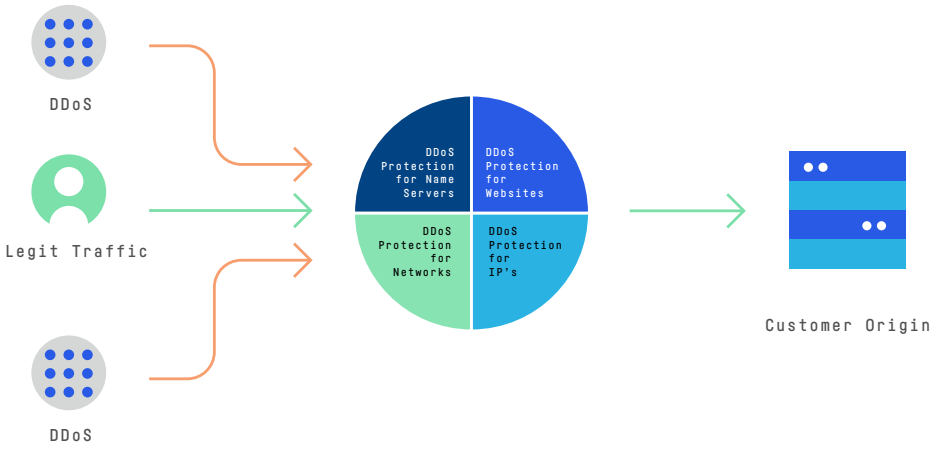
imperva

SOLUTION BRIEF

Imperva DDoS Protection

Formidable attack mitigation

Maybe you've been hit by a DDoS attack and need to better understand how to protect your organization, regardless of whether this was a minor nuisance, or you incurred significant harm. Or you may be simply looking for a replacement DDoS solution that is better equipped to handle the changing threat environment. Perhaps you're one of the few who haven't been attacked yet, (but chances are you will be!) Imperva has the solution: DDoS protection for websites, networks, application servers, DNS servers and individual IPs. Imperva has mitigated the largest attacks in history, immediately and without incurring latency or interfering with legitimate users. DDoS cybercrime is an ever-changing landscape, but our cloud service is prepared to protect you, whatever attack comes your way and no matter what the future holds.



Imperva DDoS Protection options are designed to meet your specific needs, whether you want protection for websites, networks, DNS or individual IPs.

DDOS PROTECTION AT A GLANCE

- Global cloud network (> 6 Tbps) absorbs the largest attacks with specialized support for massive volumetric attacks
- Advanced algorithms solve the most difficult application layer attacks without challenging legitimate users
- Protects Web, DNS, network devices, application servers and individual IPs in cloud
- Deploy for a single server or an entire class C network
- Supports Anycast DNS and Unicast DNS routing
- Supports on-demand BGP routing
- Monitors attacks as they happen
- 24/7 operations center
- Backed by the Imperva security research team
- Part of a comprehensive solution that includes web security, content delivery, RASP and WAF

Global full-stack network

Our high-capacity global network holds more than six Terabits per second (6 Tbps) of on-demand scrubbing capacity and can process more than 65 billion attack packets per second. This global network allows us to track emerging attack methods and incorporate them into our solution via machine learning, so you benefit from the most up-to-date and advanced security protection learned globally.

Attack analytics

Imperva Attack Analytics provides visibility into attacks as they are happening. But we don't stop with visibility: we condense a multitude of events and alerts into a small number of actionable insights. Via the dashboard, you can quickly analyze attacks and adjust security policies on the fly, to stop attacks in their tracks.

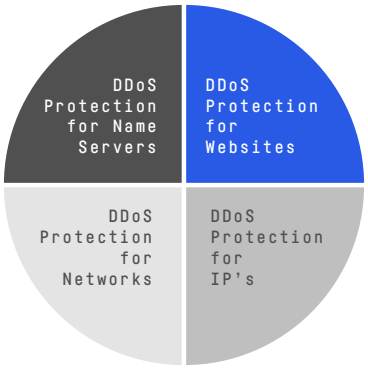
3-second mitigation SLA

DDoS attacks can strike anywhere, anytime. While it can take only minutes for a website or network to go down, it can take hours to recover. Imperva is the only company to provide a guarantee – backed by an SLA – to detect and block any attack, of any size or duration, in three seconds or less.

SIEM integration

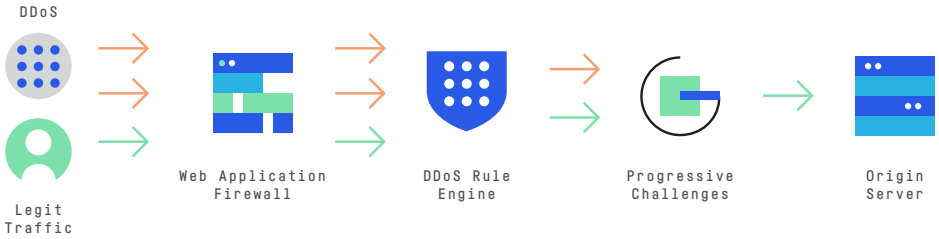
Imperva offers an optional connector for integrating leading security information and event management (SIEM) solutions including HP ArcSight, Splunk, McAfee Enterprise Security Manager, IBM QRadar, GrayLog, Sumo Logic, and AlienVault USM Anywhere.

DDoS protection for websites



Imperva protection for websites is an always-on service that simultaneously protects websites from the largest network layer attacks and the most devious application layer attacks. Your web traffic is directed through the Imperva global network that includes an integrated CDN to improve response time for visitors to your site. DDoS activation can be completed in minutes by changing your website DNS settings, even when you're under attack. No on-site hardware or software is needed and no changes to your hosting provider or applications are required. Acting as a secure proxy, Imperva DDoS protection for websites masks your origin server IP and constantly filters incoming traffic and stopping DDoS attacks while delivering legitimate users to your websites.

Unlike other solutions, our multi-layer approach to DDoS mitigation does not rely on CAPTCHA challenges and we don't reject legitimate users as attackers, even when you are under heavy attack. Imperva transparent mitigation ensures your web visitors, and your business, will never suffer during an attack.



Fastest attack mitigation

Imperva DDoS protection automatically blocks all assaults and does not require you to notify Imperva that you are under attack. We offer an industry-first three-second DDoS mitigation SLA for any attack, of any size or duration – but in fact we typically block assaults in less than one second

High-capacity network

The Imperva software-defined network serves as a distributed global scrubbing center that holds more than six Terabits per second (6 Tbps) of on-demand scrubbing capacity and can process 65 billion attack packets per second. The Imperva network has successfully defended clients against some of the largest attacks on record.

Continuous traffic visibility

You get a single-pane-of-glass view of your protected infrastructure, with real-time information about incoming traffic, and the ability to update security policies on the fly.

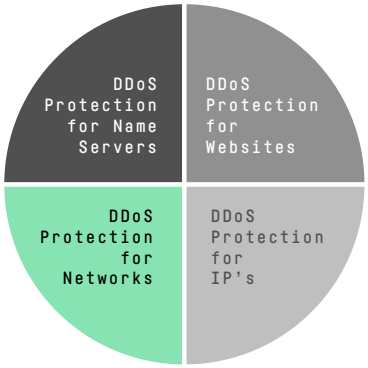
PROTECTION AGAINST ALL TYPES OF DDOS ATTACKS

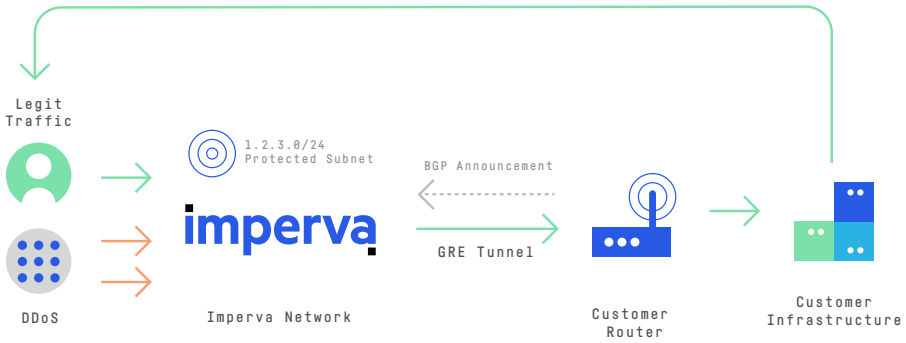
- TCP SYN+ACK
- TCP FIN
- TCP RESET
- TCP ACK
- TCP ACK + PSH
- TCP Fragment
- UDP
- ICMP
- IGMP
- Sloloris
- Spoofing
- DNS flood
- Smurf
- Ping of Death
- Mixed SYN + UDP or ICMP + UDP flood
- Attacks targeting Apache, Windows or OpenBSD vulnerabilities
- Zero-day DDoS attacks
- Brute Force
- Connection Flood
- Teardrop
- Reflected ICMP and UDP
- HTTP Flood
- Zero-day attacks
- Attacks targeting DNS servers
- And more

DDoS protection for networks

Imperva DDoS mitigation shields entire networks by leveraging the Imperva network's multi-terabit scrubbing capacity and high-capacity packet processing capabilities to instantly mitigate the largest, most sophisticated DDoS attacks. Imperva supports multiple deployment models, including Cross Connect, GRE tunnels and Equinix Cloud Exchange. DDoS protection for networks is available as an always-on or on-demand service, with flow-based monitoring and support for automatic or manual switchover.

Imperva DDoS protection for networks is designed for organizations that need to protect an entire C Class range of IP addresses against DDoS attacks. It is the ideal solution to mitigate very large volumetric and advanced DDoS assaults that target any type of Internet protocol or network infrastructure – including HTTP/S, SMTP, FTP, VoIP and others. You subscribe to Infrastructure Protection service as either always-on or on-demand.





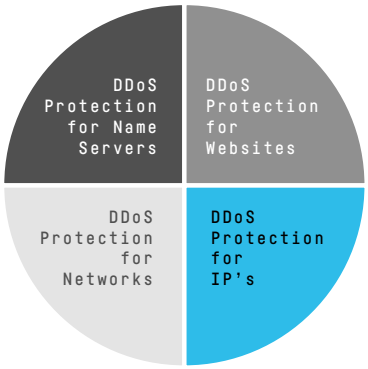
On-demand

Based on BGP (Border Gateway Protocol) routing, the Imperva on-demand service is ideal for organizations that are particularly sensitive to any latency and want to call for DDoS protection only when needed. In the event of an attack, traffic is rerouted through Imperva data centers using Imperva-initiated BGP announcements. All incoming network traffic is then directed to Imperva's global network of full-stack data centers where it is inspected and filtered. Only legitimate traffic is forwarded to your network via single or redundant GRE tunneling. We offer expertise in the areas of BGP setup and ongoing configuration management and can offer full BGP switchover management via the Imperva services organization, so you can offload the responsibility for attack monitoring and switchover.

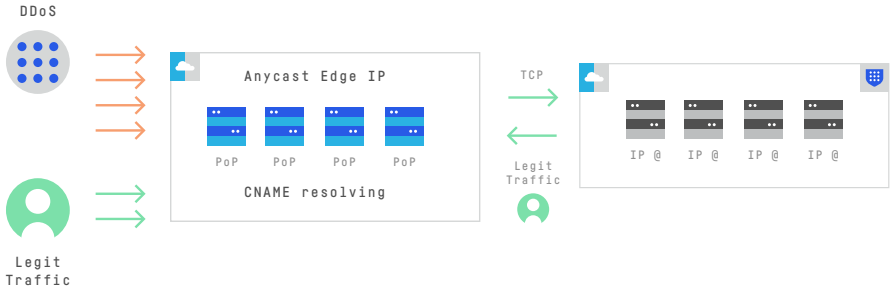
Always-on

For organizations that need to react to DDoS attacks instantly and continuously, always-on affords protection without the need to monitor for attacks or implement BGP routing. With always-on protection, Imperva advertises your C Class subnet and routes all traffic to our global network of DDoS mitigation data centers. Similar to on-demand, we route legitimate traffic to you via GRE tunneling. Unlike other always-on services, Imperva offers a 99.999% network uptime SLA and an industry-first 3-second mitigation SLA - critical requirements if you are considering an always-on solution.

DDoS protection for individual IPs



Imperva DDoS protection for Individual IPs is ideal for organizations that run websites and services in the cloud, and need the same level of guaranteed, 3-second DDoS SLA protection provided by Imperva for networks and websites. If you run your applications on a single host, and do not control the entire network, Imperva can meet your specialized protection requirements. Imperva provides a single, simple, integrated DDoS solution for environments that include cloud-hosted websites and services to protect against ever-increasing attack volumes with proven mitigation techniques.



Hybrid environments

Imperva DDoS protection for IPs is critical if you are migrating critical workloads to the cloud but still need to run applications on premises. Not just for websites, this solution protects any service exposed to the Internet. Best of all, it is easy to implement and manage.

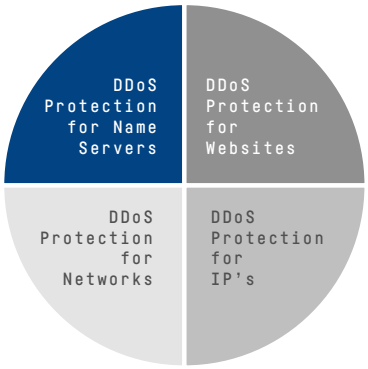
Flexible deployment options

Organizations that cannot afford to experience the impact of a DDoS attack, including downtime, disruption and cost, can implement DDoS Protection for Individual IPs. Deployed in always-on mode, it provides cost-effective, continuous protection of any website or service on a public cloud. DDoS Protection for Individual IPs works hand-in-hand with other Imperva application security solutions that protect networks, websites, DNS and applications, while optimizing the user experience.

Global network of full-stack PoPs

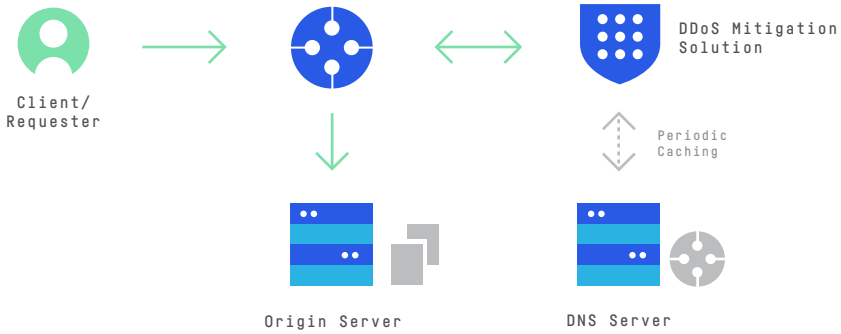
The Imperva global network holds more than six Terabits per second (Tbps) of on-demand scrubbing capacity and can process 65 billion attack packets per second. The Imperva network has successfully defended clients against some of the largest attacks on record, and this protection is extended to individual IPs to protect workloads in the cloud.

DDoS protection for DNS servers



Imperva Domain Name Server (DNS) DDoS protection, deployed as an always-on service, is a proxy-based solution that safeguards DNS servers from DDoS attacks. Imperva handles all incoming DNS requests, using a combination of reputation and rate-based heuristics to inspect incoming queries; it filters out malicious packets without impacting legitimate visitors. Only safe queries are forwarded to your DNS servers. Imperva DDoS protection for DNS also blocks attempts to use your DNS servers as a platform to launch DNS amplification attacks against other servers.

Implementation of the service takes just minutes, and activation follows the TTL settings of your name server. Once enabled, the Imperva proxy becomes your authoritative DNS server, while you continue to manage your DNS zone files outside of the Imperva proxy network.



Improved DNS performance and control

Improved control: From the dashboard, you can whitelist specific queries. For additional peace of mind, you can also set a threshold to rate-limit the queries your server receives. Improved performance: Legitimate queries are cached for a set period of time, during which all subsequent queries are resolved directly from the nearest location on the Imperva network. This accelerates performance and reduces the load on your own DNS server.

Eliminate malicious traffic and its side-effects

If you use a DNS provider, Imperva can help you avoid unexpected bills by eliminating malicious traffic that targets your DNS server. If you use a DNS service provider, Imperva DDoS protection for DNS reduces the likelihood you'll be blacklisted from your provider due to DDoS attacks originating from your site.

Why Imperva DDoS Protection should be your solution

Imperva anti-DDoS brainpower

The Imperva global network was designed to handle the largest volume-based attacks, such as SYN flood and DNS amplification. To complement our network, the Imperva software stack was designed by Imperva security experts to mitigate the most sophisticated HTTP application layer (layer 7) attacks while keeping the impact on legitimate users to an absolute minimum. Unlike other solutions, Imperva does not rely on other security vendors' software nor are we reliant on open source. Complete control over our software affords us the ability to adapt quickly to the changing DDoS threat—often in hours rather than days, weeks or even months with other providers.

A foundation of security expertise and response

Underlying our network and software are the Imperva Security Operations Center engineers and Security Threat research team. These groups work unremittingly, leveraging crowdsourcing techniques to uncover the most devious emerging threats and attacks as they are happening. Because we control all of our technology, we can quickly apply rules to stop threats—often in a matter of minutes around the globe.

Proven track record of DDoS mitigation

DDoS attack sizes in terms of Mbps and Mpps are growing unabated. We can predict that 500Mbps attacks will become common, but we can't predict when and where they will occur. So we built a software-defined network that condenses our global network of DDoS Super PoPs into a single massive 6+ Tbps DDoS mitigation engine that we can direct to an attack anywhere in the world, on-demand. Most other services are only as large as the DDoS-enabled POP nearest you. Imperva has successfully mitigated the largest DDoS attacks in history – with a guaranteed SLA of 3-second mitigation.

Defense in depth

Imperva offers a complete suite of defense-in-depth security solutions providing multiple lines of defense to secure your data and network. Our web-facing solutions, including WAF, bot protection, DDoS attack mitigation, account takeover prevention, API security and more, ensure that your network is protected against all application-layer attacks as well as smokescreen DDoS assaults. All solutions are based on a global content delivery network for optimal application availability, and global threat intelligence curated by our threat team. Intelligent attack analytics provides in-depth information and actionable intelligence on known and unknown attacks. Defense-in-depth means you benefit from the right protection, at the right time, regardless of where your applications and data reside.

Imperva is an analyst-recognized, cybersecurity leader championing the fight to secure data and applications wherever they reside.

+1 (866) 926-4678
imperva.com

imperva