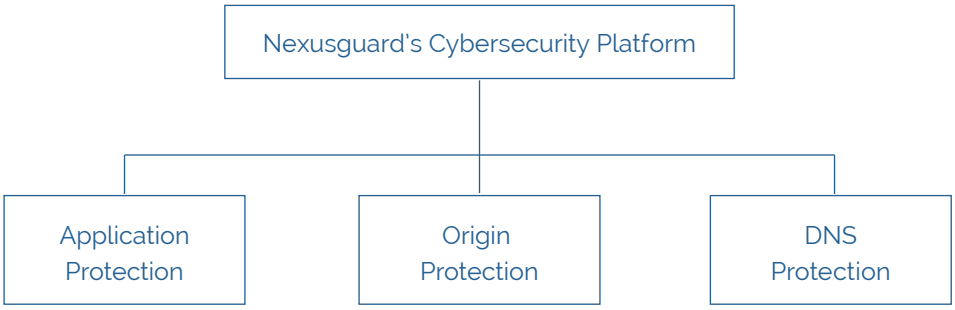
Service Provider Enablement 3.0

Achieving Accelerated Business Gain

Nexusguard Service Provider Enablement (SPE) is a turnkey, low-capex and easy-to-operate solution that enables service providers to provide end-customers with essential DDoS and cyber threat protection solutions—all marketed under your own brand.

The SPE program is built upon Nexusguard's Cybersecurity Platform, which encompasses Application Protection (AP), Origin Protection (OP), and DNS Protection (DNSP), leveraging our global scrubbing network of more than 1.44Tbps, state-of-the-art mitigation system, including various proprietary and patented technologies, as well as our 24x7x365 Security Operations Center (SOC).



AP protects businesses who mainly rely on their websites and web applications from application attacks. The OP solution, which protects all network elements, is especially beneficial for organizations that cannot afford any downtime of their network assets. DNSP is specifically designed to protect mission-critical domain name services from DNS attacks.

Application Protection (AP)

Application Protection (AP) is designed to deliver a perfect balance of protection and performance for public-facing websites and applications utilizing a multi-layered mitigation platform, which features various proprietary and patented technologies, security best practices and a 24x7x365 Security Operations Center (SOC) to detect, mitigate and analyze attack traffic.

How It Works

During normal, peacetime operations, protected applications are served from the edge of provider's network, and content is securely cached and passed along to the origin server. The AP solution leverages TCP Anycast, assigning each of protected business resources a secure Anycast Virtual IP (VIP) address and providing high-performance global accessibility.

* Partner's scrubbing centres are also used to mitigate malicious traffic only if the Partner uses Nexusguard's hybrid solution. In the pure cloud model, Nexusguard's scrubbing centres are responsible for filtering all inbound traffic.

Technology at a Glance

Volumetric DDoS Mitigation

Application DDoS Mitigation

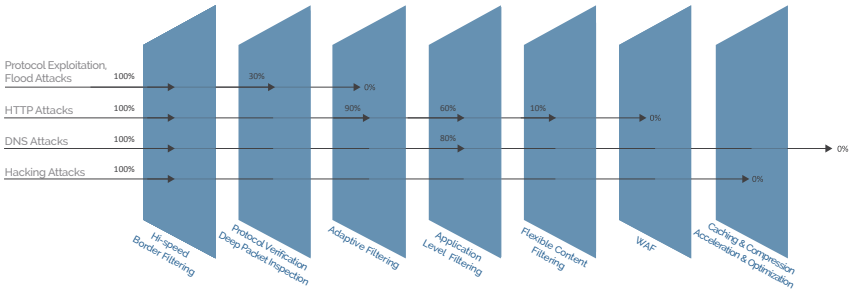
Web Application Firewall

Caching and Load Balancing

Multi-layered Mitigation Defense System

Nexusguard guards against application attack traffic through multiple layers of inspection to deliver fast, clean traffic. The excessive capacity also serves as the last layer of protection to absorb the final bit of attack traffic, if any, that has slipped through the preceding layers. Mitigation layers include:

- Hi-speed border filtering
- Protocol verification
- Deep Packet Inspection (DPI)
- Adaptive filtering
- Application-level filtering
- Flexible content filtering
- Rate limiting
- Web Application Firewall (WAF)
- Caching and load balancing



Volumetric DDoS Mitigation

Nexusguard's volumetric DDoS mitigation solution is built on state-of-art technology. Issues concerning IP spoofing and high-volume DDoS attacks are solved in an innovative, reliable way.

Highlighted Features

- **Anti-Reflection** – Uses attack fingerprints to avoid sending reflected DDoS traffic. By collecting and analyzing attack patterns, the technology differentiates real users and drops requests from botnets without interrupting web services.
- **No Bandwidth Abuse** – Powered by a proprietary spoofing detection algorithm, our volumetric DDoS mitigation never sends abusing traffic.
- **Zero User Impact** – Identifies popular attack fingerprints using Big Data correlation analysis from systems, networks, and industry types, and stops DDoS attacks without affecting real users.

Application DDoS Mitigation

Application DDoS attacks (aka Layer 7 attacks) are increasingly popular with attackers due to their "cost effectiveness." Such attacks generally consume less bandwidth and are stealthier in nature when compared to volumetric attacks.

Application attacks are difficult to detect because a connection has already been established and is frequently encrypted (HTTPS/SSL), and therefore requests may appear to be from legitimate users. Nexusguard's solution offers total defense against application DDoS attacks that attempt to exhaust the resources of web applications and servers.

Application Protection (AP)

- Multi-layered Mitigation Defense System
- Volumetric DDoS Mitigation
- Application DDoS Mitigation
- Web Application Firewall (WAF)
- Caching and Load Balancing

Origin Protection (OP)

DNS Protection (DNSP)

Visibility & Control

24x7 SOC

Highlighted Features

- **Progressive C/R Authentication**: Challenge-response (C/R) algorithms can effortlessly defend the application layer of the network against all sorts of abuses and attacks, while keeping the user experience as smooth and seamless as possible. The challenge authentications are based on continuous learning of user behaviors followed by dynamically tuned progressive challenge thresholds. Requests that do not comply with the unique identifiers in a browser are considered suspicious and will be directed to go through a set of progressive challenges, which include HTTP protocol behavior validation, HTTP redirect authentication, HTTP secure-cookie authentication, JavaScript compute engine verification, and finally Captcha authentication as the validation methods in order to minimize the impact on user experience.

- **SSL Attack Mitigation**: Nexusguard's SSL certification management follows the PCI Data Security Standard and ISO 27001. We offer three SSL traffic-handling options to maximize DDoS mitigation and minimize false-negatives.
  1. **Offloading** – SSL traffic is decrypted at our scrubbing centers and returned to your web servers in clear-text format. This method relieves your servers of processing heavy encrypting/decrypting traffic via SSL, thereby improving server performance.
  2. **Bridging** – SSL traffic is decrypted at our scrubbing centers and re-encrypted when sent back to your servers. As data is SSL-encrypted en route, this method offers the highest level of security.
  3. **Forwarding** – SSL traffic is forwarded to your web servers directly without decryption in between.

- **Smart AI**: mitigates DDoS attacks with greater accuracy. Smart AI identifies visitors using a unique, encrypted tracking tag that prevents users behind proxies from being mistaken for bots. In addition, a smart, state-monitoring machine adjusts filter settings automatically for different circumstances, effectively keeping legitimate users undisturbed.

- **Patented Crawler Identification**: Effectively identifying bad bot traffic, good bot traffic and human traffic needs a great deal of expertise, experience and technology that are far beyond the capability of most site owners. Nexusguard has developed a proprietary, patented search engine crawler identification technology that accurately segregates legitimate crawlers from spoofed or illicit ones, delivering:
  - 100% search engine access
  - Rejection of all forged search engine requests
  - Enhanced SEO optimization and improved search engine rankings

- **Wildcard Domains Supported** - Grouping all sub-domains under one wildcard domain simplifies profile management for sub-domains with the same security setting.

- **Customizable Mitigation Filter** - Provides partners with full control over DDoS protection, hacking protection, caching and load balancing for their customers.

- **Dynamic Backend** - Supports web servers behind dynamic IP addresses using CNAME.

Web Application Firewall (WAF)

Unlike just a few years ago when WAFs were only available as a form of expensive hardware appliance, you can offer your end-customers our cloud-based WAF at highly affordable costs. The WAF protects web applications against unsolicited intrusions, including OWASP Top 10 threats. It examines all HTTP requests and applies rules to filter out malicious traffic from legitimate users.

Because we centrally manage the WAF platform, threat intelligence is collected from and shared among a large pool of clients. Externally, we constantly collect and analyze threat intelligences from multiple sources, keeping us one step ahead of the cyber threat. This collaborative, proactive approach results in improved detection rates and lower false positives, and is remarkably effective in combating zero-day attacks and advanced persistent threats.

Highlighted Features

- **Protection Against OWASP Top 10 Threats** – Protects web application from SQL injection, cross-site scripting, OS command injection and other OWASP top 10 threats.
- **High Detection Rates and Low False Positives** - Because our WAF platform is centrally managed, threat intelligence is collected from and shared among a large pool of clients, resulting in improved detection rates as well as lower false positives.
- **Downloadable WAF Event Log** - A detailed log is available for every WAF event and can be downloaded for post-attack analysis.
- **Easy-to-use Reports** - Easy-to-use reports provide detailed forensic information.
- **Customizable Rule-set** - WAF rule-set for individual customers can be customized on the Customer Portal.
- **PCI DSS Requirement 6.6** - Integration of our WAF into cyber-security measures enables PCI merchants to meet PCI DSS requirement 6.6 effortlessly.

Caching and Load Balancing

During "peacetime," your customers have little tolerance for slow loading pages and website downtime. Leveraging our Global Cloud infrastructure, Nexusguard's goal is to deliver pages without a glitch — and deliver them fast.

The solution's dynamic and static content caching mechanism offloads excessive HTTP requests from the server. All traffic going through the cloud is compressed and cached for speedy delivery. The load-sharing traffic services support multiple backend configurations. Automatic, backend failover is also implemented in the event of a backend server failure.

Highlighted Features

- **Custom Caching Rules** - Partner can create custom caching rules to explicitly control caching per URL and resource types, all of which can be managed on the Partner and Customer Portals.
- **Static/Dynamic Caching** - Speeds up content delivery by caching content on the edge.
- **Multiple Backend Load Balancing** - Improves backend resilience.

Origin Protection (OP)

Nexusguard's Origin Protection covers all elements of a customer's network, e.g. internal websites, email servers, FTP servers, and other applications, against all volumetric and protocol-based DDoS attacks, such as UDP, SMTP or SYN floods. All incoming traffic is routed through all the scrubbing centers using BGP announcements and only clean traffic will be routed through secure GRE tunnels back to customer's servers.

How It Works

Using BGP announcements, all incoming traffic is routed through all the scrubbing centers, collectively equipped with over 1.44Tbps of mitigation capacity. Only clean traffic is routed through a secure Generic Routing Encapsulation (GRE) tunnel back to your customers' servers. Nexusguard advertises all protected IP range announcements on your behalf.

* Partner's scrubbing centres are also used to mitigate malicious traffic only if the Partner uses Nexusguard's hybrid solution. In the pure cloud model, Nexusguard's scrubbing centres are responsible for filtering all inbound traffic.

Highlighted Features

- **Protect Entire Backend Infrastructure** - Protect entire backend infrastructure, e.g. internal websites, email servers, FTP servers, DNS and all other applications

- **Multi-layered mitigation system** - Multi-layered mitigation system blocks known bad source IPs outright, filters out bad traffic (spoofed IPs, botnets, etc.), and let legitimate traffic in.
  1. **Anti-Flood**: Deals with flood attacks that will consume substantial amount of resources from target system. Partners can easily filter flood attacks by type, such as invalid IP, ICMP Fragmentation, TCP Malformed, NTP amplification, and even use customized filter to block attack traffic based on protocol metrics.
  2. **Flexible filter**: Filters traffic based on detail packet header parameters on IPs, ports, protocols, packet size and payloads.
  3. **Traffic Policing**: Allows you to rate limit the amount of clean traffic routed back to customer through the GRE tunnel, preventing line congestion on the customer side.

- **Protection Down to Single IP Address** - Customizable mitigation profile on network level and host level

- **Built-in GRE Tunnel and BGP Routing** - Capability simplifies network setup and configuration management

- **Remote DDoS Monitoring and Traffic Analysis** - Detects attacks through flows collected from customers without the need to swing traffic; defines alert triggering thresholds based on different network protocols, TCP, UDP, ICMP, and IP; scalable for partners of all sizes

DNS Protection (DNSP)

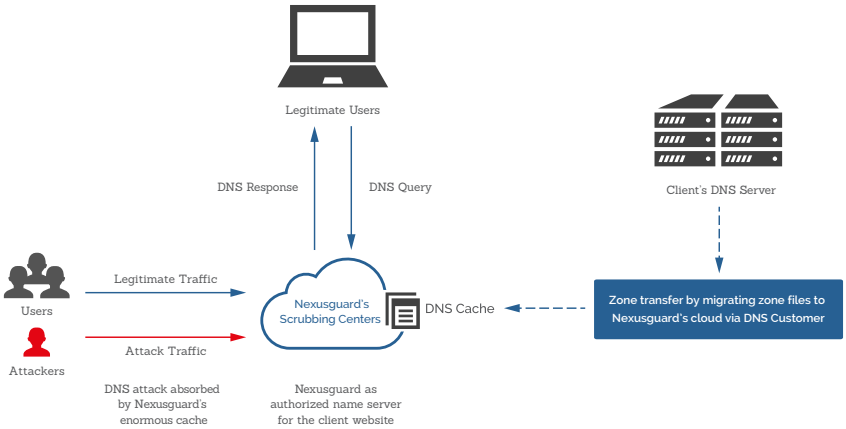
Nexusguard's DNS Protection protects mission-critical online services from all DNS attacks. The solution leverages Nexusguard's globally distributed scrubbing centers to resolve incoming DNS queries quickly and reliably.

How It Works

In a typical recursive DNS query, a client requests the resolution of a domain name or the reverse resolution of an IP address on a local DNS server. The DNS server performs the queries on behalf of the client and returns a response packet with the correct information or an error message. The specification does not allow for unsolicited responses. In a DNS amplification attack, the main indicator is a query response without a matching request.

Residing in front of a customer's infrastructure, Nexusguard DNS Protection Service replaces the DNS server by directly fetching zone records from the customer's servers and caching them in our globally distributed scrubbing centers. The client first has to change the name servers for the domain and point the domain name to Nexusguard's name servers, which can be accomplished at Nexusguard's selfservice Customer Portal.

As the destination for all incoming queries, Nexusguard's cloud-based DNS caches absorb all DNS attacks, while filtering out malicious traffic from incoming queries. Your DNS servers never need to respond to any malicious DNS query — Nexusguard handles everything. Our service protects against direct attacks on DNS services, and abuses of server vulnerabilities as a leverage to launch DNS amplification attacks on other servers.



As Nexusguard acts as the authoritative server on behalf of the client's DNS server, its excessive, redundant caching capability, leveraging Anycast technology to balance load across its high-performance scrubbing network distributed around the globe, can filter out and absorb all DNS attacks and malicious traffic, including but are not limited to the following:

- DNS amplification
- NXDomain
- Phantom domain
- Random sub-domain
- Look-up domain

Highlighted Features

- **DNS Server Cache Snooping Loophole Closed** - Nexusguard does not cache any DNS records while acting as the authoritative DNS servers on behalf of its clients, so that attackers cannot snoop specific DNS records to reveal sensitive information.
- **Dynamic Update Security Threats Eliminated** - Dynamic updates are not permitted and so there is no such dynamic update threat.
- **Fingerprinting Tools Blocked** - Fingerprinting tools such as fpdns, Nmap, and Nessus are unable to identify any information about the software or operating systems our clients are using.
- **Full Control by End-Customers** - End-customers have full control over the DNSP service and configuration through the Customer Portal, reducing the partner's workload in ongoing operations.

Visibility & Control -- Partner Portal

Designed with ease of use in mind, the Partner Portal boasts a comprehensive dashboard and controls, through which you can easily track network traffic, monitor current attacks, review event logs, and manage multiple customer accounts all from one log-in.

Highlighted Features

- **Full Administration** - Full administrative control over services to end-users, including our AP, OP and DNSP solutions, as well as their respective settings.
- **Global Policy** - You can create global policy during initial deployment, and then customize lower-level policies to override the global policy.
- **Mitigation Policy** - Mitigation policy is dispatched to all scrubbing centers in sub-seconds in order to quickly stop attacks near the source.
- **Account Management** - You can manage all customer accounts, configure their mitigation settings and control access on this multi-tenancy platform.
- **Traffic and Attack Analytics** - The dashboard integrates visually appealing maps, graphs and charts that show all traffic and attack analytics as well as other insightful site analytics.
- **Powerful Diagnostic Tools** - Powerful diagnostic tools, such as Packet Capture, to troubleshoot network problems and detect security breaches.
- **Live Monitoring -** Live monitoring of visitors, botnet IPs, edge-to-origin latency, website and backend health monitoring, track the pulse of end-customers' online business.
- **Self-Explanatory Illustrations** - The self-explanatory illustrations save your team a great deal of time in familiarizing themselves with the provisioning and operational procedures.
- **Integrated Dashboard** - With our integrated dashboard, you don't have to build yours, which usually takes a considerable amount of resources and time.
- **Error Code Monitoring** - Error code monitoring allows you to immediately assess the situation, fix and troubleshoot the problems.
- **Regular Reports** - As a value-added service to your customers, you can also create regular reports containing statistics of events, site performance and other site analytics.

24x7 SOC staffed with DDoS experts

Solely relying on automated filtering tools and large bandwidth for DDoS mitigation is not enough. Nexusguard has a 24x7x365 Security Operations Center (SOC) staffed with security experts to monitor and respond to attacks and threats around the clock while providing seamless support to you and your end-customers. Their experiences, skills and availability are essential part of our comprehensive mitigation mechanism, all being combined can flexibly and timely respond to the changing techniques used by attackers. The SOC provides the best DDoS protection at all times, with local language support.

Data Sheet

NEXUSGUARD

Founded in 2008, Nexusguard is the global leader in fighting malicious internet attacks. Nexusguard protects clients against a multitude of threats, including distributed denial of service (DDoS) attacks, to ensure uninterrupted internet service. Nexusguard provides comprehensive, highly customized solutions for customers of all sizes, across a range of industries, and also enables turnkey anti-DDoS solutions for service providers. Nexusguard delivers on its promise to maximize peace of mind by minimizing threats. Headquartered in San Francisco, Nexusguard's network of security experts extends globally.

Twitter twitter.com/nexusguard
Facebook facebook.com/NXG.PR
LinkedIn linkedin.com/company/nexusguard

nexusguard.com
contact@nexusguard.com

20160426-EN-A4