SECURE THE SOFTWARE SUPPLY CHAIN:

LAYERED DEFENSE

with Veracode SCA, Package Firewall, Supply Chain Intelligence & Fix for SCA

1 THE OPEN SOURCE EXPLOSION

Open Source is Every-where.

Modern development relies heavily on open-source software (OSS) to accelerate development.

This widespread use of OSS introduces significant security and compliance risks.



USE AI TO GENERATE CODE
82% OF ORGS

COMES FROM 3RD-PARTY CODE
65% OF CRITICAL SEC DEBT

DEPENDENCIES CONTAIN OPEN-SOURCE
62% OF APPS

2 THE HIDDEN DANGERS

Unseen Threats Lurk.

9X INCREASE IN MALICIOUS PACKAGES

Malicious packages have increased dramatically, posing a severe risk to software supply chains.

Many organizations don't thoroughly vet open-source dependencies for security risks. Open-source components can contain known vulnerabilities and license compliance issues.

These vulnerabilities can be exploited in supply chain attacks, leading to data breaches and system compromise.

61% OF APPS HAVE HIGH-RISK FLAWS



THE REMEDIATION BOTTLENECK

Finding vulnerabilities is automated. Fixing them isn't. Manual research, version selection, and testing for every dependency update creates a backlog that grows faster than it shrinks.

THREAT VELOCITY

New malicious packages emerge daily. Reactive, post-incident analysis means learning about threats after the damage is done.

3 SCA: VISIBILITY & CONTROL

Veracode SCA: Find & Prioritize



Veracode Software Composition Analysis (SCA) continuously monitors software and its ecosystem. SCA finds, prioritizes, and tracks vulnerabilities and license compliance risk in open-source libraries. It provides comprehensive visibility across direct and transitive dependencies, different environments, and codebases.

4 PACKAGE FIREWALL: YOUR FIRST LINE OF DEFENSE

Veracode Package Firewall: Block Threats

Veracode Package Firewall secures your software supply chain by vetting open-source components before they're integrated. It prevents malware and non-compliant software from entering your development environment.

Package Firewall offers real-time alerts and comprehensive package visibility. It simplifies governance and enhances security.

Powered by real-time threat intelligence from Veracode's proprietary threat feed, Package Firewall blocks newly identified malicious packages the moment they're discovered.

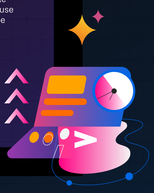


5 VERACODE SOFTWARE SUPPLY CHAIN INTELLIGENCE: STAY AHEAD

Veracode SSCI: Inform

Veracode's proprietary SSCI threat feed delivers real-time, actionable intelligence on emerging supply chain threats — curated by an in-house Threat Research team. Not generic CVE data. Proprietary intelligence that feeds directly into prevention controls.

- Real-time threat feed built by dedicated security researchers
- Actionable insights that block new threats before they reach the pipeline
- Proactive monitoring for compliance and audit readiness





6 VERACODE FIX FOR SCA: AUTOMATED REMEDIATION

Veracode Fix for SCA: Remediate

Finding vulnerabilities is the first step. Fixing them is the bottleneck. Veracode Fix for SCA automates the entire remediation workflow — generating secure, ready-to-merge pull requests for vulnerable open-source dependencies.

- Automated, context-aware fixes that suggest optimal secure library versions
- Contextual analysis evaluates upgrade impact on first-party code to prevent breaking changes
- Ready-to-merge pull requests delivered directly in GitHub and GitLab
- Fixes in minutes, not months — no developer context switching required

7 THE VERACODE ADVANTAGE

Secure Your Supply Chain

Four solutions. One layered defense.

- **Prevent** with Package Firewall — block malicious packages before they enter the pipeline
- **Detect** with SCA — find and prioritize vulnerabilities across direct and transitive dependencies
- **Inform** with Software Supply Chain Intelligence — stay ahead of emerging threats with real-time, proprietary threat intelligence
- **Remediate** with Fix for SCA — automatically generate secure, ready-to-merge pull requests



Together, they enable developers to use open-source software safely and efficiently — improving security posture, ensuring compliance, and reducing the risk of software supply chain attacks.

Source: Veracode 2026 State of Software Security

VERACODE

Ready to secure the software supply chain? Visit www.veracode.com to schedule a demo.