Meeting Compliance Challenges as Increasing Data Breaches Drive Further Modifications to PCI DSS Global Payment Security Standard

Every enterprise in every industry has compliance requirements for industry regulations and internal policies and best practices. The Payment Card Industry (PCI) Data Security Standard (DSS) is one of the most wide-reaching standards since virtually every enterprise has individuals or organizations conducting transactions that accept, process or receive payments. Whether safeguarding payment information is an integral part of the core business – as in online retail and financial services – or an important aspect of the core business (such as internal purchasing departments, consumer payments for services provided in the public and private sector), compliance with PCI DSS is essential.

The PCI DSS standard is updated periodically to address growing cyber threats to customer payment information and enterprises must keep pace. Yet, according to Dark Reading, “7 out of 10 companies that achieve PCI compliance fail to maintain that status even for a year. Verizon’s research showed that only 28.6% of companies managed to remain compliant for the full year between annual assessments.”

Enforcing compliance and readiness for internal and external audits is certainly a challenge and crucial to the bottom line. This has been acutely apparent with recent breaches spanning international borders that were directly linked to lack of compliance with current PCI DSS network security standards.

The Tufin Orchestration Suite™ Solution for PCI DSS Version 3.2 Continuous Compliance & Audit Readiness

IT managers and PCI internal auditors must perform periodic audits every 6 months. It is not feasible for network security teams to manually integrate the new policies, the management and testing required for compliance, while maintaining business-as-usual. The numerous security devices (firewalls, routers and others) manage hundreds to thousands of rules which add up to an extremely complex enterprise network environment. Maintaining continuous compliance with the latest PCI DSS version requires the right set of tools and automated solutions.

The Tufin Orchestration Suite™ solution helps organizations meet the various PCI DSS v3.2 network security requirements simply and efficiently with full accountability and documented processes. Tufin’s network security policy orchestration and automation supports a wide range of technologies and integrations end-to-end across the enterprise, spanning physical networks and hybrid cloud platforms. The Tufin Orchestration Suite includes TLS v1.2 support for encrypting communications between internal processes, as required for PCI DSS v3.2 compliance.

Enterprises benefit from Tufin’s orchestration of an automated policy compliance process with continuous change tracking and alerting. The Tufin Orchestration Suite solution monitors all network security policy changes; it performs proactive risk analysis by checking for PCI DSS v3.2 compliance automatically, and alerts to potential violations before changes are implemented and in advance of upcoming audits. Automated change and approval workflows enforce compliance policies including segmentation requirements and separation of duties, as well network access life-cycle management. By maintaining a state of continuous compliance and audit readiness for PCI DSS v3.2, IT and security managers and their teams are freer to focus on network security challenges.


www.tufin.com
Using the Right Network Security Tools for Quick Visibility & Remediation

Tufin’s PCI DSS v3.2 solution manages change and approval processes that integrate seamlessly and can be fully customized for your current enterprise ITSM process. Tufin’s PCI DSS audit report and other documentation make it easy to prepare quickly and thoroughly for an internal or external audit with an accurate record of who made changes, for full accountability.

Proper network segmentation must be addressed from the start, and is strongly recommended by the PCI DSS Council. Tufin’s Unified Security Policy (USP) matrix provides a robust, yet simple method of enforcing network segmentation and zones, which can reduce the attack surface as well as scope and cost of compliance.

Reducing PCI DSS Audit Preparation Time By Up To 70%

Establishing PCI DSS compliance can be extremely resource-intensive. For most enterprises, the many tasks involved in documenting, tracking and auditing network security procedures manually can take weeks. With the Tufin Orchestration Suite, enterprises can substantially reduce the time and cost of PCI DSS compliance. Tufin’s solution typically reduces audit preparation time by up to 70% through continuous compliance with the PCI DSS standard. With Tufin’s solution, IT operations, PCI internal auditors and security teams are able to do more with their existing resources.

Technology Partners

Tufin® is the leader in Network Security Policy Orchestration, serving more than half of the top 50 companies in the Forbes Global 2000. Tufin simplifies management of some of the largest, most complex networks in the world, consisting of thousands of firewall and network devices and emerging hybrid cloud infrastructures. Enterprises select the award-winning Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. Tufin reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. Its network security automation enables enterprises to implement changes in minutes with proactive risk analysis and continuous policy compliance. Tufin serves over 2,000 customers spanning all industries and geographies; its products and technologies are patent-protected in the U.S. and other countries.

Copyright © 2018 Tufin
Tufin and SecureChange are registered trademarks of Tufin. Unified Security Policy, Tufin Orchestration Suite, SecureTrack and SecureApp are trademarks of Tufin. All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

8-04-18