NEXUSGUARD®
Global Leader in DDoS Mitigation

Application Protection

What is Application Protection?

The Nexusguard Cybersecurity Platform encompasses three essential elements: Application Protection, Origin Protection, and DNS Protection.

Nexusguard Application Protection service is designed to deliver a perfect balance of protection and performance for public-facing websites and applications while allowing organizations to operate without interruption. The solution leverages Nexusguard's global scrubbing centers, which are equipped with more than 1.44Tbps of mitigation capacity and multi-layered filtering systems, enabling them to mitigate and absorb the largest, most complex DDoS attacks.

How Does It Work?

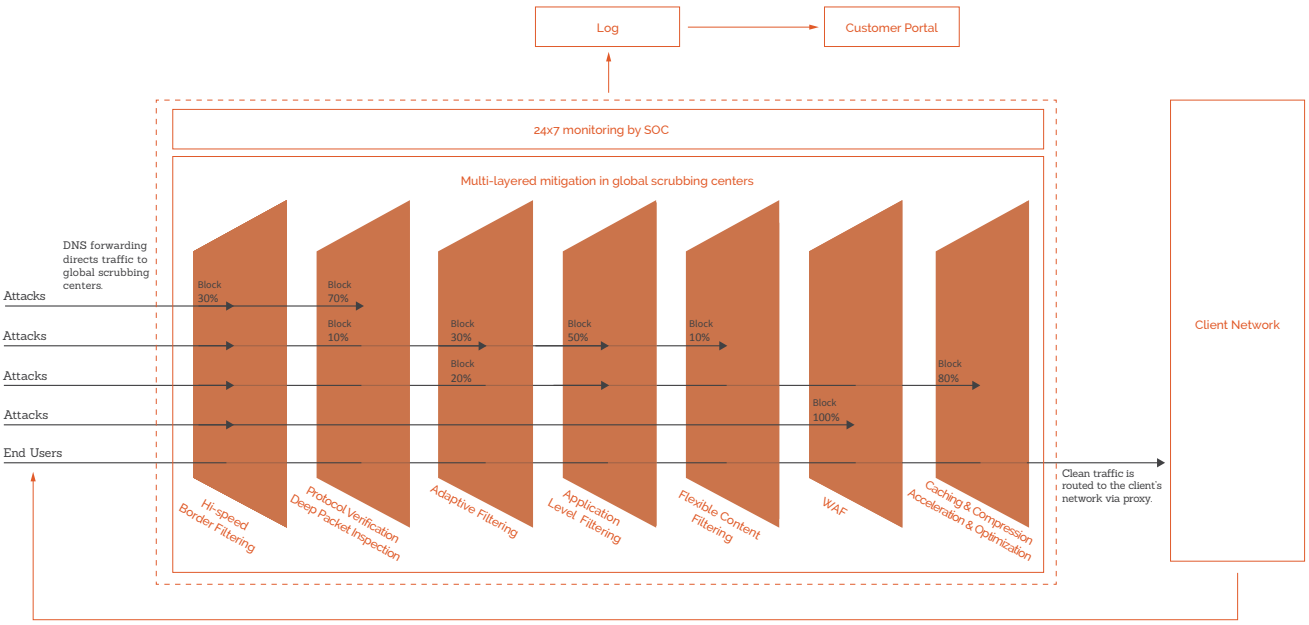
A multi-layered mitigation mechanism, including Nexusguard's proprietary technologies, is used to identify, mitigate, and analyze attacks effectively. Because it is a pure-cloud solution, there are no upfront costs or ongoing maintenance and upgrade costs. Mitigation can start immediately. Multi-layered protection is based on two methods of protection: signature-based detection complemented by statistical behavior analysis.

nexusguard.com
contact@nexusguard.com

Mitigation Layers

- High-speed Border Filtering defends against bandwidth flooding using wire-speed access control lists.
- Protocol Verification filters packets by verifying that Layer 3 network switching and routing protocols and layer transport protocols are being used correctly, enabling it to mitigate packet floods.
- Deep Packet Inspection (DPI) filters out SYN flood and similar attacks attempting to exploit TCP/IP protocol vulnerabilities by examining the packet header and information all the way down to the application layer.
- Adaptive Filtering uses both statistical analysis and anomaly recognition to guard against zero-day attacks.
- Application-level Filtering blocks HTTP traffic that does not conform to protocol specifications and unwanted HTTP applications or content based on Nexusguard's DPI engine.
- Progressive Challenge-Response (C/R) algorithms are employed to further distinguish between spoofed and legitimate traffic.
- Intelligent HTTP Malformed Filtering mitigates application-specific level attacks (HTTP attacks) as they arise.
- Flexible Content Filtering deters morphing HTTP Flood attacks by adapting flexible-content filters to rapidly counter evasive intentions.
- Rate Limiting further limits the exploitation of system and bandwidth resources against baseline statistics.
- Web Application Firewall (WAF) protects web applications, mobile apps, and application program interface (API) apps against common threats such as OWASP Top 10 Attacks. It is custom rule-set enabled.
- Caching serves as the last layer of protection to absorb the final bit of attack traffic, if any, that may have slipped through the preceding layers.

Mitigation Process



Types of Attacks Mitigated

Category	Attack Type	
Bandwidth/ Network Depletion Attacks	Protocol Flood / Exploitation Attacks	TCP Flood
		UDP Flood
		ICMP Flood (Smurf, Ping Flood, Ping of Death, ICMP Echo)
		TCP SYN, SYN/ACK, RST, FIN Flood (Spoofed and Non-spoofed)
		IP Null
		Fragmentation (IP/UDP, IP/ICMP, IP/TCP, Teardrop)
		DNS Amplification
		Fraggle
		Nuke
		TCP Flag Abuse
		Zombie / Bots Attack
Application-based Attacks	HTTP Attacks	HTTP GET/POST Flood
		HTTP Page Flood
		HTTP Connection Flood
		HTTP Malformed Request
		HTTP 404
		Slowloris
		Socketstress
		Slow HTTP
	DNS Attacks	Reflected DNS
		DNS Query
		DNS UDP flood
		DNS TCP flood
		DNS Malformed Query
		Protocol and Vulnerability Exploitation DoS/DDoS
	Hacks	SQL Injection
		Cross Site Scripting (XSS)
		Cross Site Request Forgery (XSRF)
		Session Hijack
Others		Malicious Headers
		Malicious Payloads
		Pucodex
		Zero Day Exploits

Deployment Method

Proxy deployment can be set up quickly using DNS forwarding. The proxy mode supports any application running TCP or UDP such as HTTP, HTTPS, SIP, FTP, DNS, and more on either IPv4 or IPv6. It is especially useful for those preferring minimum network changes and not wishing to control a full public class CIDR/24 network, or those who simply need protection on individual applications.

"White-glove" Provisioning

Nexusguard's Application Protection Service is primarily offered on an always-on basis, while on-demand protection is also available. Subscribers are on-boarded for service provisioning via various methods, including proxies and tunnels, following a detailed analysis of their infrastructure. Each customer provisioning follows a set of well-defined processes and procedures:

Contact — establish key customer requirements and describe the service offering.

Pre-sales — technical requirements evaluation and information gathering by a technical manager, who then appoints a dedicated provisioning manager.

Provisioning — the provisioning manager carries out configuration, implementation, and testing and keeps track of project status to ensure service delivery and quality.

Fine Tuning — a customer service profile is built to ensure optimum traffic flow.

Go Live — the Nexusguard service team elicits customer requirements and briefs the customer on ongoing configurations and operations.

Monitoring and Reporting — ongoing service improvements and dialogue.

Technical Features

- Patented Crawler Detection Technology blocks malicious crawlers, spammers, hackers, and bad bots and even those using forged IP addresses before they can do damage, steal site content or login information, and launch DDoS attacks on customer websites.
- SSL Attack Mitigation protects against SSL-based attacks. SSL decryption and challenge-response mechanisms are enforced only on suspicious traffic. Nexusguard SSL certification management follows the PCI Data Security Standard and ISO 27001 to ensure the highest security standards.
- Content & Network Optimization compresses and caches all traffic going through the cloud, effectively speeding up the delivery of high-traffic websites and online service access for users worldwide. Load-sharing traffic services support multiple backend configurations. Automatic, backend failover is also implemented in the event of a backend server failure.
- Progressive C/R Algorithms defends the application layer against all abuses and attacks. Nexusguard's proprietary C/R protocol employs non-intrusive authentication challenges depending on user behavior and delivers a non-disruptive browsing experience and zero false-positive mitigation errors.
- Web Application Firewall employs blacklist rules to address known security risks, especially OWASP Top 10 Most Critical Web Application Security Risks. Clients can also define site-specific rule sets on the Customer Portal.

Solution Benefits

- Enables consistent uptime connections and high availability
- Delivers "Always On" reliability
- Enables effective security cost management through real-time network insights
- Eliminates security risks from issues impacting uptime goals
- Delivers a superior end-user experience
- Manages risk through optimized mitigation
- Ensures the integrity of mission-critical applications
- Enhances end-user confidence and trust
- Reliable uptime is a customer expectation — compromise is not an option