

WHITEPAPER

Secure the SDLC Across DevSecOps



In an era defined by the escalating volume of application security code, increasing development streams, and the expanding complexity of diverse software environments, the rapid adoption of AI-powered software development tools, is further amplifying the attack surface, presenting unprecedented challenges for application security. This includes new vulnerabilities and other risks introduced by AI-generated code, which is underscored by the fact that 82% of developers are using AI tools to write code,¹ and overall, 78% of organizations have adopted AI technologies.²

82% of
developers are
using AI tools to
write code

78%
organizations
have adopted
AI technologies

The traditional approach of patching vulnerabilities at the end of the development cycle is no longer viable. Organizations must embed security throughout the entire Software Development Life Cycle (SDLC). The critical importance of a secure SDLC and the inherent challenges modern organizations face, now compounded by AI's influence, necessitate enabling comprehensive, accurate, and scalable application security across the DevSecOps pipelines.

The Strategic Imperative of a SDLC

The modern enterprise runs on software. From customer-facing applications to internal systems, software underpins every aspect of business operations. The methodologies driving this software creation — Agile, DevOps, and Continuous Integration/Continuous Delivery (CI/CD) — prioritize rapid iteration and frequent releases. While this velocity is crucial for market competitiveness, it has fundamentally reshaped the cybersecurity landscape, making security an intrinsic, rather than an incidental component of software creation. This shift necessitates a proactive and comprehensive approach: the Secure Software Development Lifecycle (SSDLC). A SSDLC integrates security measures and considerations into every phase of the software development process, from initial design and ideation, to coding, to testing, deployment, and ongoing maintenance. This framework moves beyond reactive vulnerability patching to a preventive security-by-design philosophy, ensuring that security is *built in*, not *bolted on*.

Why a Secure SDLC Matters:

- **Expanded Attack Surface:** The proliferation of microservices, third-party libraries, open-source components, and containerized environments significantly broadens the potential entry points for attackers. Each new dependency or service represents a potential vulnerability. Three in ten organizations have more than 96% of critical debt from third party code.³
- **Escalating Cyber Threats:** Cyberattacks are growing in sophistication and frequency. Organizations face constant threats from data breaches, intellectual property theft, and operational disruptions, which can incur millions of dollars in costs annually. In fact, 80% of applications tested have at least one security flaw.⁴
- **Regulatory Demands:** An increasing number of industry regulations and compliance frameworks (e.g., [PCI DSS](#), [GDPR](#), [HIPAA](#), [NIST](#)) mandate robust application security practices, making a demonstrable Secure SDLC essential for avoiding severe penalties.
- **Developer Empowerment:** The *shift-left* movement places more responsibility on developers to address security early. However, these developers often lack the specialized security knowledge and resources to effectively integrate security testing across the SDLC.

- **Balancing Velocity and Security:** While developers are under immense pressure to deliver software rapidly, application security teams are tasked with ensuring that software is secure before it reaches production. This creates a significant challenge, as the constant demand for speed often comes at the expense of security. In fact, 80% of developers reported feeling some level of burnout due to high workload and tight deadlines.⁵ This intense pressure means that for many organizations security simply cannot keep pace with development velocity, resulting in 50% of organizations admitting that they carry critical security debt.⁶ Thus, the need for accuracy and comprehensive coverage without compromising quality.

The primary objective of a Secure SDLC is to proactively identify, assess, and remediate security vulnerabilities throughout the development pipeline. By doing so, organizations can significantly reduce the risk of critical flaws reaching production, thereby minimizing the financial, reputational, and operational impact of a breach.

Navigating the Complexities of Modern AppSec



Despite the clear imperative, implementing an effective Secure SDLC presents significant challenges for many organizations. The complexities of modern application software development environments often create bottlenecks and expose organizations to persistent risks. Additionally, many stakeholders from across the organization tend to be involved in the decision-making processes for application security, presenting many opportunities for frustration and organizational friction. This underscores the importance of ensuring consistent tooling and ensuring that findings can be identified and either prevented or remediated as early as possible.

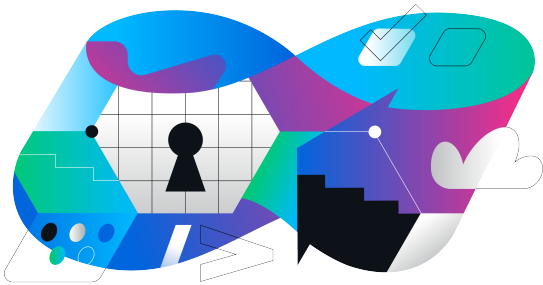
Key Challenges in Application Security

- **Fragmented Tooling:** Many organizations rely on a patchwork of disparate security tools for different testing types (Static Analysis Testing, Dynamic Analysis Testing, Software Composition Analysis). This leads to manual correlation of findings, inconsistent data, delayed remediation, and an incomplete, fragmented view of overall application risk. Seventy percent of businesses say their companies have more than 10-point solutions in their security stack, with 26% admitting that they have more than 30.⁷
- **Security Debt:** The velocity of development often outpaces security remediation. New flaws are introduced faster than existing ones can be fixed, resulting in a growing backlog of vulnerabilities known as security debt. This debt slows down software delivery and increases operational risk. Alarming, 74% of organizations have security debt.⁸
- **Balancing Speed and Security:** Development teams are under immense pressure to deliver features rapidly. Integrating security without impeding velocity is a constant balancing act, often leading to security being perceived as a barrier rather than an enabler.
- **Evolving AI:** The emergence of new technologies, such as AI-generated code and increasingly complex software supply chains, introduces novel vulnerabilities and other supply chain related risks that traditional security approaches are unable to adequately address.
- **Lack of Unified Risk Visibility:** Without a centralized platform, security and development teams lack a single source of truth for understanding application risks across their entire software portfolio, making informed decision-making difficult. This fragmented view directly contributes to security debt and inefficient remediation processes.

The DevSecOps Opportunity: Automating Security for Velocity

The solution to these challenges lies in DevSecOps – the integration of security practices and tools directly into the DevOps pipeline. DevSecOps transforms security from a separate, reactive phase into a continuous, automated, and collaborative effort across development, security, and operations teams. This approach ensures security is embedded from code to cloud and empowers teams to write more secure code from the start, ensuring continuous risk mitigation and building applications securely.

A Unified, Intelligent, and Comprehensive Platform with Veracode



Veracode operates at the forefront of the [Application Security Risk Management](#) market, providing an innovative, cloud-native, and AI-assisted platform that directly addresses the challenges outlined above. Unlike fragmented point solutions, Veracode offers a unified, comprehensive approach to application security, integrating seamlessly across the [SDLC](#) to deliver continuous visibility, intelligent prioritization, and accelerated remediation. This unified approach provides a single source of truth, eliminating the need for manual correlation and bridging the communication gap between security and development teams.

Unmatched Depth of Analysis and Comprehensive Thoroughness

[Veracode's Static Application Security Testing](#) (SAST) solution provides unparalleled accuracy and coverage, ensuring no critical flaws are missed. As an intelligent software security core, Veracode SAST proactively prevents and identifies flaws through advanced source to sink analysis. This comprehensive coverage spans over 30 languages and 100 frameworks, offering a remarkably low false positive rate, which can be configured to optimize speed and accuracy across the SDLC. Veracode's unique scanning approach lies in its ability to provide findings quickly, with the quality, coverage and comprehensiveness organizations need. Veracode SAST produces more accurate testing results, leading to fewer false positives, allowing development and security teams to focus on remediation rather than sifting through non-threats.

Comprehensive Runtime Vulnerability Detection

Complementary [Dynamic Application Security Testing](#) (DAST) provides deep insights into runtime vulnerabilities, offering a complete and actionable picture of security risks from code to cloud. This commitment to deep, accurate analysis means comprehensive feedback for developers, allowing them to identify and fix issues early in their workflow within their IDEs, contributing to fewer vulnerabilities in production aligning to software security maturity models. Veracode DAST can scan web applications in both authenticated and unauthenticated states, and behind your firewall, providing broad coverage for various application types. It offers flexible scanning options, including scheduled, on-demand, and continuous scans, making it adaptable to different development workflows and security needs. Furthermore, Veracode DAST offers advanced scanning capabilities like API discovery and testing, ensuring comprehensive coverage for modern applications built on APIs.

Veracode also extends its risk coverage with [External Attack Surface Management](#) (EASM) integrated with Veracode DAST. EASM proactively scans an organization's entire digital footprint, including internet-facing assets, to discover, classify, and prioritize unknown or unmanaged risks. By providing complete visibility into the external attack surface and enabling risk-based prioritization, EASM helps minimize potential entry points for attackers. While DAST focuses on runtime vulnerabilities within known applications, EASM complements this by identifying and monitoring all external assets, reducing visibility gaps across an organization's digital presence.

Bridging Security and Development

Crucially, Veracode provides actionable insights and a shared platform for managing findings, helping to bridge the common communication and workflow gap between security teams and developers. Veracode's platform enables security teams to effectively guide developers, enforce consistent policies, and foster a shared understanding of risk across their entire application portfolio. This directly supports the [OWASP Software Assurance Maturity Model \(SAMM\)](#), a framework that helps organizations formulate and implement a strategy for software security tailored to their specific risks.

Veracode's SDLC approach directly correlates and supports multiple SAMM business functions. Veracode's powerful Static Application Security Testing (SAST) for proactive flaw identification significantly strengthens SAMM's [Implementation](#) function by empowering developers to find and fix issues early in the coding phase. Complementary Dynamic Application Security Testing (DAST) provides deep insights into runtime vulnerabilities, aligning with SAMM's [Verification](#) function by testing the security of running applications. Furthermore, External Attack Surface Management (EASM) bolsters SAMM's [Operations](#) function, proactively managing the external digital footprint to discover and mitigate unknown or unmanaged risks before they can be exploited. This comprehensive suite provides unified visibility and robust policy enforcement across all applications, ensuring end-to-end risk coverage across the SDLC and beyond.



Proactive Software Supply Chain Defense

The increasing reliance on open-source components and containerized environments introduces significant risk. Veracode directly tackles this with robust offerings that enable organizations to advance their [Secure Supply Chain Consumption Framework \(S2C2F\)](#) maturity. S2C2F is a framework for managing the risks associated with consuming software components from external suppliers, with increasing levels of maturity from basic governance to proactive malware analysis.

Open-Source Governance

[Veracode Software Composition Analysis \(SCA\)](#) continuously monitors open-source components for known vulnerabilities (CVEs) and license risks throughout the SDLC, supporting standard formats like CycloneDX and SPDX for Software Bill of Materials (SBOM) creation. For compliance officers and enterprise security teams, this provides smarter foundational visibility, helping meet S2C2F Level 1 ([Minimum OSS Governance](#)) requirements by maintaining a comprehensive inventory and scanning for known risks. Furthermore, incorporating [Veracode Container Security](#) ensures container images are free of vulnerabilities and misconfigurations at every stage, safeguarding cloud-native deployments by performing SCA-style scans on container components. This helps identify and address open-source vulnerabilities within your containerized applications, just as you would with traditional software. As organizations progress to S2C2F Level 2 ([Strong OSS Governance](#)), SCA helps developers and DevSecOps leaders shift further left by providing vulnerability information directly within IDEs and CI/CD pipelines, enabling faster and more informed decisions about dependencies.

Advanced Supply Chain Threat Defense

To address the most sophisticated supply chain threats and reach S2C2F Level 3 ([Proactive Security Review and Malware Analysis](#)), [Veracode Package Firewall](#) (VPF) proactively detects and blocks malicious packages with up to 60% greater accuracy than competitors. This capability is crucial for identifying and neutralizing suspicious packages before they enter the development pipeline, building a safer and more resilient supply chain for CISOs and security teams. For developers and DevSecOps leaders, VPF extends the shift-left approach even further by preventing compromised or risky packages from ever being introduced into their environments. This means fewer security issues surfacing later in the development cycle, reducing rework, accelerating release cycles, and allowing teams to build with greater confidence and agility, ultimately streamlining DevSecOps workflows. VPF's precision in blocking malicious packages is a key differentiator, offering superior protection against advanced supply chain attacks.

60%
greater accuracy
in detecting and
blocking malicious
packages

Addressing Threats from the Most Sophisticated Adversaries

Achieving S2C2F Level 4 ([Addressing threats from the most sophisticated adversaries](#)) demands advanced, adaptive threat intelligence to counter sophisticated adversaries. [Veracode Software Supply Chain Intelligence](#) (SSCI) delivers real-time, high-fidelity threat intelligence, proactively detecting emerging and stealthy attacks. Its Core Tier enables malicious packages to be identified and blocked, while the Pro Tier extends this with comprehensive reputation data across five critical risk domains (Vulnerabilities, License & Compliance, Engineering, Author & Contributor, and Malicious Behavior Indicators), curated by the expert Veracode Threat Research team. This enables swift action for SOC and Threat Hunt teams and streamlines security workflows for AppSec, solidifying an organization's S2C2F Level 4 posture against the most advanced threats.

Intelligent Remediation and Risk Management at Scale

Veracode significantly reduces security debt and optimizes remediation efforts through intelligent automation and unified visibility, enhancing the [Implementation](#) and [Governance](#) functions of OWASP SAMM.

AI-Driven Remediation

[Veracode Fix](#), an AI-driven tool, trained on proprietary data, creates clean, expert-designed code fixes that developers can apply directly in their IDE or CI/CD pipelines. This dramatically reduces the work and time needed to remediate flaws, enabling secure coding and directly improving the [Implementation](#) function of OWASP SAMM. For DevSecOps leaders, this accelerated remediation means maintaining high development velocity without compromising security. [A commissioned study conducted by Forrester on behalf of Veracode](#) has shown that Veracode Fix customers achieve a 92% faster mean time to remediate security flaws and 200% reduction in time detecting flaws.

**Veracode Fix customers
achieve a 92% faster
mean time to remediate
security flaws**


Unified Risk Management and Prioritization

To manage the overwhelming volume of findings, [Veracode Risk Manager](#) is a tool-neutral platform that unifies findings from all sources (SAST, DAST, SCA, Container, etc.), automates investigation and prioritization, links issues to their root cause and owner, and provides Next Best Actions™ to eliminate the most risk with the least effort. This provides smarter prioritization and unified insights for enterprise security teams and CISOs, allowing them to efficiently reduce security debt and gain comprehensive visibility as per the [Governance](#) function of OWASP SAMM.

The Six Essential Steps to Secure the SDLC

Veracode's industry experience, outlined in the *Secure Your SDLC in 6 Steps* framework, identifies the critical components of a successful Secure SDLC:

1. **Discover and Assess Risks:** Identify all applications, their owners, open-source dependencies, AI usage, and associated risk levels to establish a baseline.⁷
2. **Establish Prevention Methods:** Implement security controls early in the SDLC. Use appropriate testing tools, continuously monitor open-source libraries and third party components and use AI-assisted remediation tools. Unify and prioritize findings across all sources.
3. **Onboard and Scale Apps:** Integrate automated security scans into the development process and continuously scan applications to establish a security posture baseline.
4. **Set Policies:** Define clear security policies based on risk tolerance, regulatory requirements, and application criticality, enforcing them through technical controls in CI/CD.
5. **Prioritize and Address Findings:** Categorize and resolve policy-violating flaws efficiently through remediation or mitigation, focusing on critical security debt.
6. **Leverage Reporting and Analytics:** Use unified reporting systems to track progress, identify areas for improvement, set goals, and demonstrate compliance to stakeholders.



By addressing these steps systematically, organizations can optimize the developer experience through automation, build a culture of security awareness, and reduce risk across their entire software supply chain.

Veracode's Unrivaled Leadership

Securing the SDLC is an ongoing process that demands continuous effort and adaptation. Veracode is a global leader in [Application Risk Management](#). Powered by trillions of lines of code scans and its proprietary AI-assisted remediation solution, the [Veracode platform](#) is trusted by organizations worldwide to build and maintain secure software from code creation to cloud deployment.

Thousands of the world's leading development and security teams leverage Veracode every second of every day to gain accurate, actionable visibility of exploitable risk, achieve real-time vulnerability remediation, and reduce their security debt at scale. [A commissioned study conducted by Forrester on behalf of Veracode](#) reveals a return on investment of 184% to customers over a three-year period.

By integrating Veracode Fix, Static Application Security Testing, Dynamic Application Security Testing, Software Composition Analysis, Package Firewall, Risk Manager, Container Security, and more, Veracode provides a comprehensive, unified solution that ensures your software is built and deployed safely, protecting sensitive data, and helping you stay ahead of potential cyber threats.

Veracode doesn't just offer tools; it provides a strategic partnership in transforming your SDLC into a truly secure and efficient DevSecOps powerhouse.

Ready to accelerate your secure development and build software with confidence?

Request a Demo of Veracode today. Visit www.veracode.com

Sources:

1. Jordana A., Hostinger, "How many companies use AI in 2025?", May 2025.
2. Stack overflow, 2024 Developer Survey, AI.
- 3,4. Veracode 2025 State of Software Security Report.
5. Alex Vasylenko, The Frontend Company, "60+ Frontend Development Statistics in 2025: Trends and Insights," May 2025
6. Veracode 2025 State of Software Security Report.
7. 2025 Cisco Cybersecurity Readiness Index
8. Veracode 2025 State of Software Security Report.

The Veracode logo, featuring a stylized 'V' in blue and white, followed by the word 'ERACODE' in white capital letters.

Learn more at

www.veracode.com

