

Imperva Elastic WAF

Security Must Scale with Innovation in Modern DevOps

As organizations adopt cloud-native infrastructures, DevOps teams face increasing challenges in harmonizing security requirements with the demands for agility and efficiency.

Modern Application Security Challenges for Distributed Architectures

- Managing security across multi-cloud and hybrid environments
- Maintaining consistent policies across diverse deployments
- Integrating seamlessly into CI/CD pipelines without delays
- Ensuring centralized visibility across applications and traffic
- Balancing agility, performance, and cost-efficiency
- Securing microservices with customizable controls
- Simplifying security transitions across platforms
- Minimizing reliance on third-party inline network solutions

Organizations increasingly seek solutions that seamlessly integrate security into CI/CD pipelines, reduce operational friction, and enable centralized management without compromising performance.

Flexible Security Without Compromising Agility—Anywhere

Imperva Elastic WAF meets the evolving security demands of modern DevOps workflows by providing strong, architecture-agnostic protection. It offers best-in-class security directly within your deployment environment and can be easily managed through a SaaS platform. Additionally, it integrates quickly and seamlessly into the DevOps CI/CD pipeline.

Who uses Imperva Elastic WAF?

Organizations choose Imperva Elastic WAF to:

- Strengthen security without disrupting agility—Elastic WAF integrates directly into DevOps workflows and CI/CD pipelines.
- Reduce complexity with centralized control—Seamlessly manage security across on-prem, hybrid, and multi-cloud environments.
- Minimize TCO while maintaining robust security—Imperva's out-of-the-box security reduces the need for ongoing policy updates or custom configurations.
- Enhance existing CDN deployments—Adding enterprise-grade security without overhauling current traffic routing.

Why Imperva Elastic WAF?

- **Enterprise-Grade Protection:** Strengthens application defenses beyond CDN security with market-leading threat mitigation.
- **Streamlined Security Management:** Provides a SaaS-managed, architecture-agnostic solution, enabling effortless deployment and centralized control via UI, Terraform, and APIs across diverse environments.
- **Cost-Effective & Low Overhead:** Simplifies security operations, reducing policy maintenance and manual exception handling.
- **Local Data Control with SaaS Efficiency:** Deploy Imperva security engines in Kubernetes to protect sensitive data locally while leveraging centralized SaaS management for streamlined operations.
- **Enhanced Agility Without Compromise:** Enables businesses to maintain their current CDN setup while adding enterprise-grade, customizable security measures tailored to dynamic needs.

How does it work?

Deploy Elastic WAF in minutes within your Kubernetes environment—integrating directly with ingress controllers to inspect and secure traffic with zero added complexity. It integrates seamlessly with ingress controllers to inspect and secure incoming traffic. Leveraging Imperva’s SaaS ecosystem, it provides best-in-class threat protection by detecting vulnerabilities, applying automatic mitigation rules, and managing policies through the Cloud Security Console.

Security events are logged in a location of your choice and synchronized with real-time insights, ensuring centralized visibility and management across both on-prem and cloud WAF environments. This architecture empowers DevOps to integrate advanced security measures natively into their CI/CD process.

Security that Works for You

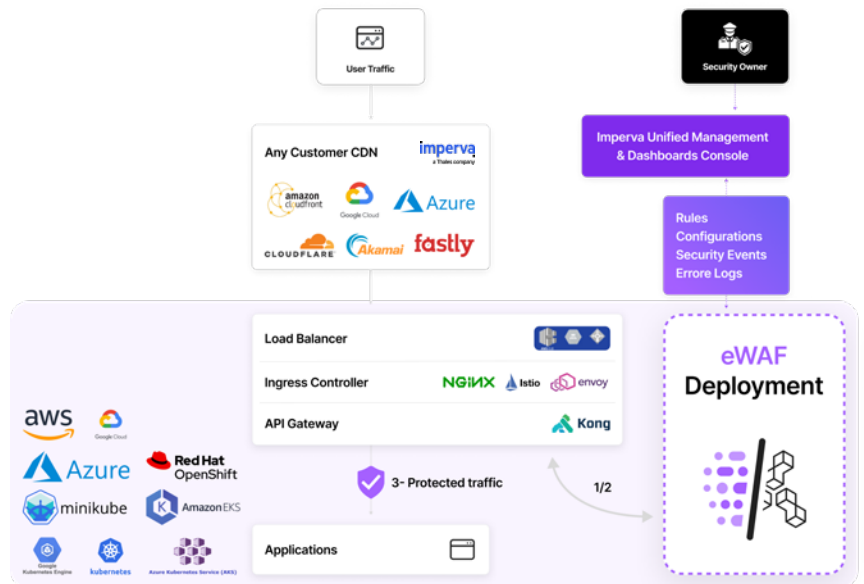
95%
of Imperva WAF customers use blocking mode

97%
of policies work effectively out-of-the-box

3.6
trillion requests analyzed per month

<5
minutes from deployment to full protection

0
Zero added latency for uninterrupted performance



Trusted by the World’s Largest Enterprises



Technology and platform integrations

Container Orchestrators



Load Balancer



API Gateways & Ingress controllers



DevOps Configuration and Operations Management Tools



Security Information and Event Management (SIEM)

