imperva

DATASHEET

Runtime Application Self-Protection (RASP)

Imperva RASP keeps applications secure 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. According to the 2019 Verizon Data Breach Investigation Report and for the past several years, web application targeted attacks have remained the most likely attack vector to trigger a data breach. 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, struggle to stop zero-day attacks, suffer from high false positive rates, and lack real-time context and visibility. Imperva believes that securing applications requires radical thinking, applications must defend themselves.

Imperva Runtime Application Self-Protection = Security by Default

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, portable, and works in any type of deployment architecture including on-premise, in the cloud, and in containers. Imperva RASP's autonomous plugins enable applications to protect themselves using an industry-leading, lightning-fast attack detection method called Language Theoretic Security (LANGSEC) that 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 with attack-based risk mitigation informed by real attack data. 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 have more time to implement patches and more insight into which vulnerabilities are actually being attacked.

IMPERVA APPLICATION SECURITY

- RASP-protected applications are secure by default, no matter where they are deployed.
- RASP buys you time to fix or patch vulnerabilities, with the assurance that your applications are secure regardless of latent vulnerabilities in original or third-party software.

"Forrester's research uncovered a market in which Prevoty (now Imperva RASP) leads the pack."

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

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 buys you time to fix and patch vulnerabilities, because your applications are secure regardless of latent vulnerabilities in original or third-party software.

Additional benefits

- A new context-enriched perspective of security from the inside of your apps with unprecedented visibility into application attacks, events & risks.
- DevOps scalability.
- More efficient secure software development lifecycle (SSDLC) and vulnerability management using real attack-based risk management.

Embed Security
RASP plugin attached from the start

SSDLC
RASP is part of the app throughout SSDLC

Hardened APP
Applications are secure by default

Data Analytics
Lof data for insights in SIEM / analytics platform

Deployment

RASP deploys quickly and quietly via autonomous plugins that live inside applications, no matter where they are deployed. Deployment is unobtrusive, allowing critical business functions to continue as usual without disrupting user experience secure by default from day one.

Imperva RASP protects against

- 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

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:

- Monitoring all data activity
- Protecting against DDoS attack
- Mitigating botnet attacks
- Providing actionable security insights
- Providing RASP protection

Learn more about Imperva Application Security at www.imperva.com.

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

+1 [866] 926-4678
imperva.com

imperva