imperva

DATASHEET

Runtime Application Self-Protection (RASP)

Securing applications by default

Applications are prime targets for cyber attacks as they handle troves of personally identifiable information, intellectual property, financial information, and other critical data. Many traditional application security tools fail to protect organizations from attacks because they mostly rely on signatures and rules that are easy to circumvent, cause performance degradation, suffer from high false positive rates, struggle to stop zero-day attacks, and lack real-time context and visibility. Imperva believes that securing applications requires radical thinking- applications must defend themselves.

Imperva RASP

Imperva RASP fills the security gaps that leave applications vulnerable to attack with a single plugin that protects both legacy and modern applications. The RASP plugin is completely autonomous, requiring no network calls, and works in any type of deployment architecture including on-premise, in the cloud, and in containers. Imperva RASP enables applications to protect themselves using an industry-leading, lightning-fast attack detection method called Language Theoretic Security (LANGSEC). LANGSEC understands how payloads will execute within the context of a given environment and neutralizes known and zero-day attacks. The result is applications that are secure by default, regardless of any latent vulnerabilities in the application software that would otherwise be susceptible to attack.

RASP integrates security into application development lifecycles, augmenting the traditional vulnerability-management approach to AppSec. Because RASP not only pinpoints the vulnerabilities a neutralized attack would have exploited - down to the exact line of code - but also secures applications despite those vulnerabilities, organizations can patch vulnerabilities on their own schedule, minimizing disruption.

KEY CAPABILITIES

Secures applications no matter where or how they are deployed: on-prem, in the cloud or via containers

Fast time to value with no signatures and no learning mode

Simple deployment via existing build pipelines, with no network calls

Secures latent vulnerabilities in original or third-party software

Zero-day protection

Comprehensive out of the box reporting

FORRESTER®
NEW WAVE
LEADER 2018
Runtime Application
Self-Protection

“Forrester’s research uncovered a market in which Prevoty (now Imperva RASP) leads the pack”

The Forrester New WaveTM: Runtime Application Self-Protection Q1 2018. Download the full Forrester report here.

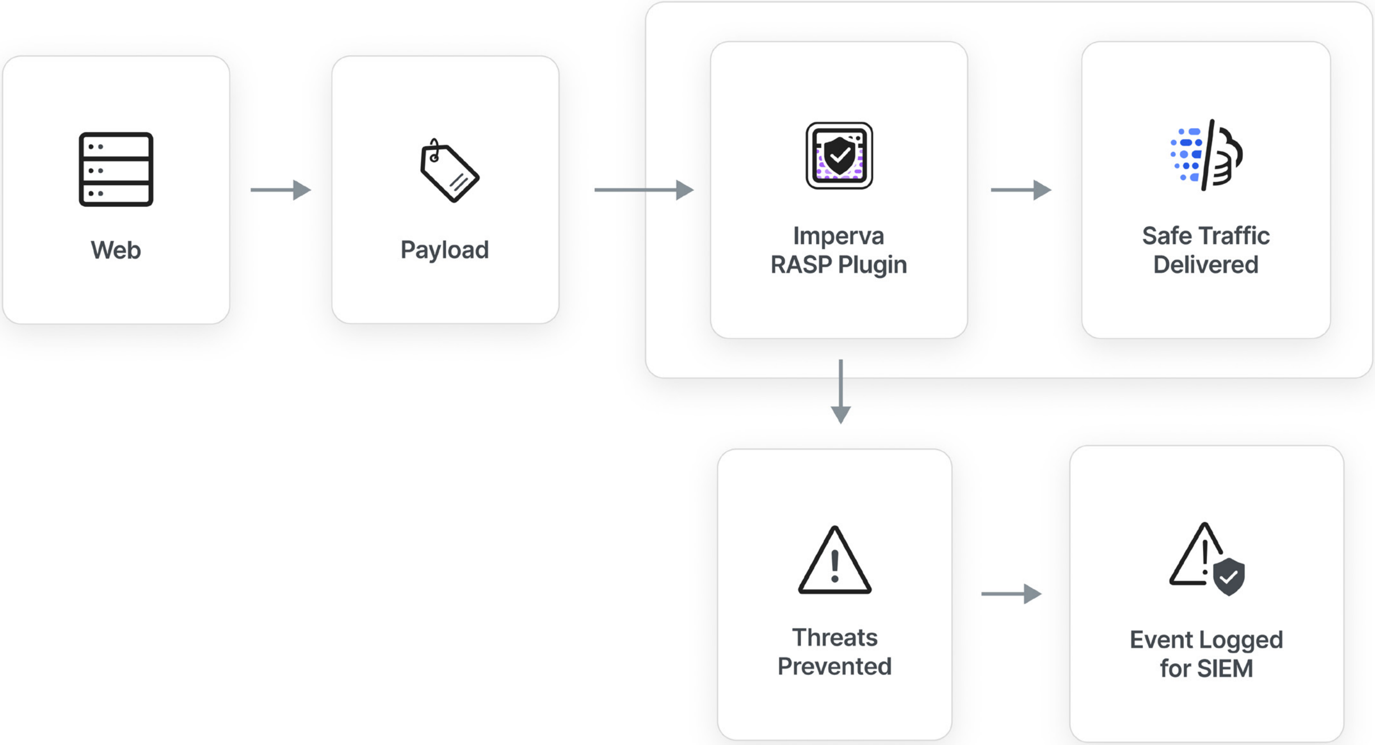

Figure 1: Imperva RASP plugins sit within applications to examine threats in real-time and with full application context, delivering reputable site traffic while blocking threats

Imperva RASP at a glance

Benefits of Imperva Runtime Application Self-Protection

- RASP-protected applications in production are secure by default, no matter where or how they are deployed.
- RASP requires no signature updates or learning mode, no external network calls, and negligible CPU and memory consumption by leveraging patented LANGSEC techniques, leading to fast time to value and low total cost of ownership (TCO).
- RASP buys you time to fix and patch vulnerabilities, because your applications are secure regardless of latent vulnerabilities in original or third-party software.
- RASP provides a context-enriched perspective of security from the inside of your apps with unprecedented visibility into application attacks, events & risks.

Deployments that scale with DevOps

RASP deploys quickly and quietly via autonomous plugins that live inside applications, no matter where or how they are deployed. Because RASP leverages LANGSEC- which combines high detection accuracy with very low performance overhead- deployment is unobtrusive, allowing critical business functions to continue as usual without disrupting user experience.

Imperva RASP supports the following application runtimes:

Java

Microsoft .NET

node JS

.NET

- Command Injection
- Clickjacking
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF/ XSRF)
- Database Access Violation (Advanced SQLi)
- HTML Injection
- HTTP Method Tampering
- HTTP Response Splitting
- Insecure Cookies
- Insecure Transport
- JSON Injection
- Large Requests
- Logging Sensitive Information
- Malformed Content-Types
- OGNL Injection
- Path Traversal
- SQL Injection
- Logging Sensitive Info
- Insecure Transport Protocol
- Unauthorized Network Activity
- Uncaught Exceptions
- Unvalidated Requests
- Vulnerable Dependencies
- Weak Authentication
- Weak Browser Cache Management
- Weak Cryptography & Ciphers
- • XML External Entity Injection (XXE)
- XML Injection
- And more...

IMPERVA APPLICATION SECURITY

RASP is a key component of Imperva Application Security, which reduces risk while providing an optimal customer experience. The solution safeguards applications on-premises and in the cloud by:

Providing actionable security insights

Protecting against DDoS attacks

Mitigating botnet attacks

Monitoring all data activity

Providing WAF protection

Blocking cyber-attacks that target API's

Ensuring optimal content delivery

Learn more about Imperva Application Security at +1.866.926.4678 or online at **imperva.com**

Imperva is an analyst-recognized, **cybersecurity leader** championing the fight to **secure data and applications** wherever they reside.