IMPERVA®

Imperva Incapsula DDoS Protection

DATASHEET

Automated Mitigation of the Largest and Smartest DDoS Attacks

Imperva Incapsula secures websites against the largest and smartest types of DDoS attacks—including network, protocol and application level (Layers 3, 4 & 7) attacks—with minimal business disruption. Our cloud-based service keeps online businesses up and running at high performance levels even under attack, avoiding financial losses and serious reputation damage.

Incapsula service is built to handle the largest volume-based attacks, such as SYN flood and DNS amplifications, and also mitigates sophisticated application layer attacks by implementing advanced and progressive challenge mechanisms. The service automatically and transparently mitigates DDoS attacks with minimum false positives, so that site visitors won't know that the site is under attack.

Incapsula DDoS Protection service includes real-time dashboards to monitor & analyze attacks as they happen and features a dedicated 24/7 NOC, manned by our experienced security experts, in order to ensure enterprise-grade uptime SLA when under attack.

What You Get

- Powerful backbone across globally distributed data centers
- Specialized support of massive SYN flood, DNS targeted, and DNS amplificiation attacks
- Advanced algorithms which mitigate sophisticated application layer attacks
- Real-Time dashboards to monitor and analyze attacks as they happen
- Dedicated 24/7 NOC for enterprise-grade uptime
- Support for anycast, unicast and hybrid routing techniques for effective DDoS mitigation.
- Infrastructure Protection enables protection for entire subnets from network layer attacks

Why Imperva Incapsula?

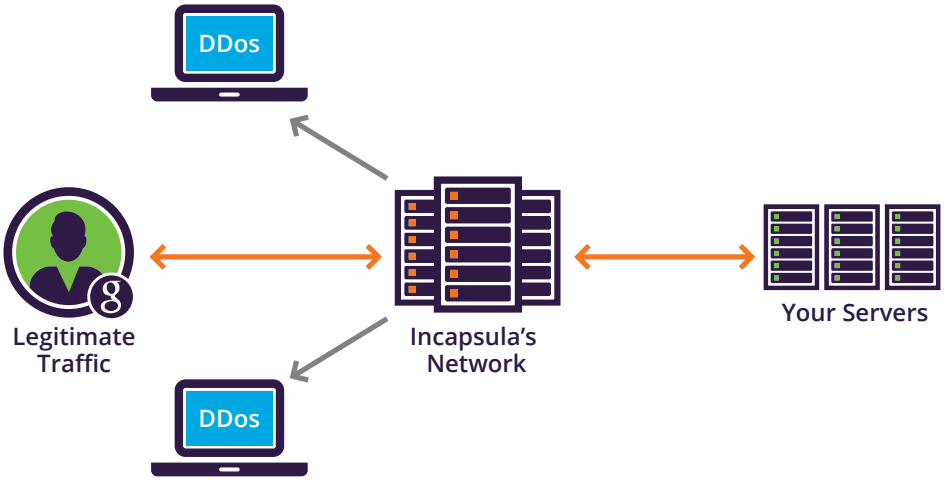
- Automatic always-on detection & triggering of "under attack" mode
- Zero business disruption based on transparent mitigation with minimum false positives
- End-to-end protection against the largest and smartest DDoS attacks
- Activated by simple DNS change—no hardware or software installation, integration or changes to the website

Incapsula protects your website from all types of DDoS attacks:

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

Comprehensive Protection Against Any Type of DDoS Attack

Incapsula protects your website against all types of DDoS threats, including network-based attacks, like Sloworis, ICMP or TCP & UDP floods, and application-level attacks such as GET flood, that attempt to overwhelm server resources. The service detects and mitigates advanced attacks that exploit applications, web server, and DNS server vulnerabilities, hit-and-run attacks and large botnet threats.



Scalable High-Capacity Network to Handle Volume-Based Attacks

As the size of volume-based DDoS attacks such as SYN flood and DNS amplification routinely exceeds 100 Gbps, organizations require robust network capacity to mitigate ever-growing assaults. With our global network capacity exceeding 1 Tbps (terabits per second), Incapsula is well-equipped to defend against even the largest volumetric barrages. Our always-on cloud service ensures that mitigation is applied outside your own network, allowing only filtered traffic to reach your host servers.

Intelligent Multi-Layer Protection

Incapsula ISP grade edge routers are set to filter out and isolate immediately identifiable malicious packets, such as DNS amplification and Martian packets. The rest of the traffic is prioritized by Class of Service and distributed across the Incapsula scrubbing centers, each with multiple 10-Gig uplinks. Each Incapsula scrubbing center holds several interconnected, high-powered scrubbing clusters. These clusters are used for real-time DDoS traffic profiling and blocking. When under attack, they seamlessly process incoming packets and HTTP sessions and use the Incapsula unique intelligent traffic profiling solutions and bot detection technology to accurately weed out malicious traffic, without affecting legitimate visitors.

Incapsula was able to withstand the massive distributed denial-of-service (DDoS) attack and keep the targeted website up and running...

1/10/13 "LATEST 100 GIGABIT ATTACK IS ONE OF INTERNET'S LARGEST"

eWEEK

Advanced Mitigation of Layer 7 Attacks

Incapsula visitor identification technology differentiates legitimate website visitors (humans, search engines, etc.) from automated or malicious clients. This capability is critical with respect to application layer (Layer 7) attacks, where the DDoS requests look like legitimate visitors. Unlike other DDoS protection services that are based on easy-to-evade and false-positive prone techniques (e.g., rate limiting or splash/delay screens), Incapsula distinguishes between humans and bot traffic, between "good" and "bad" bots, and identifies AJAX and APIs. Legitimate bots, such as Google and Bing, continue to access your website, even when it is under attack.

DNS DDoS Protection

Incapsula DNS DDoS feature protects DNS servers from targeted attacks, which is critical for site availability. Just change your NS records to point to Incapsula, and all DNS queries for the protected domains will be inspected and filtered for malicious traffic in the Incapsula cloud, ensuring that only "safe queries" reach your origin DNS server. This protects your server from direct DDoS attacks, as well as blocking attempts to use it as a platform for DNS amplification attacks against other servers. In the event of an attack, customers receive email alerts and GUI notifications.

Transparent Mitigation

Incapsula protects your site not only from complete denial of service, but also from disruptions related to DDoS attacks, mitigation false-positives, etc. We offer transparent mitigation with less than 0.01% false positives, and without degrading the normal user experience in any way. This lets you enjoy true DDoS protection, even from lengthy attacks, without disrupting business performance. Moreover, 99.99% of your legitimate site visitors will not be impacted in any way by the attack, and will continue browsing normally without annoying splash screens or delays.

Automatic Detection and Triggering

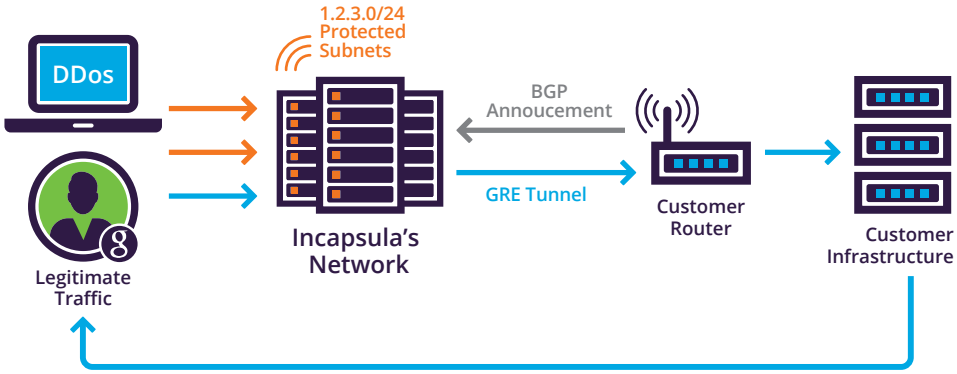
Incapsula offers automatic always-on DDoS mitigation, which is well-equipped to handle "hit and run" attacks consisting of short bursts of traffic in random intervals over a long period of time. This type of attack can wreak havoc with DDoS mitigation solutions that need to be manually turned on and off on every burst. Automatic detection and activation enables Incapsula to take full responsibility for both detection and mitigation of the attack.

Fast, Easy Onboarding—DNS-Based Routing

DDoS Protection can be rolled out without the need for hardware, software, integration or web application code changes. Customers can provision this service simply by changing their website's DNS setting. This effortless deployment allows customers to be protected in a matter of minutes while maintaining their existing hosting provider and application infrastructure.

Infrastructure Protection for Subnets

For enterprises that need to protect multiple service types and protocols across an entire subnet range of destination IP addresses, Incapsula offers on-demand DDoS protection based on BGP routing. In the event of an attack, traffic is re-routed through the Incapsula scrubbing centers using BGP announcements. From this point on, Incapsula acts as the "ISP" and advertises all protected IP range announcements. All incoming network traffic is inspected and filtered, and only legitimate traffic is securely forwarded to the enterprise network via GRE tunneling.

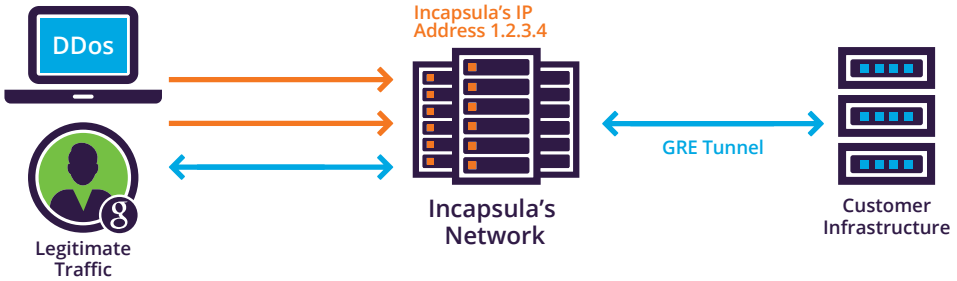


Traffic flowing via Incapsula during a DDoS attack. BGP announcement is used to route protected subnets through Incapsula for mitigation.

Infrastructure Protection for Individual IP Addresses

Using this unique deployment model, Incapsula brings the benefits of infrastructure protection to customers not owning an entire Class C subnet. This feature enables smaller organizations to protect multiple service types and protocols—even for a single IP address—without using BGP routing. You receive a protected IP address from Incapsula, after which we inspect and filter all incoming traffic. A redundant, secure, two-way GRE tunnel is then used to forward clean traffic to your origin IP and return outbound traffic from your application to your users.

Single IP address protection is ideal for gaming servers and SaaS applications. These have high-traffic, critical non-HTTP assets with low IP counts, as well as cloud deployments in dire need of direct-to-IP attack prevention.



Traffic flowing via Incapsula during a DDoS attack. Customer traffic is routed to an Incapsula IP address, allowing it to pass through the Incpauls network for cleansing before being forwarded over a secure GRE tunnel to the customer.

IMPERVA INCAPSULA

Collaborative Security

Incapsula protects websites using collective knowledge about DDoS threats, including new and emerging attack methods. Using crowdsourcing techniques, this information is aggregated across the entire service network, comprising thousands of websites, to identify new attacks as they happen and to detect known malicious users. Based on this information, mitigation rules can be applied in real-time across all protected websites.

Cost-Effective Cloud-Based DDoS Protection

Incapsula offers a cloud-based service that gives you 24x7 protection against DDoS attacks without the need for multi-gigabit Internet connections and additional hardware and operational costs. This eliminates the costs associated with over-provisioning bandwidth and deploying additional servers and load balancing appliances on premise. For enterprise plan customers, Incapsula assigns a personal account manager to act as a single point of contact for all DDoS security needs.

World-Class Support by DDoS and Security Experts

The DDoS Protection service provides organizations with continuous monitoring and mitigation by our battle-proven team of experienced Security Operations Center (SOC) engineers. Our service includes proactive security event management and response, continuous real-time monitoring, adept policy tuning, summary attack reports, and 24x7 technical support.

Learn more: imperva.com/incapsula