VERACODE

WHITEPAPER

Secure Your Future With a Compliance-First AppSec Posture

Compliance-First AppSec Posture

In the age of software-defined business, compliance is no longer a checklist; it's the bedrock of market trust and the key measure of risk management maturity. However, the confluence of rapid development, complex global mandates (GDPR, EU CRA, SEC rules), and a vulnerable software supply chain has pushed traditional AppSec approaches past their breaking point. Fragmentation, tool sprawl, and late-stage security checks at the end of the Software Development Lifecycle (SDLC) helps to guarantee rising costs and catastrophic risk.

The solution to compliance is not more tools, but a unified Application Risk Management Platform that transforms compliance from a reactive burden into a proactive, automated, and strategic function. Veracode supports a Compliance-First AppSec Strategy. Let's dive into the critical failures of the status quo and how the right platform is the path to achieve AppSec posture compliance, delivering verifiable risk reduction and a proven 184% ROI.

The Compliance Crisis: The Broken Status Quo

78%

of applications contain at least one security flaw.

The modern regulatory landscape demands that organizations maintain total control over the software creation process. Yet, security leaders are fighting an unwinnable battle with fragmented tools, delayed enforcement, and compounding technical debt.

The Financial and Operational Toll

The cost of inaction is staggering, confirming that security debt is the most expensive debt an organization can accrue

- **The Cost of Non-Compliance:** The average cost of a data breach has reached $4.88 million[1], a figure amplified when non-compliance is a factor.
- **The Time Bomb:** An overwhelming 78% of applications contain at least one security flaw[2]. Compounding this risk, the average time to fix a flaw increased by 47% in five years, rising to 252 days[3] leaving critical vulnerabilities exposed for over eight months.
- **The Fragmented Failure:** 76% of CISOs report that tool sprawl and the fragmentation of regulations greatly affect their ability to maintain compliance, leading to paralysis and audit anxiety[4].

The Late-Stage Security Check

The traditional compliance approach is fundamentally broken because it treats security as a reactive, costly checkpoint at the end of the SDLC. This fragmented, late-stage method fails to keep pace with modern DevSecOps speed; on average, only 54% of major code changes undergo a full security review before deployment[5].

To overcome this fatal flaw, security cannot be a final check; it must be a continuous, policy-driven mandate.

The Veracode SAST Policy Scanner

Veracode sets itself apart with its unique SAST Policy Scanner, which enforces rigorous custom policy rules directly to the code analysis process. This is not merely a post-scan compliance check; it is a fundamental part of the security assessment:

- **Internal Risk Categorization:** The scanner utilizes a policy framework that is rigorously developed based on an internal risk categorization, a fundamental aspect of security policy creation and implementation.
- **Policy Mapping:** Findings are assessed according to the risk they pose to the application, which is mapped directly to profiles on the Veracode platform. This ensures a consistent and effective evaluation of vulnerabilities.
- **Enforcement at the Source:** By embedding policy enforcement during the static scan, the SAST Policy Scanner ensures a high standard of security is maintained early in the software lifecycle, enabling organizations to define and enforce acceptable security debt thresholds before code is merged or deployed.

The Strategic Imperative: Securing the SDLC for Compliance

Given the profound failures of the late-stage, manual security model and the necessity of policy-driven gates like the SAST Policy Scanner, a paradigm shift is necessary. The methodologies driving modern software creation — Agile, DevOps, and Continuous Integration-Continuous Delivery (CI/CD) — demand security integration at the same pace as development velocity. This is especially critical as 84% of developers are using AI tools to write code[6], further amplifying the attack surface.

The solution is a **Secure Software Development Lifecycle (SSDLC)**. This framework integrates security measures into every phase of the process — from design to deployment — moving beyond reactive patching to a preventive security-by-design philosophy, ensuring that security is built in, not bolted on.

Compliance as a Built-In Quality

Regulatory compliance (mandates like **PCI DSS**, **GDPR**, **HIPAA**, etc.) requires a demonstrable, continuous security practice throughout the SDLC. Veracode enables this compliance mandate by adopting a "shift-left" posture through unified tooling.

Deep Defense: Static Application Security Testing (SAST)

Static Analysis is fundamental to securing the SDLC, examining source code and binaries to identify security flaws without executing the application. **Veracode SAST** is engineered for developer speed and accuracy, integrating natively into development environments (IDEs), CI/CD pipelines, and bug trackers. This deep integration allows developers to execute fast scans and receive prioritized, actionable findings right where they work.

Runtime Validation: Dynamic Application Security Testing (DAST)

Generic DAST solutions offer a basic runtime view, but **Veracode Dynamic Analysis** provides a complete, actionable, and verifiable picture of security risks from code to cloud, specializing in modern applications and complex authentication methods. DAST validates the security posture of running applications by simulating real-world attacks, ensuring critical runtime controls meet mandates like **PCI DSS** and **HIPAA**. Veracode DAST ensures end-to-end security by testing the application as an attacker sees it and validates policy enforcement in deployed, live environments.

Continuous Visibility: External Attack Surface Management (EASM)

External Attack Surface Management (EASM), integrated with Veracode DAST, proactively scans an organization's entire digital footprint, including internet-facing assets, to discover, classify, and prioritize unknown or unmanaged risks. EASM complements DAST by identifying and monitoring all external assets, eliminating "Shadow IT" and unknown assets to close regulatory gaps across an organization's digital presence.

Deployment Control: Seamless Integration

To maintain velocity while ensuring compliance, security must be automated directly into the build and deploy process. Security policies are enforced by integrating checkpoints directly into CI/CD pipelines. **Veracode's unified platform** provides the necessary APIs, plugins, and custom tooling to integrate comprehensive policy enforcement directly into continuous delivery workflows. This ensures that the combined results from all Veracode analysis (**SAST**, **DAST**, **SCA**) are leveraged at the critical moment of deployment. This deep integration ensures security policies are enforced consistently and automatically across all teams and projects, providing a verifiable compliance step at every stage of the release process.

The complexity of modern AppSec compounded by tool sprawl and resulting security debt (cited by 82% of organizations[7]) necessitates a unified, programmatic approach. The integration of Veracode's comprehensive tooling — from Deep Defense (SAST) to Deployment Control — is the strategic mechanism for embedding security throughout the entire development lifecycle. This unified platform directly supports the **Six Essential Steps to Secure the SDLC**, ensuring a continuous, integrated process that meets the dual demands of developer velocity and regulatory scrutiny.

Intelligent Remediation: Veracode Fix and AI-Guided Security

Identifying security weaknesses is only half the battle; the true measure of an effective application security program lies in the ability to fix them efficiently and for decades, the final, most expensive bottleneck in compliance has been the manual remediation of flaws. Security teams identify vulnerabilities, but developers lack the time and guidance to fix them quickly, leading to massive security debt and persistent compliance failures (an average MTTR of 243 days[8]).

Veracode transforms this bottleneck into a source of competitive advantage through intelligent, AI-guided remediation.

AI-Powered 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 drastically accelerates the Mean Time to Remediate (MTTR) by eliminating the friction between identifying a flaw and fixing it securely.

- **Quantified Compliance Velocity:** A commissioned study conducted by Forrester on behalf of Veracode confirms that Veracode Fix customers achieve a 92% faster mean time to remediate security flaws and a 200% reduction in time detecting flaws.
- **Targeted Remediation Guidance:** Veracode Fix offers specific code suggestions, allowing developers to review and apply expert-designed fixes quickly.
- **Performance:** Leading customers fix half of their flaws in just five weeks, compared to the industry average of five months[3]. This rapid flaw closure is the key differentiator between compliance laggards and leaders.

This dedicated focus on AI-powered fixes ensures that teams can achieve real-time vulnerability remediation and reduce their security debt at scale, a capability that is distinct from the Platform's general policy and governance features.

Achieve a 92%
Faster MTTR.

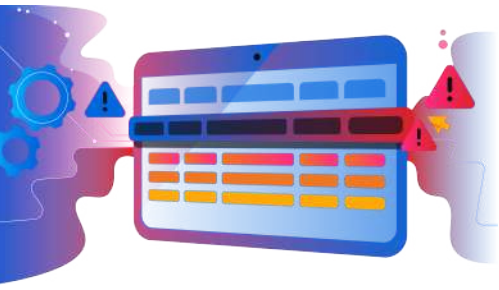
Compliance, Governance, and Risk Management

To achieve full compliance, security leaders must move beyond simply finding flaws and focus on proving that security policies are consistently enforced, risks are properly prioritized, and governance is centralized. The individual tools discussed above (SAST, DAST, Fix) are powerful, but their effectiveness relies on a unified, strategic platform to manage policy and risk at scale.

The Veracode Platform delivers:

- **Policy Compliance Overview Dashboard:** This pre-built dashboard provides a comprehensive, executive-level view of application compliance with organizational and regulatory policies. Security leaders can immediately see which applications are in compliance and which are not, filtering data by business unit, team, or publish date. This capability is crucial for demonstrating adherence to standards like GDPR, HIPAA, and industry-specific requirements.
- **Centralized Governance:** The platform replaces the chaos of fragmentation by centralizing governance and automating enforcement across all scanning types (SAST, DAST, SCA). This allows security teams to create a single source of truth for security policies.
- **Intelligent Risk Prioritization:** Veracode Risk Manager consolidates findings from multiple security tools, normalizing and deduplicating data to provide a clear, unified view of risk. By leveraging contextual analysis, the platform prioritizes vulnerabilities based on asset criticality, business impact, and environmental factors.
- **Verifiable Metrics:** The platform offers advanced dashboards and data visualizations through Veracode Analytics, enabling organizations to measure, report, and optimize their AppSec programs. This verifiable data is essential for regulatory audits and stakeholder confidence.

Veracode Risk Manager Unifies Findings and Proves Compliance



Policy enforcement ensures developers meet compliance gates, but security leaders require actionable intelligence to guide remediation efforts across the entire application portfolio.

To manage the overwhelming volume of findings, Veracode Risk Manager is a tool-neutral platform that unifies findings from all analysis types unifying risk insight and providing prioritization of risk.

- **Intelligent Risk Prioritization:** Risk Manager unifies findings from all scanning types (SAST, DAST, SCA) and provides Next Best Actions™ to guide teams in eliminating the most risk with the least effort. This intelligent prioritization ensures that remediation efforts are both efficient and effective, focusing resources where they matter most for compliance and risk reduction.

- **Audit Readiness and Policy Mapping:** This capability fundamentally connects application security findings to external regulatory requirements. It directly answers the auditor's key question: *How does a customer fare against either policy based on findings and controls?*
  - **Evidence Collection: Risk Manager** systematically collects technical evidence (the raw security findings) and maps it against defined security controls and policies (like **SOC 2**, **ISO 27001**, or industry-specific standards).
  - **Control Sufficiency Assessment:** By correlating the severity and presence of application flaws with the required controls of a given standard, the platform provides a clear status on whether the customer's existing security practices and controls are sufficient to meet the standard's requirements. This visibility is vital for major compliance and audit needs, which often rely on connectors to AST products to gather this evidence for the final compliance report.
- **Executive Compliance View:** Through tailored views, **Risk Manager** allows security leaders to immediately see which applications are in compliance and which are not based on real-time scan data, filtering by business unit, team, or publish date. This capability is crucial for demonstrating adherence to standards like **GDPR**, **HIPAA**, and emerging mandates.

Mastering the Attack Surface: The Software Supply Chain

Even with addressing the internal development process and establishing governance, the majority of compliance risk is inherited, not generated internally. Modern applications are built, not written, relying heavily on third-party components and Veracode testing shows that 66% of an organization's critical security debt (high-severity, high-exploitability flaws[10]) stems directly from this third-party code.

70%
of critical debt stems from third party code.

Effectively securing the **SDLC** for compliance must therefore extend beyond the application layer to mastering the entire **Software Supply Chain** — a regulatory imperative driven by the **EU CRA** and **SEC** rules.

Proactive Supply Chain Mastery

Veracode provides unparalleled visibility and proactive control over all code — proprietary, third-party, and open-source — producing (and securing) the entire Software Bill of Materials (SBOM).

Software Composition Analysis (SCA): Generating Verifiable SBOM

Veracode SCA protects the integrity of your **software supply chain** by generating a verifiable Software Bill of Materials (SBOM) in a compliant format and identifying risks in third-party libraries. To ensure that supply chain security does not slow down innovation, **Veracode SCA** is built with the same developer-first philosophy as our SAST engine. It integrates natively into IDEs, CI/CD pipelines, and bug trackers, allowing developers to manage open-source risk within their existing workflows.

A key differentiator is Veracode's Vulnerable Method Analysis (Reachability Analysis). This advanced technology pinpoints whether a vulnerable open-source function is actually called by your application, drastically reducing noise by filtering out vulnerabilities that are present but not exploitable. By prioritizing these reachable, high-risk flaws and providing automated remediation paths, Veracode accelerates the Mean Time to Remediate (MTTR) in a way that's focused on reducing real risk. This is essential for meeting strict regulatory deadlines and proving a verifiable, reduced risk posture for continuous compliance.

Proactive Component Defense: Veracode Package Firewall

Veracode Package Firewall (VPF) eliminates inherited risk by enforcing security policies before code enters the build pipeline. It acts as a mandatory gate, ensuring only approved, policy-compliant components are used. Crucially, it proactively detects and blocks malicious open-source packages, eliminating a major entry point for supply chain attacks and regulatory failure. This proactive defense serves as a mandatory security control that directly addresses regulatory demands for supply chain integrity, creating an automated, documented control point that provides auditors with an irrefutable audit trail.

Upstream Governance: Veracode Software Supply Chain Intelligence (SSCI)

Veracode Software Supply Chain Intelligence (SSCI) provides the upstream governance needed for truly secure component usage. By offering deep, actionable insights into open-source risk, SSCI helps developers select secure components from the outset, dramatically reducing future remediation costs and security debt.

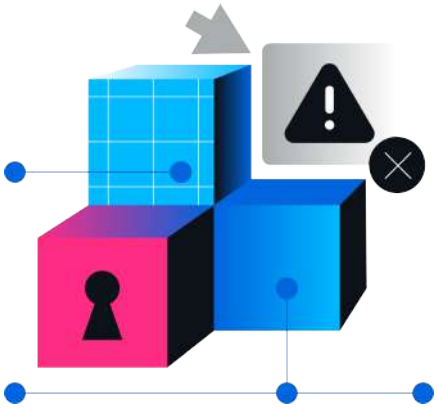
How Veracode Supports Regulatory Compliance Frameworks

PCI DSS: Automated Security Testing for Continuous Compliance

The Payment Card Industry Data Security Standard (PCI DSS) 4.0 mandates rigorous application security testing throughout the software development lifecycle. Veracode's Application Risk Management Platform is engineered to directly satisfy these critical mandates through policy-driven enforcement:

- Requirement 6.2 **(Bespoke Software Integrity)**: Veracode automates pre-release code reviews to identify and remediate vulnerabilities — such as injection attacks, business logic abuse (XSS/CSRF), and access control flaws — ensuring all custom software adheres to secure coding guidelines before deployment.
- Requirement 6.4.1 **(Public-Facing Application Security):** The platform facilitates the mandatory annual vulnerability assessments of web-facing applications. By combining expert-led analysis with automated scanning, Veracode ensures all vulnerabilities are ranked and corrected after significant changes or at least every 12 months.
- Requirement 11.4.1 **(Multi-Layer Penetration Testing):** Veracode supports a documented penetration testing methodology, providing the deep application-layer analysis required to identify complex vulnerabilities that automated tools alone might miss.

Organizations adopting the PCI Software Security Framework (PCI-SSF) benefit from Veracode's integrated approach combining Static Analysis for code review, Dynamic Analysis for runtime vulnerability assessments, and Software Composition Analysis (SCA) for supply chain security. By utilizing pre-configured PCI policies, the platform automatically enforces vulnerability ranking, remediation workflows, and grace periods. This transforms manual compliance exercises into a continuous, automated process that generates audit-ready reports and provides the actionable guidance necessary to maintain a defensible security posture. Learn more about Veracode PCI Compliance.



ISO 27001/27002: Evidence-Based ISMS Implementation

Achieving ISO 27001 certification requires documented evidence of security controls aligned with Annex A objectives and ISO 27002 guidance. Veracode provides automated assessments to implement and maintain an effective Information Security Management System (ISMS). Detailed reporting and mapping to ISO control requirements enable organizations to demonstrate compliance with both high-level and detailed standards.

Read this customer story on how Veracode helped to achieve ISO 27001 certification.

NIST Frameworks: Federal-Grade Security

Veracode supports compliance with a broad range of NIST Special Publications — particularly NIST SP 800-218, the Secure Software Development Framework (SSDF) — by prioritizing secure code construction through automated tools and continuous vulnerability testing. This foundation extends to NIST Special Publications 800-53 and 800-37, providing federal-grade security for both public and private sectors. NIST SP 800-53 focuses on selecting and implementing security controls, while SP 800-37 emphasizes integrating these controls into the system development lifecycle through the Risk Management Framework (RMF). By embedding security controls and automated vulnerability detection directly into the development lifecycle, Veracode enables organizations to operationalize NIST requirements on a continuous basis — transforming compliance from a manual audit exercise into an actively enforced, data-driven security posture backed by definitive scan evidence. Discover NIST compliance capabilities.

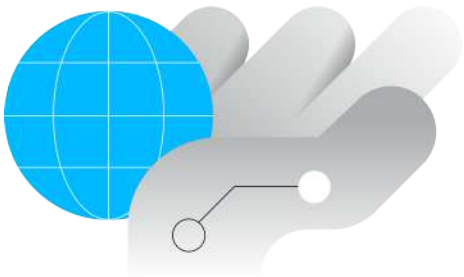
FedRAMP Moderate: Federal Authorization for Enterprise Confidence

In March 2022, Veracode received FedRAMP Moderate Authority to Operate (ATO), affirming that the company's cloud-based application security platform meets the comprehensive security and risk management requirements of the Federal Risk and Authorization Management Program. As a FedRAMP authorized SaaS service for Static Analysis, Dynamic Analysis and Software Composition Analysis, Veracode provides a vetted environment that implements over 300 NIST SP 800-53 Rev. 5 security controls and passage of an independent third-party assessment. Our FedRAMP compliance helps organizations meet federal security standards and requirements, providing the assurance needed for secure application development in regulated environments. For comprehensive details on our security practices and compliance certifications, visit the Veracode Trust Center.

SOC 2 Type II:
Operational Excellence in Security and Privacy

Veracode's SOC 2 Type II attestation demonstrates the operational effectiveness of its security controls over an extended period. Veracode enables customers to document their own SOC 2 internal controls by providing automated assessments and detailed evidence of the design and operating effectiveness of their security environment. Through the **Veracode Platform**, organizations can access the granular reporting necessary to satisfy auditor requests, transforming the labor-intensive evidence-gathering process into a streamlined, audit-ready workflow. This independent validation provides customers with transparent evidence that their sensitive data is protected by enterprise-grade controls. Visit the **Veracode Trust Center** to learn more.

Data Privacy and Global Compliance: Meeting Evolving Requirements



Veracode supports organizations in addressing data privacy and security obligations such as **GDPR**, **HIPAA**, and **CCPA** by providing application security testing, compliance reporting, and risk based remediation capabilities. Through secure software development practices, integrated vulnerability assessment, and reporting automation, Veracode helps customers strengthen their security posture and demonstrates alignment with aspects of global data protection laws. Built-in privacy-oriented controls and processes help customers embed security into development lifecycles, supporting their own privacy compliance efforts. Learn more about our **polices and reporting** capabilities.

Strengthening Digital Operational Resilience under DORA

The **Digital Operational Resilience Act (DORA)** is a regulation introduced by the European Union that establishes stringent requirements for financial entities and their third-party providers to ensure robust digital resilience. Veracode supports DORA compliance through its comprehensive **Platform**, which addresses key pillars such as risk management, incident reporting, and operational resilience testing. By leveraging comprehensive testing capabilities like **Static Analysis**, **Dynamic Analysis**, **Software Composition Analysis**, and **Penetration Testing**. Veracode helps organizations identify vulnerabilities, manage third-party risks, and automate compliance workflows. Our platform can give you quick access to information about when an app was scanned last, what the results of the scan were, how many open and closed findings you have, benchmarks against peers in your industry and more. Learn more about our support for **DORA compliance**.

Continuous Compliance Competency Training

PCI DSS Section 6.2.2 mandates that all software developers receive specialized security training at least annually. To meet this requirement, organizations must provide verifiable instruction covering job-specific security for relevant development languages, mastery of secure design and coding techniques, and practical proficiency in using security testing tools to detect and remediate vulnerabilities.

Veracode transforms this annual requirement from a manual check-box exercise into a proactive, automated, and strategic function that provides an unbroken, verifiable audit trail for continuous compliance.

- Veracode eLearning **(Foundational Knowledge)**: Our library of self-paced modules provides the theoretical foundation for secure design and regulatory standards. The curriculum is tailored to specific job functions and development languages, ensuring developers understand how to identify and prevent vulnerabilities within their specific coding environments.
- Veracode Security Labs **(Practical Mastery)**: To fulfill the mandate for "secure coding techniques," Security Labs provides hands-on training environments where developers actively exploit and then patch real-world vulnerabilities. This interactive experience bridges the gap between theory and practice, equipping developers with the skills to remediate flaws effectively.

The combination of Veracode's e-Learning modules and hands-on Security Labs provides a comprehensive training solution that addresses both the theoretical knowledge and practical skills needed to meet PCI-DSS Section 6.2.2 requirements. By automating progress tracking and reporting, Veracode delivers the documentation necessary to prove to auditors that annual training requirements have been met across the entire global development team.

Leadership in Compliance Through Unified Risk

Regulatory compliance is no longer a burden; it is a strategic function that dictates market trust, drives customer confidence, and protects shareholder value. Veracode is the vendor leader positioned as the Compliance-First AppSec Posture approach by enforcing consistent security policies as code across all teams and projects, providing an unbroken, verifiable audit trail for continuous compliance. This approach moves beyond simple vulnerability counts; we prioritize risks based on exploitability, asset criticality, and exposure, ensuring development teams focus on the flaws that pose the greatest regulatory threat to the business.

By providing the tools to achieve this "leader" status, Veracode customers achieve a proven **184% return on investment** over three years, demonstrating that a unified, compliance-focused approach is not just a security necessity, but a verifiable financial imperative.

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

Sources:

1. IBM, Cost of a Data Breach Report 2024.

2. Veracode 2026 State of Software Security Report.

3. Veracode 2025 State of Software Security Report.

4. Banking Info Security, Navigating the Complexity of Regulatory Fragmentation in Cybersecurity, March 2025.

5. Jane Gale, CrowdStrike, Key Findings from CrowdStrike's 2004 State of Application Security Report, February 2024.

6. Stack Overflow, 2025 developer survey.

7, 8. Veracode 2026 State of Software Security Report.

9. Veracode 2025 State of Software Security Report.

10. Veracode 2026 State of Software Security Report.

VERACODE