

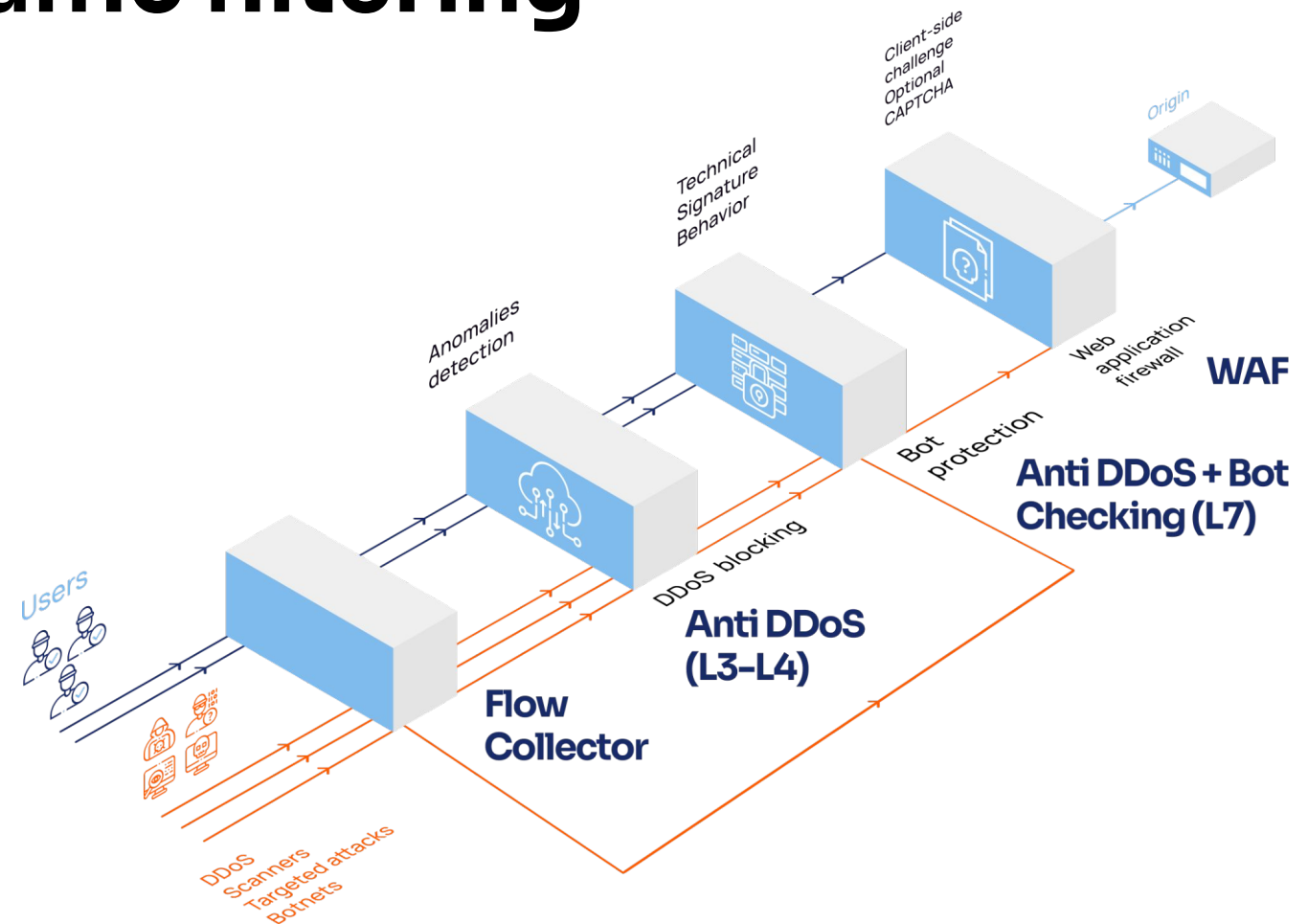
Secwell

Ideal Customer Profile (ICP)



We offer 4-level traffic filtering

0. **Flow Collector** — a monitoring system for collection, storage, and analysis of network storage data
1. **Anti DDoS** — a broad filter that removes the bulk of parasitic traffic from your service
2. **Anti DDoS + Bot checking** — granular, request-by-request traffic filtering that detects intelligent bots masquerading as real users
3. **WAF** — targeted filtering to block “manual” attacks and SQL injections





Key Features

Features for End-Clients

- **Technical Support Response Time:** Less than 15 minutes.
- **Mitigation Time:** 1 second for bad request detection.
- **False Positives:** Less than 0.01%.
- **CPU/SSD Utilization:** Decrease of up to 30% on load balancers and web servers due to web-scraping blocking.
- **Bot Blocking Efficiency:** An average of 23% of total daily web requests generated by persistent bad bots is blocked without affecting legitimate customer traffic.

Features for Partners

- **Profitability:** Over 30% margin on sales, making this a high-margin business.
- **Notable Clients:** Companies like Metro and DPD are among their clients, with others under NDA.
- **Integration & Flexibility:** Seamlessly integrates with SIEM SOC platforms, showing strengths in cybersecurity and managed security services.



Product Capabilities

FlowCollector

- **100 ms for any anomaly detection**
- 30+ DDoS attacks vectors
- 250K fps NetFlow processing
- Identifies both wide-scale DDoS attacks (targeting the entire IP range) and targeted attacks (focused on a specific destination IP)

AntiDDoS (L3-L4)

- high performance and fault tolerance based on Linux Kernel
- Up to 150 M filtration rules
- 50+ rule presets
- **Built-in filtering rule builder**
- Continuously updated signature database
- 400Gbps 400Mpps per 1U server
- universal solution with flexible deployment options and additional use cases



Product Capabilities

AntiBot (DDoS & Bot cheking L7)

- no changes to application code and development process required
- 100+ metrics real-time analysis
- **superior accuracy of detection and flexible custom rules engine**
- no negative impact on SEO
- **90%+ less incidents on WAF**

WAF

- OWASP Top 20 vulnerabilities and zero-day threats protection
- PCI DSS Compliant
- No impact on legitimate traffic



Technology & Expertise

- **Proprietary Signature Database:** Regularly updated with new threat signatures, supported by a dedicated team of analysts.
- **Real-Time Traffic Analysis:** The system continuously analyzes traffic patterns, signatures, and technical anomalies to provide high-precision filtering.
- **Deployment Options:** SaaS, On-premise, Hybrid, or custom-built solutions, making the product adaptable to diverse infrastructure needs.
- **Single Vendor Solution:** Provides unified protection for all automated cyberattacks across L3-L7, offering comprehensive coverage.



Customer Segments

1. ISPs, Telecom, and Cloud Providers:

Real-time detection of network anomalies, protecting critical IT infrastructures.

2. Finance & Banking:

Provides pre-cleaned traffic for financial institutions, ensuring operational continuity during large-scale DDoS attacks.

3. High-Load Services:

Guarantees 100% availability of popular online services and gaming platforms during attacks exceeding 300 Gbps.

4. E-Commerce & Retail:

Protects against content scraping, API business logic abuse, and other OWASP threats for online retailers.

5. Payment Services:

Ensures compliance with PCI DSS and GDPR while maintaining 100% uptime for payment platforms.

6. Ticketing & Travel:

Prevents scalping, scraping, account takeovers, and fraud for airlines, travel agencies, and entertainment industries.



Key clients and decision makers

IT/Security related

Chief Information Security Officer
Enterprise Solutions Architect
Chief Technology Officer
Chief Technical Officer
Head of Information Technology
Head of Security
Fraud Officer
Head of Digital
Security Engineer

Marketing related

Head of Product Management
Chief Marketing Officer
Director of Ecommerce

ISPs, Telecom, and Cloud Providers

Niche solutions



Key problems

Up to 70% of traffic on critical infrastructure networks consists of malicious activity, ranging from botnets to advanced DDoS attacks

What Threatens?

Service Outages

Malicious traffic, including DDoS attacks, can overwhelm the network and transport layers, leading to performance degradation of network equipment, service interruptions, complete unavailability of the network

Multi-Vector Attacks

Sophisticated attackers often employ multi-layered approaches:

- Volumetric DDoS Attacks (L3/L4): Large-scale attacks that flood the network with traffic, acting as a diversion.
- Targeted L7 Attacks: Exploit vulnerabilities at the application or API endpoint level, bypassing traditional defenses.



How it can manifest

Channel Overload

Abnormal, unexplained traffic spikes on specific resources (e.g., registration or login pages, product pages)

Denial of Service

A deliberate flood of millions of synthetic requests aimed at overloading the server and blocking access for legitimate users. This attack is often used for extortion or sabotage.

Exploitation of content and services

Abuse of critical resources such as DNS amplification or the use of IP address ranges for malicious activity



Slow site performance, reduced service quality, SLA violations, customer churn



Service failures, unauthorized access and increased operational costs



Loss of trust, IP blocking and regulatory fines



Secwell Solution



Defends against multi-vector DDoS attacks: advanced protection for L3-L7 traffic, ensuring uninterrupted service delivery



Mitigates API and application threats: blocks unauthorized access and abuse of application endpoints



Supports cloud signaling: the system notifies of detected attack. Rapid activation of protection measures minimizes damage from the attack and ensures service continuity (SLA up to 99.99%)



Why Secwell

Proprietary traffic processing kernel based on XDP and eBPF
multi-layered security: Network and session-based security

Comprehensive protection without user disruption

Ensures seamless protection for web applications from all types of DDoS attacks while avoiding blanket IP address blocking, preserving legitimate user access and experience

Pre-packaged rule sets

Up to 150 million unique rules across the entire system. A unique rule builder that enables you to create highly accurate defense solutions in minutes.

Flexible integration options

- On-premise: Software or PAC to infrastructure
- Hybrid: On-premise + Cloud Signaling + Cloud

Finance and Banking

Niche solutions



Key problems

The finance industry is one of the **most regulated** yet highly vulnerable to attacks. Recently, the maximum volume of application attacks has increased **tenfold**.

What threatens?

Record DDoS Attacks

While the usual load on a bank application rarely exceeds 5,000 requests per second, attacks of up to 300,000 requests per second have become the new norm

Sophisticated Web Threats

Over 25% of financial application traffic consists of automated requests from bots, which continuously introduce new threats



How it can manifest

Denial of Service

Abnormal, unexplained traffic spikes on specific resources (registration, login, product pages)



Lost profits, reputational damage, and customer churn

Account Creation, Account Aggregation, New Account Fraud

An unusual increase in the number of new accounts, comments, and spam activity



Loss of confidence in the platform, key metrics distorted

Credit Card Fraud, Carding, Card Cracking

A rise in card fraud incidents, increase in customer support requests



Sufficient financial losses, reputational damage, regulatory violations, fines (PCI-DSS, GDPR)



Secwell Solution



Ensures service availability during DDoS attacks of any size and duration



Blocks advanced bot attacks targeting APIs and personal banking offices, payment systems, and insurance platforms



Provides precise filtering of encrypted HTTPS traffic, helping you comply with regulatory requirements



Why Secwell

Single Provider for L3-L7 Protection

We filter all DDoS attacks at L3-L7 and mitigate threats listed in the OWASP Automated Threats to Web Applications, Top 10, and API Security Top 10

PCI DSS Compliance

We block parasitic financial application traffic without exposing SSL encryption keys by utilizing an NGINX module installed on the customer's infrastructure

API Protection Without Code Changes

Training mobile application traffic models takes no more than 3 days

Bot Management

Our solution includes a request classifier (bot/user) and flexible request filtering rules. Ensure your services remain stable while meeting regulatory requirements.

High-Load Services

Niche solutions



Key problems

High-Load Services represent the **#1 segment targeted by sophisticated bad bots** that mimic legitimate users, making it challenging to be detected

What Threatens?

Volumetric DDoS Attacks

- DNS Flood: overwhelms a DNS server by sending a high volume of queries from multiple IP-addresses
- DNS Amplification: a type of volumetric attack that exploits DNS servers to amplify traffic, creating significant disruption

Low-Frequency DDoS Attacks: a distributed attack originating from multiple IP-addresses, where each source mimics normal user activity, making it hard to be detected

Attacks on APIs: business logic exploits, including fraudulent activities like fake orders, scalping, or SMS bombing, which can disrupt operations and harm revenue



How it can manifest

Denial of Service

A targeted flood of synthetic requests intentionally overwhelms server resources, denying access to legitimate users (for extortion or disruptive purposes)

Infrastructure overload

Increased consumption of resources (e.g. CPU, memory) without an increase in legitimate user traffic

API Errors

The server may return error codes such as HTTP 503 (Service Unavailable) or 429 (Too Many Requests), API endpoints may cease functioning or become temporarily inaccessible



Service failures, unauthorized access and increased operational costs



Increased infrastructure costs, degradation of network equipment, inability to handle peak loads and reduced scalability



Poor performance, frequent errors, loss of user trust, direct financial losses



Secwell Solution



Prevents over 99% of network attacks: protects TCP and UDP protocols and ensures the availability of services running on SMTP, FTP, SSH, VoIP, VPN, and many other protocols



Detects attacks in <1ms: responds instantly to threats with Always-On filtering, preventing potential damage before it occurs



Defends against DDoS attacks without volume limits: up to 700 Gbps and 400 Mpps represent record-breaking attacks that our solution has successfully defended against. This includes stable filtering for 300+ hours during a continuous DDoS attack



Why Secwell

High performance and stability

Protection against L3-L7 DDoS attacks, up to 700 Gbps and 400 Mpps per device

Own geo-distributed infrastructure

Located in Tier-3 data centers or higher, with at least two independent upstreams supporting flowspec on each node, full component redundancy, and no single points of failure

Load balancing

Filtering parasitic load on the application and IT infrastructure optimizes total cost of ownership (TCO) and increases the efficiency of existing IT resource usage

Retail & e-Commerce

Niche solutions



Key problems

Up to 85% of resource requests during Black Fridays are made by bots and targeted attacks

What Threatens?

Service unavailability and customer data leaks

IT infrastructure costs increase, personal, and payment data are leaked, and companies suffer multimillion-dollar losses and reputational damage

Multi-vector attacks

A large-scale DDoS attack on L3/L4 may be just a cover for a botnet, a low-frequency attack on L7, or a hacking attempt



How it can manifest

Server overload

Abnormal, unexplained traffic spikes on specific resources (e.g., registration or login pages, product pages).

Content scraping

Your content appears on other sites, and your SEO ranking drops. Decreased conversions, unexplained site slowdowns (usually caused by aggressive parsers).

Gift card abuse

Sudden spikes in requests on the gift card balance page, an increase in support calls.

Denial of inventory

An increase in the number of abandoned items in shopping carts, a decrease in conversions, and more customer complaints about missing items.



Lost profits, reputational damage, and customer churn



Lost customers, lost revenue, and decreased site performance



Financial losses due to theft by bots, reputational damage



Loss of revenue from unsold items held in carts by bots, reputational damage



Secwell Solution



Repels DDoS attacks on online stores and blocks malicious bots



Prevents competitors from scraping your unique content



Protects against card abuse, ad fraud, and fake orders



Why Secwell

High Accuracy

With multifactor traffic analysis, we block unwanted automation from the first request without compromising the user experience

Cost Savings

Reduce the burden on IT resources, mitigate sufficient financial and brand reputational losses

SEO-Friendly

Bot blocking has no negative impact on SEO, thanks to our continuously updated global whitelist of beneficial bots (e.g., search engines, social media platforms, analytics tools)

Payment Services

Niche solutions



Key problems

Under GDPR, regulatory fines can reach **up to 4% of a company's annual global turnover or €20 million**, whichever is greater

What Threatens?

Volumetric, Protocol, and Application DDoS attacks: regardless of the attack type or scale, they overload servers and network infrastructure, causing payment systems to become unavailable for anywhere from several minutes to several hours

Automated attacks on business logic: bots can simulate fraudulent orders or transactions, making the system inaccessible. Equally dangerous are attempts to extract sensitive information (e.g., card details), carry out fake fund transfers, or cancel legitimate payments.



How it can manifest

Denial of Service

A deliberate surge of artificial requests floods server resources, blocking access for legitimate users, often with the intent to extort or cause disruption

Card fraud

Increase in the number of customer support calls, number of processed refunds, etc.

Account Takeover, Credential Stuffing, Credential Cracking

Increase in user accounts blocking, technical support requests (lost points, stolen credit cards, unauthorized purchases), cancellations and refunds



Service failures, unauthorized access and increased operational costs



Sufficient financial losses, reputational damage, regulatory violations, fines (PCI-DSS, GDPR)



Reduced productivity, reputational damage, regulatory violations, fines (PCI-DSS, GDPR)



Secwell Solution



Prevents bandwidth and infrastructure overload: filters malicious traffic, alleviating strain on core resources while ensuring scalability



Protects against card fraud, account takeover, and fake transactions



Ensures accurate filtering of encrypted HTTPS traffic, helping to meet regulatory compliance standards



Why Secwell

One vendor for all attacks

We filter L3-L7 attacks and protect against the OWASP Top 20 automated threats

Fine-tuning

Our three-stage filtering system (including customizable rule sets and over 100 bot/human detection parameters per request) effectively blocks intelligent attacks by advanced bots targeting payment system APIs and private accounts

PCI DSS compliance

We block parasitic traffic without disclosing SSL certificate information

Ticketing, travel & hospitality

Niche solutions



Key problems

The entertainment and hospitality industry remains one of the **most targeted** industries by bot attacks

70% of bots in this niche are advanced — can imitate human behavior, use software to automate malicious actions or embed malware in browsers

What threatens?

Attackers use automation to book and resell products, commit price fraud, steal loyalty points, and abuse promotions



How it can manifest

Price Scraping

SEO performance loss, lower conversion rates

SMS Leak

SMS authorization costs unreasonable growth, monthly budget limit exhaustion within days

Scalping

Unexplained website slowdowns and reduced conversion rates



Loss of customers, unfair market positioning, prices, and products misrepresentation



A blow to brand reputation, as recipients receive SMS confirmations for actions they did not perform. Increased workload on tech support, unnecessary SMS expenses



A blow to brand reputation, operational downtime, and reduced LTV (Lifetime Value)



Secwell Solution



Identifies and stops bots that track prices without permission or steal content for unfair pricing strategies



Blocks bots that misuse web application features, like SMS-based form authorization or registration



Prevents bots from buying rare or limited-stock items



Why Secwell

Invisibility

Our high-precision parasitic load filtering ensures no impact on user experience or web speed

Unified web management interface

We provide a personal account to monitor anomalies and access detailed traffic statistics along with visual analytics on queries, either in real time or retrospectively for a selected period

Reports

You receive comprehensive traffic statistics and visual analytics on queries, both in real time and retrospectively, starting from the moment of connection

Trial is the best proof of our effectiveness

Get in touch to discuss integration details
and get additional materials

Salima NABULSI

Business Development manager

Sec-Well LLC FZ

+971 58 556 57 66

Alexander VAKHTIN

General manager

Sec-Well LLC FZ

+971 58 554 50 70