securityMETRICS®

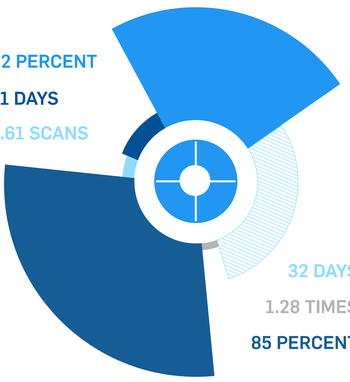
2019

PCI Compliance Trends

How Does Your Organization Rank?

2018 SecurityMetrics Customer Trends

- **72%** Percentage of SecurityMetrics customers that passed their first scan
- **11 DAYS** Average time from finished first scan to first passing scan
- **1.61 SCANS** Average number of times scanned until merchants pass their PCI scan
- **32 DAYS** Average time to reach PCI DSS compliance
- **1.28 TIMES** Average number of support incidents before customers became compliant
- **85%** of SecurityMetrics customers that started their SAQ have achieved a passing status



Top 10 Failing SAQ Sections

We reviewed our merchant database in search of the top 10 areas where organizations struggle to become compliant. Starting with the least adopted requirement, these are the results:

01 REQUIREMENT 12.1
Establish, publish, maintain, and disseminate a security policy.

02 REQUIREMENT 12.6.1
Educate personnel upon hire and at least annually.

03 REQUIREMENT 12.5.3
Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.

04 REQUIREMENT 12.10.1
Create an incident response plan to be implemented in the event of system breach.

05 REQUIREMENT 12.1.1
Review the security policy at least annually and update the policy when the environment changes.

06 REQUIREMENT 12.4
Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.

07 REQUIREMENT 12.8.5
Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

08 REQUIREMENT 9.9.2
Periodically inspect device surfaces to detect tampering (e.g., addition of card skimmers to device) or substitution (e.g., device swapped with a fraudulent one).

09 REQUIREMENT 12.3.5
[Verify that the usage policies define] acceptable uses of the technology.

10 REQUIREMENT 12.8.4
Maintain a program to monitor service providers' PCI DSS compliance status at least annually.

TOP 5 FAILED Vulnerabilities

SSL SELF-SIGNED CERTIFICATE

Occurs when organizations use an identity certificate that they create, sign, and certify rather than a trustedcertificate authority (CA)

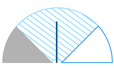
TLS VERSION 1.0 PROTOCOL DETECTION

Exists if the remote service accepts connections using TLS 1.0 encryption

SSL CERTIFICATE WITH WRONG HOSTNAME

Happens when an SSL certificate for the tested service is for a different host

SSL MEDIUM STRENGTH CIPHER SUITES SUPPORTED



Occurs when a remote host supports the use of SSL ciphers that offer medium strength encryption

SSL 64-BIT BLOCK SIZE CIPHER SUITES SUPPORTED (SWEET32)

Exists if a remote host supports the use of a block cipherwith 64-bit blocks in one or more cipher suites

DOWNLOAD THE 2019 SECURITYMETRICS GUIDE TO PCI COMPLIANCE HERE