NEXUSGUARD ®

DDoS Protection Made Simple

Application Protection Service

Guaranteed Maximum Uptime

NODE 01
NODE 04
NODE 05
NODE 02
NODE 06
NODE 03
BLOCK 01
BLOCK 01

Reliable uptime are customer expectations, compromise is not an option.

Protect web applications , APIs from a variety of attacks, including automated bots, injection & application-layer denial of service.
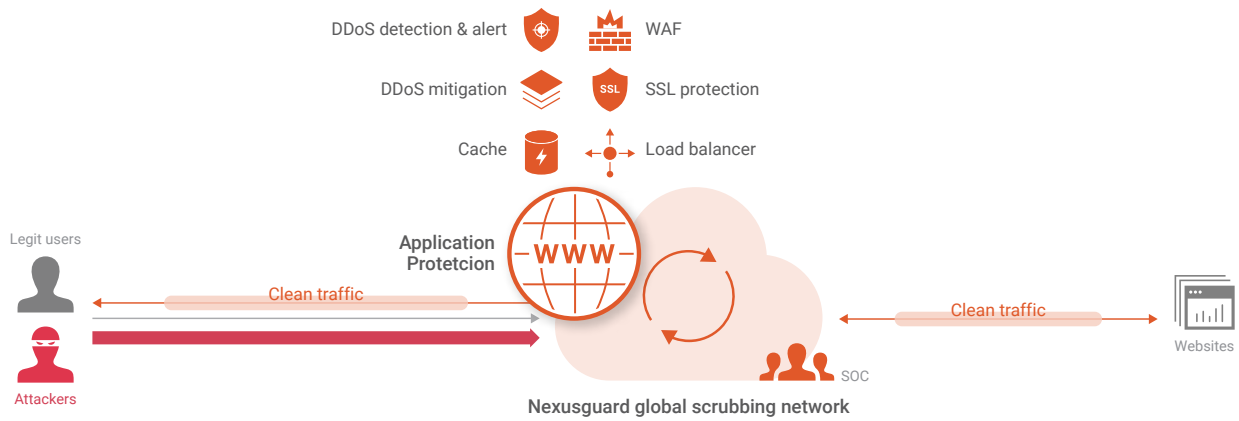
Key Features

✔ Multi-layered L3/4 and L7 protection against attacks on public-facing websites, applications, & APIs.

✔ Cloud-based, enterprise-grade WAF with protection from TOP 10 OWASP vulnerabilities.

✔ SSL Attack Mitigation, Content Caching & Acceleration, Connection Load Balancing.

✔ Real-time mitigation with customized Dashboard, view real-time traffic & attack events with periodic reports.

✔ Continuous development by Nexusguard against latest threats.

Key Benefits

✔ Maximize user experience and performance even during DDOS attacks.

✔ Mitigate SSL-encrypted attacks effectively, with secure Key Management.

✔ Accelerate the delivery of high-bandwidth content to customers worldwide through content caching and acceleration.

✔ Enjoy unparalleled visibility of application traffic and threats in real time.

✔ SLA commitments with monthly performance review reports.

✔ Avoid negative publicity & customer churn.

✔ Attain regulatory compliance & avoid monetary penalties.

Application Protection Service Architecture

DDoS detection & alert

WAF

DDoS mitigation

SSL protection

Cache

Load balancer

Legit users

Application Protecion

WWW

Clean traffic

Clean traffic

Attackers

SOC

Websites

Nexusguard global scrubbing network

	Features	Advantages	Benefits
Volumetric Attack L3-L4	• Mitigate TCP SYN, TCP SYN/ACK, TCP RST, TCP FIN flood, IP fragmentation • Deny UDP and ICMP flood	Protected application stays online even being DDoSed for over 100 Gbps attack.	Maximum Uptime
Detection	• HTTP GET / POST flood • HTTP malformed flood • HTTP connection flood • Slowloris	Protected application can still handle requests from legit users even when victim website is being polled by millions of requests.	Maximum Availablilty
Mitigation Mode	SQL injection, Session fixation, Cross site scripting, Cross site request forgery, Phishing	Prevent hacker stealing confidential information, such as username, password and credit card, from website.	Maintain website integrity, keeping online transcations secure.
SSL Handling	• SSL Bridging/Offload • SSL Cipher Modification	• Reduce SSL loading in origin server. • SSL cipher modification helps to improve SSL rating.	Boost page load speed time, faster response from the Web server
Load Balancing	• Backend Load Balancing • Routing Load Balancing	• Improve service and server resilience for traffic surge or server failure. • Improve network resilience over attack.	Evenly distribute network traffic with redundacny
Caching	• Static Caching • Dynamic Caching. • Customized Caching	Requested content can be delivered to end users faster.	Improve overall user experience

Application Protection Service Overview

Slow Attack Protection

RangeAmp Attack Protection

Auto Detection & Mitigation

Managed SOC

Guaranteed Uptime

Maximize User Experience

View Real-Time Network Traffic & Threats

24
24x7 Access To Dedicated Engineers