



SaaS Security Scanner S4 for Salesforce



Security compliance and assurance for Salesforce

S4 rapidly identifies threats against cardholder data

Compliance Requirement

S4 Control



Penetration Testing

Implement additional security features for any insecure, required services (PCI DSS 2.2.3).



Performs Penetration Testing

S4 uses smart fuzzing to perform automated penetration testing.



Compliance Demonstration

Ensure security policies are documented, in use, and known to all affected parties (PCI DSS 2.5).



Provides Comprehensive Overview

S4 security checks can be used to demonstrate data protection compliance.



User Accounts

Shared hosting providers must protect each entity's cardholder data (PCI DSS 2.6).



Examines Account Configurations

S4 identifies duplicate user accounts and other security configurations (password policies, etc.).



Access Control

Do not store the full contents of any track after authorization (PCI DSS 3.2.1).



Audits Data Access

S4 can audit access to cardholder data in Salesforce.



Transmission Security

Ensure wireless networks transmitting cardholder data use industry best practices (PCI DSS 4.1.1).



Audits Transmission Settings

S4 audits transmission settings on integrations and seeks out areas of concern.



Secure Dev. & Maintenance

Establish a process to identify vulnerabilities using reputable outside sources (PCI DSS 6.1).



Identifies Security Vulnerabilities

S4 identifies vulnerabilities to cardholder data and uses code auditing and scanning.



registered ISV
partner

www.digitsec.com | info@digitsec.com | +1.206.659.9521
DigitSec, Inc. - 214 1st Ave S, Suite B03, Seattle, WA 98104, USA

