Pulse Secure®

Meeting Key Challenges of PCI-DSS Compliance

1. The Importance of Information Security Compliance

Business today is measured by the value of data, including product designs, patents, financial records, and importantly, customer confidential information such as credentials and credit cards. The **SECURE ACCESS**, transmission, processing and storage of this information is critical to the success of any business. Failure to protect not only results in direct business loss but hefty fines, legal liability and erosion of customer loyalty.

The global nature of the internet reduces the cost of collaboration significantly but carries significant business risks including an increasing number of cyber criminals. Unlike common criminals who target a specific business, these cyber thugs troll the internet for vulnerable businesses and attempt to compromise them, regardless of their country, size or type. Governments around the world are attempting to combat this threat by introducing numerous compliance regulations.

There is no standard formula to achieve compliance and every organization must examine its own business and IT infrastructure to come up with the most appropriate approach. However, there are common business drivers and trends such as Bring Your Own Device (BYOD) and mobility that significantly impact the compliance process.

This paper discusses the topic of the Payment Card Industry Data Security Standard (PCI-DSS) compliance in detail.

2. What is PCI-DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

The latest version of PCI-DSS V3.2 was released in April 2016 by the Payment Card Industry Security Standards Council (PCI SSC).

A common misunderstanding about PCI-DSS compliance is that it's only relevant to merchants or retailers that handle large amount of credit card transaction. But the truth is that if your business handles any credit card transaction or E-commerce transaction with payment card information, you are obligated to meet and maintain PCI-DSS compliance.

3. The ROI of PCI-DSS Compliance

Advances in payment technologies such as contactless payment cards and payment by mobile devices have given users increased convenience and improved security at the point of sale. Payment cards continue to be the dominant payment method in E-commerce with 48% of American on-line shoppers choosing credit card and 30% choosing debit card in 2014. (Source: www.creditcards.com Payment Method Statistics)

Because of the growth, PCI related security data breaches are also increasing at an alarming rate. They now account for 27% of all data breach incidents and over 50,000 records are stolen per incident on average. Hacked credit card fraud reached a record level of $4 billion in 2015 alone. (Source: the 2016 Data Breach Investigations Report by Verizon).

The consequences for not being PCI compliant are severe and range from fines and penalties to loss of existing customers and new business.

The fines by financial institutions can run from $5,000 to $500,000, based on forensic research prompted by a potential breach. Credit card institutions may impose fines as a punishment for noncompliance. The information below is used by VISA as an example of costs related to a breach.

- $50—$90 fine per cardholder data compromised
- Suspension of credit card acceptance by a merchant's credit card account provider
- Loss of reputation with customers, suppliers, and partners
- Possible civil litigation from breached customers
- Loss of customer trust which affects future sales
- These fines can be incurred regardless of the source of the breach.

In addition to the immediate financial loss, a data breach can turn your hard-earned loyal customers away. A cisco survey found that 50% of companies face public scrutiny after a breach, leading to reputational risk,

and 20% reported that they lost customers after the data breach. Additionally, 23% of them had identified lost business opportunities from prospects as a result. (Source: Cisco 2017 Annual Cybersecurity Report)

Comparing to the potential direct and indirect loss, PCI-DSS compliance is a mandatory investment for any business that handles payments.

4. About Pulse Secure

Pulse Secure's mission is "Delivering Secure Access Solutions for people, devices, things and services". Remote Access to data center resources has evolved to **Secure Access** – where the location and type of resource being securely accessed is more than just data centers, including Cloud/SaaS applications, and Mobility. Devices must be secured whether outside or inside the organization, laptop or mobile.

Pulse Secure Access Suite is a comprehensive Secure Access solution that securely connects workers to company resources and protects company devices, regardless of location – in the data center, cloud or mobile. Pulse Secure delivers access to all company resources via a single client or mobile application – dramatically simplifying access and increasing user productivity.

Administrators configure contextual access policies to control access based on devices, locations, resources, users and groups, or even endpoint profiling. Policies can be extended to internal networks, allowing organizations to identify, profile secure and manage internal devices, Guest User access, and even BYOD devices. Detailed management and reporting meets the needs of the toughest regulatory compliance environments.

Pulse Secure is well positioned to deliver comprehensive Secure Access, given our 15+ years of experience, over 20,000 customers and 20 million endpoints.

In this paper, we will discuss how Secure Access Suite can help to meet the challenges of PCI-DSS compliance.

5. Addressing Key Technical Challenges with PCI-DSS Compliance

The top three areas of concern for PCI-DSS compliance in the digital payment era are: remote access, mobility/ BYOD and visibility.

5.1. Secure Access

Remote access technology allows a smaller business access to resources that are previously only available to large establishments, it also allows larger merchants to spawn off new branches quickly to adapt to the changing

consumption and competitive landscape. However, remote access technology also has the potential to be used by an attacker to compromise the merchant's network. MasterCard analysis of Account Data Compromise Events has shown that insecure remote access is the #1 point of entry for attacks against brick-and-mortar merchants.

With the Secure Access Suite, when a user attempts to connect to the corporate network from both on-prem and remote devices, in addition to user authentication, the host checker function will automatically check for policy compliance of the host machine which include Antivirus, Firewall, Anti-Spyware, OS version and patch management. Only valid users on compliant devices will be allowed access to the corporate network. This helps to protect the users and the organization from malicious cyberattacks like the recent WannaCrypt ransomware.

To secure remote access, many organizations require users to first authenticate into the remote sessions, then authenticate separately to access the full range of protected resources such as payment data. The Pulse Connect Secure solves this problem through SAML (Secure Authentication Markup Language) integration to allow a user to authenticate once and gain access to separately secured systems both on-prem and in the cloud without resubmitting credentials.

The Secure Access Suite takes an integrated approach with the session federation to add the ability to seamlessly provision SSL VPN user sessions into Pulse Policy Secure (PPS) and internal firewall upon login, enabling a seamless end user experience in these types of environments.

With the federation framework, IT admins can now enable policies based on user identify and roles instead of IP address, and can set up coordinated security response across multiple network entities. For example, a POS machine from the remote branch is only allowed to connect to dedicated payment system in the backend. Even if the POS is compromised, the intruder would not be able to access payment card records.

5.2. Mobility and BYOD

BYOD and Mobility have gone from luxury to necessity for modern enterprises. Many retailers allow the use of BYOD devices in their shops and show rooms and there are even more mobility and BYOD devices in use at the corporate HQ. Every one of these devices could pose a threat to data security and PCI compliance. While solutions such as Mobile Device Management (MDM) ensure only qualified mobile devices are on the network provide some mitigation, they are often not adequate.

Payment card data should not be stored on mobile and BYOD devices as they could be lost and stolen. Mobile and BYOD devices could also be infected with malicious software or be the point of breach on the network without end users even knowing it. The Secure Access Suite provides the ability to maintain a consistent remote and on-prem policy based network separation to prevent mobile and BYOD devices from accessing payment card data.

Furthermore, the Secure Access Suite can restrict the access privilege of BYOD devices if the operating system or application is out of date. For example, if there is a security loophole with one of the known apps, it will take time for the patch to be rolled out; rather than banning the BYOD devices from the network altogether, IT administrators could take actions to restrict the potentially exposed devices to certain VLAN and/or limit the devices to browsing only function.

5.3. Visibility

Over 80% of data breach incidents happened in minutes but over 60% of the incidents are discovered days after

the breach happened (Source: 2016 Data Breach Investigation Report by Verizon). Many of the stolen payment card data would have made their way to the black market and cause fraudulent transactions before the incident was reported. Visibility is key aspect of PCI-DSS compliance to prevent a breach before it happens and reduce of the impact of a breach after it happens.

There are multiple network entities that could be targeted by intruders and the scenario is further complicated by the adoption of mobile and BYOD devices. While it is possible to go through all the system and event logs and switch back and forth between different dashboards to be vigilant of potential breach, the Pulse Secure Access Suite integrates with leading eco-system partners in Firewall, SIEM, WLC to provide a single pane of glass to provide a holistic view for both remote to on-prem sessions:

- Who (is accessing the services? Are they authorized users?)
- Which (devices are they using? Which OS does it run? Are there any vulnerabilities that the device is exposed to that could in turn expose the business data to risk?)
- What (services are they accessing? Are they on premise or cloud? Are the services sanctioned or unsanctioned?)
- Where (are they accessing the services from?)
- When (did they access the services?)

6. Conclusion

PCI-DSS compliance is a must have for any business that accepts, processes, stores or transmits payment information. The digital payment era means there are significant more payment data to be protected. Technology trends such as remote-access, mobility and BYOD have boosted productivity and efficiency for all the merchants but they have also become hot bed for cyber criminals to gain access to payment data.

Pulse Secure's Secure Access Suite takes a proactive approach by enforcing consistent user and role based policy for both remote and on-prem sessions from any device while maintaining a great user experience. It integrates eco-system partner solutions to provide a highly integrated and visible PCI-DSS compliant solution. The full PCI-DSS compliance matrix can be found in Appendix A.

Click **here** to learn more about the Pulse Access suite.

Appendix A: The 12 principle requirements of PCI DSS and how you can use the Secure Access suite to meet them are shown below.

Table 1: Meeting PCI-DSS Requirements using the Secure Access Suite

Requirement	Sub-requirement	How the Secure Access Suite solves it
1 Install and maintain a firewall configuration to protect cardholder data	**1.1.6** Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	Pulse Profiler collects a list of open ports from all the devices on the network and provides this information to the admin for role based access control.
	1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	Pulse Policy Secure integrates with firewalls to provide Identity information which is essential for providing role-based access control to sensitive resources and information.
	1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties.	Pulse Connect Secure protects servers in the data center by allowing only authenticated access to these resources while preventing unauthorized access.
	1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE.	Host checker can verify whether personal firewall is running on an endpoint and ensure compliant access to network.
2 Do not use vendor-supplied defaults for system passwords and other security parameters	**2.1.1** For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	Pulse Profiler can discover wireless APs and WLCs and test them whether they have SNMP v2 or v3 enabled with default public community strings or credentials.
	2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)	Pulse Profiler can collect list of ports that are running on servers which can be mapped to services. This can be used to figure out the functions on the servers and verify that they have only one primary function.
	2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	Profiler can find out list of open ports on a system and this information can be used to figure out whether only necessary services are running.
4 Encrypt transmission of cardholder data across open, public networks	**4.1** Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.	Pulse Connect Secure protects data in flight by transmitting all information protecting using TLS.

Requirement	Sub-requirement	How the Secure Access Suite solves it
	4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.	Pulse Connect Secure implements all industry standard TLS modes for protecting of data in flight.
5 Protect all systems against malware and regularly update anti-virus software or programs	**5.1** Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Host Checker can verify that anti-virus software is installed and running.
	5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	Host Checker can verify that anti-virus software is running and up to date.
	5.2 Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7.	Host Checker can check whether virus signatures are up to date.
6 Develop and maintain secure systems and applications	**6.2** Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	Host Checker can check patch status of a system and enforce access based on this status
	6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.	Pulse Policy Secure can enforce VLAN separation between test and development environments.
7 Restrict access to cardholder data by business need to know	**7.1** Limit access to system components and cardholder data to only those individuals whose job requires such access.	Pulse Policy Secure can authenticate users and enforce segmented access by assigning VLAN or ACL to access ports on switches/WLCs.
8 Identify and authenticate access to system components	**8.1.1** Assign all users a unique ID before allowing them to access system components or cardholder data.	Pulse Connect Secure and Pulse Policy Secure can integrate with different identity stores like AD, LDAP, SAML, MFA. This can be used by admins to track user access based on unique user ID.
	8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.	Admins can use PPS's guest management abilities to securely authenticate guests onto the network and provide them access for a limited period.
	8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	Pulse Connect Secure and Pulse Policy Secure can enforce session timeout forcing users to re-authenticate once the session expires.

Requirement	Sub-requirement	How the Secure Access Suite solves it
	8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric.	Pulse Connect Secure and Pulse Policy Secure support multi-factor authentication using SecurID, Duo, Google Auth for enhanced security.
	8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	Pulse Connect Secure uses TLS to encrypt all data in flight.
	8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	Pulse Policy Secure supports MFA (Secure ID, Duo and Google Authenticator)
	8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.	Pulse Connect Secure supports MFA (Secure ID, Duo and Google Authenticator)
9 Restrict physical access to cardholder data	**9.1.2** Implement physical and/or logical controls to restrict access to publicly accessible network jacks.	Pulse Policy Secure allow access only for authenticated users to get on to the network by setting VLAN/ACL on ports.
10 Track and monitor all access to network resources and cardholder data		
11 Regularly test security systems and processes	**11.1** Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.	Admins can use PPS Profiler to discover and monitor all wireless access points in the network. The Profiler dashboard can be used to act on unauthorized devices by removing them from the network (either physically, or via policy)
	11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.	PPS Profiler dashboard shows data on all discovered devices.
12 Maintain a policy that addresses information security for all personnel	**12.1** Establish, publish, maintain, and disseminate a security policy.	Pulse client and web access can show corporate access policy on login.

References

1. Internet Live Stats
   http://www.internetlivestats.com/one-second/
2. Verizon's 2016 Data Breach Investigations Report
   http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/?utm_source=pr&utm_medium=pr&utm_campaign=dbir2016
3. Cisco 2017 Annual Cybersecurity Report
   http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017
4. 2016 Cost of Data Breach Study: Global Study
   https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN
5. PCI DSS
   https://www.pcisecuritystandards.org