EIN PRESSWIRE

PCI DSS v3.2 Requires a Formal Compliance Program

Operationalize PCI DSS Compliance and Integrate Security as a Business-As-Usual Mindset with AuditLocker

InfoSecure provides the most comprehensive PCI policy template available

BOERNE, TEXAS, USA, April 12, 2016 /EINPresswire.com/ -- Once PCI DSS version 3.2 is released, organizations will be required to validate that PCI compliance is incorporated into business-as-usual (BAU) activities. This requirement formalizes BAU activities and mandates that certain activities are performed and tracked throughout the year in greater detail then every perviously required.

> AuditLocker helps organizations avoid the yearly audit scramble and ensures year-long PCI DSS compliance.
>
> *Patrick Bass*

That presents a lot of issues for many organizations. Tracking compliance activities throughout the year can be an arduous task, especially as PCI DSS requirements become increasingly complex. Now, thanks to AuditLocker, organizations can focus on their core competencies while ensuring that PCI DSS requirements are properly operationalized. How? Using our patent-pending compliance approach, AuditLocker, powered by InfoSecure (http://policytoolkit.infosecurepci.com) ensures ongoing, year-long compliance with a three step approach:

STEP ONE: We operationalize PCI requirements based on your validation type. No matter if you are a merchant or service provider. Supporting all SAQs types and Reports on Compliance (ROC). Our operation's prioritization makes sure that your organization integrates security into its operations as business as usual.

STEP TWO: Action Alert Notifications provide your organization with specific actions to be performed based on your compliance validation type. Whether you represent a merchant or service provider, any type of SAQ or ROC, AuditLocker Action Alert Notifications let you know when, how, and why to perform specific compliance actions.

STEP THREE: PCI certified experts make sure that your efforts meet the intent and rigor of the data security standard. Each action alert notification results in verifiable audit evidence that is vetted by a QSA and then stored in an encrypted vault. Stop guessing and act with the confidence of a PCI qualified security auditor.

In addition, AuditLocker clients receive the following value-added benefits:

Operationalization of all PCI controls, customized to your organization and validation type
Task tracking, audit evidence review, and annual comprehensive PCI report

Annual PCI Internal/External Penetration Test ($3,000 - $7,000 value)
Annual PCI Risk Assessment ($2,400 value)
Unlimited access to InfoSecure’s PCI DSS security awareness training program ($590 value)
InfoSecure’s PCI Policy Toolkit ($475 value)
Quarterly external vulnerability scanning and reporting ($275 value)
Data incident management with up to $100,000 in breach coverage
Unlimited support from a PCI expert
Menu pricing for additional PCI related services

For more information, visit us at http://www.auditlocker.com.

Patrick Bass
InfoSecure Redteam, Inc.
877-674-6965
email us here

This press release can be viewed online at: http://www.einpresswire.com

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases.