



## Joint Solution Brief

# Comprehensive Security with Imperva SecureSphere WAF and the Gigamon GigaSECURE Security Delivery Platform

### The Challenge

Imperva SecureSphere Web Application Firewalls are an essential part of protecting your applications and data from cyber attacks, but successful, manageable, and efficient deployment on a large scale requires careful design.

### Integrated Solution

Gigamon's GigaSECURE® Security Delivery Platform provides the perfect complement to Imperva SecureSphere Web Application Firewall (WAF) appliances by filtering unnecessary traffic before it loads the WAFs, allowing intelligent load balancing of high-bandwidth flows across multiple SecureSphere devices, easy movement into and out of an inline deployment mode, and additional fault tolerance options to the native Imperva offerings that are especially useful where traffic needs to flow through a chain of inline security devices.

### Joint Solution Benefits

- Enable multi-vector data and application protection with full visibility
- Deploy inline and/or out-of-band – changable at the touch of button without link downtime
- Optimize Imperva SecureSphere WAF performance with advanced aggregation, filtering and data manipulation
- Ensure data flow at line rate from 1Gb to 100Gb with the scalable platform
- Chain Imperva SecureSphere WAF devices with other inline security tools easily while maintaining fault tolerance and manageability

### Introduction

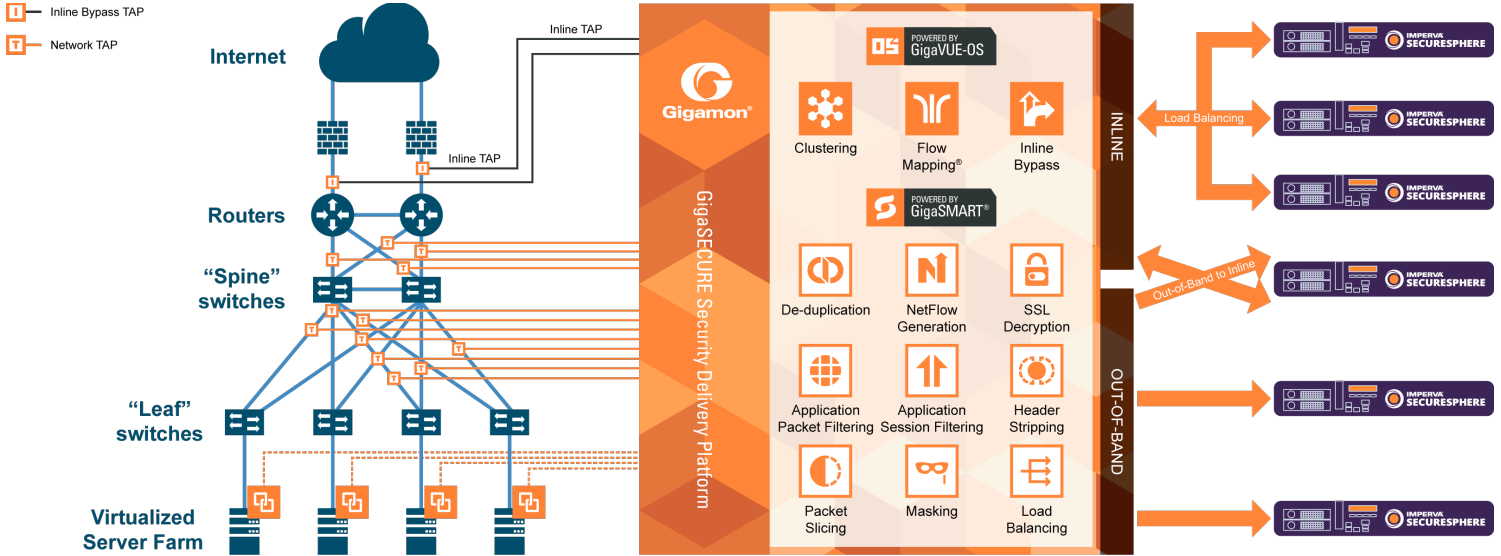
Web applications are a prime target of cyber attacks because they are readily accessible and offer an easy entry point to valuable data. To combat attacks, organizations need to protect websites and applications from existing and emerging threats without impacting performance or uptime. As web traffic increases, link speeds increase and multiple types of security appliance may be used inline to inspect traffic and block different threats. Frequent changes to web applications require mechanisms to enable the web firewalls to learn new normal behavior without creating false-positive alarms. Network operators and security teams need to carefully design their implementations to ensure security is maintained while operational efficiency is maximized and costs are contained. Together, Gigamon and Imperva offer a solution to these challenges.

### The Gigamon and Imperva Joint Solution

Imperva SecureSphere WAF appliances analyze all user access to the organization's business-critical web applications and protect those applications and the data from cyber attacks. They dynamically learn the applications' normal behavior and correlate this with the threat intelligence crowd-sourced from around the world and updated in real-time to deliver superior protection. The firewall identifies and acts upon dangers maliciously woven into innocent looking website traffic; traffic that slips right through traditional defenses. This prevents application vulnerability attacks such as SQL injection, cross-site scripting and remote file inclusion; business logic attacks such as site scraping and comment spam; botnet and DDoS attacks; and account take-over attempts in real-time, before fraud can be performed.

The GigaSECURE platform provides easy access to the traffic flowing to your web applications that the WAF needs to inspect. Intelligent traffic filtering, through the Application Session Filtering feature, only forwards web traffic to the WAF. Non-web traffic such as voice packets can bypass the device without inspection thus increasing the efficiency of the organization's Imperva investment.

In addition to increasing efficiency through the filtering out unnecessary traffic types, large traffic flows greater than the capacity of the Imperva appliances can be intelligently load balanced across multiple devices, thus 40Gb and even 100Gb links can be safely monitored. Similarly, smaller traffic flows can be aggregated while maintaining traffic source and destination information and all sent to a single Imperva device for inspection.



Often, when deploying WAFs, organizations will first put them out-of-band while normal behavior is learned. The GigaSECURE platform allows operators to deploy Imperva devices in this way and then move them inline at the touch of a button without having to take down the network link. This action can be repeated whenever necessary to take an appliance out of service for maintenance or to relearn new application changes.

Finally, the GigaSECURE platform's inline bypass functionality can be utilized for advanced fault tolerance, particularly in implementations that require chained security devices to inspect the same traffic. By protecting each device and enabling traffic filtering to ensure only relevant traffic passes through each tool, the joint solution allows organizations to meet all the challenges of creating a secure, scalable and efficient infrastructure for their web applications and data.

### Learn More

For more information on the Imperva and Gigamon solution, contact:

**IMPERVA**  
www.imperva.com

**Gigamon**  
www.gigamon.com