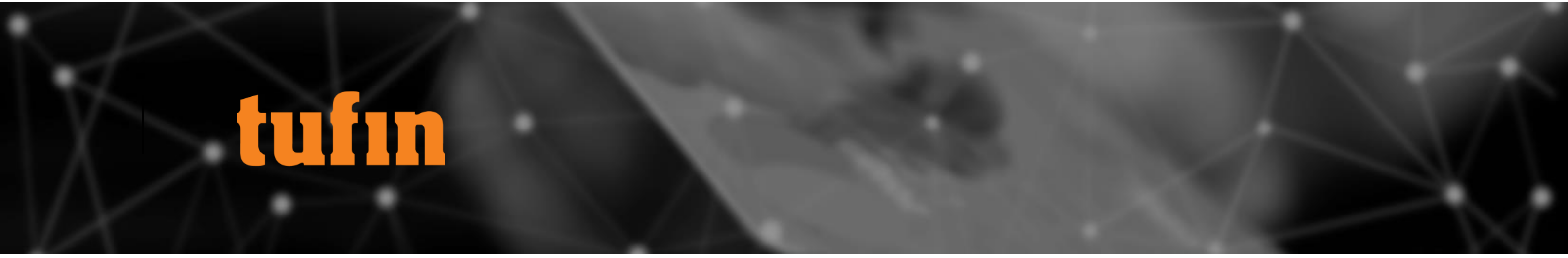
Best Practices for PCI DSS v3.2.1 Network Security Compliance

Table of Contents



Executive Summary

Payment data fraud by cybercriminals is a threat not only to financial institutions and retail organizations, but to enterprises across every industry. And with the reliance on credit card payment processing, the Payment Card Industry Data Security Standard (PCI DSS) is one of the most wide-reaching standards today. The goal of PCI DSS is to encourage and enhance payment data security and facilitate the broad adoption of consistent data security measures globally. It protects against fraud and security threats by providing a baseline of technical and operational requirements designed to protect payment data and the systems that contain or process it.

To comply with PCI DSS, IT, security, and compliance teams must perform periodic audits or assessments. Furthermore, the PCI DSS Council updates the standard periodically to remediate growing threats by cybercriminals. Therefore, complying with the latest PCI DSS standard and ensuring that the enterprise network is audit-ready is a pressing concern of many IT managers and PCI DSS internal auditors today.

Yet, according to Verizon’s 2018 Payment Security Report, “Lack of sustainable control environments remains a top contributor and precursor to ineffective controls, which in turn become susceptible to data breaches.” So, maintaining compliance and audit-readiness is certainly a challenge.

This paper provides information to IT executives, security architects, compliance officers and internal auditors for understanding how PCI DSS version 3.2.1 requirements translate to network security mandates and best practices through Network Security Policy Management (NSPM). Security practitioners and network operation teams will learn how to automate, design, plan, and integrate controls required to comply with PCI DSS into everyday processes. NSPM solutions like Tufin Orchestration Suite™ make network security management and audit preparation simple by providing policy-based automation across some of the most complex hybrid networks.

Protect Payment Data with PCI DSS

PCI DSS defines 12 high-level requirements, grouped into six control objectives. To assess compliance, compliance officers and internal auditors perform periodic audits in a frequency determined by the business and the financial transaction volume they process. For example, audits can be performed monthly, quarterly, semiannually, or annually. Audits assess compliance via numerous testing procedures and sub-requirements to determine adherence to regulatory requirements, as seen in the table below.

PCI DSS Control Objectives	Requirement Description
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs
	6. Develop and maintain secure systems and applications

PCI DSS Control Objectives	Requirement Description
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know
	8. Identify and authenticate access to system components
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

The main PCI DSS principle: Payment data is only as secure as the pathways that provide access to it. PCI DSS requirements are designed to ensure that your network security practices have a risk management process. Beyond establishing a process, PCI DSS requirements ensure that your organization defines and documents well-structured policies, procedures, and practices that are trackable and auditable. Automation of these practices and procedures saves you valuable time and effort, streamlines the identification of risks and eliminates human error while ensuring full auditability. To ensure data pathways are secure and adhere to strict network security policies, PCI DSS requires organizations to have:

- Specific guidelines to process card payments to prevent payment data fraud, skimming and other security threats
- Alignment with industry best practices to increase the trust of both customers and partners
- Limited external network access to sensitive data, combined with a formal process to monitor all changes to your firewall configuration and cloud security groups
- Trackable and auditable firewall and cloud operations, including clear definitions of roles and responsibilities
- Strict limitations of internal access to your organization's sensitive data
- Documentation, enforcement, and auditing of all your operational procedures and practices

In summary, PCI DSS demands organizations maintain continuous compliance through an ongoing process of: Assess, Remediate and Report. To comply, your team must have an accurate picture of your compliance posture, the tools to address issues, and the ability to demonstrate compliance through internal and external audits.

PCI DSS Compliance Requires Continuous Demonstration

PCI DSS compliance is required for businesses that store, process, or transmit payment cardholder data, but demonstrating compliance only at a specific point in time is insufficient. PCI DSS compliance requires a state of continuous compliance that involves much more than a periodic preparation and review process. The most effective means to ensure compliance beyond periodic audits is to build security and privacy controls into your daily business activities. Your organization needs to incorporate risk identification, proactive change analysis, and mitigation into the operational levels within the organization, achieve visibility over their existing state of compliance and create enforceable guardrails to avoid introducing compliance violations.

Operational-level risk assessments trigger alerts generated by your operational-level systems and processes that can be used to escalate issues to management when events exceed pre-defined tolerances. Similarly, explicit risk-assessment discussions need to be included as part of business planning, execution, and evaluation meetings. Integrating risk analysis into your operational-level activities ensures compliance throughout change processes. Furthermore, continuous risk analysis and automated change tracking enables your organization to save considerable time and effort for audit preparation.

Digital Transformation is the Security Challenge

About 40% of PCI DSS is related to network security, but the growing complexity of hybrid networks makes this compliance the largest headache. Fragmented ownership over the different networking platforms, coupled with constant changes, necessitate operational adjustments to enforce security and compliance controls.

Frequent changes to networking and security systems are necessary to support digital transformation and evolving business needs; for example, opening firewall ports to support connectivity of a new business application. Your organization may make agility the top priority because it directly impacts revenue. However, prioritizing business agility over security and compliance typically introduces risk, increasing susceptibility to attacks and the likelihood of costly audit failures.

Your team requires a repeatable process, one that doesn’t interrupt business momentum, by ingraining compliance during changes. This goal of repeatability and consistency is even more important when considering the effort and time required when you manually document, track, and audit network security changes, and resolve the inconsistent results. Your network security devices (e.g. firewalls, routers), SDN, and cloud platforms that often contain hundreds or thousands of rules produce an extremely complex enterprise network environment that can render security unmanageable without consolidating policy and network management.

To ensure compliance, your team must first have clear and centralized visibility over network topology and security configurations across your network and cloud platforms. To demonstrate continuous compliance, your security and network teams should use a zone-to-zone connectivity matrix with a list of permissible or blocked services to assess the compliance of changes to avoid delaying implementation. This compliance-based connectivity matrix serves as a technically referenceable benchmark for PCI DSS compliance. Automated solutions for visibility, risk assessment, and enterprise network change management use this compliance benchmark to identify violations in the network and ensure that new violations aren’t introduced inadvertently.

In cases where rules violate compliance but are still justified as they enable connectivity of a critical application, the violation should be designated as an exception. Designating a violation as an exception can be allowed to maintain a state of continuous compliance without impeding the business. However, this process requires full documentation and the ability to assign an expiration date to recertify or decommission the rule.

Ten Best Practices for Complying with PCI DSS Network Security Mandates

PCI DSS serves as the de-facto standard for any company that stores, processes, or transmits payment cardholder data. Because of the widespread applicability to businesses, IT, security, and compliance managers, regardless of industry, continually align their enterprise security program to adhere to the stringent standards of PCI DSS.

Before getting into the PCI DSS requirement details, it's best to understand how leading enterprises enforce compliance with PCI DSS network security mandates. If your IT, security, and compliance managers execute compliance adherence effectively, their work on PCI DSS compliance serves as a springboard into a tighter security posture, higher efficiency, and securely-enabled business agility.

Ten best practices for complying with PCI DSS network security mandates:

1) **Create a clear separation with proper network segmentation** of cardholder data environment and cardholder data from the rest of the network. Even if you have a flat network, it is important to segment it to logically isolate sensitive data. If you fail to do so, since all systems will have access to one another in a flat unsegmented network, your whole network is subject to PCI DSS regulations.
2) **Identify and remediate policy violations** in real time by designating alert mechanisms differently than other automated alerts. Security professionals are overwhelmed with automatically generated alerts. However, PCI DSS violations need to be addressed as quickly as possible to maintain continuous compliance.
3) **Establish consistent, auditable exception designation and management** to ensure that violations that have been approved exceptions unto your network don't prompt a failure of your PCI DSS audit. Reasons for exceptions need to be documented, as does the owner along with a date for expiration and a method for consistently reviewing exceptions prior to expiration.
4) **Institutionalize an enterprise-wide network change workflow process** that meets PCI DSS requirements. Your company should automate change processes and execute them through automation to ensure consistency in steps and completion.
5) **Ensure every network change has a complete audit trail** with the who, what, when, and why.
    a. The who is important to align to requirements for segregation of duties and for providing documentation for auditors
    b. The what is important for understanding modified policies, especially those connecting to PCI-regulated network zones
    c. The when is important to understand adherence to a change window, identify emergency changes, or flag unscheduled and undocumented changes as anomalous behavior for investigation
    d. The why aspect is critical for ensuring effective reporting for auditors, particularly in consideration of retaining necessary violations as exceptions
6) **Validate every network change** with the following:
    a. Risk analysis based on your security policy to determine whether access control configurations violate PCI DSS
    b. Approval by the business owner to close the change request ticket as complete and close the process

   c. Implementation according to the PCI-compatible network change workflow to ensure consistent adherence to PCI DSS process requirements

7) **Ensure that access controls protecting cardholder data adhere to** the following guidelines:
   a. Every rule has a comment that includes a date for regular recertification or expiration
   b. Every rule has a log
   c. No rules with “Any” in the source, destination, and service
   d. No rules with risky services (un-encrypted)
   e. Delete unused and redundant rules
   f. Adopt a process for recertifying aging access rules
8) **Enforce proper documentation of every access rule** to ensure your audit preparedness with the following information:
   a. Business justification
   b. Business owner
   c. Application name
   d. Expiration or recertification date
9) **Mandate that firewall and cloud security groups logs are kept** for at least 12 months for retrieval during your PCI DSS audit and align to data retention best practices
10) **Automate the rule cleanup and recertification processes** to ensure all rules comply with PCI DSS

Leveraging PCI DSS v3.2.1 Beyond Continuous Compliance: Improve Your Security with Automation

PCI DSS v3.2.1 compliance is a business mandate that may also be used to get the buy-in and budgets to ensure your network security is capable of ongoing success. To set high, sustainable security standards, experts suggest you pay special attention to sub-requirements within PCI DSS requirement 1.

Taking a broader look at PCI DSS requirement 1 opens the door for implementing ongoing network security solutions. This is significant if your organization has historically relied on manual processes that won’t scale to meet the needs of the business and that diminish your network security posture.

Enterprises with large networks need to automate access changes and security operations to enable business agility. Investing in solutions for automating security processes reduces costs and efforts of maintaining continuous compliance with a variety of industry regulations and internal policies, and provides ongoing benefits for the enterprise.

The five PCI DSS requirements below require an ongoing process, not just a specific tool, to align with compliance best practices, and can help you present the business case for automation to your executive team.

1.1.1 Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.

Compliance managers need to ensure that a clearly defined, enforceable change process for access policies exists. The PCI DSS external auditor will ask to see a change report with a full audit trail, and then select some random changes and request to see the sign off.

The Challenge: Many organizations still don't have a change process in place, and even if they do, the process is often too loose or reliant on manual implementation rather than a consistent, structured flow.

Security Best Practice: The best way to implement formal, auditable change processes is to automate a well-defined process flow. Having a solution that enforces and automates change processes ensures consistent approval and execution to align with the PCI DSS requirement of implementing an approved formal process. As an example, organizations can automate the risk analysis of access changes, the approval chain of risk, and the integration with LDAP for identifying approvers.

1.1.6 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of risky services include FTP, Telnet, POP3, IMAP, and SNMP.

This sub-requirement focuses on three main risks:

1. Are connections required for business known? Are business justifications documented?
2. Are access controls implemented with the Principle of Least Privilege?
3. Are any of these connections insecure? Do compensating controls for them exist?

The Challenge: Most organizations don't have an up-to-date list of allowable services that are permissible for business. In the best case, documentation per access rule exists. Although it is most likely that some existing access rules contain insecure services.

Best Practice: IT managers must document business reasons for each service used and ensure the information is retrievable and technically referenceable. Automation is the primary method to enforce consistent documentation of all rules and services. Beyond compliance, tracking this information can be used to ensure continuity in documentation during personnel changes, or to identify unused rules that are not justified and should be removed.

1.1.7 Requirement to review rule sets for firewalls, routers and cloud security groups at least every six months

Security and network operations managers must prove that a review process exists and that outcomes are documented. To comply with this requirement you need a report to show that rule sets were reviewed, flagged rules from the last audit were treated appropriately, and that new rules added since the last audit were approved, documented, and designated as an exception if needed.

Best Practice: Based on the 2018 Verizon Payment Security Report, change record validation is the largest control gap for PCI DSS compliance. Many organizations find they cannot provide the required documentation for the PCI DSS external auditor because manual processes make documentation impossible. It is important to ensure well-defined processes for reviewing and recertifying access rules are implemented, stringently followed, and documented. The best way to achieve all three is by automating these processes. Automation will also improve SLAs, reduce costs and efforts of manually reviewing thousands of rules, and free the team to focus on more strategic security projects.

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the payment data environment

PCI DSS external auditors often look for a set of rules that permit specific allowed services, such as approved known protocols used by the PCI DSS servers, followed by an explicit drop rule for all other traffic. Exceptions must include proper documentation (such as rule comments and expiration) that satisfy the auditor.

Best Practice: Setting explicit drop rules is easier than trying to correctly restrict inbound access. Proper definition of network zones protecting cardholder data makes compliance much simpler. It’s therefore important to ensure that your PCI DSS external auditor agrees to the zone definition and access control scheme. Secondly, your company must prove that you have a process to identify and decommission redundant or unused access rules.

An automated process for adding “necessary” access and for decommissioning redundant access improves consistency by eliminating human error and generates alerts whenever violations are introduced. Beyond consistency and awareness, automation also allows proactively checking access changes for additional risks and misconfigurations.

1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ

IT and security managers must allow traffic from the Internet to specific servers in the DMZ — everything else should be dropped. Proper definition of traffic that is Internet (e.g. all non-local IP addresses) and proper definition of the accessible systems within the DMZ are critical for compliance. Most important, your PCI DSS external auditor must agree that definitions are correct.

Best Practice: Configure an active alert mechanism for non-compliant policies that allow unauthorized traffic so that IT managers can ensure network compliance. An automated workflow for processing access changes can proactively identify an attempt to allow unauthorized Internet traffic and address it even before it is implemented. Beyond documenting compliance, alerts can also flag malicious behavior, such as compromised credentials, to alert your security team of an incident.

1.3.4 Block unauthorized outbound traffic from the cardholder data environment to the Internet

Network operation teams need to properly define the 'Internet' and 'cardholder data' environments by creating network segments that can be isolated. Your PCI DSS external auditor will validate that there is no direct access between these entities with supplied evidence.

Best Practice: Utilize automation to manage and document access to integrate PCI DSS audit requirements into the everyday IT and business activities. This ensures that your:

1) Documentation is ready
2) Alerts of violations have been generated and violations removed or designated as exceptions
3) Access changes that allowed unauthorized outbound traffic were proactively flagged as risky and mitigated prior to implementation

Necessary Functions for PCI DSS v3.2.1 Compliance: Network Security Checklist

Security and network operations teams can use the PCI DSS Network Security Checklist to prepare for audits. The checklist summarizes the key PCI DSS Requirements and Testing Procedures related to network security. If best practices for network security are implemented in the organization, the PCI DSS audit is simply a healthy routine versus a compliance headache. Perhaps most important, compliance is continuous rather than occurring at a single point in time.

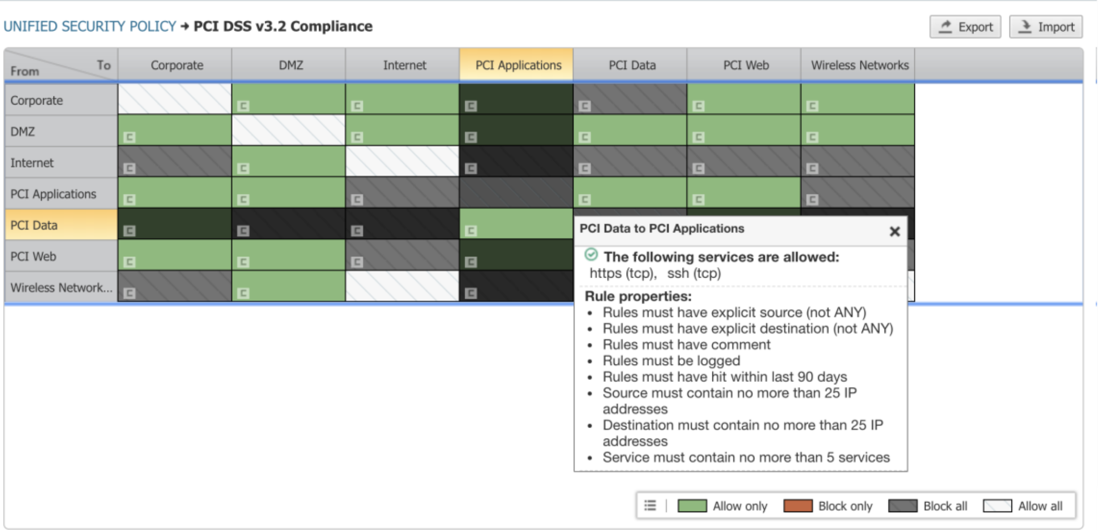
To meet the requirements related to network security in an efficient, quick, and manageable way, Tufin's security policy management solution helps organizations to comply with PCI DSS version 3.2.1:

PCI DSS Requirements & Testing Procedures		Necessary Tool Functions
Build and maintain a secure network and systems	**1.1** Establish and implement firewall and router configuration standards that include the following: Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:	Automation and documentation of all firewall and router configuration changes, PCI DSS firewall and router checks, PCI DSS requirements deviation detection and reporting
	1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	Automatic risk analysis, automation and documentation of all firewall and router configuration changes
	1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	Network segmentation, PCI DSS zone designation, network topology modeling, and tagging for cloud applications
	1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	Network topology to identify internet access by all zones.
	1.1.6a Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification and approval for each.	A searchable zone-to-zone-based connectivity matrix with PCI DSS risky services and rule properties to compare against firewall and router configurations, network-wide policy search, exception tracking
	1.1.7 Requirement to review firewall and router rule sets at least every six months	PCI DSS compliance reporting, risks and policy violations reporting, rule recertification automation, task-based management for network security admins
	1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. (1.2.1a, 1.2.1b, 1.2.1c)	PCI DSS firewall and router checks, automated risk analysis against a central zone-to-zone-based connectivity matrix with PCI DSS risky services and rule properties, violations alerting and reporting, exception designation and tracking
	1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment (1.3.1,1.3.2,1.3.4,1.3.6)	Topology mapping; centralized network management to restrict traffic between Internet and PCI zone, alerts for violations
Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted	**2.2.2** Enable only necessary services, protocols, daemons, etc., as required for the function of the system. **2.2.3** Implement additional security features for any required services, protocols, or daemons that are considered to be insecure	Automated risk analysis against a central zone-to-zone-based connectivity matrix with PCI DSS risky services and rule properties, rule documentation, network-wide policy search, and expiration date tracking, and rule decommissioning

PCI DSS Requirements & Testing Procedures		Necessary Tool Functions
system hardening standards	**2.2.4** Configure system security parameters to prevent misuse	Definition of required rule properties, rule decommissioning and rule expiration for removing unused/unnecessary access
Track and monitor all access to network resources and cardholder data	**10.1** Implement audit trails to link all access to system components to each individual user.	Full accountability of policy changes with automated audit trail and reports; separation of duties
	10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (e.g., online, archived, or restorable from backup).	Retain a full audit trail of all changes and traffic logs, for any user-configured time-range
	10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: Firewalls, IDS, FIM, anti-virus, physical access controls, logical access controls, audit logging mechanisms, segmentation controls (if used)	Risks and violations reporting and alerts, network-wide policy search, reporting, network topology map for connectivity troubleshooting

As most enterprises are adopting public and/or private cloud platforms, it is important to note that although the PCI DSS standard relates predominantly to firewall environments, the Tufin Orchestration Suite solution for Network Security Policy Management supports all leading network security platforms, SDN and hybrid cloud platforms.

Tufin Solutions for Continuous Compliance with PCI DSS



UNIFIED SECURITY POLICY → **PCI DSS v3.2 Compliance**

From / To	Corporate	DMZ	Internet	PCI Applications	PCI Data	PCI Web	Wireless Networks
Corporate	□	🟩	🟩	🟩	▨	🟩	🟩
DMZ	🟩	□	🟩	🟩	🟩	🟩	🟩
Internet	▨	🟩	□	▨	▨	▨	▨
PCI Applications	🟩	🟩	▨	▨	🟩	🟩	▨
PCI Data	🟩	▨	▨	🟩	▨	🟩	▨
PCI Web	🟩	🟩	▨	🟩			▨
Wireless Network...	▨	🟩	□	▨			□

PCI Data to PCI Applications ×

✓ **The following services are allowed:**
https (tcp), ssh (tcp)

Rule properties:
- Rules must have explicit source (not ANY)
- Rules must have explicit destination (not ANY)
- Rules must have comment
- Rules must be logged
- Rules must have hit within last 90 days
- Source must contain no more than 25 IP addresses
- Destination must contain no more than 25 IP addresses
- Service must contain no more than 5 services

☰ | 🟩 Allow only 🟥 Block only ▨ Block all □ Allow all

Tufin offers Network Security Policy Management solutions for physical networks and networks comprised of SDN, cloud, and containers. Tufin's policy management capabilities enrich policy data across your multi-vendor network to provide unified visibility over risky rules and violations, and enable their decommission or exception designation and recertification through workflows. Tufin provides PCI DSS templates to generate a technically referenceable zone-to-zone connectivity matrix with the services and ports allowed or blocked between zones. The Unified Security Policy provides alerts on violations within your network for decommission, exception designation, and automated recertification with full audit tracking. Automated change tracking provides audit readiness while dashboard and preconfigured reports provides visibility over your state of compliance.

Organizations utilizing DevOps to achieve innovation and decrease time to market use Tufin cloud solutions to gain visibility into cloud-native environments, define and control security policies, and use automation to enhance the DevOps CI/CD pipeline to integrate security into the process.

For more information on how you can achieve continuous compliance with PCI DSS using the Tufin Orchestration Suite, please visit the Tufin website or learn how Monext uses Tufin for demonstrating PCI compliance.