VERACODE | FACT SHEET

HIGHLIGHTS:

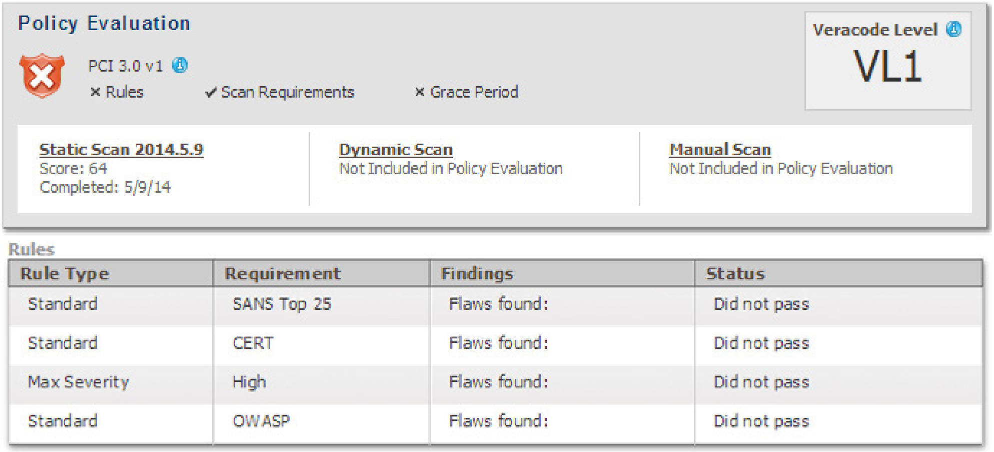
- ✔ Cloud-based platform for scale and simplicity
- ✔ Detective controls for PCI, SOX, HIPAA, NIST, MAS, BaFIN
- ✔ Centralized policies, metrics and reporting across global teams
- ✔ Automated compliance reporting and approval workflows
- ✔ Secure audit trails (e.g., approval of mitigating controls)
- ✔ Single platform for both static and dynamic analysis
- ✔ Addresses recommended FS-ISAC control for managing 3rd-party risk
- ✔ Addresses security training requirements via eLearning

Streamline Compliance

Automation. Centralization. Standardization.

According to the Verizon PCI Compliance Report, 84% of organizations that suffered a data breach were out of compliance with application-layer security controls (Requirement 6) — compared to an average of only 47% of all organizations assessed by Verizon QSAs in 2013. This suggests a strong correlation between the likelihood of suffering a data breach and non-compliance with application security.

Veracode's cloud-based platform assesses applications for compliance with standard controls such as PCI, the OWASP Top 10 and the SANS Top 25. Policies can easily be customized to support specific corporate audit requirements as well as compliance requirements for SOX, HIPAA, NIST 800-53, MAS and other mandates.



Policy Evaluation

PCI 3.0 v1

× Rules ✔ Scan Requirements × Grace Period

Veracode Level
VL1

Static Scan 2014.5.9
Score: 64
Completed: 5/9/14

Dynamic Scan
Not Included in Policy Evaluation

Manual Scan
Not Included in Policy Evaluation

Rules

Rule Type	Requirement	Findings	Status
Standard	SANS Top 25	Flaws found:	Did not pass
Standard	CERT	Flaws found:	Did not pass
Max Severity	High	Flaws found:	Did not pass
Standard	OWASP	Flaws found:	Did not pass

Veracode offers a single cloud-based platform for multiple assessment techniques — including static analysis, dynamic analysis and manual penetration testing — with custom policies for addressing a range of compliance requirements.

Simplify Compliance

We help you simplify and lower the cost of compliance by automating common processes such as:

- **Compliance/audit reporting** showing enterprise-wide compliance status — by business unit, development team and application — across your global application infrastructure.
- **Compliance workflows** to automate tasks such as notifications about policy changes and approval workflows for compensating controls.
- **Maintaining a secure audit trail** of notifications and approvals.
- **Information sharing and collaboration** across multiple teams that share responsibility for achieving compliance including development, security, audit/compliance and network operations.
- **Enterprise compliance reporting** via integration with a range of Governance, Risk and Compliance (GRC) frameworks.

Continuous Compliance

Organizations understand that true security and real compliance are not periodic events but rather ongoing activities that require continuous assessment. We help deliver continuous compliance by ensuring that:

- **Discovery searches** are conducted on a regular basis to identify all web applications associated with your domain, including temporary marketing sites, international domains and sites obtained via M&A.
- **Production web applications** are continuously monitored for vulnerabilities to maintain your security posture.
- **WAFs are continuously updated** with security intelligence obtained from assessments.
- **Applications are automatically assessed prior to deployment** as a standard step in the software development lifecycle (SDLC).

Automated Workflows with Secure Audit Trails

We provide built-in automated workflows to reduce communication overhead as well as to provide a secure audit trail of your approval processes. For example, you can specify that:

- **Notifications about policy changes** be sent automatically to the team assigned to the application; to any users with the Security Lead role; and to the application Business Owner. You can also send notifications about upcoming scans that are due, and when a flaw will go out of the grace period set in the policy.
- **Approvals must be obtained for critical items such as mitigating controls** that temporarily remove the need to address the flaw via code-level remediation (e.g., changes to WAF rules, operating system features, network implementation or application design). You can also specify that approval is required for all new scan requests, such as requests from developers or third-party vendors to re-scan their applications; and for new users that self-register via SAML authentication.

Integration with GRC Frameworks

Governance, Risk and Compliance (GRC) frameworks are often used to track strategic programs at the corporate level.

Our platform natively integrates with EMC/RSA Archer via XML to share critical information such as application security scores; listings of all discovered flaws; and flaw status information (new, open, fixed, or re-opened). Summary data is also included for third-party assessments, including scores and top-risk categories.

Similar integrations exist for other GRC systems such as IBM OpenPages, Rsam, and Symantec Control and Compliance Suite (CCS).

Achieving Security and Compliance

Strategic organizations understand that compliance does not equate to security. By implementing best practices for ongoing security, organizations can demonstrate compliance while at the same time preventing:

- **Data breaches** of sensitive customer and financial data.
- **Cyber-espionage** of corporate intellectual property such as business plans, new product designs and proprietary algorithms and source code.
- **Fraud** due to unauthorized access by malicious insiders or outsiders.
- **Brand impact** due to website defacement by cyber-activists.
- **Downtime** due to outages in critical application components such as payment systems.

PCI-DSS Compliance

PCI-DSS Version 3.0 states that "the application layer is high-risk and may be targeted by both internal and external threats." It goes on to say that "Public-facing web applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems." Veracode helps enterprises address a number of PCI-DSS requirements related to securing both custom and third-party code, including:

- **Requirement 6.1: Establish a process to identify security vulnerabilities**, using reputable outside sources for security vulnerability information, and assign a risk ranking to newly discovered security vulnerabilities. Veracode provides an outside source for vulnerability information and a risk ranking for all findings.

- **Requirement 6.3.2: Review of custom code prior to release** to production in order to identify any potential coding vulnerabilities. Veracode provides automated, binary static analysis (SAST) to accomplish this.

- **Requirements 6.5.1 to 6.5.9: Develop applications based on secure coding guidelines,** and prevent common coding vulnerabilities in software development processes such as injection flaws, buffer overflows, insecure cryptographic storage, cross-site scripting (XSS) and broken authentication and session management. This is accomplished via automated binary static analysis (SAST) and/or dynamic analysis (DAST) depending on the type of vulnerability. Veracode also helps identify vulnerabilities based on best practices such as the OWASP Guide and the SANS CWE Top 25.

- **Requirement 6.6: For public-facing web applications,** address new threats and vulnerabilities on an ongoing basis and ensure that these applications are protected by reviewing them via automated application vulnerability security assessment tools, at least annually or after any changes. Veracode meets the PCI requirement of being "an organization that specializes in application security."

- **Requirement 11.3.2: Verify that the penetration test includes application-layer penetration tests.** The tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5. This is accomplished either through automated testing or manual penetration testing services provided by Veracode.

- **Requirement 12: Maintain an information security policy.** With Veracode, you can define centralized policies that govern the maximum level of risk permitted for an application to be deemed compliant, based on its level of business criticality. There are five levels, from Very High to Very Low (based on the NIST definitions of assurance levels). Veracode policies also govern mandated frequency of re-testing and the grace period within which any policy-relevant flaws should be fixed. Users with the role of "Mitigation Approver" can also approve mitigations to vulnerabilities, such as updates to WAF rules.

SOX Compliance

Auditors concerned with Sarbanes-Oxley (SOX) Section 404 (Management Assessment of Internal Controls) are primarily focused on the integrity and accuracy of corporate financial data. In particular, we help achieve SOX compliance related to:

- **Fraud prevention:** Application security is crucial for SOX compliance because vulnerabilities in corporate financial applications—such as ERP, Accounting, HR and CRM systems – can lead to unauthorized access and potentially fraudulent changes to financial data.
- **Integrity of audit trails:** SOX requires the creation of audit trails for critical components such as financial applications and database servers; application security is critical here because vulnerabilities can lead to unauthorized modification, or deletion, of these audit trails.

SEC Guidance

The Securities & Exchange Commission (SEC) has also published guidance for public companies related to the disclosure of cyber-security risks and the financial impact of cyber incidents such as data breaches. We can help by providing detailed analytics about the current risk profile for your application infrastructure as well as an assessment of the remediation work required after a successful application-layer attack.

FS-ISAC Recommended Controls

The Financial Services Information Sharing and Analysis Center (FS-ISAC) recently issued recommended controls for addressing the security of third-party software. We can help implement a critical FS-ISAC control which relies on binary static analysis to identify vulnerabilities in third-party software. We can also help you implement a governance process for programmatically managing the risks associated with third-party software.

OCC Guidance

For banks, the Office of the Comptroller of the Currency (OCC) released new guidance (Bulletin 2013-29) in October 2013 that requires regulated entities to assess and manage risks associated with their third-party relationships. We can help by assessing the security of third-party software and helping you implement a governance process for managing third-party risk at the application layer.

HIPAA Compliance

The HIPAA Security Rule requires health care institutions to ensure the confidentiality, integrity and availability of all electronic protected health information (PHI) and protect against any reasonably anticipated threats or hazards to the security or integrity of such information. In particular, we help address sections §164.308 to §164.31 of the Security Rule including:

- **Risk analysis and management:** Assess risks and vulnerabilities in applications that handle Protected Health Information (PHI)
- **Authentication:** Verify that session identifiers are not vulnerable to authentication based attacks
- **Data security:** Ensure that applications have properly implemented encryption for all data-in-transit and data-at-rest
- **Malicious code:** Protect applications from malicious code and backdoors

NIST Compliance

NIST has mandated several controls related to application security in federal systems. In particular, “Recommended Security Controls for Federal Information Systems and Organizations” (NIST 800-53) specifies the following relevant controls:

- RA-5: Vulnerability scanning of systems and hosted applications
- SA-11: Creation and implementation of a security test and evaluation plan by developers, in consultation with security personnel; implementation of a verifiable flaw remediation process to correct weaknesses and deficiencies; documentation of results from the security testing/evaluation and flaw remediation processes
- SC-7: Boundary protection achieved via essential controls such as authentication mechanisms

NIST 800-54 (Security Considerations in the System Development Life Cycle) is also relevant because it focuses on the need to integrate security into all phases of the Software Development Life-Cycle (SDLC), and especially in the early phases. NIST 800-54 also addresses the need to assess the security of the software supply chain.