network, services, end users and subscribers.

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

Features

• Agile and accurate DDoS detection with advanced threat/attack thresholding
• Support for a wide range of mitigation options, from router-based to scrubbing center-based and hardware-based

• Proven interoperability with major third-party mitigation devices
• Out-of-the-box protection, with advanced and easy-to-deploy options for network-wide protection

Benefits

• Delivers cost-effective infrastructure and network services protection against DDoS threats and attacks
• Facilitates DDoS security automation for agile response and improved customer experience
• Provides real-time visibility into details about incidents through intuitive user interface with multidimensional/multi-vector views and reports

Why Deepfield Defender?

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 volumetric—terabyte-level—attacks that can take down an entire network or a data center. Threats that have been known for more than a decade, such as reflection and amplification attacks (e.g., TCP SYN/SYN-ACK reflection) are also gaining momentum because they are now capable of addressing an increased attack surface.
Attackers are also using combinations of attack techniques and vectors to “shape-shift” their attacks, changing the mix and intensity of DDoS attacks over time and across different parts of the network.

These evolving attack techniques make it impossible to accurately and quickly detect the sources of DDoS attacks with legacy tools. To combat the new generation of threats, your defense must be context-aware, with cloud-era visibility into services, content delivery networks (CDNs), sites and the IoT—not just IP addresses.

Deepfield Defender provides fast, flexible and accurate DDoS protection by automatically combining the knowledge obtained from many sources in your network to detect and mitigate DDoS attacks as they happen.

Defender coordinates network-wide mitigation countermeasures from a single control point using remotely-triggered black hole (RTBH) and Border Gateway Protocol (BGP) Flowspec filtering, and integrates with major third-party hardware and virtual mitigation devices.

The detection technology used in Defender is also a foundation for our most comprehensive DDoS security solution, Deepfield Network Firewall, which extends mitigation capabilities to the network edge routers, representing a new method for agile, cost-effective mitigation of volumetric attacks.

How Deepfield Defender works

Service providers, webscale companies and large digital enterprises are concerned about security threats originating from outside of their networks and data centers (inbound DDoS) as well as threats and attacks originating in their networks and data centers (outbound DDoS).

Deepfield Defender leverages the Deepfield Secure Genome data feed, which contains security-related details of the global internet, to detect and mitigate threats across your entire network (see Figure 1). Defender allows you to monitor network protocols used for DDoS attacks in real time and to benchmark traffic volumes and query/response ratios against normalized or pre-set values.

Because of its ability to correlate your network’s data with the most up-to-date security-related data from Secure Genome, Defender can minimize DDoS threat/attack false positives (i.e., mislabeling legitimate network flows as insecure) and false negatives (i.e., failing to detect real threats and attacks by declaring them as legitimate network traffic). Minimizing false positives and false negatives results in unprecedented accuracy of DDoS detection.

Figure 1. How Deepfield Defender works
When anomalies are detected, various mitigation scenarios can be initiated:

- BGP RTBH filtering
- BGP Flowspec filtering
- Scrubbing-center traffic cleaning.

**BGP RTBH filtering**
Malicious traffic can be removed by creating a black hole as a next hop in the BGP route. BGP RTBH filtering removes all traffic from or to a particular source or destination. This mitigation scenario works with network devices (routers) that install a black hole as the next hop.

**BGP Flowspec filtering**
BGP Flowspec filtering removes the malicious traffic and leaves the legitimate traffic unaffected. It provides additional granularity over RTBH filtering by using Layer 3/Layer 4 access control list (ACL) filtering; this approach narrows the scope of mitigation to the misused protocol or port numbers. BGP Flowspec is used to signal requests to a router (or group of routers) to drop, rate-limit or redirect traffic.

This mitigation approach is available for any router that supports standard Flowspec filter options.

Nokia service routers (e.g., 7750 SR and 7750 SR-s product families) provide improved protection and mitigation efficiency due to advanced processing and filtering capabilities based on the Nokia FP4 network processor.

**Scrubbing-center traffic cleaning**
Scrubbing-center traffic cleaning diverts the traffic to a third-party scrubbing center for analysis and cleaning, so the clean traffic can be passed to its destinations.

We have integrated Deepfield Defender with major third-party scrubbing devices. Full interoperability of detection and mitigation is achieved through API integration, and you can use mitigation feedback from scrubbing platforms to monitor mitigation and create customized reports.

**Deploying Deepfield Defender**
Deepfield Defender is a software application that you can run in your network on dedicated servers or in the virtualized environment, or you can deploy it in the cloud using the software-as-a-service model. Seamless scalability is ensured in all these modes of deployment using sophisticated software architecture.

**Using Deepfield Defender**
Deepfield Defender provides an intuitive user interface to manage complex security policies across a wide and diverse range of DDoS filtering appliances, BGP Flowspec routers, RTBH routers, and virtual appliances (see Figure 2).

New detection and mitigation options can easily be added. Sophisticated features such as protection groups and auto-mitigation help define and implement diverse and comprehensive network security frameworks that maximize the integrity and security of the network.
Figure 2. Deepfield Defender user interface showing a snapshot of forensic analysis of an incident.
Dashboard

Important and commonly executed queries can be saved for repeated and quick access in the form of a dashboard. Dashboards can be customized for different users or user groups.

Automation

Implementation of sophisticated machine-learning algorithms equips Deepfield Defender with the ability to continuously improve its detection capabilities and adapt to the changing nature of network threats and attacks.

Through seamless functional and operational integration with third-party systems and processes, you can achieve further workflow optimization and security automation.

Leveraging Secure Genome for better Deepfield Defender context

Deepfield Secure Genome is a cloud-based data feed that continuously probes and tracks billions of IPv4 and IPv6 addresses on the internet, maps them to Domain name Server (DNS) names, and employs advanced machine-learning rules to further tag the addresses into security-related types and categories.

Because Secure Genome provides a holistic security-related perspective of all internet applications and services, it allows Deepfield Defender to have a complete, real-time view of internet security.

Secure Genome empowers Defender with full visibility into many customizable, security-related categories, including whitelists, blacklists, threats and secure browsing data. This detailed, security-related insight allows Defender to deliver superior accuracy, agile mitigation and unique features, such as:

- **Detailed security context:** Identify security threats by service/application, domain, hosting provider, CDN, carrier network and country.
- **Accuracy:** Monitor and inspect the most relevant IP sessions with per-flow granularity.
- **Customized protection:** Customize your security policies by specifying and ingesting new security-related data sets as they become available (e.g., multi-operator shared security insights).
- **Open-ecosystem solution:** Mix and match to use your existing and the best new hardware and virtual mitigation devices and techniques for total DDoS defense.
- **Third-party threat feeds on demand:** Flexibility to add access to third-party databases of evolving threats.

Use cases

Deepfield Defender provides scalable, contextual awareness to identify inbound and outbound DDoS threats and attacks and engage immediate mitigation scenarios. A few examples of this new generation of threats follow.

**Botnets**

Your customers’ insecure web cameras could be involved in the next DDoS attack. The increasing number of terabit-level DDoS attacks stem from hackers who hijack thousands of poorly protected or unprotected IoT devices, including home routers, video cameras and smart TVs. All of these devices can be compromised at the same time by a botnet that coordinates an attack to flood your company with bogus traffic to make your website and servers unavailable.

**Brute force attacks**

Due to a largely increased attack surface, attackers can launch volumetric traffic attacks that begin as 10 Gb/s traffic from an unsecured cloud server and can quickly escalate to over 1 Tb/s.
“Carpet bombing” attacks
Using a combination of attack vectors, attackers can launch multivector “carpet bombing” attacks that affect tens of thousands of customers even though no single endpoint goes down. This type of attack can affect the quality of over-the-top video streaming, with a large number of customers receiving only SD quality instead of HD.

Deepfield Defender response
With its real-time, end-to-end security intelligence, Deepfield Defender understands the difference between normal network behavior and identifies incorrect traffic signatures, making it possible to detect anomalies with improved accuracy and agility.

Through its set of sophisticated features, including auto-mitigation capabilities, Defender can dramatically improve security workflows and further facilitate security automation.

For details on use cases, visit the Deepfield web page.

The Nokia Deepfield advantage
The real-time cloud and network context provided by the Nokia Deepfield solution enables service providers to extract the actionable intelligence needed to better design their networks, react to performance anomalies and changing traffic patterns, manage security threats, and better package their product offerings to attract and retain subscribers.

Nokia Deepfield enables service providers to understand, in real time, the service delivery path from the internet/cloud through the peering edge and at the customer edge—a path that can span multiple clouds, data centers, CDNs and networks. This visibility is the critical first step to intelligent network automation, which will enable networks to respond immediately to changing conditions with minimal manual or physical intervention, lowering costs and improving performance.

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