imperva

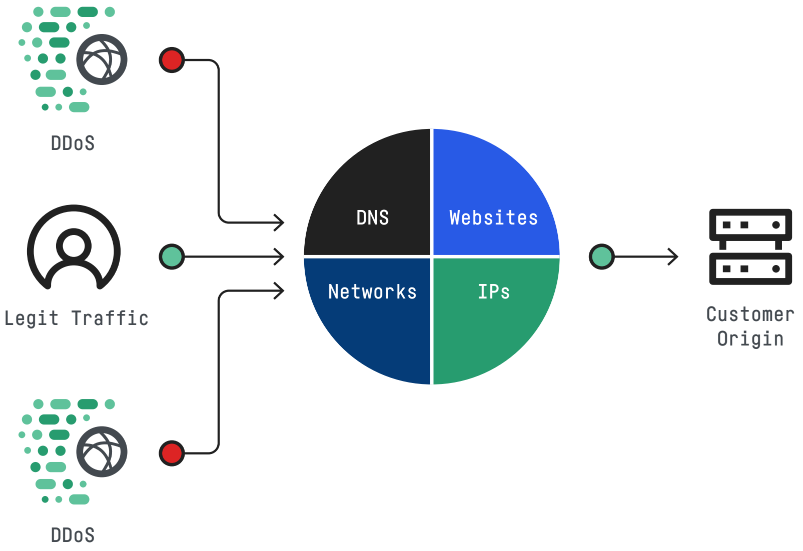
CAPABILITY BRIEF

DDoS Protection

Formidable attack mitigation

Maybe you've been hit by a DDoS attack and know you need better protection in the future. Or perhaps your current DDoS solution isn't equipped to handle the changing threat environment, and your business has suffered as a result. Even if you're one of the few who hasn't been attacked yet, chances are you will be at some point. Imperva has the solution to reduce your risk: Comprehensive DDoS protection for websites, networks, DNS servers and individual IPs.

Imperva has mitigated the largest attacks in history, immediately and without incurring latency or interfering with legitimate users. While DDoS cybercrime is an ever-changing landscape, our cloud service protects you better than any on-premises or hybrid protection can, no matter what attack comes your way or 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.

KEY CAPABILITIES:

Global network (> 6 Tbps) of 44+ scrubbing centers scales to absorb large volumetric attacks

Industry-best 3-second mitigation SLA

Always-on, automated attack protection

Advanced algorithms accurately identify and mitigate application layer attacks without challenging legitimate users

Protects websites and applications, network devices, domain name servers and individual IPs

Supports Anycast DNS and Unicast DNS routing

Integrated analytics correlates DDoS and related events to focus on what really matters

24/7 operations center

Backed by security experts at Imperva Research Labs

Single-stack speed, capacity, and accuracy

Our high-capacity global network holds more than six Terabits per second (6 Tbps) of scrubbing capacity and can process more than 65 billion attack packets per second. This global network of 44+ points of presence (PoPs), each outfitted with a DDoS scrubbing center powered by proprietary Behemoth custom technology, cloud-based WAF, advanced bot mitigation services and more, acts as a software-defined mesh network for optimal performance. It scales as needed to absorb the largest attacks that can overwhelm legacy appliances. It also doesn't rely on a hybrid approach where failover to the cloud can mean the more persistent, small-scale attacks of today do damage before mitigation even starts. We incorporate crowdsourced learnings from emerging attack methods across our network, utilizing machine learning for the most up-to-date, accurate, and advanced protection.

> **"When a large attack happened over a holiday, watching Imperva automatically handle it was a giant sigh of relief for myself and our entire executive team."**
>
> Aaron Blakely
> Digicert

Visibility with analytics and insights

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. Integrated Attack Analytics correlates DDoS attacks with other attack vectors occurring in parallel, lifting the DDoS smokescreen which may normally pivot your attention away from more sophisticated and precise offenses like account takeover or phishing. Via the dashboard, you can quickly adjust security policies on the fly based on recommended actions in order to stop attacks in their tracks.

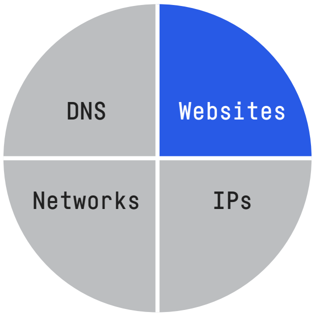
SLA-backed protection that scales

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. With automated, always-on attack mitigation at the edge, Imperva is the only company to provide a 3-second SLA guarantee to detect and block any attack, of any size or duration, with less than one-second mitigation typical. Automation based on out-of-the-box rules allows you to rely on Imperva expertise for peace of mind, with the option at any point to augment your security posture with self-service custom security policies. Our Terraform integration helps you scale quickly with automated DevOps provisioning, rolling out thousands of rules across your assets as quickly as possible.

Centralized management

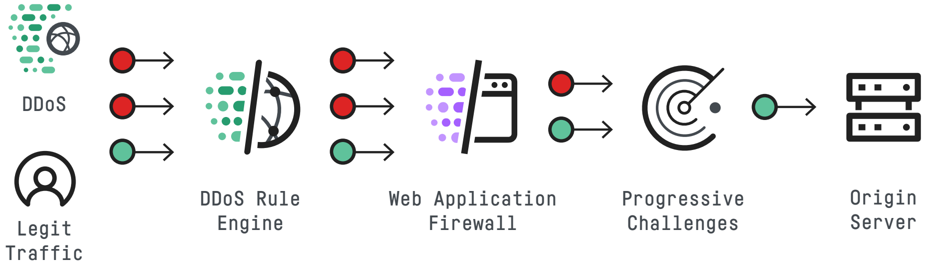
Imperva DDoS protection is part of a consolidated dashboard of cloud application security services for the ultimate in ease of use. An optional connector integrates with your SIEM (security information and event management) solution, whether it be HP ArcSight, Splunk, McAfee Enterprise Security Manager, IBM QRadar, GrayLog, Sumo Logic, or AlienVault USM Anywhere.

DDoS protection for websites

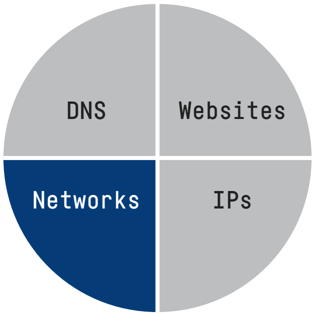


Imperva protection for websites is an always-on service that does not require you to notify Imperva that you are under attack. It simultaneously protects websites from the largest network layer attacks and the most devious application layer attacks. Your web traffic is directed through the Imperva global network that includes an integrated CDN to improve response time for visitors to your site. Activate protection 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.



DDoS protection for networks

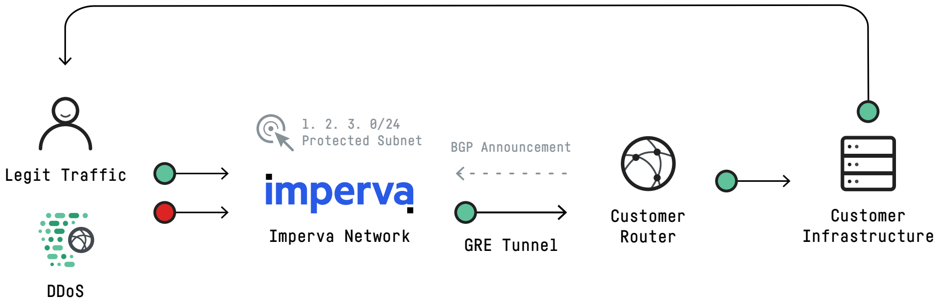


Imperva DDoS protection for networks shields your infrastructure by leveraging the Imperva network's multi-terabit scrubbing capacity and high-capacity packet processing capabilities to instantly mitigate the largest, most sophisticated DDoS attacks. Imperva supports multiple deployment models, including 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.

> **"We were pleasantly surprised by how easy it was to set up and deploy the system. It took us one week from our decision until the full system was up and running. We performed the onboarding by ourselves and didn't need any assistance from the support team."**

Riccardo Rosapepe
Co-Founder, Indiegala

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.



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 DDoS protection only when needed. Even in the case of on-demand deployments, there is no need for a trigger call from your team to Imperva. 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 our industry-first 3-second mitigation SLA - critical requirements if you are considering an always-on solution.

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

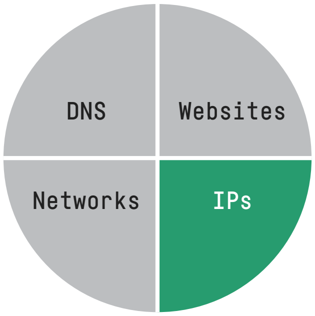
HTTP Flood

Zero-day attacks

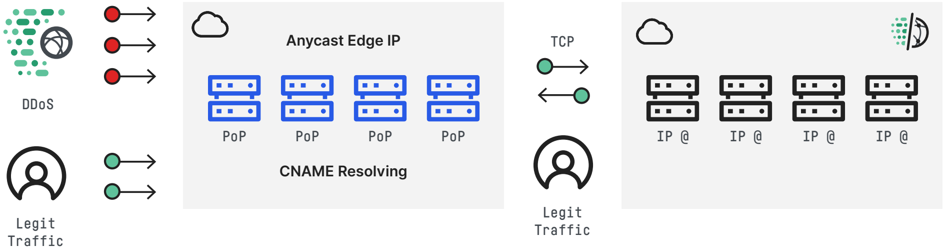
Attacks targeting DNS servers

And more...

DDoS protection for individual IPs



Imperva DDoS protection for Individual IPs is ideal for organizations that run websites and services in the cloud. 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 volumetric DDoS solution for environments that include cloud-hosted websites and services.



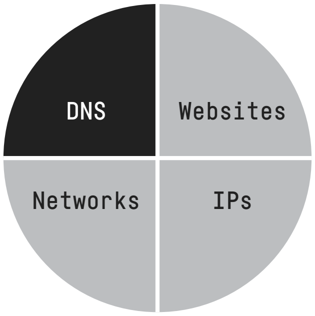
Hybrid environments

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

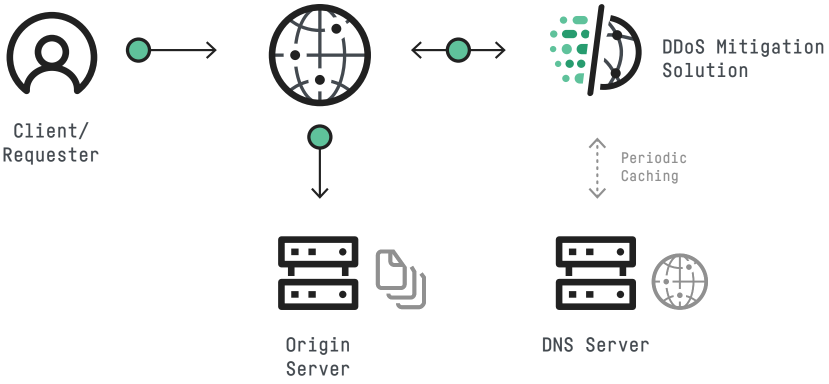
Organizations that cannot afford to experience the impact of a DDoS attack, including downtime, disruption and cost, can implement DDoS Protection for Individual IPs. Deployed in always-on mode, it provides cost-effective, continuous protection of any website or service on a public cloud. DDoS Protection 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.

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 network layer 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.



> **“Imperva proved to have a near zero false positive rate, and legitimate users had no trouble accessing Enjin websites during prolonged attacks.”**
>
> Maxim Blagov
> CEO, Enjin

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

Imperva anti-DDoS brainpower

The Imperva global network was designed to handle the largest volumetric attacks on a network infrastructure - Layer 3 / 4 attacks like SYN flood and DNS amplification. To complement our network, the Imperva software stack was designed by Imperva security experts to accurately identify and 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 opensource. Complete control over our software, with proprietary Behemoth scrubbing technology 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 experts at Imperva Research Labs. 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 cloud-based DDoS mitigation

DDoS attack sizes in terms of Mbps and Mpps are growing unabated. We've already seen 500Mbps attacks become common, but we can't predict when and where attacks of an even larger size and complexity 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, and some rely on legacy, on-premises architectures which attackers can easily overwhelm. Imperva has successfully mitigated, in less than 3 seconds, the largest DDoS attacks in history, like a Layer 7 attack over 290,000 RPS (requests per second) and Layer 3 attack over 650 million PPS (packets per second).

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, Advanced Bot Protection - including account takeover prevention, DDoS Protection, 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 Imperva Research Labs. 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.