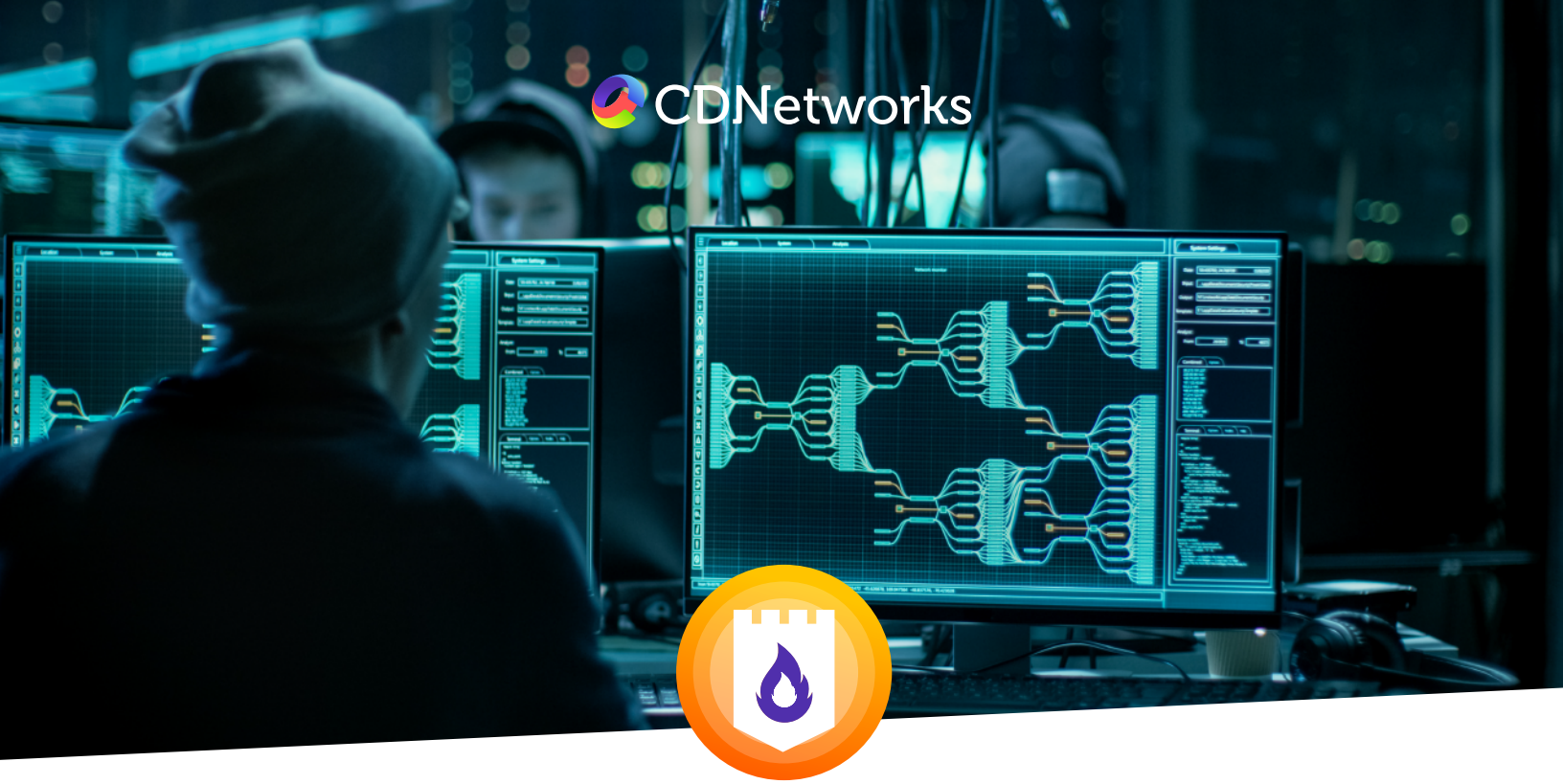


Flood Shield

Distributed Cloud-based DDoS Mitigation Solution

Flood Shield is a comprehensive cloud-based DDoS protection service that delivers fast, simple, and effective DDoS protection to ensure the stability of your origin against distributed denial of service attacks (such as SYN Flood, ACK Flood, UDP Flood, HTTP Flood, etc.) in real time and simultaneously provides an acceleration service to legitim users to optimize the user experience. This solution functions as a shield to ensure the stability and reliability of online services and infrastructures.

Huge Mitigation Capacity (with Abundant Resources)

With over 20 Global DDoS Scrubbing Centers and 15+ Tbps of Mitigation Capacity, Flood Shield protects your business against even the most sophisticated and large-scale volumetric attacks.

Integrated DDoS Protection & Acceleration

Flood Shield is a cloud-based DDoS protection solution that is rooted in CDN acceleration technology. In addition to providing DDoS protection, Flood Shield also offers CDN acceleration services that include smart routing, smart scheduling, load balancing, and caching.

One-stop WAAP Integration

Flood Shield integrates seamlessly with Web Application Firewall (WAF), Bot management, API security, and other security solutions. This interoperability allows you to build a comprehensive WAAP defense strategy that enhances your current website security protection level.

24/7 Support Service

CDNetworks offers a comprehensive range of 24/7 services through its global local support teams. Services include phone, instant messaging, and email support. We also provide multilingual support in English, Chinese, Japanese, Korean, Vietnamese, Thai, Indonesian, and other languages.

Contact us at **sales@cdnetworks.com** or visit **cdnetworks.com**

L3/L4 DDoS Mitigation and Dashboard

Enable real-time detection and automatic blocking of network-layer DDoS attacks such as SYN Flood, ACK Flood, ICMP Flood, and UDP Flood, while achiving sub-second scrubbing capabilities based on an overall 15Tbps+ scrubbing capacity. Keep your network infrastructure safe and available by filtering out malicious traffic and migrating the volumetric attacks to the edge, effectively making edge PoPs the frontline defense against such attacks; Generate a dedicated dashboard and log services to gain insights into network-layer DDoS attacks.

L7 DDoS Mitigation and Dashboard

Protect against HTTP/S floods, low and slow attacks, and other rapidly evolving Layer 7-based DDoS attacks with threat intelligence, advanced rate limitations, transparent challenges and AI protection. Keep your sites and apps up, running, and protected against sophisticated distributed attacks that imitate real human users. Robust mitigation capacity exceeds 1 billion QPS backed by a dedicated application-layer DDoS dashboard and log services.

Multiple Scheduling Techniques

Provide both DNS and Anycast scheduling technologies to achieve mitigation as close to the point of attack as possible, and then pass the normal business traffic back to the origin site while cloaking the origin site.

Preset Protection & Custom Policies

Offer mutiple preset protection policy templates based on more than 10 years of SOC operation experience. Templates can be easily switched to address different types of attacks. Provide custom policies to meet different application scenarios.

Easy Certificate Management

Support flexible SSL certificate management services, and allow self-service uploads of SSL certificates and self-service configuration of free one-click certificates, such as Let's Encrypt.

AI Protection & Machine Learning

Utilize AI intelligent analysis and machine learning to generate normal user access baselines, and then automatically apply appropriate protection strategies. Offer multiple analyzing criteria or indexing for machine learning, which includes IP, HTTP Header, cookies, and JavaScript fragments.

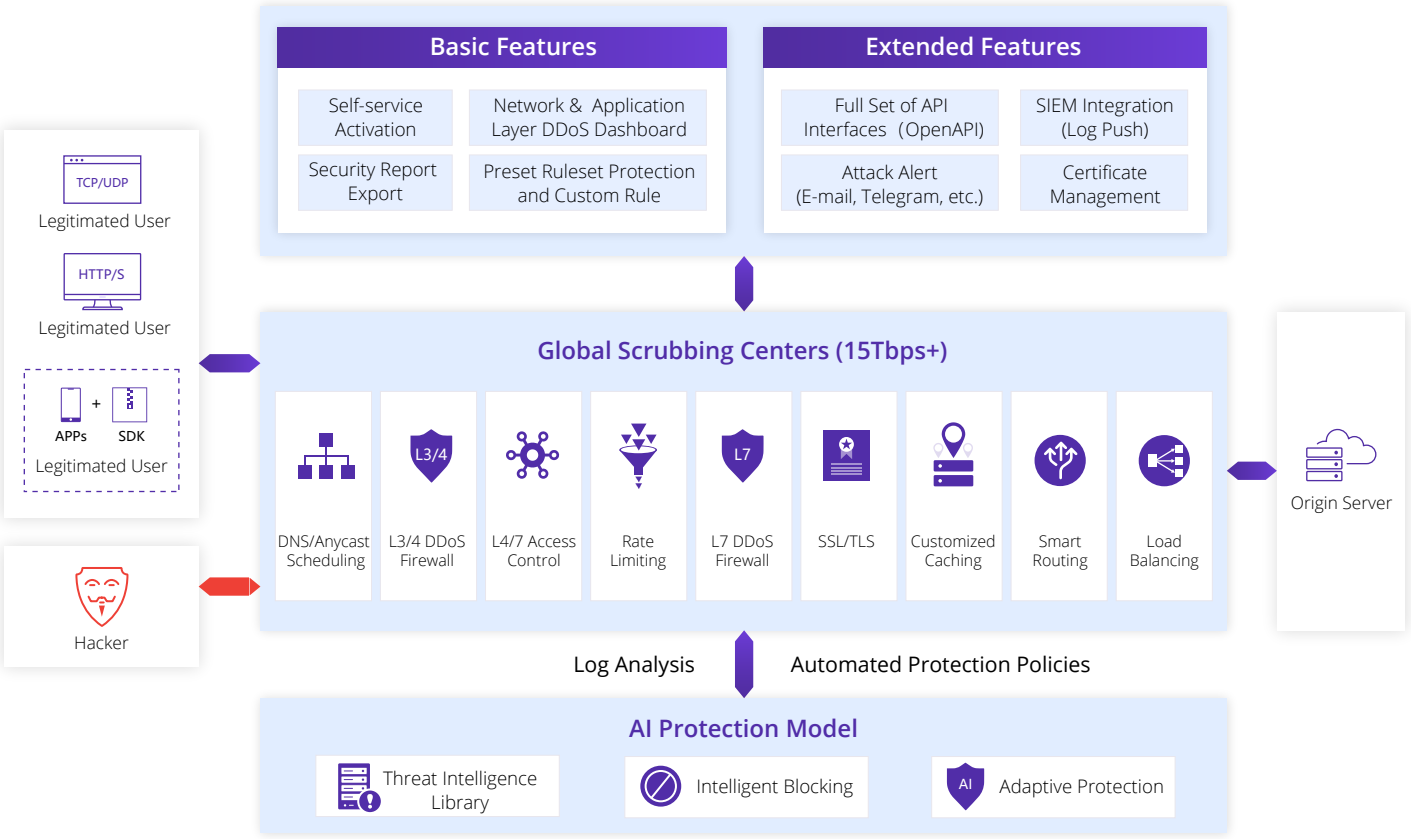
Real-time Monitoring and Alert

Provide multi-dimensional and comprehensive real-time monitoring and alert services, such as network-layer and application-layer DDoS attack alert and CPS switching alert to report immediate alerts about suspicious website activities. Alerts can be sent using various methods including email, telegram, etc.

Multiple Protocol Support for Business Scenarios

Support both HTTP/S, TCP/UDP protocols to meet different business scenarios.

Product Architecture



Product Highlights

Robust Mitigation Capacity

Backed by more than 2,800 globally distributed CDN PoPs, Flood Shield boasts large-scale DDoS scrubbing centers around the world. With 15Tbps+ and 1 billion QPS mitigation capabilities, It has been designed to deflect even the largest, virulent attacks, That's why Flood Shield is the solution of choice for today's large gaming sites, streaming sites and other verticals that are exposed to such attacks.

- **DDoS Scrubbing Centers:** 17 in the Asia-Pacific region outside China's Mainland, 60 in China's Mainland, and 6 in Europe and the U.S.
- **Emerging Market Needs:** New scrubbing centers can be built quickly based on CDNetworks'existing 2,800+ CDN global PoPs.
- **China Premium Service:** CDNetworks provides a Dedicated Internet Access (DIA) service - China Premium Service for global enterprises to access the Chinese audience with superior performance, high reliability, and low latency.

200,000+
Global Servers

2,800+
Global CON PoPs

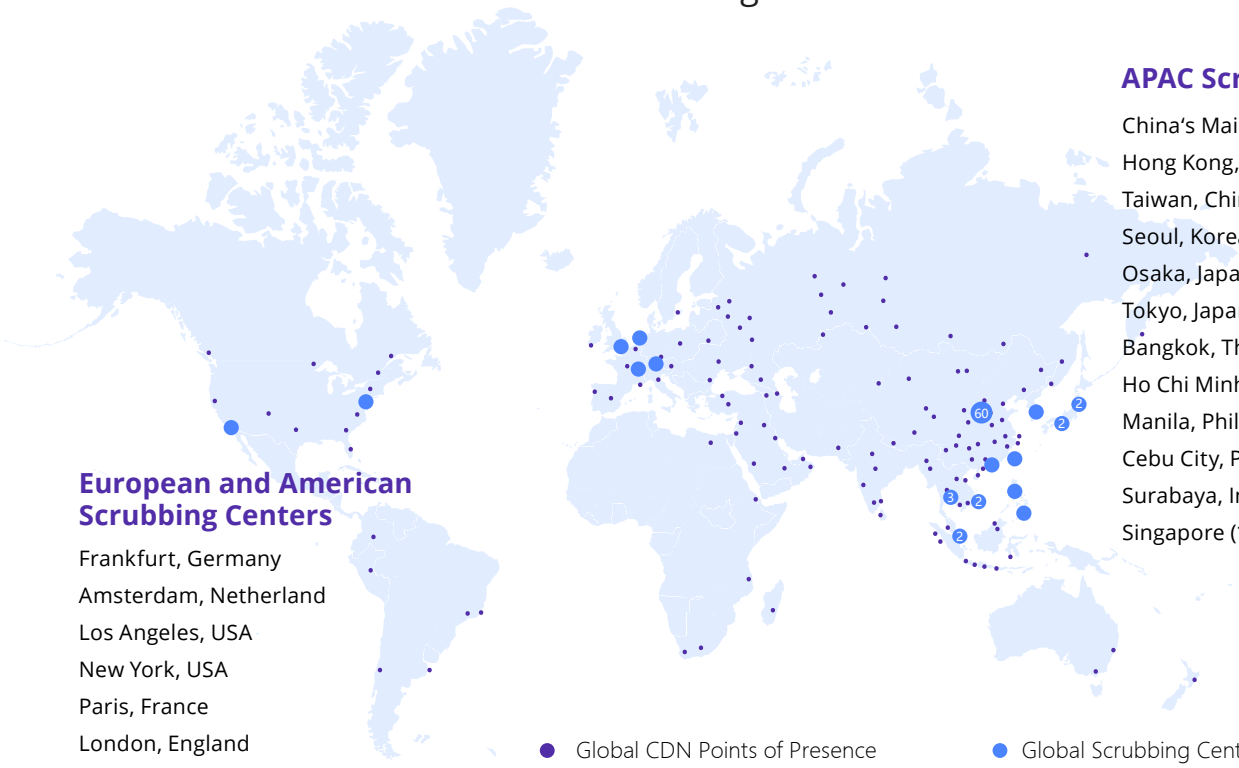
70+
Cities in 70+ Countries

3.3B+
Average Number of Dally Cyberattacks Mitigation

2.09Tbps
DDos Mitigation Peak Volume Record

34.7M QPS
L7 DDos Mitigation Peaked Record

Global Scrubbing Centers Location



APAC Scrubbing Centers

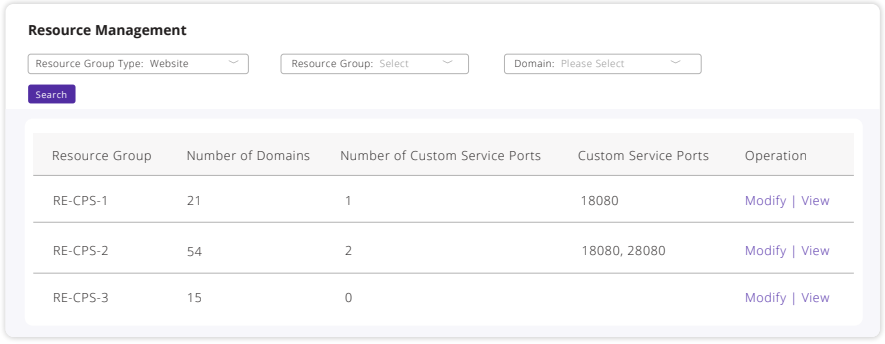
China's Mainland (*60 Centers)
Hong Kong, China
Taiwan, China
Seoul, Korea
Osaka, Japan (*2 Centers)
Tokyo, Japan (*2 Centers)
Bangkok, Thailand (*3 Centers)
Ho Chi Minh City, Vietnam (*2 Centers)
Manila, Philippines
Cebu City, Philippines
Surabaya, Indonesia
Singapore (*2 Centers)

European and American Scrubbing Centers

Frankfurt, Germany
Amsterdam, Netherland
Los Angeles, USA
New York, USA
Paris, France
London, England

Exclusive IP Solution

CDNetworks provides exclusive IP solutions that allocate an exclusive IP group to each customer. This approach not only meets resource isolation requirement, but also collects and displays attack log data at the Layer 3/Layer 4 network layers. Exclusive IP groups also supports the concept of "dedicated MAPs" which allows customers to use multiple IP resource groups to meet the resource-isolation needs of different businesses.



Quick Deployment And Easy Operation

- Providing CNAME (DNS config) or Anycast IP access method to quickly activate services.
- Offering 7*24 monitoring and alert. Security expert team provides services such as onboarding assistance, configuration migration, fine-tuning, and emergency attack incident handling.
- Supporting SIEM integration and push attack logs in nearly real time to meet automated operation and maintenance needs.

SDK Solution for Mobile Apps (Gaming Shield)

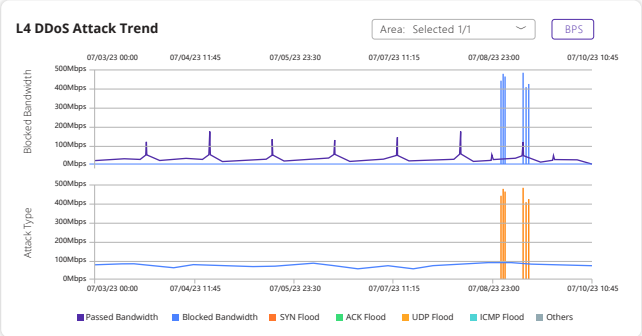
Flood Shield's SDK solution, assumes control over all communication traffic by embedding the SDK on the apps, performance scheduling, and encrypted transmissions, effectively meeting the needs of today's DDoS protection, encryption, and anti-hijacking requirements.

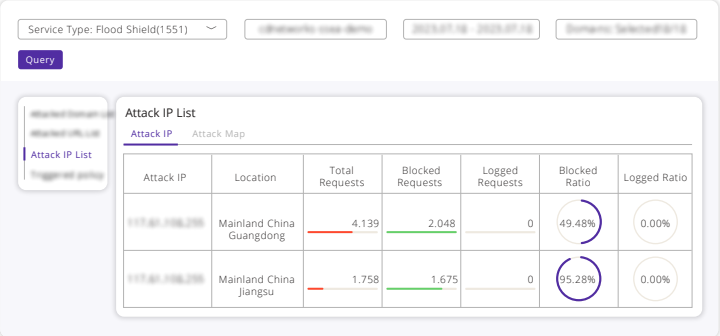
- **High compatibility:** with more than 10 years of experience in SDK development and operation, and proven multi-version compatibility tests including Android and iOS.
- **High-strength encrypted transmission:** SDK link aggregation converges customer domain names to third-party domain names for encrypted transmissions. Support for dynamic changes in server name indication (SNI) prevents SNI hijacking, and prevents the customer's real domain name from being hijacked by grabbing packets from network I/O.
- **Anti-hijacking:** Prevent DNS hijacking by using IP scheduling to obtain PoP IP addresses and automatically switching over if a PoP goes down.

Fully Self-service On Console

CDNetworks provides a simple, unified, easy-to-use, and fully friendly self-service console portal that can be used out of the box to meet self-service query and operation needs and facilitate efficient operation and maintenance.

- Dashboard with rich and multi-dimensional attack log analysis tools.
- Self-service provisioning, including domain name creation, custom port access, security service management, CDN configuration management, and resource group management.
- Assistance with security policy configuration, including preset policies, rate limiting policies, black and white lists, access control, and alert configuration.
- Full API interface list and Open API support, including security configuration, and security reporting API interfaces.
- Console IAM feature: role-based account control, read-only user access, and multi-user administrative access.





Flexible Pricing

- Offering flexible pricing models that fit your risk profile, allowing you to get the best solutions at the best price to suit your business needs. Unlimited mitigation and elastic mitigation plans are available based on your budget.
- Allowing easy integration with WAF, Bot management, and API security to quickly build web application security and API security (WAAP) protection capabilities that comprehensively improve website security protection levels.

CDNetworks

Accelerate. Secure. Control.

As the APAC-leading network with over 2800 global Points of Presence and more than 20 years of technology experience, CDNetworks embraces the new era of Edge and takes it to the next level by using the Edge as a service to deliver the fastest and most secure digital experiences to end users.

Our diverse products and services include web performance, media delivery, cloud security, zero trust security, and colocation services — all of which are uniquely designed to spur business innovation.

To learn more, visit cdnetworks.com and follow us on LinkedIn.

Start Free Trial

Follow Us