SOLUTION BRIEF

IMPERVA®

# Eliminate DDoS Attacks in the Cloud and On-Premise

## DDoS Attacks Can Be Devastating

DDoS attacks have become the weapon of choice of cybercriminals, hacktivists, and nation-states because they are inexpensive to perform and difficult to stop. For $50, a malicious user can rent a botnet to launch an attack on the Website of their choosing. But the impact on the targeted organization is much more expensive, costing businesses $27 million on average for a 24-hour outage.[1]

## New DDoS Attacks Can Evade Traditional Defenses

To circumvent network defenses, an increasing number of DDoS attacks target Web applications and application databases. These DDoS attacks mimic regular Web traffic and they initiate requests too slowly to be detected by traditional firewalls. For example, hundreds of bots might perform online searches to cripple a website's back-end database, taking the site offline. Application DDoS attacks often fly under the radar of traditional network-based defenses, resulting in hours, days or weeks of downtime.

## DDoS Security Services Often Come Up Short

Service providers often provide security services to mitigate DDoS attacks. However, most of these services focus on blocking volumetric attacks – not advanced application DDoS attacks. In fact, many of these services cannot inspect SSL traffic, so they are blind to advanced attacks targeting HTTPS applications. Moreover, many of these services are fully managed, preventing enterprises from monitoring or fine-tuning their own security defenses.

## DDoS Appliances Expose Businesses to Upstream Attacks

While dedicated DDoS security appliances prevent application DDoS attacks, they cannot handle massive volumetric attacks – attacks that top 200 Gbps of throughput and surpass customers' internet bandwidth limits. To eliminate downtime, organizations must block volumetric attacks before they reach the network.

## End-to-End DDoS Protection from Imperva

Imperva offers hybrid cloud and on-premise DDoS security that can stop large-scale volumetric attacks in the cloud, but still provide enterprises on-site visibility and control.

The SecureSphere Web Application Firewall blocks application DDoS attacks on-premise. DDoS Protection Service for SecureSphere, a managed security service for SecureSphere customers, prevents volumetric attacks and app-layer DDoS attacks in the cloud. With a hybrid DDoS security solution from Imperva, organizations can avoid brand damage and lost revenue due to denial of service threats.

## Financial Services Giant Stops a Hacktivist Attack from the Middle East

### Customer

- A Fortune 500 bank serving consumers, small businesses, and commercial clients.
- With over $20 billion in revenues, the bank is one of the most widely-known brands in the U.S.

### DDoS Attack

- In the spring of 2013, the hacktivist group Izz ad-Din al-Qassam Cyber Fighters launched a DDoS attack targeting a number of U.S. banks.
- As part of the Operation Ababil campaign, Izz ad-Din unleashed powerful DDoS assaults lasting over 40 hours.
- Attackers used the "Ababil Assassin," a variant of the KamiNa attack tool, to send HTTP POST messages to banking sites' account login pages.
- Users from 54 countries participated in the DDoS attack.

### Solution

- SecureSphere Web Application Firewall
- ThreatRadar Reputation Services
- DDoS Protection Service for SecureSphere

### SecureSphere and DDoS Protection Service Highlights

- SecureSphere handily stopped the application DDoS attack through a combination of out-of-the-box and custom policies.
- With Imperva's ThreatRadar Reputation Services, the bank stopped known malicious sources and requests from unauthorized countries.
- Bot mitigation policies blocked bots flooding the bank's account login page.
- When the attackers began flooding the site with network traffic, the customer activated DDoS Protection Service for SecureSphere. The service handily defeated the DDoS attack.

### Bottom Line

- According to the customer, Imperva eliminated attack traffic and kept the site up, averting millions of dollars in lost revenue and damage.
- No users reported issues accessing the site after DDoS policies were applied, indicating a near-zero percent rate of false positives.

## DDoS Protection Service for SecureSphere

Imperva offers a cloud-based security service to complement the SecureSphere Web Application Firewall. DDoS Protection Service for SecureSphere, an add-on subscription for SecureSphere customers, mitigates attacks that saturate organizations' ISP connections and prevent legitimate traffic from reaching organizations' networks. It also stops application DDoS threats like Slowloris and RUDY.

### Ironclad Protection Scaling to Stop 350 Gbps Attacks

Powered by Imperva Incapsula, this service offers a complete defense against all types of DDoS threats, including network-based attacks like SYN flood, UDP flood, teardrop, and smurf attacks.

***Imperva has stopped several of the largest DDoS attacks in history, including a 100+ Gbps attack in 2013***

*DDoS Protection Service for SecureSphere scales on demand to stop the most powerful denial of service attacks in the world. With over a dozen datacenters around the globe, the service can block DDoS traffic before they overwhelm customers' ISP connections. Anycast routing prevents attackers from taking down a specific cloud datacenter.*

With DDoS Protection Service for SecureSphere, customers can rest assured that their applications are always accessible without needing to over-provision Internet bandwidth.

### Supercharged Bot Detection Eliminates App DDoS Attacks

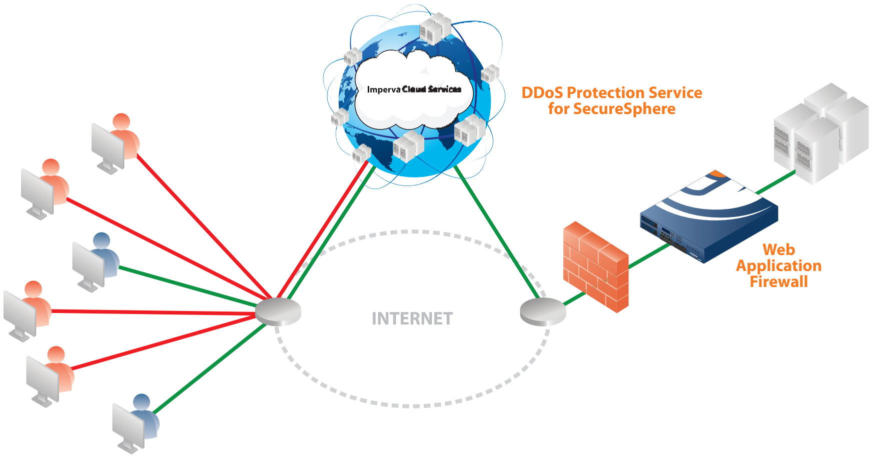
DDoS Protection Service for SecureSphere sets itself apart from other DDoS security services by accurately identifying and stopping application DDoS attacks.

DDoS Protection Service for SecureSphere stops known DDoS attack tools like DirtJumper, #RefRef, and Hulk and prevents slow rate attacks like Slowloris from ever reaching protected web servers. Because the service proxies connections and decrypts SSL traffic, it can stop SSL-based attacks that circumvent many ISPs' DDoS mitigation services. However, the single most important technology powering this DDoS protection service is an advanced bot mitigation engine. Virtually all DDoS traffic originates from automated clients.

DDoS Protection Service for SecureSphere can detect automated clients based on behavior and user agent information. It can recognize when a bot claims to be well-known browser, but deviates from expected browser behavior. It can spot HTTP requests that are too fast, mismatched user agent data, and other attributes that expose bots. And it can issue a series of challenges, starting with JavaScript checks and ultimately concluding with CAPTCHAs to correctly stop automated DDoS clients without blocking legitimate users.

### Fast, Easy Deployment

DDoS Protection Service for SecureSphere can be rolled out without any hardware, software or Web application changes. When customers are under attack, they simply change their Website's DNS settings. This effortless deployment allows customers to be protected in a matter of minutes while maintaining their existing hosting provider and application infrastructure.



*The SecureSphere appliance provides continuous protection against app DDoS attacks. When DDoS attacks threaten to overwhelm customers' Internet connections, they can update DNS settings to route traffic through the Imperva cloud. Then DDoS Protection Service for SecureSphere blocks DDoS traffic and forwards legitimate requests to the protected web application.*

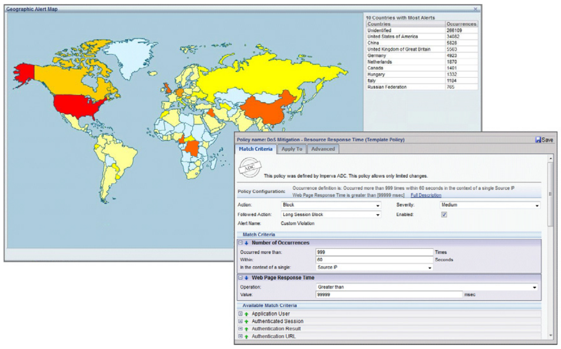
## SecureSphere for Always-on Application DDoS Protection

The Imperva SecureSphere Web Application Firewall is an on-premise security appliance that stops application DDoS attacks as well as Web attacks like SQL injection, site scraping, and fraud.

SecureSphere uses the following defenses to thwart app DDoS attacks:

- **ThreatRadar Reputation Services** provides an up-to-date feed of users that are actively attacking other websites, anonymous proxies, and TOR networks, and IP geolocation data.
- **Up-to-Date Web Attack Signatures** identify known bot user agents and known DDoS attacks vectors.
- **DDoS Policy Templates** detect users that generate HTTP requests with long response times or download multiple large-sized files.
- **Bot Mitigation Policies** send a transparent JavaScript challenge to users' browsers to detect and block bots.
- **HTTP Protocol Validation** uncovers buffer overflow attempts and evasion techniques.
- **Patented Dynamic Profiling Technology** learns applications – URLs, cookies, and parameter values – to block anomalous behavior.
- **Custom Security Rules** can examine multiple attributes, from IP reputation and header agent information to the rate of HTTP requests to block DDoS attack traffic.

The SecureSphere Web Application Firewall offers organizations granular DDoS security policies and detailed alerting and reporting.



10 Countries with Most Alerts

| Countries | Occurrences |
|---|---|
| Unidentified | 266109 |
| United States of America | 34082 |
| China | 5828 |
| United Kingdom of Great Britain | 5563 |
| Germany | 4923 |
| Netherlands | 1870 |
| Canada | 1401 |
| Hungary | 1332 |
| Italy | 1184 |
| Russian Federation | 765 |

Policy name: DoS Mitigation - Resource Response Time (Template Policy)

This policy was defined by Imperva ADC. This policy allows only limited changes.

Policy Configuration: Occurrence definition is: Occurred more than 999 times within 60 seconds in the context of a single Source IP
Web Page Response Time is greater than [99999 msec] Full Description

Action: Block
Severity: Medium
Followed Action: Long Session Block
Enabled: ☑
Alert Name: Custom Violation

Match Criteria

Number of Occurrences
Occurred more than: 999 Times
Within: 60 Seconds
In the context of a single: Source IP

Web Page Response Time
Operation: Greater than
Value: 99999 msec

Available Match Criteria
Application User
Authenticated Session
Authentication Result
Authentication URL

*SecureSphere stops application DDoS attacks with laser precision.*

## Midwest Manufacturer Staves off Powerful SYN Flood Attack

### Customer

- A leading manufacturer of recreational vehicles including travel trailers and fifth wheel trailers.
- Headquartered in Indiana, the RV manufacturer boasts nearly 1,000 dealer locations throughout the U.S. and Canada.

### DDoS Attack

- An unknown attacker launched a SYN flood attack on the RV manufacturer's corporate website and partner portal.
- The RV manufacturer received reports from dealers that the website and partner portal were unavailable.
- The lead security administrator contacted the company's web hosting provider; the hosting provider attempted to allocate more application bandwidth, but the hosting provider's "solution fell apart under the attack. We were caught behind the eight ball."

### Solution

- DDoS Protection Service for SecureSphere

### DDoS Protection Service Highlights

- DDoS Protection Service for SecureSphere successfully stopped a massive SYN flood attack that was hammering the company's website.
- At the height of the attack, website bandwidth was over one hundred times greater than typical levels.
- Two days after implementing the DDoS Protection Service, the attack subsided. Two follow-on attacks occurred over the next month and Imperva was able to stop these attacks as well.
- The Imperva SOC managed all aspects of deployment, configuration and tuning. According to the security administrator, "Everyone we've worked with at Imperva has been knowledgeable and responsive."

### Bottom Line

- Within two hours of contacting Imperva, the company had redirected web traffic through the Imperva cloud, the DDoS Protection Service had stopped the attack, and the website was up and running.
- According to the manufacturer's security administrator, "Every aspect of the service has been stellar."

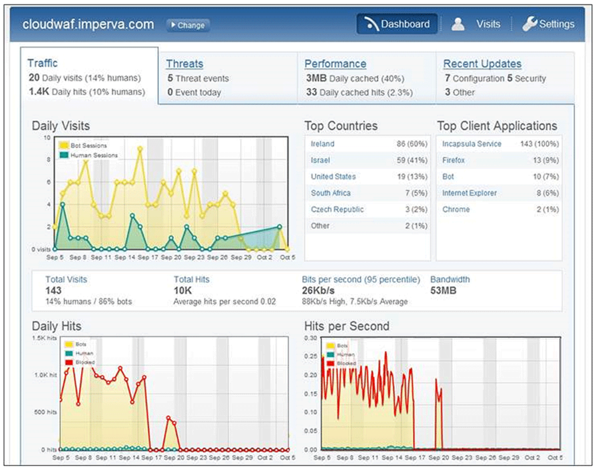
### Imperva's Managed Security Service Provides:

- Proactive security event management and response: Imperva's SOC assesses and proactively responds to events and bursts of traffic throughout the duration of a DDoS attack.
- Continuous, real-time monitoring: Vigilant application monitoring verifies that applications are always accessible.
- Proactive policy tuning: Immediate analysis and policy tuning delivers enables Imperva to quickly adapt to new attack vectors.
- Summary attack reports: Graphical reports summarizing DDoS attack traffic, attack sources, attacks by country, and bandwidth utilization after a DDoS attack occurs.
- Around-the-clock support: Continuous support and services backed by an industry-best SLA.

## Management and Monitoring from DDoS Security Experts

While automated defenses can stop most DDoS attacks, they cannot mitigate all attacks, especially application-layer assaults that exploit business logic flaws. Advanced attacks can target specific weaknesses in an application and evade standard DDoS defenses. Detecting and stopping anomalies, such as repeated user login attempts that slow down a database or millions of requests from an obscure country, requires monitoring and tuning by security professionals.

As part of its DDoS Protection Service, Imperva offers 24x7 managed services delivered by knowledgeable Security Operations Center (SOC) engineers. Imperva's team of SOC engineers quickly investigate and respond to new DDoS security threats. They can pinpoint never-before-seen threats, such as modified DDoS attack tools or application exploits, and create policies to block these attacks.



Traffic
20 Daily visits (14% humans)
1.4K Daily hits (10% humans)

Threats
5 Threat events
0 Event today

Performance
3MB Daily cached (40%)
33 Daily cached hits (2.3%)

Recent Updates
7 Configuration 5 Security
3 Other

Top Countries

| | |
|---|---|
| Ireland | 86 (60%) |
| Israel | 59 (41%) |
| United States | 19 (13%) |
| South Africa | 7 (5%) |
| Czech Republic | 3 (2%) |
| Other | 2 (1%) |

Top Client Applications

| | |
|---|---|
| Incapsula Service | 143 (100%) |
| Firefox | 13 (9%) |
| Bot | 10 (7%) |
| Internet Explorer | 8 (6%) |
| Chrome | 2 (1%) |

Total Visits
143
14% humans / 86% bots

Total Hits
10K
Average hits per second 0.02

Bits per second (95 percentile)
26Kb/s
88Kb/s High, 7.5Kb/s Average

Bandwidth
53MB

## Complete Protection Against DDoS Attacks

Organizations can rely on Imperva's cloud and on-premise security solutions to stop powerful DDoS attacks. DDoS Protection Service for SecureSphere, a simple add-on subscription for SecureSphere customers, provides ironclad protection against application and network DDoS attacks. With a global network of datacenters and an advanced bot mitigation engine that correctly identifies and stops bots, this security service fends off the most complex DDoS attacks. The SecureSphere Web Application Firewall offers granular policy control and detailed alerting and reporting to ensure applications are always available and responsive.

With Imperva, customers receive both on-site and cloud-based DDoS security from a single vendor. Imperva delivers integrated and complete DDoS protection and managed security services to thwart high-volume attacks and advanced application DDoS threats.

**www.imperva.com**