

Payment Card Industry Data Security Standard (PCI DSS) Compliance

Address your application security PCI DSS-related requirements

These requirements outline how to deliver and deploy secure applications. Organizations must meet these requirements to achieve PCI DSS compliance.

The Payment Card Industry Data Security Standard (PCI DSS) is a set of controls for organizations that store, process, or transmit payment cardholder data. To be PCI DSS compliant, organizations must meet requirements for developing and deploying secure applications. Synopsys provides a blend of products, services, and training to help you meet these requirements and achieve PCI DSS compliance.

Overview

We enable organizations to address PCI DSS requirements related to application security, network penetration testing, and secure code review (6.3, 6.5, 6.6, 6.7, and 11.3). If you want to take a strategic approach to software security, we can help you establish a software security initiative (SSI), which will also address your PCI DSS requirements. Here are some of our offerings:

- Products (PCI DSS 6.3, 6.6)
 - **Coverity SAST:** Enable your developers to detect and remediate quality defects and security vulnerabilities while they code with high accuracy.
 - **Black Duck SCA:** Discover license compliance issues and known vulnerabilities from binary, open source, and third-party code.
 - **Seeker IAST:** Identify and verify security vulnerabilities that expose sensitive data.
- Managed Security Testing (PCI DSS 6.3, 6.6)
 - **Static Application Security Testing (SAST):** Scan source code and systematically identify and eliminate software security vulnerabilities.
 - **Dynamic Application Security Testing (DAST) and Penetration Testing:** Use automated and manual penetration exploitation approaches to identify security vulnerabilities while web applications are running.
- Software Security Training (PCI DSS 6.5)
 - **eLearning:** Equip development teams with the skills and behaviors to produce more secure software.
 - **Instructor-Led Training:** We have courses to fit the needs of everyone from new professionals to advanced experts.
- Professional Services
 - **Program Design and Development:** (PCI DSS 6.3, 6.5, 6.7) Our experts can help you define, implement, and measure a software security initiative (SSI).
 - **Secure Coding Guidelines:** (PCI DSS 6.3, 6.5, 6.7) Give your developers actionable guidance on risk prevention and mitigation and secure coding techniques.
 - **Network Penetration Testing:** (PCI DSS 11.3) Identify security vulnerabilities in your internal- and external-facing networks, and get a clear mitigation strategy. Segmentation validation testing is included in all network testing as directed.

Benefits

- Increases your developers' efficiency by providing security guidance as they code and teaching them how to build security in
- Delivers independent code reviews to identify software vulnerabilities, develops a process for regular custom application code review, and re-evaluates updated code
- Helps you implement, enhance, and scale your penetration testing capabilities through the Global Synopsys Assessment Center (AC) and a variety of DAST offerings
- Improves your security posture immediately and sets the course for ongoing improvement of your software integrity through the delivery of standards, tools, and education
- Promotes cross-functional software security awareness, adoption, and efficiencies

Key PCI DSS requirements	Our services and products
2.4 Maintain an inventory of system components in scope for PCI DSS.	<ul style="list-style-type: none"> • Black Duck SCA
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: <ul style="list-style-type: none"> • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices • Incorporating information security throughout the software-development life cycle 	<ul style="list-style-type: none"> • Coverity SAST • Black Duck SCA • Seeker IAST • Managed Security Testing • Architecture Risk Analysis • Program Design and Development
6.5 Address common coding vulnerabilities in software-development processes as follows: <ul style="list-style-type: none"> • Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. • Develop applications based on secure coding guidelines. 	<ul style="list-style-type: none"> • Secure Coding Guidelines • Software Security Training • Program Design and Development
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes.	<ul style="list-style-type: none"> • Coverity SAST • Black Duck SCA • Seeker IAST • Managed Security Testing
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	<ul style="list-style-type: none"> • Program Design and Development • Secure Coding Guidelines
11.3 Perform external and internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification. ... If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods.	<ul style="list-style-type: none"> • Network Penetration Testing
12.3 Develop policy for critical technologies and define proper use of these technologies.	<ul style="list-style-type: none"> • Black Duck SCA • Program Design and Development
12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.	<ul style="list-style-type: none"> • Software Security Training

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com

©2020 Synopsys, Inc. All rights reserved. Synopsys is a trademark of Synopsys, Inc. in the United States and other countries. A list of Synopsys trademarks is available at www.synopsys.com/copyright.html. All other names mentioned herein are trademarks or registered trademarks of their respective owners. February 2020