PCI COMPLIANCE IN THE IOT AGE

With the advent of the Internet of Things (IoT), businesses are experiencing a digital transformation bigger than the PC and Mobile revolution combined. Companies are using these wirelessly connected devices to become more productive, collect and gather information, and conduct transactions. But these new unmanaged devices bring new issues and questions as businesses look to ensure compliance with the Payment Card Industry Data Security Standards (PCI DSS). This white paper outlines how the Armis' agentless IoT security platform helps organizations protect themselves and meet PCI DSS requirements.

The Problem

Traditionally, enterprises have deployed a variety of IT controls to comply with the PCI DSS regulation – strong access controls, vulnerability assessment, file integrity monitoring, log monitoring, antivirus, and other controls. This combination of controls works fine when all devices that handle cardholder data are 1) on the wired network, 2) manageable with agents, and 3) can not communicate via unmonitored radio frequencies such as Bluetooth.

However, for most organizations, those conditions can no longer be guaranteed. Businesses are in the midst of a digital and wireless transformation that leverages a new breed of devices that are always on, always connected, and contain many options for transferring data. These modern devices bring difficulties in terms of proving compliance with PCI regulations. When you try to use traditional PCI security controls with this new breed of devices, you encounter the following gaps:

- Traditional host-based security products – These rely on the presence of security agents or administrative credentials to the host system. Many modern devices cannot accommodate an agent or traditional host scanning technologies.
- Traditional network-based security products – These are only effective on traditional wired (802.3) and wireless (802.11) IP networks. But many modern devices – including PCs, laptops, tablets, point of sale (POS) devices, and others – are able to communicate via Bluetooth and other non-traditional wireless protocols that are invisible to the traditional security products.

	Traditional PCI Controls
Host can run an agent	✅
Wired networks	✅
WiFi (802.11) Networks	✅
Host cannot run an agent	❌
Bluetooth communication	❌
Zigbee	❌
Unauthorized 802.11	❌

In response to the rapidly growing number of breaches that involve Internet of Things (IoT) and unmanaged devices, PCI auditors and assessors have started asking very pointed questions as to whether organizations have appropriate controls to meet the expansive requirements of PCI DSS. Here are some of the trends and predictions that PCI assessors are aware of:

- The number of unmanaged but communicating “things” grew 31% in 2017. (Gartner)
- 46.6% of enterprises reported that they have had a breach or security incident associated with IoT security. (IDC)
- Market research firm Gartner predicts that by 2020, one-third of successful attacks experienced by enterprises will be on data located in shadow IT resources, including shadow Internet of Things (IoT)."
- A new type of exploit, called an “airborne” attack, is able to travel through wireless protocols and attack the target device without the need for any user interaction. BlueBorne is one such attack that was announced in late 2017.

The Solution: Armis

Armis helps you meet PCI-DSS 3.2 requirements by documenting, monitoring, and enforcing policy on all devices in the cardholder data environment – including those that are beyond the reach of traditional controls such as endpoint security or network firewalls. The Armis solution monitors wired, WiFi, Bluetooth, and a wide variety of wireless protocols to ensure that organizations can see what is truly happening in both their retail and corporate environments. Armis continuously monitors all devices for threats and signs of risk, and can proactively prevent any unauthorized access. This includes providing coverage and security for:

- Point-of-sale devices
- Mobile devices, personal computers, or servers
- IoT and unmanaged devices
- Wireless hotspots
- The transmission of cardholder data to service providers
- Network connections

Designed to help ensure that merchants meet minimum levels of security when they store, process and transmit cardholder data, PCI DSS covers six objectives that are mapped to 12 specific requirement areas. Below is a summary of how Armis can help you meet specific PCI DSS requirements.

PCI Requirements Addressed by Armis

PCI Requirement 1

Install and maintain a firewall configuration to protect cardholder data.

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a sensitive area. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All cardholder data systems and networks must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems which violate the PCI requirements.

Req.	Definition	Armis
1.1.2	Maintain a current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	Armis helps organizations identify all connections between the cardholder data environment and other networks including wired, WiFi, Bluetooth, and other common IoT protocols. This helps organizations identify all unintended connections including connections to rogue access points, network bridging, and direct device-to-device connections or pairing.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	Armis can identify unauthorized connections between the managed network and unmanaged network environments such as rogue 802.11 devices or pineapples. These connections can provide hidden pathways to the Internet and the cardholder data environment.

PCI Requirement 2

Do not use vendor-supplied defaults for system passwords and other security parameters.

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

Req.	Definition	Armis
2.3	Using strong cryptography, encrypt all non-console administrative access. (Where Secure Sockets Layer (SSL)/early Transport Layer Security (TLS) is used, the requirements in PCI DSS Appendix A2 must be completed.)	Armis can detect unencrypted WiFi traffic within the cardholder data environment.
2.4	Maintain an inventory of system components that are in scope for PCI DSS.	Armis discovers and documents all devices in the cardholder data environment, including non-traditional devices such as keyboards and mice that can communicate via wireless protocols with systems that store cardholder data. Armis tracks this information over time, providing a historical view of devices and their activity, including transient devices. This helps you build a complete inventory of components that are within scope of the PCI DSS requirements.

PCI Requirement 4

Encrypt transmission of cardholder data across open, public networks.

Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including:

- The Internet
- Wireless technologies, including 802.11 and Bluetooth
- Cellular technologies
- General Packet Radio Service (GPRS)
- Satellite communications

Req.	Definition	Armis
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks (e.g. Internet, wireless technologies, cellular technologies, General Packet Radio Service [GPRS], satellite communications). 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.	Armis can detect and alert on unencrypted WiFi traffic within the cardholder data environment.

PCI Requirement 6

Develop and maintain secure systems and applications.

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.

Req.	Definition	Armis
6.1	Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities..	Armis' Risk Analysis Engine will tell you which devices in your environment (on and off your network) are vulnerable. The numerical risk score ranges from 1 to 10 and is based on factors such as device type, behavior, operating system, connections, reputation, version, and other factors. The scope includes all devices in your environment including non-computing devices such as point-of-sale devices, building automation devices, routers, switches, etc.
6.4.1	Separate development/test environments from production environments, and enforce the separation with access controls.	Armis can identify connectivity between development, test and production environments and, in doing so, validate that your existing controls are comprehensive and effective.

PCI Requirement 9		
Restrict physical access to cardholder data. Any physical access to data or systems that house cardholder data provides the opportunity for persons to access and/or remove devices, data, systems or hard copies, and should be appropriately restricted. To protect physical access, first you need to have an accurate inventory of all devices.		
Req.	**Definition**	**Armis**
9.9.1	Maintain an up-to-date list of devices. The list should include the following: ● Make, model of device ● Location of device (for example, the address of the site or facility where the device is located) ● Device serial number or other method of unique identification.	Armis discovers all devices on your network and provides information such as the make, model number, location, and other important details.

PCI Requirement 10		
Track and monitor all access to network resources and cardholder data. Logging mechanisms and the ability to track user activities are critical for effective forensics and vulnerability management. The presence of logs in all environments allows thorough tracking and analysis if something goes wrong. Determining the cause of a compromise is very difficult without system activity logs.		
Req.	**Definition**	**Armis**
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity. Perform critical log reviews at least daily.	Armis' Risk Analysis Engine automatically analyzes logs and security events from all devices in the cardholder environment, including devices that do not have IP addresses such as Bluetooth keyboards or card readers, to identify anomalies or suspicious activity. Armis compares observed device characteristics and behavior against a baseline of normal behavior for each type of device. The baseline includes both what we have observed in the customer's environment over time and also what we have observed in other customers' environments, allowing us to detect threats from "patient zero" devices.
10.7	Retain audit trail history for at least one year; at least three months of history must be immediately available for analysis	Armis maintains historical data for future analysis. The data is always visible in the user interface.

PCI Requirement 11

Regularly test security systems and processes.

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

Req.	Definition	Armis
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. Maintain an inventory of authorized wireless access points and implement incident response procedures in the event unauthorized wireless access points are detected.	Armis continually monitors the local airspace and automatically detects and alerts on the presence of any unauthorized access points on or near to the enterprise network. Rogue access points near to the enterprise network represent a very high risk as they could provide a path for data exfiltration which bypasses traditional network firewalls and PCI controls. Armis monitors for a wide variety of intrusion techniques, bridges, or unsafe connections that could expose cardholder data. Armis can automatically implement incident response procedures in the event that unauthorized wireless access points are detected — alert administrators and/or block unauthorized communication. Armis can automatically isolate unauthorized wireless access points either connected to the enterprise network or near to the enterprise network. The latter condition represents a much higher risk as it could be a direct path for data exfiltration which bypasses traditional network firewalls. Armis can identify details of wireless access points (model number, SSID, location, etc.) in order to build an inventory. Armis can automatically

		implement incident response procedures in the event that unauthorized wireless access points are detected — alert administrators and/or block unauthorized communication.
11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change in the network. Address vulnerabilities and perform rescans as needed, until passing scans are achieved. After passing a scan for initial PCI DSS compliance, an entity must, in subsequent years, complete four consecutive quarters of passing scans. Quarterly external scans must be performed by an Approved Scanning Vendor (ASV). Scans conducted after network changes and internal scans may be performed by internal staff.	Armis can provide an internal network vulnerability assessment. Armis' risk analysis engine will tell you which devices on your network are vulnerable. Armis assigns a risk score, from 1 to 10, for each device on your network. The scope includes all devices on the network including non-computing devices such as routers, switches, point-of-sale devices, building automation devices, etc.
11.4	Use network intrusion detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. IDS/IPS engines, baselines, and signatures must be kept up to date.	Armis' Risk Analysis Engine uses machine learning behavioral analysis in addition to expert rules to detect network intrusions within the cardholder data environment.

About Armis

Armis is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust our unique out-of-band sensing technology to discover and analyze all managed, unmanaged, and IoT devices—from traditional devices like laptops and smartphones to new unmanaged smart devices like smart TVs, webcams, printers, HVAC systems, industrial robots, medical devices and more. Armis discovers devices on and off the network, continuously analyzes endpoint behavior to identify risks and attacks, and protects critical information and systems by identifying suspicious or malicious devices and quarantining them. Armis is a privately held company and headquartered in Palo Alto, California.

arims.com

(20190523.1)