Formidable Attack Mitigation

Maybe you’ve been DDoSed and need to better understand how to protect your organization. Or like others, you may be looking for a replacement DDoS solution that is better equipped to handle the changed threat environment. Like others who’ve been attacked, you’ve suffered something between a minor nuisance and some significant harm. And if you’re one of the few that haven’t been attacked yet, chances are you will be. Imperva has analyzed and solved the DDoS, or Distributed Denial of Service threat for several years now and we are certain the menace isn’t going away soon. We can’t predict exactly how DDoS attacks will evolve, but our cloud service is prepared to protect you whatever attack comes your way and no matter what the future holds.

Imperva Incapsula
DDoS Protection

Incapsula at a glance
- Over 2 Tbps global cloud network 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 and application servers
- 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
Incapsula DDoS Protection is built on three essentials:

- A global network that absorbs the largest attacks while minimizing latency.
- Exclusive software that solves difficult application layer attacks without confusing your real users for attackers.
- Deployment options that give you the flexibility to apply protection where and when it’s needed.

### Deflect Network Layer Attacks

DDoS attackers target your network and servers with the intention of slowing or denying legitimate users access. Network layer 3 and 4 volumetric attacks that try to saturate or bring your network down come in two varieties: High bitrate attacks measured in Mbps (megabits per second) that try to consume all available network bandwidth, and high packet rate attacks measured in Mpps (thousands of packets per second) that attempt to overwhelm networking gear.

Both types of attacks are almost always performed by botnets. The way to eliminate these volumetric botnet attacks is to fight power with power. Incapsula solves the volumetric challenge with our unique software-defined mesh network that can absorb the Internet’s largest DDoS attacks. By combining the power of worldwide DDoS mitigation centers, Incapsula stops attacks that would quickly overload in-house appliances.

### Foil Application Layer Attacks

Attackers try to overload your servers by sending large numbers of resource-intensive server requests with the goals of slowing, hanging or crashing a Web application. Layer 7 application attacks are targeted at HTTP servers in particular and consist of seemingly legitimate requests. Application layer DDoS attacks are measured in requests per second (RPS) with each request attempting to extract as much processing power from the server as possible.

Like network layer DDoS attacks, application attacks also typically rely on botnets. But because they utilize HTTP requests, application layer attacks can be difficult to detect and prevent without denying legitimate users and bots access during an attack. While volumetric attacks can be solved with a brawny network, it takes brains to solve application layer attacks. Incapsula employs an effective five-ring approach to solve application layer attacks while letting legitimate users right through. Unlike other solutions, Incapsula does not need to resort to splash screens or CAPTCHA challenges to separate bots from humans.

### Customize DDoS Protection for Your Ecosystem

Incapsula DDoS Protection subscriptions are available to meet the distinctive protection requirements of all your online assets. Offered by server type, by attack level protection (Mbps and Mpps), by network requirements (C Class and GRE tunnels), and by availability (on-demand or always-on), Incapsula DDoS protection fits into any environment. Essential protection for any website, Incapsula Website Protection is included with Incapsula Business plans. Incapsula Website Protection, Infrastructure Protection and Name Server protection are offered as add-on subscriptions to Incapsula Enterprise plans.
Why Incapsula?

- Automatic always-on detection & triggering of “under attack” mode; on-demand option available.
- 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 DDoS Protection Plans for Business

<table>
<thead>
<tr>
<th>DDoS PROTECTION SERVICE LEVEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website Protection</td>
</tr>
<tr>
<td>Always-on</td>
</tr>
</tbody>
</table>

Incapsula DDoS Protection Plans for Enterprise

<table>
<thead>
<tr>
<th>DDoS PROTECTION SERVICE LEVEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website Protection</td>
</tr>
<tr>
<td>Always-on</td>
</tr>
<tr>
<td>Infrastructure Protection</td>
</tr>
<tr>
<td>For single IP address</td>
</tr>
<tr>
<td>Always-on</td>
</tr>
<tr>
<td>For Class C network</td>
</tr>
<tr>
<td>Always-on or on-demand*</td>
</tr>
<tr>
<td>Name Server Protection</td>
</tr>
<tr>
<td>Always-on</td>
</tr>
</tbody>
</table>

Always-on DDoS mitigation - designed to mitigate attacks immediately to reduce the possibility of network saturation. Available for Website DDoS Protection, IP Protection, Infrastructure Protection and Name Server Protection.

On-demand DDoS mitigation - relies on the client to monitor traffic and report the detection of malicious traffic. Available for Infrastructure Protection for Class C networks; requires BGP routing.

*Proactive on-demand DDoS mitigation - relies on the Incapsula Network Operations Center to monitor traffic. In the event of a DDoS traffic spike, Incapsula initiates rerouting traffic through the Incapsula network. Requires Incapsula External Monitoring service.
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…

Incapsula Website Protection

- Always-on
- Protects HTTP/HTTPS from network and application layer attacks
- Activate by CNAME – domain or IP address
- Integrated CDN for web acceleration

Incapsula Website Protection 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 Incapsula global network that includes an integrated CDN to improve response time for visitors to your site. Website Protection 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.

Incapsula stops all DDoS attacks at our network and only delivers legitimate users to your website. 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. Incapsula transparent mitigation ensures your web visitors, and your business, will never suffer during an attack.

Incapsula Website Protection is included with all Incapsula Business and Enterprise plans. For Incapsula Enterprise, DDoS protection is available to match your website traffic, number of sites and desired DDoS attack protection level. Unlimited DDoS protection is the ultimate—ensuring your website can deflect whatever is thrown at it. Unlimited DDoS is the essential upgrade when downtime or latency due to DDoS attacks simply cannot be tolerated.
“We were pleasantly surprised by how easy it was to setup and deploy the system. It took us one week from our decision to use Incapsula until the full system was up and running. We performed the onboarding by ourselves and didn’t need any assistance from the Incapsula support team.”

RICCARDO ROSAPEPE, CO-FOUNDER, INDIEGALA

<table>
<thead>
<tr>
<th>WEBSITE PROTECTION DDOS OPTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incapsula Business plan</td>
</tr>
<tr>
<td>Incapsula Enterprise plan</td>
</tr>
</tbody>
</table>

**Incapsula Infrastructure Protection**

Incapsula Infrastructure Protection is available as an always-on or an on-demand service that protects any asset against any size DDoS attack. With Infrastructure Protection, all of your network traffic is directed through the Incapsula global network.

Incapsula offers two infrastructure protection solutions:

- Incapsula IP Protection – for single IP addresses
- Incapsula Infrastructure Protection – for C Class subnets

**Incapsula IP Protection**

- Always-on network layer protection
- Protects any service and any protocol
- Eliminates direct-to-origin attacks
- Does not require a C Class, BGP or specialized routers

Traffic flowing via Incapsula during a DDoS attack. Customer traffic is routed to an Incapsula IP address, allowing it to pass through the Incapsula network for cleansing before being forwarded over a secure GRE tunnel to the customer.
Incapsula IP Protection provides network layer (layer 3 and 4) protection for individual IP addresses regardless of service type and protocol. Designed for smaller organizations who may not own an entire C Class network, IP protection delivers strong DDoS protection for the following applications:

- **Proprietary protocols** - Protecting non-HTTP assets like gaming servers has often required protecting the entire C Class range. Like others, you may have a subset of servers you need to protect and you either don’t own or can’t protect an entire C Class.

- **Public cloud servers** - Because these servers are outside of your infrastructure, you need a solution that can target specific servers across one or more cloud providers. IP Protection will protect non-HTTP servers or DNS servers in any cloud provider.

- **Network infrastructure** - An attack on one server within your network can bring down your entire infrastructure. Providing always-on IP Protection for your most vulnerable servers and routers can ensure your network remains unaffected by DDoS attackers. This can be particularly useful if you are a service provider. With IP Protection, you can protect the problem servers to keep them from affecting the performance of your entire network.

- **Direct-to-origin attacks** - Even with the best DDoS protection, there’s still a possibility that a determined attacker can uncover a server’s IP address and launch an attack. Incapsula IP Protection affords an extra level of security by completely hiding the origin IP, making it virtually impossible to launch a direct-to-origin attack on any server.

With IP Protection, Incapsula gives you a protected IP address for each one of your origin servers. After updating clients with the new IP addresses, traffic to the protected servers will be routed through the Incapsula network and scrubbed of layer 3 and layer 4 DDoS attacks. Clean traffic is forwarded to your origin servers over a GRE tunnel (IP over IP) that is established during the onboarding process. IP Protection can be deployed in full symmetric (both ingress and egress traffic) or asymmetric mode, depending on your requirements and server configuration.

Incapsula IP Protection requires an Enterprise plan (always on) and is based on the number of servers protected. IP Protection also requires a DDoS plan. Unlimited DDoS protection is also available for IP Protection subscriptions.
Incapsula Infrastructure Protection

- On-demand or always-on options
- Protects an entire Class C network from attacks
- Supports BGP routing and GRE tunneling

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

Incapsula Infrastructure Protection is designed for organizations that need to protect an entire C Class range of IP addresses against DDoS attacks. Infrastructure Protection 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.

Infrastructure Protection – On-Demand

Based on BGP (Border Gateway Protocol) routing, on-demand service is for organizations that are particularly sensitive to any introduction of latency and therefore only want to call on the DDoS protection service as needed. In the event of an attack, you would re-route your traffic through Incapsula data centers using Incapsula-initiated BGP announcements. All incoming network traffic is then directed to Incapsula, inspected and filtered, with only legitimate traffic forwarded to your network via single or redundant GRE tunneling.

Incapsula offers expertise in the areas of BGP setup and ongoing configuration management. We can even offer full BGP switchover management through our services organization so that you can offload the responsibility for attack monitoring and switchover/switchback to us when you are not available to make the switch.

Infrastructure Protection – 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, Incapsula 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, Incapsula offers a 99.999% network uptime SLA—a critical requirement if you are considering an always-on solution.
DDoS Protection for infrastructure requires a C Class network. Subscriptions are offered based on network bandwidth requirements and require the selection of an appropriate DDoS protection level similar to Website Protection. Subscriptions also require the addition of a pair of GRE tunnels in addition to a one-time setup and configuration engineering fee.

**Incapsula Name Server Protection**

- Always-on DNS server protection
- Proxy-based solution
- Reduces bandwidth costs and improves response time

Deployed as an always-on service, Incapsula Name Server Protection is a proxy-based solution that safeguards DNS servers from DDoS attacks.

Incapsula handles all incoming DNS requests, filters out malicious requests and then forwards only safe queries to your DNS servers. Name Server Protection also blocks attempts to use your DNS servers as a platform to launch DNS amplification attacks against other servers.

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

If you use a DNS provider, Incapsula can help you avoid unexpected bills by eliminating malicious traffic that targets your DNS server. If you use a DNS service provider, Name Server Protection reduces the likelihood you’ll be blacklisted from your provider due to DDoS attacks originating from your site. Performance is also improved because Incapsula caches DNS requests across our global network and can return DNS query results closer to the origin thereby accelerating DNS response time.

Name Server Protection is offered as an add-on to Enterprise plans and is based on the number of DNS zones protected. Subscriptions include setup and require a subscription to the unlimited DDoS protection level.
“Upon the deployment of Imperva Incapsula, we saw an increase in security with no added slowdown in user experience. Within days of the implementation, use of the Incapsula Infrastructure DDoS Protection services helped mitigate multiple DDoS attacks at all three of our datacenters with zero downtime after an attack ended and traffic was switched back to the ISP.”

RAIMUND SCHLICHTIGER, HEAD OF SYSTEM ADMINISTRATION, INNOGAMES

Incapsula Global Network

Unlike other services where DDoS was added to an existing content delivery network or web application firewall appliance, Incapsula designed a DDoS protection network from the ground up as an integral component of our comprehensive security and web acceleration solution. The Incapsula network fights the power of distributed attackers with an even greater distributed global defense. As the DDoS threat grows, so does the power of the Incapsula network.

At the core of our network architecture is the multi-function PoP, distributed globally at strategic locations and served by major transit and hosting providers to ensure we remain close to your origin servers and end users. At the center of our DDoS mitigation capability is a purpose-built appliance that can manage up to 160 Gbps of traffic or 50 Mpps (millions of packets per second) – in fact, we call this The Behemoth.

Each PoP is equipped with multiple Behemoths as well as WAF, bot protection, caching and load balancing services. The Incapsula network of PoPs continues to grow and can be seen on the Incapsula network map.

We also deploy Incapsula Super PoPs that are located inside Internet connectivity hotspots to provide on-demand DDoS mitigation power with minimal latency if you ever get hit by the world’s biggest attack. Our network of Super PoPs provides reserve capacity that can manage the needs of clients that subscribe to unlimited DDoS protection levels. Reserve scrubbing capacity is amplified by the Incapsula Mesh Network, a software-defined network that describes a worldwide virtual pool of DDoS mitigation centers. Unlike other services that are only as large as your closest PoP, Incapsula offers you the aggregate capacity of our entire network.

Incapsula Anti-DDoS Brainpower

The Incapsula global network was designed to handle the largest volume-based attacks, such as SYN flood and DNS amplification. To complement our network, the Incapsula 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, Incapsula 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.

Client classification provides DDoS monitoring tools with an edge in identifying attacks by allowing them to pinpoint the bots creating these attacks.
While other providers focus most of their attention on network capacity, Incapsula solves the complicated application layer attack issue which is often more complex than an attack itself. At the heart of our exclusive ability to prevent sophisticated HTTP application attacks while minimizing false-positives is a unique multi-layer system of advanced and progressive challenges.

- **Client classification** - separates volumetric attacks that are launched to mask targeted application layer attacks.
- **Visitor reputation** - leverages crowdsourcing to separate legitimate users from attackers.
- **Web application firewall** - separates and stops application attacks disguised as DDoS attacks.
- **Progressive challenge** - is a sophisticated challenge mechanism that separates real users from bots with extremely low false-positives.
- **Behavioral anomaly detection** - is a set of rules or a safety net that detects and stops behavior that is non-human.

Other DDoS mitigation techniques rely heavily on lists that focus on negative client reputation. Incapsula is unique in that we also consider positive reputation. Looking at both positive and negative client reputation concurrently allows us to focus our efforts only on the exceptions, giving us a distinct advantage when it comes to minimizing processing time and false positives.

The Incapsula multi-layer approach yields effective results—attacks are mitigated while legitimate users get to your network. Unlike other solutions, legitimate users don’t face challenges or delay even when your site is under heavy attack.
A Foundation of Security Expertise and Response

Underlying our network and software are the Incapsula 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.

Cohesive Management

Incapsula DDoS Protection is part of an integrated set of solutions to protect and accelerate your infrastructure. A single console manages the entire set of Incapsula capabilities.

- Custom security rules
- Content delivery network
- Load balancing and failover
- Web application firewall

Security Information and Event Management Integration

Incapsula offers an optional connector for integrating leading security information and event management solutions. The Incapsula SIEM connector resides on the enterprise network and acts as a link between selected SIEM solutions and the Incapsula API. It supports syslog formats including CEF, W3C and LEEF. In addition, SIEM integration offers direct support for HP ArcSight, Splunk, McAfee Enterprise Security Manager and IBM QRadar.

Incapsula SIEM integration offers automated import of Incapsula-generated security events into support SIEM solutions to achieve a near real-time snapshot of all important events. Logs from Incapsula are securely transmitted to the SIEM platform. Incapsula SIEM integration also includes custom dashboards and reports for ArcSight, Splunk, McAfee and IBM to save you time and effort related to getting the information you need while simplifying your security, compliance and operations reporting.

Incapsula SIEM

Security Logs

Incapsula PoPs

Behemoth

Incapsula SIEM Connector Client

Incapsula SIEM Package
- HP ArcSight
- McAfee
- Splunk

Your Servers

Your Network

“Incapsula helped BTC China stay up during some of the biggest DDoS attacks on record. This happened at a critical business juncture, when our increasing trading volumes were turning us into the number one bitcoin trading site in the world.”

BOBBY LEE
CEO, BTC-CHINA
• Incapsula aggregates the security events from all its PoPs into a separate security event log file for each account/customer.
• Security logs may or may not be encrypted, in accordance with the account configuration. Encryption mode secures any log file generated at the Incapsula cloud repository. Logs are decrypted upon their arrival at the customer perimeter.
• The Incapsula SIEM Connector resides at the enterprise perimeter and provides an automated solution for importing security events from the Incapsula cloud to the SIEM.
• Predefined packages are tailored to integrate Incapsula events into HP ArcSight, Splunk, McAfee Enterprise Security Manager and IBM QRadar.

Additionally, Incapsula SIEM Integration offers the following advantages:
• Support for CEF, W3C and LEEF formats
• Near-real time event reporting
• In-depth event information, such as attacker geo-location and client application signature
• End-to-end log encryption
• Pre-defined dashboards, alerts and rules for Splunk, HP ArcSight and McAfee

### SIEM Supported Platforms

<table>
<thead>
<tr>
<th>HP ARCSIGHT</th>
<th>McAfee</th>
<th>SPLUNK</th>
<th>IBM QRADAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 5.0 and up Both ESM and Express</td>
<td>Version 9.4 and up</td>
<td>Version 6.2 and up</td>
<td>Version 7.2.6 and up</td>
</tr>
</tbody>
</table>

### Supported Operating Systems

<table>
<thead>
<tr>
<th>LINUX</th>
<th>WINDOWS</th>
</tr>
</thead>
</table>
| - CentOS 6 and up  
- RHE-L 6 and up  
- Ubuntu 12 and up  
- Debian 6 and up  
- OpenSuse13.2 and up  
- Suse 12 and up | - Windows XP and up  
- NET Framework 2 and up |
External Monitoring

Our 24/7 External Monitoring service complements our on-demand Infrastructure Protection, alerting you to DDoS attacks so you can quickly reroute traffic through Incapsula for mitigation. Through this service, Incapsula SOC experts:

- Monitor and analyze NetFlow and sFlow statistics emanating from your routers and other network elements.
- Detect anomalies that indicate a DDoS attack
- Immediately notify your team based on your existing incident response workflows

Backed by a SLA, External Monitoring helps you protect your online business assets around-the-clock, ensuring fast attack detection and mitigation triggering.

Support and Managed Services

Imperva standard support for Incapsula includes:

- 99.999% availability service level agreement
- 24/7 worldwide technical support
- 2/4 hour critical/high severity response time
- Incident notification
- Weekly activity report

Upgraded support programs are available that include priority support, attack response, custom rule creation, configuration change support, custom monitoring and more. Gold and Platinum support programs are available based on subscription level.

Why Incapsula DDoS Protection Should Be Your Solution

Our cloud-based DDoS mitigation solution is better matched for the DDoS threat profile than any on-premises solution.

- The unpredictability of a DDoS attack, its sheer force, and the need to fight power with more power demands a large community defense. The Incapsula cloud offers shared protection that is larger and faster than any organization could deploy on their own. Beyond network power, the huge Incapsula client community offers us the benefits of crowd sourced threat intelligence.

Our cloud is modern and is better at defending against DDoS attacks than legacy networks designed to deliver content.

- 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 2Tbps+ 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.
We’re security geeks that build and manage our own software, so we can deliver better results than alternatives that outsource their technology.

• Our founders and engineers have deep roots in the security industry and we use our collective knowledge to outwit the attackers. We’ve found over the years that the mitigation process is getting more complex. But unlike other solutions, we’ve figured out how to stop attacks without ever slowing or annoying your legitimate users with splash screens or CAPTCHA challenges.

• Our software, our network and our operations team were all built as a cohesive system that was designed to respond quickly. We deploy new rules in minutes to shut down your attackers while alternative can take hours or days.