NOKIA | worldstream

Next-gen DDoS protection for high-performance hosting environments

Worldstream deploys Nokia Deepfield Defender and Nokia IP routers for improved security and protection of its hosting services against DDoS

About Worldstream

Worldstream is a Dutch cloud infrastructure provider with company-owned data centers and delivers clear, solid IT infrastructure, including bare metal servers, private cloud environments, and reliable hosting and storage options for cloud, security, and backup services.

Founded in 2006 by friends with a passion for hosting, Worldstream has grown into one of the most trusted infrastructure providers in the Netherlands. Its strong focus on trust and transparency is reflected in market-leading customer satisfaction scores and predictable pricing.

Worldstream operates three data centers in the Netherlands and ensures full compliance and control — without interference from third parties. It offers 24/7/365 support from in-house engineers, with an average response time of just seven minutes.

Its global network backbone and local-first approach allow customers to build secure, future-ready IT environments. With predictable pricing, freedom of choice, and full ownership, Worldstream helps IT teams regain control over their infrastructure.

Worldstream's customers

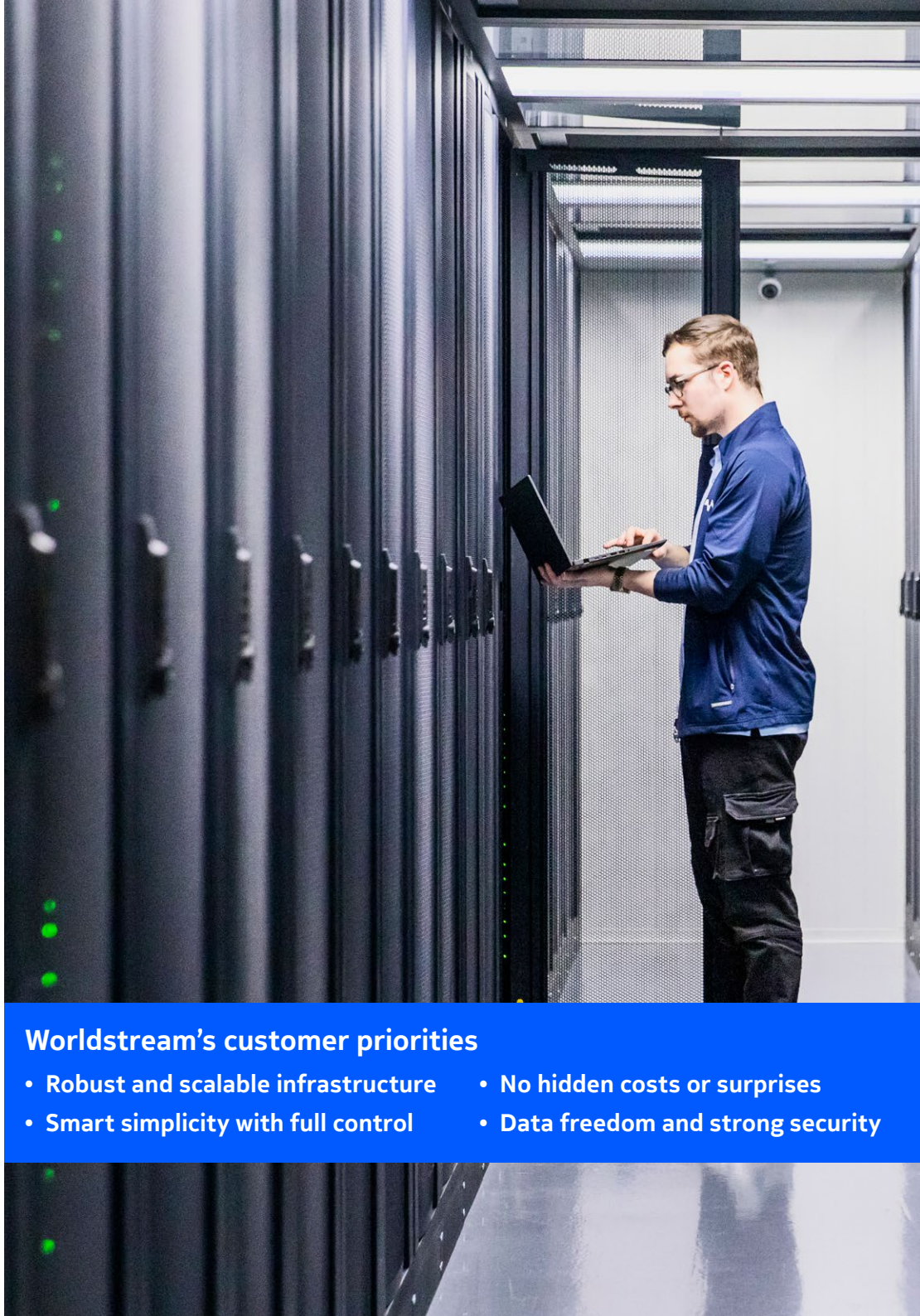
Worldstream serves a diverse clientele across various industries, providing IaaS solutions to address diverse IT infrastructure needs. Its notable customers include:

- **EasyTerra**, a car rental comparison platform
- **Dutch Drone Company**, a drone services provider
- **PerfGrid**, an enterprise-focused hosting company
- **Bookmate**, an e-book subscription service
- **AppSignal**, a provider of application monitoring tools
- **Navaio**, a cybersecurity firm
- **BICT Group**, an IT solution provider
- **Deltics**, an IT service provider
- **DAEL**, a telecom company.[1]

Worldstream's customer base extends to multiple continents and includes companies from all over the world: approximately 51% of its customers are based in Europe, and 15% are in the Americas.

Worldstream serves customers in multiple sectors, including IT services, software development, cybersecurity and telecommunications. This diversity highlights Worldstream's ability to deliver flexible and scalable IT solutions tailored to various industry requirements and customized to meet each customer's needs.

To keep growing its already impressive list of satisfied customers, Worldstream prioritizes scalability, reliability, transparency and security. It also strives to scale all these aspects in a cost-efficient manner, ensuring that none of them come at the expense of the others (e.g., maintaining simplicity without compromising reliability or security).



Worldstream's customer priorities

- **Robust and scalable infrastructure**
- **Smart simplicity with full control**
- **No hidden costs or surprises**
- **Data freedom and strong security**

1 "Case studies | Worldstream," Worldstream.com, 2024. https://www.worldstream.com/en/cases (accessed Apr. 10, 2025).

Why Worldstream focuses on security

Security is crucial for Worldstream's clients, which rely on its IaaS solutions to store, process and manage business-critical data. Many of these companies operate in highly regulated segments such as IT services, software development, cybersecurity, telecommunications and finance, where data breaches, cyberattacks and downtime can have severe consequences.

Worldstream's high-security data centers protect clients from threats such as DDoS attacks, unauthorized access and data loss, and ensure compliance with national and international standards and regulatory frameworks. Its 24/7/365 monitoring, advanced firewalls, encryption and system architecture redundancy provide high reliability and minimize risks.

For enterprises that handle customer data, intellectual property or mission-critical applications, Worldstream's strong security measures help maintain trust, regulatory compliance and business continuity.

Enhancing hosting services with the DDoS Shield

Worldstream has enhanced its leading hosted services with the DDoS Shield service, which offers robust protection against DDoS attacks and ensures that customers' business operations remain stable and secure.

This protection reflects Worldstream's unwavering focus on key features such as:

- **Scalability:** DDoS Shield uses multi-tiered intelligent clustering to seamlessly adapt to evolving threats and scale mitigation efforts as needed.
- **Automatic traffic protection:** Worldstream's Security Operations Center monitors the DDoS Shield 24/7/365 to enable real-time analysis and response.
- **High-capacity protection for customers:** DDoS Shield uses a global network backbone and an anti-DDoS solution with 1 Tbps of scrubbing capacity to ensure effective mitigation for large DDoS attacks.
- **Contemporary protection:** Worldstream continuously investigates every DDoS attack to stay ahead of emerging threats, ensuring that its protection strategies capitalize on the latest DDoS trends.

DDoS: A clear and present danger

DDoS is becoming an increasing concern for all participants in the internet ecosystem, including cloud providers like Worldstream.

DDoS traffic continues to grow at a faster rate than any other type of network traffic, increasing 166% between June 2023 and June 2024. New attacks are driven predominantly by botnets, which are collections of insecure or compromised IoT devices and systems. Botnet attacks now account for about 60% of all DDoS traffic.[3]

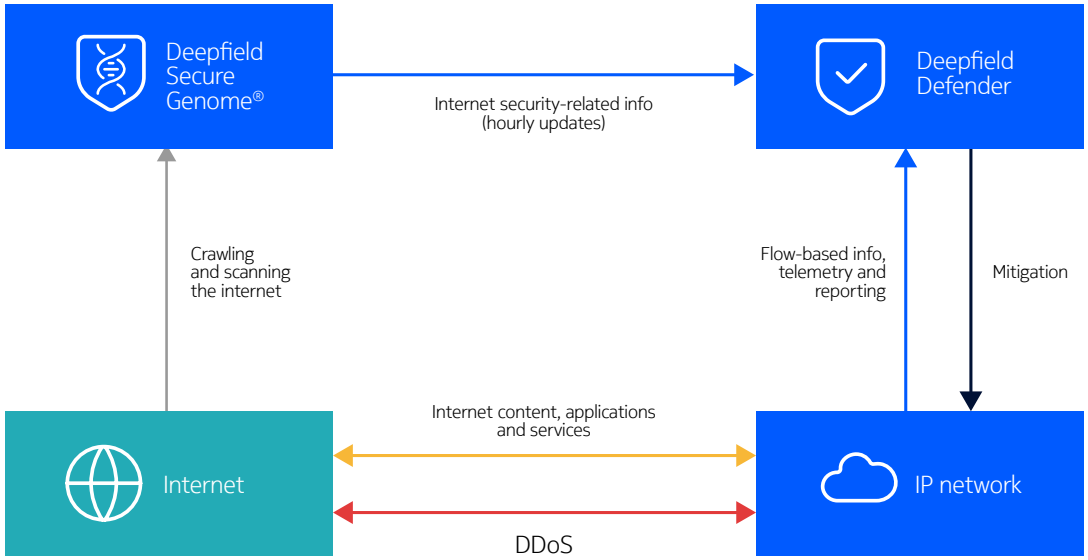
With the deployment of novel technologies such as AI and the use of mechanisms such as residential proxies, DDoS attacks have become more complex, frequent and potent than ever.

The sharp increase in the number of daily security incidents stemming from DDoS attacks is driving cloud providers to reconsider whether their existing anti-DDoS solutions are ready to defend against the latest generation of threats and attacks.

DDoS traffic and attack trends

- Many networks now face well over 100 DDoS attacks per day
- The majority of DDoS attacks are driven by DNS amplification
- 60% of all botnet DDoS attacks involve fewer than 100 bots
- 44% of the DDoS attacks observed in 2024 lasted less than five minutes

The Nokia DDoS Security solution



3 "Nokia Threat Intelligence Report finds cybercriminal attacks on telco infrastructure are accelerating, driven by Generative AI and automation," Nokia, 2024. https://www.nokia.com/about-us/news/releases/2024/10/02/nokia-threat-intelligence-report-finds-cybercriminal-attacks-on-telco-infrastructure-are-accelerating-driven-by-generative-ai-and-automation/

The quest for a next-generation DDoS security solution

Worldstream recognized that its in-house-developed DDoS solution was struggling to cope with the latest generations of DDoS attacks. The company identified several areas for improvement, including:

- **Overall DDoS mitigation capacity:** The solution had 1 Tbps of scrubbing capacity but could not scale with Worldstream's business needs. Also, diverting large volumes of suspicious traffic to scrubber traffic was costly and introduced latency that could affect some customers.
- **Resilience to the new generation of DDoS attacks:** The most challenging task for the existing anti-DDoS system was dealing with large carpet-bombing attacks that target a large number of hosts (IP addresses). These attacks often required the solution to divert a larger amount of traffic than the scrubber could support (over 1 Tbps).
- **Automated response:** The growing prevalence of short-lived attacks—lasting minutes rather than hours—called for a solution that could provide an immediate, targeted and automated response.

With these requirements in mind, Worldstream determined that it needed a next-generation DDoS security solution that could:

- Apply AI and machine learning (ML) to improve the accuracy and speed of DDoS detection and the scale, agility and efficiency of DDoS mitigation
- Detect new and future generations of attacks with greater accuracy and speed
- Automate mitigation for all types of DDoS attacks (volumetric, botnet, carpet bombing, application layer)
- Ensure compliance with new security regulations and initiatives that demand more responsive and detailed incident reports and notifications for regulators and customers.

Why Worldstream chose Nokia

Worldstream was impressed with Nokia's demonstration of network edge-based DDoS mitigation at its SReXperts event. In addition, successful testing of the Nokia DDoS security solution in the lab of a third-party European security powerhouse provided further assurance that Worldstream needed to try the solution for itself.

Worldstream chose the Nokia solution because it provides key capabilities that address the most important and pressing DDoS security needs.

- **Network-based DDoS protection:** The solution applies protection directly at the network edge, on Nokia routers (already in the Worldstream network), not as a separate layer or a dedicated scrubbing system. By eliminating the scrubbing center-based approach, network edge-based DDoS mitigation can stop sophisticated DDoS attacks as they happen, with no latency and without the need to shuffle large amounts of network traffic.
- **Fast, accurate detection:** The Nokia solution uses NETCONF and sampled packet mirroring (SPM) as telemetry methods to obtain information about good network and DDoS traffic. This combination of telemetry input dramatically improves detection time.
- **Automated, rapid mitigation:** With automated protection, the complete mitigation is brought under 30 seconds (and often much faster) for the most complex and novel attacks. With mitigation delivered in seconds, the solution eliminates human errors and gives security operations teams more time to focus on other important tasks.
- **Flexibility:** The Nokia solution allows Worldstream to customize DDoS protection for its own DDoS service definitions. Worldstream can take advantage of API-based integration with the managed security service portal offered by Nokia to tailor and customize policy configuration and DDoS protection for its customers.
- **Reporting:** The Nokia solution provides reporting capabilities that enable Worldstream to address the demands of customers, regulatory agencies and frameworks (e.g., meeting the critical incident reporting obligations specified in the EU's NIS2 directive).
- **Extending on-demand support to DDoS security:** The solution includes 24/7 expert help from Nokia security professionals.

Worldstream's next-generation anti-DDoS solution

The Nokia DDoS security solution enables Worldstream to fight DDoS attacks with unprecedented accuracy, speed, scale, efficiency and cost-effectiveness—directly at the network edge or in centralized deployments. The solution includes two main elements:

1. Nokia Deepfield Defender, an AI-driven big data analytics software application that provides fast and accurate DDoS detection and facilitates agile mitigation of all types of DDoS attacks
2. Nokia 7750 Service Routers, with built-in security capabilities that do not hinder the routing performance.

Holistic, 360-degree DDoS protection with Deepfield Defender

Deepfield Defender combines network data (including telemetry, DNS and BGP) with the patented Nokia Deepfield Secure Genome®, a cloud-based data feed that continuously tracks the security context of the internet.

Secure Genome has detailed visibility into more than five billion IPv4 and IPv6 addresses. It tracks more than 30 categories of internet traffic and applies more than 100 ML rules to automatically classify and precisely allocate applications and flows into security-related traffic types and categories. It "knows" the intricate security details of the internet, including prior attacks, insecure servers and compromised IoT devices that can be used for DDoS attacks.

Deepfield Defender correlates knowledge from Secure Genome with information obtained from the network to detect DDoS attacks faster and more accurately. It drives agile network-based mitigation using advanced IP routers such as Nokia FP4/FP5/FPcx-based IP routers or dedicated mitigation systems such as the Nokia 7750 Defender Mitigation System (DMS).

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

Nokia uses Deepfield Defender as the foundation for its next-generation DDoS detection and mitigation solution. Leveraging rich telemetry and the programmability of the IP network itself, Deepfield Defender offers significant advantages over legacy scrubber- or DPI-based approaches. These include better scalability, more accurate DDoS detection with fewer false positives, and more efficient and rapid DDoS mitigation in the most cost-efficient manner. With Deepfield Defender, Worldstream gets the holistic, 360-degree DDoS security it needs for cloud and AI applications.

Network-based mitigation with 7750 SR

The Nokia solution performs network-based mitigation using the 7750 Service Router (SR) family. Powered by the Nokia FP5 network processor, these routers deliver scalable, agile and granular DDoS mitigation on a large scale. They remove only DDoS traffic and minimize the effect of DDoS attacks on services and customers.

With the 7750 SR, Worldstream gets performance without compromise. It can scale mitigation to terabit levels while ensuring predictable IP routing and high performance.

Expert DDoS support by Deepfield ERTS

Deepfield Defender and the 7750 SR are complemented by the Deepfield Emergency Response Team Support (ERTS) service. Staffed by Nokia security experts, this 24/7 global support service further empowers Worldstream's network engineering and security operations teams to stop DDoS attacks.

Find out more

Visit our website to learn more about how our 7750 SR family, Deepfield Defender and support services can help you keep pace with growing capacity demand and fight DDoS attacks with unprecedented scale, effectiveness and cost-efficiency.

Stop DDoS traffic before it affects your customers and services.

- Deepfield Defender
- 7750 Service Router
- FP technology
- Deepfield Emergency Response Team Support Service

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID: 214696 (July)

nokia.com

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

With truly open architectures that seamlessly integrate into any ecosystem, our high-performance networks create new opportunities for monetization and scale. Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.