Solution Brief

GARLAND TECHNOLOGY
See every bit, byte, and packet®

imperva

Comprehensive Web Application Redundancy to Protect Traffic and Sensitive Data

Core networks, data centers, and large enterprises demand speed, scalability, and security without compromise with web applications being a prime target of cyber-attacks because they are readily accessible and offer an easy entry point to valuable data. Organizations need to protect web applications from existing and emerging cyber-threats without affecting performance, time to market, or uptime.

The rapid pace of application changes can make it very difficult for security teams to keep up with updating rules that properly secure web assets. This can create security gaps and vulnerabilities that cybercriminals can exploit leading to costly data breaches. Additionally, organizations look to deploy security solutions that can scale with their applications to match growth in user demand, ensuring that web assets are properly secured while preserving the end-user experience.

To do this an inline architecture is a critical component to protect the data networks of every enterprise. Inline security appliances, such as Imperva's Web Application Firewall (WAF) must operate at peak performance without failure and without affecting network uptime or application responsiveness while inspecting network traffic 24 hours a day. One challenge for inline deployments comes with ensuring the appliances themselves do not present a point of failure in the network, during maintenance or potential failures. Implementing Garland Technology's EdgeLens® Inline Security Packet Broker, not only allows ease of inline management for the Imperva WAF deployment but ensures maximum network uptime. Allowing 24/7, 365 web applications traffic analysis to stop attacks and ensure uninterrupted business operations.

Garland and Imperva Integration Benefits

The integrated Garland Imperva solution delivers maximum security and supports today's most demanding bandwidth requirements while delivering unparalleled performance, security, and visibility in 40Gbps-plus environments.

Business Benefits

- Enhance Inline network resiliency - flexibility to bypass the tool and keep the network up, or to failover to a high availability solution
- Manage the risks of downtime ensuring no lost revenue or customers
- Build high availability into mission critical deployments
- Deployment efficiency - Extend the reach of the same tools into multiple network segments
- Secure active and legacy applications, third party applications, API and microservices
- Empower your security teams to use third-party code without risk with automatic policy creation and fast rule propagation.
- Deploy Imperva WAF on-premises, in AWS and Azure, or as a cloud service
- Easy configuration and deployment improves reliability and reduces costs

Functionality Benefits

- Eliminates single points of failures for inline tool deployments
- Dynamically load balanced workloads across multiple Imperva WAFs
- Advanced failover mechanisms to prevent outages and minimize maintenance downtime.
- Monitor the health of Imperva's WAF with heartbeat packets
- Provide filtering, aggregation, and load balancing to inline links
- Simplify security stack and reduced network complexity by managing multiple inline tools
- Advanced bad bot mitigation
- Superior persistent threat protection
- Low cost of ownership
- Activation only requires DNS change
- Up-to-date signatures against existing and emerging threats

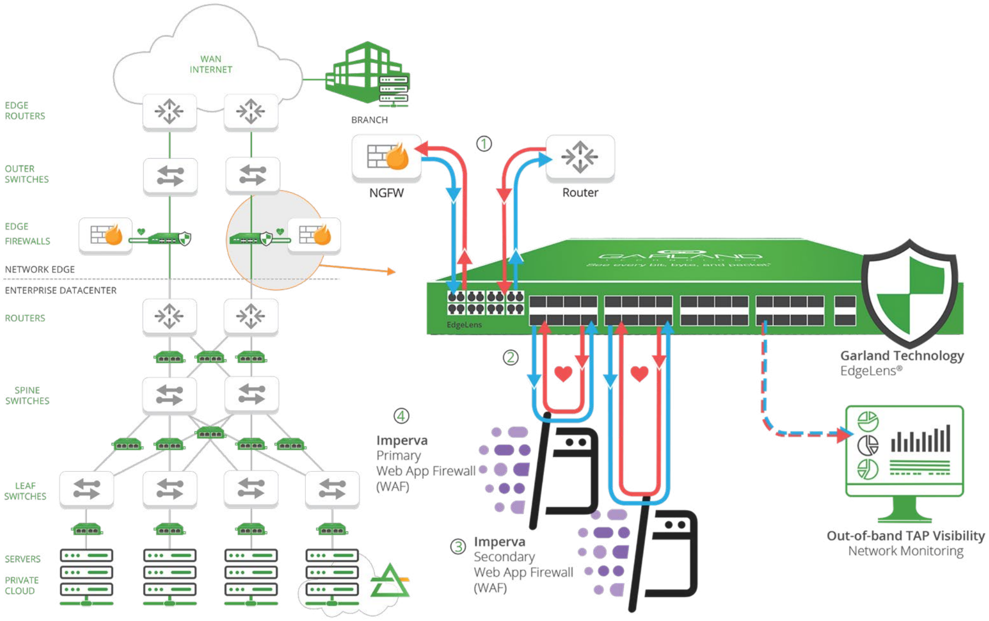
HOW IT WORKS

1. Deploying bypass technology provides inline lifecycle management for sandboxing, deployment and maintenance of the Imperva Web application firewall (WAF) out-of-band, while the live critical link is up.

2. The bypass TAP is designed to pass heartbeat packets back and forth to detect any connectivity issues with the WAF. If an issue is detected, the bypass TAP will automatically 'bypass' the tool, keeping the live network up, or failover to a High Availability (HA) solution. Preventing any single points of failure (SPOF) or network downtime.

3. With the EdgeLens' high availability (HA) functionality, you are able to deploy active/passive or active/active scenarios, ensuring the network is protected by redundant Imperva WAF tools.

4. The Imperva WAF provides a key component of a comprehensive Web Application and API Protection (WAAP) stack that secures from edge to database by analyzing traffic to your applications to stop these attacks and ensure uninterrupted business operations.



Imperva Company Overview

Imperva has a singular purpose: to defend your business-critical data and applications from cyber attacks and internal threats. Imperva's solutions enable you to discover your assets and risks, and then protect your most valuable information - such as intellectual property, business plans, trade secrets, customer and employee information, and the day-to-day data that drives your business. Imperva also helps you comply with the myriad of increasingly stringent data protection regulations and mandates, as well as enforce policies, entitlements and audit controls. For more information visit imperva.com.

Garland Company Overview

Garland Technology is an industry leader delivering network products and solutions for enterprise, service providers, and government agencies worldwide. Since 2011, Garland Technology has developed the industry's most reliable test access points (TAPs) and network packet brokers (NPB), and Cloud visibility solutions enabling data centers to address IT challenges and gain complete network visibility. For help identifying the right NPB solution for projects large and small, or to learn more about the inventor of the first bypass technology, visit GarlandTechnology.com or @GarlandTech.

Have Questions?

sales@garlandtechnology.com | 716.242.8500
GarlandTechnology.com/imperva

GARLAND
TECHNOLOGY
See every bit, byte, and packet®