IMMUNIO

Web App Security at the Speed of Dynamic Development for Python, Ruby, and Node.JS

Web App Security at the Speed of Dynamic Development for Python, Ruby, and Node.JS

Software development organizations are embracing dynamic platforms such as Python, Ruby on Rails, and Node.JS because of the imperative to develop and release applications quickly. These companies need effective web application security solutions that safeguard against vulnerabilities without slowing down release cycles.

For non-dynamic languages such as .NET and Java, organizations can turn to static code scanners. But the effectiveness and availability of such tools for platforms such as Python, Ruby, and Javascript (Node.JS) is not on par. In fast-moving, agile development shops, application security risks are often higher due to the increased pace of development; code is changing continually, usually without the necessary security controls. Continuous releases heighten the urgency for solutions to address code security at all stages of development, testing and release. In this scenario, static scanners often fall short.



STATIC TECHNOLOGIES DON'T WORK WITH DYNAMIC LANGUAGES

Static application security solutions generate significant amounts of false positives, and their support for dynamic languages is limited. These legacy solutions are complex to configure, and it can take months of configuration and tuning before they function effectively at scale. It's not uncommon to spend 20 man days tuning a tool for just one application. Customers deploying these solutions to secure apps built in Python, Ruby, or Node.JS are left hoping the risks don't outweigh the rewards.

YOUR APPLICATIONS HAVE VULNERABILITIES, POTENTIALLY SEVERE

There is almost always technical debt in projects, and quite often it is "security technical debt." While engineering teams focus on getting features and functionality out the door,

they can easily end up running an unsupported or vulnerable version of a component inside your applications. What's more, even when you manage to identify vulnerabilities in your applications, now you have to address them, and that can take months—particularly if you started the security bug finding process late in the project's lifecycle.

With both known vulnerabilities, as well as hidden zero day vulnerabilities in every project, it's vital to have a solution that protects you from the get-go. IMMUNIO is the fastest application security technology to deploy to gain visibility into threats and vulnerabilities as they happen, and effectively render them unexploitable in real time.

IMMUNIO: THE FASTEST-TO-DEPLOY, EASIEST-TO-MANAGE, MOST ADVANCED SECURITY SOLUTION FOR PYTHON, RUBY, AND NODE.JS

Dynamic languages like Python, Ruby, and Node.JS (Javascript) are best served by runtime security technologies such as Runtime Application Self-Protection (RASP). IMMUNIO provides the only RASP solution specifically designed to work with these languages.

Unlike static source code scanners:

- IMMUNIO's technology works with dynamic languages
- Offers protection and automatic remediation against the most advanced threats
- Identifies the relevant vulnerabilities, with very low false positives
- Doesn't require dedicated or specially-trained staff, or long tuning/customization efforts

IMMUNIO augments solutions like pen testing by providing an 'inside-out' view of vulnerabilities, as compared to the 'outside-in' view that pen testing offers. With IMMUNIO, you learn which line of code the vulnerabilities identified reside in, you can validate the vulns' severity, get details about the payloads that succeed, and automatically render these vulns unexploitable.

Unlike Web Application Firewalls (WAFs), IMMUNIO can be deployed in "protect" mode quickly, with very low false positive rates. Also, unlike with WAFs, there is no need for dedicated staff or niche skills to be developed to maintain and troubleshoot complex rules. And IMMUNIO's technology outshines WAFs in effectiveness against the most sophisticated web application threats.

NO APPSEC PROGRAM? IMPLEMENT ONE FAST WITH IMMUNIO

If your organization hasn't yet launched its application security program, IMMUNIO's RASP solution is an ideal place to start. You can gain critical insights into the state of your web app security and protect against the top threats and vulnerabilities in just days. You can go from no appsec to a comprehensive program covering all your Python, Ruby and Node.JS apps quickly.

IMMUNIO KEY FEATURES AND BENEFITS

Features	Benefits
Full Python, Ruby, and Node .JS Support	Agents for Python, Ruby, NodeJS provide instant, out of the box support.
Two-minute install	Get an appsec program up and running rapidly.
Industry leading protection capability	Future-proofs your application against most zero-days.
Agent architecture	Application development and appsec teams can deploy quickly, no dependency on network, or appliances.
High level accuracy	Extremely low false positive rate.
Remediation	In addition to vuln, threat, and threat actor identification, IMMUNIO can protect assets against data breaches, credential theft, and remote server execution.
Wide coverage	Protect your application stack against many common and dangerous threats such as: XSS, SQLi, RCE, Shell-Shock, Split Response Headers, Directory Traversal, Credential Stuffing, Brute Force attacks, Session attacks, CSRF, and more.
Automatic updates	Address new threats without customer involvement.

Want to learn more? To see for yourself how IMMUNIO protects web applications, your critical business data, and your customers, request a product demo today.