VERACODE

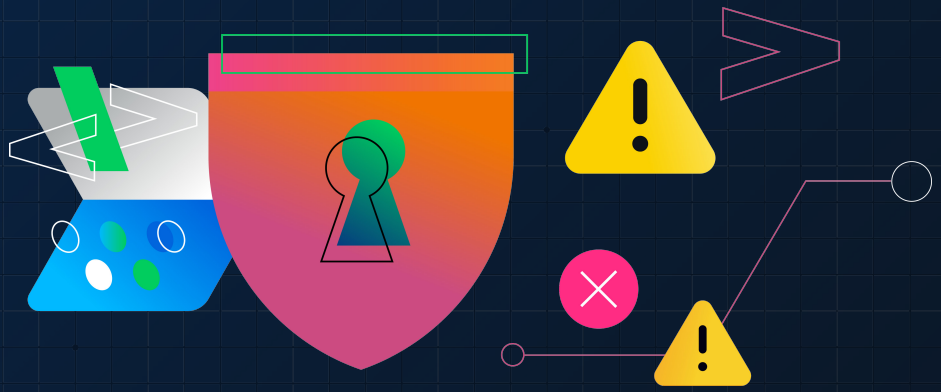
FORTIFY YOUR CODE:

Blueprint for a Secure Software Supply Chain

A Buyers Guide on What to Look for in an Enterprise Grade Solution

INTRODUCTION:

Why Securing Your Software Supply Chain Matters



Open-source and third-party packages are essential for rapid innovation in modern development, but they also introduce significant security vulnerabilities. Veracode's 2025 State of Software Security (SoSS) report reveals that *70% of critical security debt comes from third-party code*, making the software supply chain a prime target for cyber attacks.

Veracode Package Firewall empowers organizations to secure their software supply chain, ensuring that every package entering your pipeline is safe, compliant, and aligned with your security policies.

This guide equips C-level executives, security teams, and developers with the insights to evaluate AppSec solutions that balance speed, security, and compliance in protecting the supply chain.

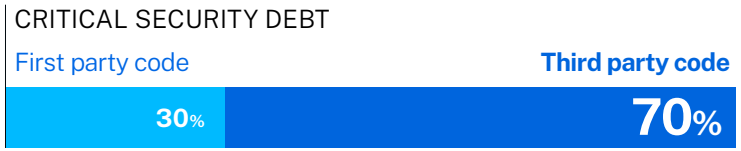
We'll explore:

- The evolving threat landscape and market trends.
- Critical challenges faced by organizations.
- Key criteria for selecting a world-class platform.
- Why Veracode leads the industry in innovation, ROI, and scalability

By the end, you'll understand how to safeguard your software supply chain while accelerating secure delivery.

MARKET OVERVIEW:

The State of Software Supply Chain Security in 2025



70% OF CRITICAL SECURITY DEBT ORIGINATES FROM THIRD-PARTY CODE.

The integrity of the software supply chain faces an unprecedented level of compromise. Veracode's 2025 State of Software Security (SoSS) report reveals a significant **180% increase in breaches exploiting vulnerabilities over the past year**, with **third-party code identified as a predominant vector.** This escalating risk is exacerbated by the pervasive integration of open-source libraries, which now constitute up to **80% of modern code-bases**, thereby expanding the attack surface considerably. High-profile incidents, such as the Log4j vulnerability, underscore the critical necessity for proactive and robust software supply chain security measures

The future of software supply chain security lies in automation, visibility, and policy enforcement. A world-class solution must not only identify risks but also prevent them at the source, ensuring secure innovation without slowing down development.

Key trends shaping the market include:

- **Rise of Supply Chain Attacks:** Malicious packages and dependency vulnerabilities are on the rise, with attackers targeting open-source repositories like NPM and PyPI.
- **Regulatory Mandates:** Regulations like the EU's Digital Operational Resilience Act (DORA), effective January 2025, require organizations to secure their software supply chains and produce Software Bills of Materials (SBOMs).
- **Shift to Proactive Security:** Organizations are moving from reactive remediation to proactive prevention, blocking risks before they enter the pipeline.

THE CHALLENGE:

Why Securing the Software Supply Chain Is Harder Than Ever

Securing the software supply chain in 2025 is a major challenge for enterprise organizations:

For C-Level Executives

- **Rising Breach Risks:** With 70% of critical security debt from third-party code, a single malicious package can lead to a costly breach, impacting revenue and reputation.
- **Compliance Pressures:** Regulations like DORA require robust supply chain security and audit trails, adding complexity to compliance efforts.
- **Innovation Delays:** Security bottlenecks in the supply chain can slow down development, hindering time-to-market and growth.

For Security Teams

- **Lack of Visibility:** Many organizations lack insight into their dependencies, with hidden risks lurking in multi-layered package dependencies.
- **Malicious Packages:** Attackers increasingly inject malware into open-source repositories, requiring proactive detection and blocking.
- **Manual Remediation:** Identifying and fixing supply chain vulnerabilities after they enter the pipeline is time-consuming and inefficient.

For Developers

- **Workflow Friction:** Security tools that interrupt development workflows reduce productivity and create friction.
- **Complex Dependencies:** Developers often lack the tools to assess the security of third-party packages, introducing risks unknowingly.
- **Pressure to Deliver:** Balancing speed with security is challenging when supply chain risks are not addressed upfront.

Broader Challenge: Organizations need a solution that proactively secures the software supply chain without slowing down development, providing visibility, automation, and compliance support in a seamless, developer-friendly way.

WHAT'S REQUIRED:

Key Capabilities for a World-Class Supply Chain Security Solution

To address these challenges, a world-class software supply chain security solution must include:

- **Proactive Malicious Detection:** Ability to identify and block suspicious packages before they enter the pipeline, preventing supply chain attacks.
- **Holistic Visibility:** End-to-end insight into package installations, dependencies, and risks, with robust logging for compliance and audit trails.
- **Contextual Prioritization:** Filtering of packages based on vulnerabilities, malware, licenses, author risks, and engineering factors for comprehensive risk assessment.
- **Seamless Integration:** Integration with CI/CD pipelines (e.g., Jenkins, GitLab) and repositories (e.g., NPM, PyPI, Maven, Artifactory) for rapid deployment and policy enforcement.
- **Developer-Friendly Experience:** Console alerts and notifications that guide developers to compliant package versions without disrupting workflows.
- **Automated Dependency Updates:** Automatic updates to secure package versions, reducing manual remediation and vulnerability risks.
- **Threat Intelligence Integration:** Real-time threat intelligence feeds to stay ahead of emerging threats and block newly identified malicious packages.
- **Customizable Policies:** Flexible policy enforcement to meet unique organizational needs, ensuring compliance and reducing risk.

A ONE-TWO PUNCH:

End to End Supply Chain Security with Veracode Package Firewall and Veracode SCA

In an era of accelerating threats to supply chain security, organizations can no longer afford piecemeal strategies to safeguard their software ecosystems. With the rise in use of AI and third-party repositories to develop code, addressing supply chain risks is an immediate imperative.

Veracode offers a powerful, integrated approach for complete supply chain security, with Package Firewall and Software Composition Analysis (SCA) solutions — a complementary "one-two punch" designed to neutralize supply chain vulnerabilities proactively and comprehensively. Both powerful solutions on their own, but, together, they deliver complete protection against today's most pressing AI, open-source and third-party risks.

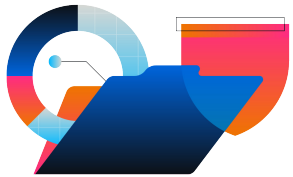
VERACODE PACKAGE FIREWALL:

Real-Time Threat Prevention

Veracode Package Firewall is an advanced security governance solution designed to shield your applications from malicious or untrustworthy packages before they ever enter your environment. By integrating proprietary threat intelligence from the Veracode Threat Research team with industry leading threat detection technology., Veracode Package Firewall ensures that potentially harmful packages are caught before they are consumed by software build pipelines.

How It Works

- **Pre-Release Intelligence:** Monitors open-source package registries (e.g., npm, PyPI) for malicious, hijacked, or misconfigured libraries.
- **Policy Enforcement:** Automatically blocks the download or installation of risky packages that violate organizational policies or are flagged as potential threats.
- **Real-Time Threat Detection:** Quickly identifies anomalies like supply chain attacks, typo-squatting (e.g., “react-moduel” instead of “react-module”), and backdoored dependencies introduced into package repositories.



Key Benefits

- **Proactive Risk Mitigation:** Stops vulnerabilities before they enter an environment.
- **Customizable Policies:** Tailors policies to your organization’s risk appetite and regulatory requirements, such as blocking packages that score below a certain security threshold or lack active maintenance.
- **Real-Time Insights:** Continuously monitor to ensures you’re always up-to-date on new package-related risks.

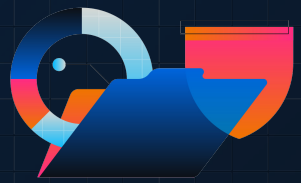
VERACODE SOFTWARE COMPOSITION ANALYSIS (SCA):

Deep Insights into Dependency Risks

Veracode SCA analyzes the entire software dependency tree to identify known vulnerabilities in open-source libraries. It digs deeply into first-party and transitive dependencies, helping organizations uncover risks hidden in their codebases, prioritize critical issues, and remediate them effectively.

How It Works

- **Dependency Mapping:** Automatically maps direct and transitive package dependencies across applications to expose hard-to-find vulnerabilities.
- **Vulnerability Detection:** Leverages comprehensive vulnerability databases, proprietary threat intelligence, and CVE data to pinpoint known issues.
- **Prioritization Capabilities:** Contextual insights help you focus on the vulnerabilities that pose the greatest risks (e.g., exploitable flaws in runtime-critical packages).
- **Automated Remediation Guidance:** Provides actionable steps, such as suggesting updated versions or offering Veracode Fix recommendations to actively patch vulnerabilities.



Key Benefits

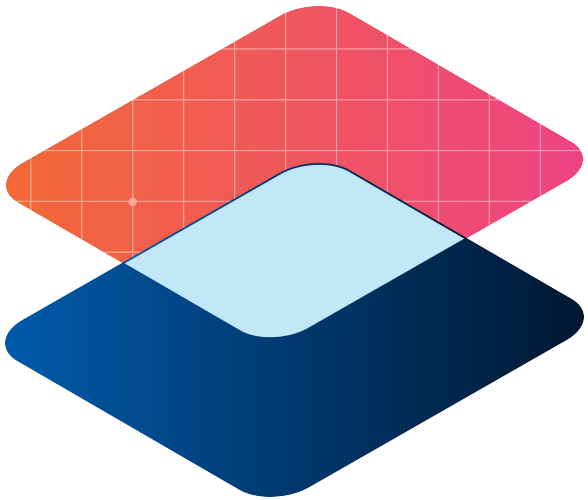
- **End-to-End Visibility:** Tracks risks from code to runtime, giving full transparency into what your software depends on.
- **Enhanced Remediation:** Ensures quick resolution of vulnerabilities using AI-powered fixes or developer-friendly guidance.
- **Compliance Assurance:** Automatically generates audits and reports to satisfy regulations like the **EU's Digital Operational Resilience Act (DORA) or GDPR.**

WHY BOTH TOOLS ARE CRITICAL:

Two Layers of Protection for the Software Supply Chain

While each tool individually strengthens supply chain security, **Veracode Package Firewall and Veracode SCA together form a comprehensive shield.** Here's how they intersect and complement one another:

LAYER 1:



Prevention with Package Firewall

- The first line of defense, preventing malicious and risky packages from entering the environment.
- Ensures developers only have access to trusted libraries by blocking **bad actors at the point of download or installation.**

LAYER 2:

Identification and Remediation with SCA

- Provides **in-depth visibility** into the risk profile of all open-source components already in use, from first-hand dependencies to transitive ones deeply nested in the dependency tree.
- Identifies vulnerabilities or noncompliance issues and helps remediate swiftly with actionable insights.

By combining **upstream prevention** (firewalling malicious packages) with **downstream remediation** (analyzing dependency risks), the two tools address distinct but interconnected aspects of securing the software supply chain.

Why the One-Two Punch Is Essential

Take the example of an organization developing a cloud-native application with dependencies from public registries like npm. Without proactive defenses, a malicious actor could poison a package repository (supply chain attack), spreading malware disguised as a dependency update.

- With the **Veracode Package Firewall**, the malicious package is flagged and blocked **before it can enter** the build environment.
- For existing vulnerabilities already residing in the dependency tree, **Veracode SCA** identifies the issues, precisely pinpoints where they are located, prioritizes them by risk impact, and recommends a path forward to remediate.

Together, these tools ensure **360-degree visibility and protection**, eliminating blind spots in both prevention and remediation workflows.

Challenge	Solution
Malicious Packages Entering Supply Chain	Veracode Package Firewall blocks suspect packages at the point of download.
Unseen Risks in Existing Dependencies	Veracode SCA maps all dependencies (direct and transitive), providing deep visibility into vulnerabilities.
Prioritization of Issues	Veracode SCA contextualizes risks to prioritize the most critical vulnerabilities based on exploitability and impact.
Regulatory or Compliance Gaps	Automatic reporting and compliance tools ensure remediation aligns with frameworks like DORA and GDPR.
Developer Workflows Impacted by Threats	Both tools seamlessly integrate with IDEs and CI/CD tools to minimize disruption while proactively addressing risks.

THE VERACODE ADVANTAGE:

Unified Supply Chain Security

What sets Veracode apart is its unified approach to supply chain security:

- **Proprietary Threat Intelligence:** With Veracode's Threat Research team's expertise integrated into Package Firewall and SCA, Veracode leverages cutting-edge intelligence tuned specifically for evolving supply chain threats.
- **Automation and Simplicity:** Both tools integrate seamlessly into DevOps workflows, ensuring security does not slow innovation. Developers can continue coding, confident that supply chain risks are being monitored in real time.
- **Proven ROI:** By detecting vulnerabilities earlier and remediating faster, Veracode helps organizations reduce **breach risks by 79%**, **save $240,000 on flaws per year**, and free up **2,400 developer hours** per 2,000 vulnerabilities. (based on a commissioned study by Forrester 2024).

Best Practices for Securing Your Software Supply Chain

To effectively secure your software supply chain with Veracode Package Firewall, follow these best practices:

- **Start with Visibility:**
  Use Veracode Package Firewall to log all package installations and gain end-to-end insight into your dependencies.
- **Define Custom Policies:**
  Tailor policies to your organization's needs, such as blocking new packages or enforcing license compliance.
- **Integrate Early:**
  Deploy Veracode Package Firewall in your CI/CD pipeline to enforce policies from the start of development.
- **Leverage Automation:**
  Enable automated dependency updates to reduce manual remediation and keep your pipeline secure.
- **Monitor Continuously:**
  Use logging and threat intelligence feeds to stay ahead of emerging threats and maintain compliance.
- **Educate Developers:**
  Provide console alerts and notifications to guide developers to secure package versions without disrupting their workflow.

CONCLUSION:

Threats to the software supply chain — whether malicious packages or hidden vulnerabilities — are a growing concern, but they do not have to derail development or innovation. With **Veracode Package Firewall and Veracode SCA**, your organization gains:

- A **proactive barrier** that blocks malicious packages before they enter your systems.
- **Deep insights** into what's already in use, enabling precise remediation of dependency risks.

Together, they deliver a powerful **one-two punch** that secures the entire software supply chain, balancing speed and security to enable innovation safely.

Take control of your supply chain security with **Veracode**. Schedule a demo today to see how Package Firewall and SCA work together to protect your organization at every layer.

VERACODE

CONTACT US:

Contact us today to learn more about how Veracode SCA can help you reduce risk and secure your application security. Contact our team at **www.veracode.com** to schedule a demo or request additional information.