VERACODE

DATASHEET

Veracode Package Firewall

Govern Smart, Code Confidently.

Organizations of all sizes grapple with mounting security and compliance challenges in managing open-source software (OSS). Outdated solutions and scanning tools flood teams with findings, heightening friction with developers, while failing to counter the surging threat of software supply chain attacks. Traditional governance frameworks drain time, resources, and budgets, erecting formidable barriers to securing modern environments.

Veracode Package Firewall is an automated governance solution designed to dynamically control and monitor the use of software packages by blocking vulnerabilities, malware, and policy violations before they enter development pipelines.

Veracode Package Firewall provides a seamless, fully automated solution that enhances security, simplifies governance, reduces friction between security and development teams, and defends against malware threats — all while supporting developer productivity.

Why Veracode Package Firewall?

- **Proactive Malicious Package Detection:** Identify and block more malicious packages with industry-leading threat detection technology.
- **Advanced Risk Insights:** Comprehensive visibility and advanced analytics that identify author vulnerabilities and engineering hygiene issues.
- **Unmatched Policy Flexibility:** Customize security policies with code for unparalleled control over your software packages.
- **Superior Developer Experience:** Empower developers with real-time, in-console feedback and seamless collaboration tools to ensure compliance.
- **Flexible Deployment:** Deploy a flexible security solution that integrates seamlessly across all development environments.

Veracode Threat Research shows malicious packages skyrocketed by **9 times in 2024**, posing an unprecedented risk to software development.

+9X

KEY USE CASES & BENEFITS

Reduce Findings Early:
Screen packages upfront to align with organizational policies on licenses, vulnerabilities, and malware — reducing CI/CD alerts and cutting remediation costs.

Defend Against Supply Chain Attacks:
Block malicious packages in real time, protecting enterprises from the rising tide of open-source threats.

Streamline Development Processes:
Reduce code review time by enforcing standards automatically, enabling developers to focus on innovation.

Ensure Compliance with Ease:
Support regulated industries with advanced license data and policy enforcement, minimizing compliance risks.

Veracode Package Firewall empowers enterprises to safeguard their software supply chain and comply with regulations effortlessly.

TECHNICAL SPECS

Supported Ecosystems:

JavaScript/NPM, Python/PyPI, Java/Maven, C#/NuGet, Golang, Rust/Cargo, Ruby/RubyGems.

Integration Options:

- Direct integration with developer package managers.
- Compatibility with JFrog Artifactory and Sonatype Nexus.

Policy Framework:

Built on Open Policy Agent (OPA), offering policy-as-code with 20+ pre-built policies and customizable analytics (e.g., vulnerabilities, author risks).

KEY FEATURES

- ✓ **Policy Flexibility with Open Policy Agent (OPA):** Leverages 20+ pre-built policies across vulnerabilities, malware, licenses, authors, and engineering risks. Customizes policies to fit unique needs, such as blocking packages less than two weeks old, in minutes.
- ✓ **Developer-Centric Experience:** Integrates notifications via Slack or Teams, with in-console error messages and alerts. Includes a workflow for requesting policy exceptions, ensuring business agility without compromising security.
- ✓ **Comprehensive Visibility:** Logs all package installations, offering end-to-end visibility into open-source usage when paired with Veracode SCA. Tracks what's installed and incorporated into products.
- ✓ **Audit Mode:** Tests policies in "warn" mode to assess impact without disrupting workflows, enabling security teams to evaluate benefits before enforcement.
- ✓ **Open Ecosystem Support:** Integrates directly with developer package managers, ensuring flexibility across environments.
- ✓ **Proactive Malware Defense:** Detects 60% more malicious packages than competitors, blocking threats in real time.
- ✓ **Automate Governance at Scale:** Replace expensive manual reviews with automated policy enforcement, saving time and resources for organizations at any maturity level.

How It Works

IDENTIFIES

Proactively detects malicious packages with advanced AI.

QUARANTINES

Isolates malicious packages to prevent their use in development.

BLOCKS

Blocks malicious packages from entering DevOps pipelines, protecting developers.

Contact Us

Contact us today to learn more about how Veracode Package Firewall can help you reduce risk and secure your application security. Visit Veracode.com to schedule a demo or request additional information.

VERACODE