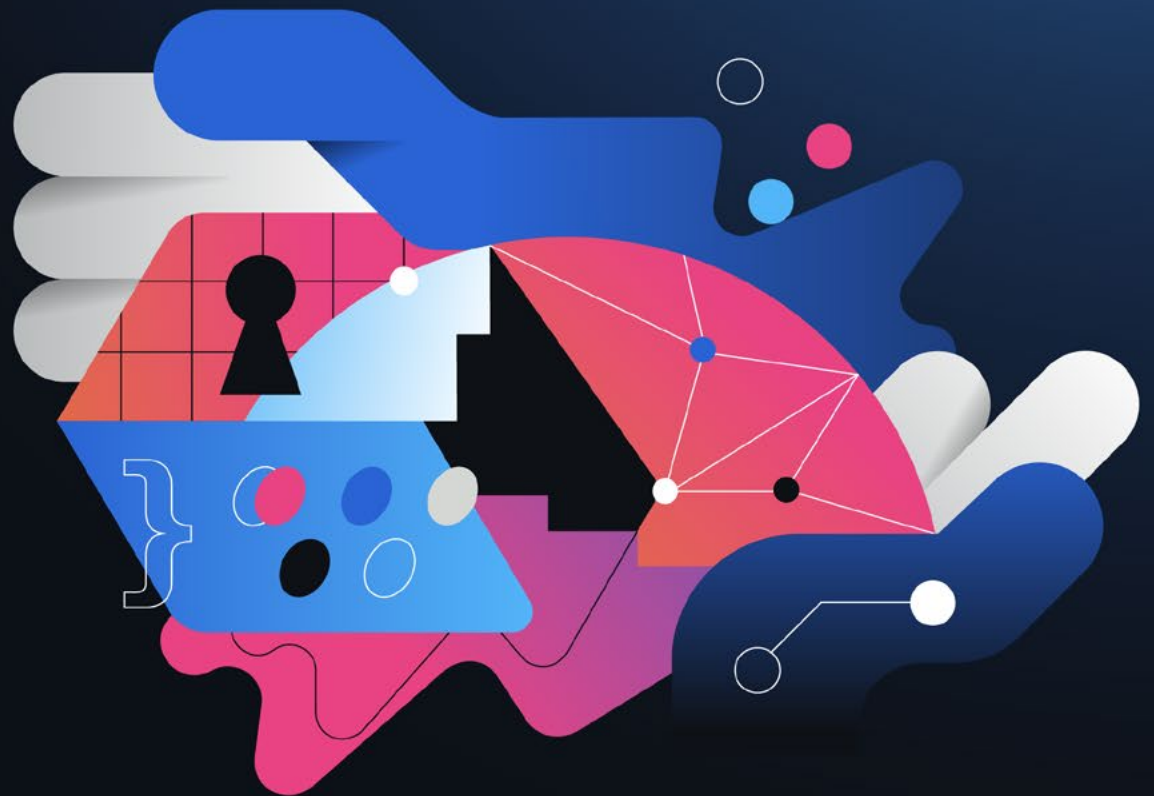


BUYER'S GUIDE

Aligning Application Security with Critical Capabilities_



VERACODE

Contents

- 03 Strategic Blueprint to Manage Application Security
- 04 National Institute of Standards and Technology (NIST) Secure Software Development Framework (SSDF)
- 05 Prepare the Organization (PO)
- 06 Protect the Software (PS)
- 07 Produce Well-Secured Software (PW)
- 08 Respond to Vulnerabilities (RV)
- 09 Conclusion

Strategic Blueprint to Manage Application Security

Organizations are grappling with a complex array of application security challenges, exacerbated by the rapid adoption of generative AI, inconsistent coding standards, and the absence of a cohesive security toolset. With **roughly 63% of applications containing flaws in first-party code and an even higher 70% in third-party components**¹, the landscape is fraught with vulnerabilities. These issues are compounded by the fact that **third-party flaws take 50% longer to fix compared to first-party ones**², leading to significant security debt in **42% of applications**³ – affecting **71% of all organizations**⁴. This underscores the urgent need for integrated and proactive security measures throughout the Software Development Life Cycle (SDLC) to mitigate risks and enhance cyber resilience.

63%

of applications containing flaws in first-party code and an even higher 70% in third-party components.

Third-party flaws take

50%

longer to fix compared to first-party ones...

...leading to significant security debt in

42%

of applications - affecting 71% of all organizations.

As businesses increasingly rely on software applications to drive growth and innovation, it's crucial to adopt a holistic approach to security that spans the entire development process. This guide aims to help enterprise organizations navigate the complex world of Application Security Posture Management (ASPM) and align their application risk management strategies with critical capabilities throughout the Software Development Life Cycle (SDLC).

*1,2,3,4: State of Software Security 2024

<https://www.veracode.com/resources/veracode-state-software-security-2024-public-sector-snapshot>

National Institute of Standards and Technology (NIST) Secure Software Development Framework (SSDF)

To enhance your application security, the NIST Secure Software Development Framework (SSDF) advises four strategic groups aimed at reducing software vulnerabilities, mitigating the impact of potential exploitations of undetected or unaddressed vulnerabilities, and addressing the root causes of vulnerabilities to prevent recurrences.

To effectively manage application security in an the ever-evolving landscape, NIST has finalized SP 800-218A, **Secure Software Development Practices for Generative AI and Dual-Use Foundation Models: An SSDF Community Profile**. This document expands upon SP 800-218 by adding practices, tasks, recommendations, considerations, notes, and informative references that are specific to AI model development throughout the software development life cycle.



Prepare the Organization (PO)_

Ensure that the organization's people, processes, and technology are prepared to perform secure software development at the organization level and, in some cases, for individual development groups or projects.



Protect the Software (PS)_

Protect all components of the software from tampering and unauthorized access.



Produce Well-Secured Software (PW)_

Produce well-secured software with minimal security vulnerabilities in its releases.



Respond to Vulnerabilities (RV)_

Identify residual vulnerabilities in software releases and respond appropriately to address those vulnerabilities and prevent similar vulnerabilities from occurring in the future.



This guide thoroughly explores each ssdf group, explaining their importance and detailing essential capabilities to enhance your application security

Source: Nist, Secure Software Development Framework SSDF, <https://csrc.nist.gov/projects/ssdf>

Prepare the Organization (PO)

Embedding security early in the Software Development Life Cycle (SDLC) is essential for reducing costs and improving security standards. Late-stage testing often results in delays and inefficiencies, while disconnected tools can impede scalability. Veracode addresses these issues by integrating security through its ***fast start and scale*** approach. This enhances visibility through a centralized platform that promotes consistent security practices and efficient knowledge sharing. Comprehensive training resources ensure teams innovate securely while aligning with SSDF guidelines. This strategy not only streamlines security but also demonstrates its adaptability to the evolving demands of software development, providing thorough protection throughout the SDLC.





Key Components	 AppSec Requirement	 Veracode Capabilities
Integrated Security Solutions	Define policies for securing software development infrastructures and their components throughout the SDLC.	Comprehensive security suite including SAST, DAST, SCA , and manual penetration testing , identifying vulnerabilities throughout the SDLC.
Manage Application Security Processes	Track flaws, reviews, and compliance through a single platform.	Central platform for tracking flaws, reviews, and compliance across all Veracode services.
Automated Security Integration	Define policies for maintaining a secure software development infrastructure throughout the SDLC.	Continuous integration with automated scanning during development, ensuring timely detection and remediation of vulnerabilities.
Robust Security Measures	Keep federal data safe, whether in internal applications or vendor systems.	Static analysis ensures proper cryptography implementation and protects against injection attacks in both internal and vendor applications.
IDE Integrations	Write more secure code and proactively address security concerns throughout the SDLC.	Integrated IDE plugins to ensure early detection of flaws for quick and easy remediation of vulnerabilities.
CI/CD (Continuous Integration/Continuous Deployment)	Automate secure development lifecycle practices.	Integrate automated security scanning throughout development and deployment pipeline.
Educate Developers in Secure Coding Practices	Best practices for developing secure code through continuous learning.	Developer enablement offers hands-on labs and eLearning for secure coding practices.
Identify Vulnerabilities	Systematically detect and assess weaknesses.	Implement continuous automated scanning to discover and prioritize security flaws.

Protect the Software (PS)



Integrating robust security measures throughout the Software Development Life Cycle (SDLC) is essential for protecting software from potential security breaches. Veracode utilizes advanced tools to analyze source code and third-party components, identifying and mitigating vulnerabilities early on while providing a holistic view of software security. This approach provides **actionable visibility** enabling developers to quickly address issues and ensure software integrity.



Key Components	 AppSec Requirement	 Veracode Capabilities
Validate All Inputs	Verify and sanitize code written.	Implement rigorous input validation to prevent injection and manipulation attacks.
Identity and Authentication Controls	Implement robust user verification mechanisms.	Integrate secure identity management and multi-factor authentication across applications.
Protect Data	Safeguard information throughout its lifecycle.	Implement encryption, access controls, and secure data handling practices.
Secure Open-Source Libraries	Know when a library contains a flaw, but whether that library is used in such a way that the flaw is easily exploitable.	Vulnerability database for assessing library flaws and their exploitability and criticality.
Release Integrity	Ensure authenticity of software releases.	Implement secure build processes, code signing, and tamper-evident releases.
Custom Roles	Streamline user management and improve security by having control over appropriate access levels.	Custom roles through robust APIs for streamlined user management and improved security access control.

Produce Well-Secured Software (PW)



Securing coding practices in modern software development environments can be challenging, especially when AI-assisted tools introduce similar flaws. Veracode's AI-powered flaw detection capabilities are integrated directly into development tools, enhancing ***real-time flaw remediation***. This integration streamlines the development process by providing immediate feedback to developers and raising security awareness. By reducing friction and delays, Veracode helps to cut the costs, and the efforts needed to address vulnerabilities. This approach leads to a more secure, efficient, and cost-effective Software Development Life Cycle (SDLC), fostering better security practices and minimizing risks in software releases.

Key Components	 AppSec Requirement	 Veracode Capabilities
Verify Third-Party Software Complies with Security Requirements	Assurance that all software components: Open source and commercial are secure.	SCA and IDE/GitHub integrations ensure security compliance of third-party components.
Review and/or Analyze Human-Readable Code to Identify Vulnerabilities and Verify Compliance with Security Requirements	Appropriate controls are built into the SDLC to detect code security flaws.	SAST and integrations detect code security flaws, controlled by AppSec but developer friendly.
Create and Maintain Well-Secured Software Components In-House	Develop internal software components with a high standard of security.	Static and dynamic analysis tools ensure that software developed in-house meets security standards.
Identify Vulnerabilities	Regular reviews and analyses to detect and remediate vulnerabilities early in the development cycle.	Automated code review tools like AI Fix provide immediate feedback and remediation suggestions.
Test Executable Code to Identify Vulnerabilities	Comprehensive testing of executable code to ensure it is free of vulnerabilities before release.	Dynamic analysis and penetration testing tools simulate real-world attacks to identify vulnerabilities.
Continuous Monitoring	Implement mechanisms for ongoing monitoring of running applications for security vulnerabilities.	Real time vulnerability assessment through DAST.
Automated Root Cause Analysis	Systematically identify underlying vulnerability sources.	Implement automated tools to pinpoint and categorize security flaw origins.
Rigorous Implementation of Cryptography Standards	Keep federal data safe, internal applications or vendor systems.	Static analysis ensures correct implementation of cryptography in applications.

Respond to Vulnerabilities (RV)

Inconsistent application security (AppSec) practices and the disruptions caused by addressing vulnerabilities may significantly hinder productivity throughout the Software Development Life Cycle (SDLC). To tackle these vulnerabilities, Veracode integrates Application Security Posture Management (**ASPM**) and an **AI-powered remediation tool** directly into developer environments. This provides real-time find-and-fix capabilities and automates root cause analysis of vulnerabilities. This approach enhances security awareness and streamlines the SDLC by minimizing disruptions and delays. Veracode reduces the costs and time associated with addressing security issues by optimizing feedback loops, ultimately improving both efficiency and the overall security posture of software development.



Key Components	 AppSec Requirement	 Veracode Capabilities
Assess, Prioritize, and Remediate Vulnerabilities	A mechanism to ensure that critical problems are remediated quickly after discovery.	AI Fix ensures quick remediation of critical problems after discovery.
Analyze Vulnerabilities to Identify Their Root Causes	The need to find root causes of issues and fix them. Automating root cause analysis pinpoints the origins of vulnerabilities and misconfigurations, addressing the underlying causes to prevent future occurrences.	Risk Manager's ASPM identifies issues that have been measured against hundreds of factors, contextualized and traced by to their origin and owner.
Identifying Residual Vulnerabilities	Security tools that scan code at various stages of development to detect security flaws and vulnerabilities effectively.	Continuous vulnerability detection using static, dynamic, and software composition analysis throughout development.
Respond to Vulnerabilities	Identify and prioritize vulnerabilities.	Provides reports and guidance on addressing identified vulnerabilities.

True Application Security_

Veracode delivers a comprehensive suite of application security solutions, empowering organizations to proactively identify, manage, and holistically unify and prioritize security issues from code to cloud. With advanced scanning technologies, continuous monitoring, and expert guidance, Veracode ensures that your applications are secure at every stage of the development lifecycle addressing the key components outlined in the NIST Secure Software Development Framework (SSDF).

By leveraging Veracode's integrated application security suite, you can:

- **Embed security early in your SDLC**
- **Streamline vulnerability detection and remediation**
- **Empower developers with real-time feedback and training**
- **Ensure compliance with industry standards and regulations**
- **Continuously monitor and improve your application security posture management**

Decrease your security debt now!
Download The Total Economic Impact™ of the Veracode Application Risk Management Platform, a commissioned study conducted by Forrester Consulting on behalf of Veracode, to see how they a composite organization achieved a 20% increase in revenue by leveraging security as a differentiator, while significantly decreasing risk, increasing productivity, and reaching ROI in less than 6 months.

Secure Your Software Development_

Don't leave your application security to chance. Take the next step in fortifying your software development process by partnering with Veracode. Contact us today for a **personalized demo** and discover how our **Application Risk Management solutions** may help you build more secure applications, reduce risk, and accelerate your development cycles.

Download

Request Demo

