servicenow

Efficient and cost effective support for maintaining PCI compliance

Payment Card Industry Data Security Standard (PCI DSS) was created to reduce credit card fraud by increasing controls. While the requirements are clear, achieving them can be challenging. And while maintaining PCI compliance is critical and a top priority for organizations—it's also expensive and resource intensive.

PCI DSS compliance journey

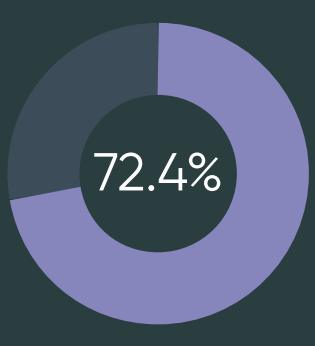
1. Define your CDE(s)
2. Access your control gaps and vulnerabilities
3. Remediate
4. Report current information

63%

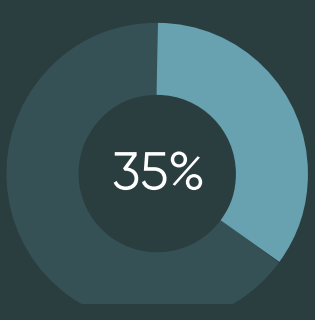
market value that global execs attribute to company's reputation

PCI DSS challenges:

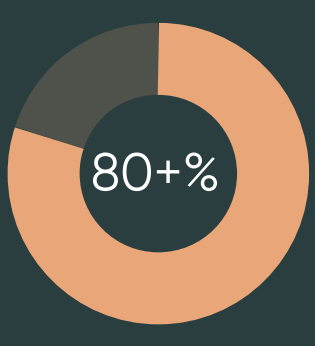
- Accurate view(s) of CDE(s)
- Organizing evidence of compliance
- Understanding all of your vulnerabilities
- Making sure all that's vital to PCI compliance remains current
- Confirming your third party providers are compliant
- Obtaining and providing timely information



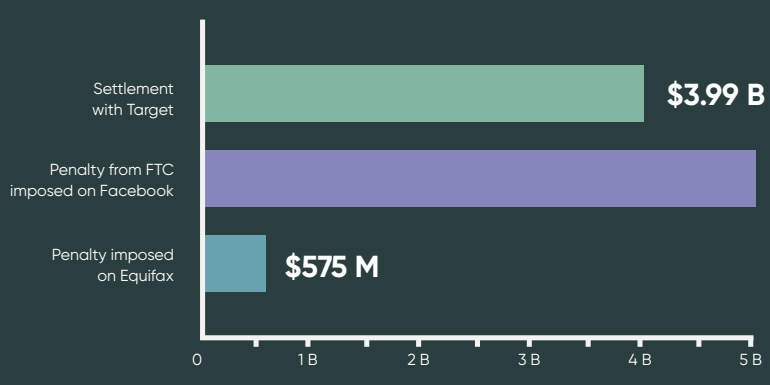
increase in credit card fraud reports[1]



of all consumers have been victims[2]



of retailer log-ins are by hackers using stolen data[3]



8 steps to help manage PCI

1. Establish and maintain view of CDE(s)
2. Review control effectiveness
3. Ensure appropriate policies are in place
4. Conduct risk assessments internally and with your 3rd and 4th parties
5. Continuously monitor for vulnerabilities and compliance
6. Ensure basic payment card security controls are in place
7. Automate response activities with cross-functional workflows to speed remediation
8. Use dynamic dashboards to effectively communicate at all levels

Handle risk with confidence—using these apps from our integrated risk portfolio:

Access Iceberg PCI Program Manager for ServiceNow in the ServiceNow Store.

[1] Federal Trade Commission (2020)

[2] Ascent survey of 1000 Americans conducted Feb 2019

[3] A report published by cybersecurity firm Shape Security

SN-Infographic-Partners-052520

servicenow.com