

Payment Card Industry Data Security Standard (PCI DSS) Compliance

Address your application security PCI DSS-related requirements

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 6.3.2 and 6.5.X)
 - **Static Analysis (Coverity and SecureAssist):** Enable your developers to detect and remediate quality defects and security vulnerabilities while they code with high accuracy.
 - **Software Composition Analysis (Protecode):** Discover license compliance issues and known vulnerabilities from binary, open source, and third-party code.
- Managed services (PCI DSS 6.3.2, 6.5.X, and 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.
- Professional services
 - Program development (PCI DSS 6.3, 6.5, and 6.7)
 - **Software Security Initiative-in-a-Box (SSIB):** Get everything you need to launch your SSI, including standards examples, tools, secure software development life cycle definitions, sample testing, and traceable policies.
 - **Secure Coding Guidelines:** (PCI DSS 6.3.2) 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

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

Key PCI DSS requirements	Our services and products
<p>6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:</p> <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"> • Static Analysis (Coverity, SecureAssist) • Software Composition Analysis (Protecode) • DAST and Penetration Testing • Architecture Risk Analysis
<p>6.5 Address common coding vulnerabilities in software-development processes as follows:</p> <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"> • Static Analysis (Coverity, SecureAssist) • Software Composition Analysis (Protecode) • SSIB • Secure Coding Guidelines • eLearning—PCI DSS • DAST and Penetration Testing
<p>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.</p>	<ul style="list-style-type: none"> • DAST and Penetration Testing • Static Analysis (Coverity, SecureAssist)
<p>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.</p>	<ul style="list-style-type: none"> • SSIB • Secure Coding Guidelines
<p>11.3.X Perform external and internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections. 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 to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.</p>	<ul style="list-style-type: none"> • Network Penetration Testing

The Synopsys difference

Synopsys offers the most comprehensive solution for building integrity—security and quality—into your SDLC and supply chain. We've united the leading testing technologies, automated analysis, and experts to create an incomparable portfolio of products and services. This portfolio enables companies to develop customized programs for detecting and remediating defects and vulnerabilities early in the development process, minimizing risk and maximizing productivity. We don't stop when the test is over. As a recognized leader in Application Security Testing, we offer onboarding and deployment assistance, remediation guidance, and training solutions that empower you to optimize your investment.

For more information go to 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