



Ensuring PCI DSS Compliance with the Mist Learning WLAN

THE SAFE CHOICE FOR MISSION CRITICAL
WIRELESS NETWORKS IN PCI ENVIRONMENTS



Table of Contents

Ensuring PCI DSS Compliance with the Mist Learning WLAN.....1
Cloud Security.....1
Network Segmentation.....1
Protect Network From External Attacks.....2
Securing Wireless in the Cardholder Data Environment (CDE).....3
Summary.....4

Ensuring PCI DSS Compliance with the Mist Learning WLAN

The Payment Card Industry Data Security Standard (PCI DSS) was created as a common standard to protect against credit card and payment data fraud in the retail space (and other industries, like banking, where online payments are made). By providing consistent and holistic security policies and best practices, PCI DSS enables security personnel and network administrators to effectively thwart various threats to payment data. The latest version of PCI DSS which is 3.2, went into effect for assessments in October, 2016.

As one can imagine, the network is a critical cornerstone of PCI DSS compliance as it is a main artery for passing payment data. PCI DSS requirements are designed to ensure that network security operations and practices eliminate or minimize known risks. Plus, they ensure that the organization defines traceable well-structured policies, procedures, and practices that can be audited.

The wireless network in particular is especially important to retail environments as business operations and digital engagement technologies rely upon mobile connectivity. Point of Sale devices, scanners, barcode readers, printers, and mobile computers, for example, all operate on Wireless LANs (WLAN) that serve as the lifeblood of retail operations. Given the importance of WLANs, there are two types of requirements specifically outlined for the PCI DSS compliance of wireless networks. These include:

- **Generally applicable wireless requirements.** These are requirements that apply even when the wireless network is not in scope of the Cardholder Data Environment (CDE). They include strong network segmentation to protect the CDE network and security against attacks from rogue or unknown wireless Access Points and clients.
- **Securing wireless in a CDE environment.** These are requirements mandated for systems that transmit payment card information over wireless technology. In addition to generally applicable wireless requirements, they impose additional security requirements for changing default passwords and configurations, using strong encryption and authentication, regular updating of the system with compliant software, and monitoring access.

This paper addresses how the Mist Learning WLAN delivers a robust PCI-compliant solution.

Cloud Security

The Mist cloud is outside the CDE environment as it does not carry any wireless packet data. Regardless, Mist takes additional measures to ensure the highest level of security in the Mist cloud. For example:

- Mist uses a type2 soc2 cloud data center.
- User access is highly restricted.
- Industry standard encryption is utilized at various levels.
- Any information stored in the cloud is obfuscated with an organization-specific key.
- Security is integrated with development cycles, and pen tests are performed to detect vulnerabilities at the network and application levels.

Network Segmentation

All of the following schemas can be implemented in a Mist environment to ensure network segmentation:

Physical Segmentation: One way to achieve network segmentation is to connect the wireless Access Points on a wired network that is physically separate from the CDE network. This would imply having an overlay wired and wireless infrastructure that does not have any intersection with the wired network for the CDE environment. In this scheme, there is no firewall or internet connection that is shared between the CDE and non-CDE networks.

VLAN based logical segmentation: It is common to use Virtual LANs (VLANs) to segment the networks into logical subnets. While it is possible to achieve logical segmentation by having the wireless network and the CDE in different VLANs, this methodology is not considered a safe and secure way to protect the network, without adequate access control policies between VLANs.

Firewall separation: If the wireless LAN is connected to the CDE, instituting a Firewall between the Wireless network and the CDE network is an acceptable form of segmentation that conforms to PCI DSS 3.2 requirements.

Software defined policy engine. Mist's integrated WxLAN policy engine can be used to isolate any wireless traffic into the CDE environment. Mist delivers a powerful platform when it comes to creating policies for role, user, application and resource based access on the network via its inline policy engine - WxLAN. The Mist wireless infrastructure allows policies to be enforced on any wired network with access to the LAN blocked for all WLANs configured in the system.

Protect Network From External Attacks

To ensure the wireless network is compliant with the generally applicable requirements for PCI DSS, retailers need to pay special attention to the following:

- **Rogue Devices:** These are accidental or malicious Access Points on the wired network that can be used to violate internal networks with access to all network resources.
- **Honeypot devices:** these are accidental or malicious Access Points that masquerade as sanctioned Access Points beaconing a retailer's Access Points.
- **Non-compliant and unsanctioned Access Points:** These range for Access Points that may be sanctioned Access Points but out of compliance running old firmware without critical security fixes. Similarly, these may also include Access Points that are neighbors as well as those causing inadvertent interference to the wireless operations inside the four walls of a retail store or warehouse.

Two activities are required for handling these external devices, often referred to as Wireless Intrusion Detection and Prevention (WIDS/WIPS):

- Monitor the RF environment to find and analyze the existence of above.
- Isolate any Wi-Fi Access Points not used to transmit or receive cardholder data.

Traditionally there have been several ways in which WLAN vendors have addressed the above requirements for WIDS/WIPS compliance:

- **Part time scanning.** In this mode, Access Points when not serving clients scan the spectrum for rogue devices. This is almost akin to having a security solution that only works some of the time – not 24x7.
- **Dedicated Access Points** provide 24x7 security monitoring of the wireless spectrum. While this does protect the network all the time, it explodes the deployment cost for additional AP's with associated installation cost of PoE cable runs to the IDF/MDF to power up the sensors.
- Some vendors use dual-banded radios in Access Points, and steal a radio within an Access Point for sensor implementation leading to nightmares in channel planning and insufficient coverage for clients in the network.
- Some vendors, while offering a tri-radio Access Point solution with a dedicated third radio, deploy a complete overlay monitoring solutions orthogonal to the rest of the Wireless infrastructure and Controller solution with isolated islands of data sources, databases, visualization and even separate controls for radio configuration, control and provisioning.

The Mist Access Points provide continuous 24x7 scanning of the spectrum alongside 2.4Ghz and 5Ghz client access. This allows Mist to continually scan the spectrum for rogues, honeypots, interferers and for other anomalies such as unsuccessful connection attempts at a site (which may be a source for a DDOS attack).

In addition, unlike traditional vendors, the Mist platform maintains a state machine and a baseline on key metrics for every physical device (Access Point, clients) and logical entity (location, site, site-groups) that complements flow information and a rich elastic cloud data store. Mist's AI powered infrastructure identifies unusual activity at every level of the network and this way the Mist platform can detect existing and zero-day threats. In addition, Mist's location technology can be used to accurately locate accidental or malicious rogue devices and





provide location-based access to resources. Mist’s Machine Learning framework can be extended to behavioral analytics whereby client device capabilities can be checked against the “normal” baseline and alerts generated when key postures change (e.g. a 4x4 client device appears as a 2x2 device or a client device sanctioned for a California location appears to access the network from New York).

Securing Wireless in the Cardholder Data Environment (CDE)

As mentioned above, the second set of requirements applies to wireless devices on the same network where credit card data is handled. Mist allows you to conduct a PCI scan for the VLAN’s and Wireless LAN’s in scope, and helps you remediate both the vulnerabilities on the wireless network and enforce policies on the wireless management system.

The following is how Mist addresses the main requirements for these “in scope” wireless networks to be PCI DSS compliant:

| PCI DSS REQUIREMENTS V3.2 FOR WIRELESS | MIST CONFORMS | MIST VALUE PROPOSITION |
|--|---------------|--|
| 1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks. | ✓ | Mist’s PCI scan report identifies the list of wireless SSIDs and Access Points that connect with the CDE. |
| 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. | ✓ | Mist does not have default passwords, encryption keys or SNMP community strings. |
| 2.4 Maintain an inventory of system components that are in scope for PCI DSS. Maintain an inventory of system components that are in scope for PCI DSS. | ✓ | Mist provides a list of wireless networks and Access Points that are in scope of PCI DSS. |
| 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. | ✓ | Mist supports strong encryption standards, including WPA2-PSK, and WPA2-Enterprise with AES encryption. As part of its PCI scan report, Mist calls out any weak encryption used on SSID in scope of the CDE. |
| 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. <i>Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.</i> | ✓ | Mist makes available the latest released firmware that includes any critical fix required for the integrity of the wireless network. Mist identifies any Access Point that has not yet been upgraded to the latest firmware. |
| 7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. | ✓ | Wireless network access is restricted to authorized administrators. All authorized administrators are listed on the Mist PCI scan report. |
| 7.2 Establish an access control system(s) for systems components that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed. | ✓ | Mist Network Administrators are assigned roles with limited scope of access. Default administrator role is Observer (View-only). |
| 8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data. | ✓ | Mist’s PCI scan report identifies the list of wireless SSIDs and Access Points that connect with the CDE. |
| 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: <ul style="list-style-type: none"> • 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 | ✓ | All Mist administrators are authenticated using complex passwords. |

| | | |
|--|---|---|
| <p>9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.</p> |  | <p>Mist Access Points can be made physically secure with the help of screws and brackets available as part of the access point kit. Additional physical security is supported with the Kensington lock slot on the Access Point.</p> |
| <p>10.1 Implement audit trails to link all access to system components to each individual user.</p> |  | <p>All system access, updates and configuration changes are tracked in an audit log.</p> |
| <p>10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.</p> |  | <p>All event logs are stored in centralized servers in the Mist cloud platform hosted in a Type 2 SOC 2 Data Center.</p> |
| <p>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.</p> <p><i>Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.</i></p> |  | <p>Mist WIDS/WIPS allows detection of authorized and unauthorized access points on the network, eliminating the need for manually intensive wireless scans. Specifically, rogue Access Point detection and containment protects the CDE network from being compromised.</p> |

Summary

As organizations rely more on wireless networks as a key enabler for business services, PCI DSS requires careful attention to WLAN security. Fortunately, Mist has you covered. By protecting wireless networks from external attack and ensuring data transferred on CDE networks is always secure, the Mist Learning WLAN is a safe choice for mission critical wireless networks in PCI environments. The key difference in the Mist architecture is how the workflows have been streamlined to enable a cohesive experience for network IT, Security Operations Teams, Marketing and other lines of business. With Mist, access layer connectivity and associated applications is now all about delivering a comprehensive, amazing and secure experience.