WHITE PAPER

HP POS SYSTEMS

PCI DSS COMPLIANCE WHITE PAPER

HP Inc.

Joel Dubin | CISSP, QSA, PA-QSA

COALFIRE

North America | Europe
877.224.8077 | info@coalfire.com | Coalfire.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

HP Inc. (HP) engaged Coalfire Systems Inc. (Coalfire), a respected Qualified Security Assessor (QSA) for the Payment Card Industry (PCI) to conduct an independent technical assessment to review the HP POS Systems for security and applicability to the requirements of the PCI Data Security Standard (PCI DSS) v3.2.1. Coalfire conducted assessment activities including technical testing, architectural assessment, and validation of compliance with PCI DSS applicable requirements.

In this paper, Coalfire will describe which requirements of the PCI Data Security Standard (PCI DSS) v3.2.1 were applicable and supported by their HP POS Systems based on the sample testing and evidence gathered during this assessment. The PCI DSS requirements that were applicable have been included in the matrix in Appendix A. This includes a table that maps the HP Security Technologies to specific requirements of the PCI DSS.

ABOUT HP POS SYSTEMS

The HP POS Systems consist of a touch display with compute power that can be mounted on the stand provided by HP or used separately from the stand as a mobile tablet in the case of the HP Engage Go. The touchscreen devices can run the Windows, Android and Linux operating systems (OS) with HP tools and security features pre-installed. However, the system was only tested for this white paper with Windows 10 Pro and Windows 10 IoT. The device comes installed only with the operating system and the HP applications and no other third-party software. None of the pre-installed HP applications are credit card payment applications. Any payment application or POS software is installed by the customer on the HP POS System. The device can accommodate any payment software chosen by the customer that can be installed on Windows 10 Pro OS. It can also work with a Magnetic Stripe Reader (MSR) to read swiped credit card data directly.

The PCI DSS scope of the HP POS Systems depends on the nature of the payment software installed by the customer. If payment software installed on the device accepts, transmits, processes or stores credit card data transactions, such as in an integrated payment solution, the device would be in scope for the customer's PCI DSS compliance. If the device serves as just a touch screen for selecting merchandise to purchase and does not handle any credit card transactions, the device may or may not be within the cardholder data environment (CDE) of the merchant and may not be in scope for PCI DSS. In one scenario, card transactions are handled by a separate system, such as a PIN-pad in a semi-integrated solution. The scope would depend on the segmentation of the merchant network where the HP POS System is deployed. Even if the device may not be in scope for PCI DSS, the customer would still be responsible, as part of their PCI DSS assessment, for identifying how the device impacts the security of the CDE.

This white paper will demonstrate how the HP POS Systems maintain PCI DSS compliance for the customer in the case where the HP POS Systems are within the CDE of the merchant as in an integrated payment solution and, as a result, are in scope for their PCI DSS compliance.

The following components of the HP POS Systems were reviewed:

1. HP Engage One Pro – A versatile AiO retail point of sale system, with screen sizes of 15.6", 19.5", or 23.8", that can be used with in a standard mount position on the counter, as a self-service kiosk or on a VESA mount. Using the merchant software, it can be configured to be a point of sale terminal or a non-attended kiosk, with payment application for accepting payments.
2. HP Engage Go – A 12" versatile tablet that can be used as a mobile point of sale system, on the HP Convertible Dock as a fixed system on the counter, or with other mount solutions including VESA, on the wall or on a pole. It serves the same touchscreen functions as the HP Engage One

Pro, and can be configured to be a point of sale terminal or a non-attended kiosk, with payment application for accepting payments.

3. HP Engage Console – Complete cloud-based endpoint management solution for remote management of HP POS Systems. Both HP and non-HP devices, including mobile Android and iOS devices, can be registered and administered remotely. The customer can add any number of devices in their network to the console, allowing all to be remotely managed from a single online location. The console can lock down any registered devices to meet security or compliance standards.

HP POS Systems Security Features

The HP POS Systems have the following security features and security software, either pre-installed or available for download, which were reviewed as part of the security assessment for this white paper:

- Device/Data Protection
    1. HP BIOSphere – Can help protect against a variety of attacks or corruption, including attacks that target the Master Boot Record (MBR) and GUID Partition Table (GPT); attacks that attempt to enter through unauthorized wireless bridging; and more, including new types of malware that may be created to target the BIOS in the future. It can also help protect against physical attacks on the device, with features like BIOS passwords, port controls, and HP Secure Erase.
    2. HP Secure Erase – Provides secure deletion of data from hard drives, including solid state drives, and destruction of media, when necessary.
    3. HP Smart Dock (available only on HP Engage Go and HP Engage Go 10) – Software that provides configuration and authentication for unlocking the HP Engage Go tablet from its dock using either privileged users or PIN.
    4. HP Sure Admin – Provides modern security for PC firmware configuration management by enabling remote administrators to securely manage BIOS settings and field support personnel to obtain secure in-person access to BIOS setup. Use of digital certificates and public-key cryptography eliminates the risks associated with legacy password-based approaches.
    5. HP Sure Recover – Uses the HP Endpoint Security Controller to allow users to support recovery from a network connection with the latest operating system image. HP Sure Recover can quickly and securely reimage HP POS Systems to the latest OS image even from a blank hard drive, enabling it to automatically recover if no OS is found on the HP POS System.
    6. HP Sure Run – Hardware enforced by the HP Endpoint Security Controller. HP Sure Run continuously monitors critical services, processes and settings. HP Sure Run detects attacks and restores applications to their original state.
    7. HP Sure Start – Automatically detects, stops and recovers from a BIOS attack. HP Sure Start is automatic firmware intrusion detection. Every time the HP POS System is booted up, HP Sure Start validates the BIOS and then acts as an intrusion detection system to monitor memory. In case of attack, HP Sure Start uses a previously stored clean copy of the BIOS to repair itself.
    8. HP Wolf Security for Business, which includes the following:

a. HP Sure Click – Provides secure browsing of the Internet and viewing of documents. HP Sure Click opens web sites and untrusted documents in a virtual machine (VM) to isolate web sites or documents that may contain malware.

b. HP Sure Sense – Uses deep learning to prevent and detect malware attacks. HP Sure Sense uses predictive models in addition to file matching. HP Sure Sense provides alert logs of possible attacks.

- Identity Protection
  1. HP Client Security Manager – Provides the strength of hardware-based security authentication to support the efforts of users and IT professionals to protect by configuring and controlling a variety of security features embedded in HP PCs within the OS, including HP Sure Run and HP Sure Recover.

- HP Endpoint Security Controller – Physically isolated and cryptographically protected hardware microcontroller below the OS creates the hardware root of trust that enables hardware-enforced, self-healing, manageable security solutions like the HP BIOSphere Sure Start, HP Sure Run, and HP Sure Recover. This is at the core of the HP security stack, providing threat protection and system recovery, starting at the hardware level.

- Manageability Solutions
  1. HP Engage Console (requires subscription) – Provides device management, software distribution, application management, remote communications, and support features for retail point-of-sale devices and apps.
  2. HP Image Assistant (HPIA) – A Windows image comparison tool for comparing image configurations and recommends configurations for optimal Windows performance.
  3. HP Manageability Integration Kit (MIK) – Helps speed up image creation and management of HP BIOS, security, hardware, software through a graphical user interface when managing devices through Microsoft Endpoint Configuration Manager (previously SCCM).

- Physical Security Features Unique to HP POS Systems
  1. Biometric & NFC – Ability to add biometric or Radio Frequency Identification (RFID) authentication to the device.
  2. Chassis Locks– Locations on device housing to allow cable locks to be attached.
  3. Encryption-capable MSRs – Ability to add MSRs that encrypt credit cards at the point of swipe.
  4. Intrusion Sensors – Cables with motion sensors for detecting tampering of the device.
  5. Port Disablement – Ability to turn off USB ports within the BIOS.

AUDIENCE

This assessment white paper has three target audiences:

1. **QSA and Internal Audit Community:** This audience may be evaluating the HP POS Systems to assess a merchant or service provider environment for PCI DSS.
2. **Administrators and Other Compliance Professionals:** This audience may be evaluating the HP POS Systems for use within their organization for compliance requirements for both PCI DSS and other security standards.
3. **Merchant and Service Provider Organizations:** This audience may be evaluating the HP POS Systems for deployment in their CDE and how the security of the system provided by the HP security features complies with applicable PCI DSS requirements.

METHODOLOGY

Coalfire completed a multi-faceted technical assessment during the course of this project using the below industry and audit best practices. Coalfire conducted technical testing in their Colorado lab from June 7, 2021 to June 18, 2021.

Testing consisted of the following tasks:

1. Performing a technical review of the architecture and documentation of the HP POS Systems solutions and their components.
2. Reviewing each of the security features by running them both directly on the HP POS Systems and remotely through the HP Engage Console. All features were installed on a Microsoft Windows 10 OS already implemented on the HP POS System.
3. Reviewing configuration settings for the security features and the menu options, where applicable, for each security feature on the HP POS System.
4. Adding test users to the HP POS Systems, both directly on the device and remotely with the HP Engage Console, to check how password policies are configured. Also, adding additional authentication, (e.g., adding a PIN), to check multi-factor authentication.
5. Reviewing audit logging both through Windows Event Viewer and the Alert Logs provided by HP Sure Sense to verify PCI DSS audit logging requirements.
6. Using the HP Engage Console to add HP POS Systems and remotely configure them, including for compliance policy and password settings. HP POS Systems can also be updated to latest firmware.
7. Reviewing each feature according to their impact on each of the requirements of the PCI DSS standard, as follows. The PCI DSS standard is made up of 12 requirements, which can be grouped into six major control objectives:

OBJECTIVES	REQUIREMENTS
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

OBJECTIVES	REQUIREMENTS
	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
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

SUMMARY FINDINGS

The following findings are relevant highlights from this assessment:

The HP POS Systems can be configured to help a merchant meet the following applicable requirements of PCI DSS.

The following are only a highlight of the key PCI DSS requirements covered by the HP POS Systems. The table that follows goes into detail with explanations about all of the requirements.

1. Do not use vendor-supplied defaults for system passwords and security parameters (Requirement 2.1)
2. Protect stored cardholder data (Requirement 3.1)
3. Protect all systems against malware and regularly update anti-virus software or programs (Requirements 5.1, 5.2 and 5.3)
4. Identify security vulnerabilities, and protect all system components from known security vulnerabilities by installing applicable vendor-supplied security patches. (Requirements 6.1 and 6.2)
5. Restrict access to cardholder data by business need to know (Requirement 7.2)
6. Identify and authenticate access to system components (Requirements 8.1.x, 8.2.x and 8.3.x)
7. Restrict physical access to cardholder data (Requirements 9.5 and 9.8.2)
8. Track and monitor all access to network resources and cardholder data (Requirements 10.3.x, 10.5 and 10.6)
9. Use an intrusion-detection system to monitor system traffic, provide file-integrity monitoring and regularly test security systems and processes (Requirements 11.4 and 11.5)
10. Provide features required for an incident-response plan (Requirement 12.10.1)

The following are the details for specific features of compliance for all 12 of the individual PCI DSS v3.2.1 requirements. Please not that any sub-requirement not mentioned is not applicable to any HP POS System feature:

Requirement	HP POS Feature	HP Responsibility	Customer Responsibility
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.	Not Applicable	Not Applicable The Microsoft Windows 10 OS hosting the HP POS Systems have Windows 10 Defender firewall, which are personal firewalls that can be implemented at the discretion of the customer, to assist in meeting this PCI DSS requirement.	Setting up, configuring and maintaining personal firewalls is the responsibility of the merchant implementing the HP POS Systems. However, the Microsoft Windows 10 OS hosting the HP POS Systems have the Windows 10 Defender firewall that can assist in meeting this PCI DSS requirement.
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	HP Engage Console	Not Applicable None of the features of the HP POS Systems have default passwords supplied by HP.	The Engage Console has the capability to create and apply password policies. You can set things such as minimum password length, enforce complex password, etc. From there you can then manage password settings such as password expiry period, maximum password history list, maximum failed attempts to Factory Reset.
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: -Limiting data storage amount and retention time to that which is required for legal,	HP Secure Erase HP Sure Click HP Sure Sense	Not Applicable The HP POS System does not by itself store card data and is not required by PCI DSS to implement card data retention and disposal policies. However, if the system is hosting a payment application, it still provides the following features that aid in securing card data:	If the HP POS System is hosting a payment application, as in a semi-integrated solution, for example, and needs to store credit card data, the customer is required to follow this PCI DSS requirement for storage and disposal of card data, including data retention period.

regulatory, and/or business requirements -Specific retention requirements for cardholder data -Processes for secure deletion of data when no longer needed -A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.		HP Sure Sense provides protection from malware attacks against files, which could include files with credit card data implemented on the system by the customer. HP Sure Click runs untrusted files in a secure VM, which could prevent attacks against credit card data. HP Secure Erase provides secure deletion of data, which could include credit card data implemented on the system by the customer.	
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: -Only trusted keys and certificates are accepted. -The protocol in use only supports secure versions or configurations. -The encryption strength is appropriate for the encryption methodology in use.	Not Applicable	Not Applicable The HP POS Systems only transmit card data when a payment application is installed on the device. The devices themselves do not provide a facility to transmit data and do not require secure transmission of data.	The payment application vendor, or the merchant where the HP POS System is deployed, would be responsible for either providing mechanisms for the secure transmission, or for the ability to configure the secure transmission, of card data from the device to the processor.
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	HP Endpoint Security Controller HP MIK HP Sure Run HP Sure Sense	HP POS Systems can assist in meeting the PCI DSS requirement for anti-virus software. HP POS Systems allow third-party anti-virus	The merchant deploying the HP POS System is responsible for providing anti-virus software, making sure it is always running and is regularly updated.

	HP Sure Start	software to be installed, as required by PCI DSS. HP Sure Run feature, which is part of the HP Endpoint Security Controller, monitors anti-virus software to make sure it is always running and enabled, also required by PCI DSS. Backs up a good copy of the BIOS, in case it gets corrupted. HP Sure Start similarly protects the BIOS from attempts at malicious activity. It validates the BIOS at boot up and then monitors it for malicious activity. HP Sure Sense using deep learning models to prevent malware attacks acting in a similar way to anti-virus software. The HP MIK can also be used to configure the above security features.	
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.	HP Endpoint Security Controller HP Sure Run HP Sure Sense	HP Sure Sense using deep learning models to prevent malware attacks acting in a similar way to the way anti-virus software is updated. HP Sure Sense provides monitoring of security alerts and logs them to its Alert Log. HP Sure Run feature within the HP Endpoint Security Controller enforces logging at the hardware level. HP Sure Run logs all its activity to Windows Event Log. HP Sure Sense provides monitoring of security	The merchant deploying the HP POS System is responsible for providing anti-virus software and making sure it is regularly updated and generates audit logs.

		alerts and logs them to its Alert Log.	
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	HP Sure Run HP Sure Start	HP Sure Run feature, which is part of the HP Endpoint Security Controller, monitors anti-virus software to make sure it is always running and enabled, also required by PCI DSS. Backs up a good copy of the BIOS, in case it gets corrupted. HP Sure Start similarly protects the BIOS from attempts at malicious activity. It validates the BIOS at boot up and then monitors it for malicious activity.	The merchant deploying the HP POS System is responsible for providing anti-virus software and making sure it is always running.
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.	HP BIOSphere HP Client Security Manager HP Sure Run	HP BIOSphere can be configured to use Windows Update to check for BIOS updates, which provides identification of security vulnerabilities. HP Sure Run protects running processes, including software and patch updating, that identify malicious attacks. HP posts security updates for each system: https://support.hp.com/us-en/product/hp-engage-go-mobile-system/23588898/bulletins-notices HP Sure Run can be configured stay up to date automatically through HP Client Security Manager: -Enable Auto Updates -Receive the latest Sure Run updates from HP	The merchant is responsible under PCI DSS for establishing a vulnerability management process in accordance with PCI DSS. The HP features can assist in identifying security vulnerabilities.

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.	HP BIOSphere HP Client Security Manager HP Sure Run	HP BIOSphere can be configured to use Windows Update to implement BIOS updates. HP Sure Run protects running processes, including software and patch updating. HP Client Security Manager can be configured to implement updates and patches.	The merchant is responsible under PCI DSS for establishing a process to implement security patches in accordance with PCI DSS. The HP features can assist in implementing patch deployment.
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.	HP Engage Console HP MIK HP Smart Dock	Both the HP Engage Console and HP Smart Dock can assist with meeting the PCI DSS requirement, by allowing separate access to be set up for privileged users on the HP POS Systems, in accordance with PCI DSS requirements to create a distinct group for privileged access. The HP MIK can also be used to configure the above security features.	The merchant is responsible for setting up user access in accordance with PCI DSS. Besides the HP features, the merchant can configure user access on the Windows 10 operating system hosting the HP POS System to create privileged groups, per PCI DSS.
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows: 8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data. 8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. 8.1.3 Immediately revoke access for any terminated users.	HP BIOSphere HP Client Security Manager HP Sure Admin	HP is not responsible for setting up authentication credentials, per PCI DSS, but provides tools for setting up authentication credentials and passwords to meet PCI DSS Requirements 8.1.1 through 8.1.8, such as unique user IDs and control over user provisioning, lockouts and time outs. HP Client Security Manager can be used to set up authentication credentials and passwords to meet PCI DSS	The merchant is responsible under PCI DSS for setting up authentication credentials and passwords to meet Requirement 8.1.1 through Requirement 8.1.8 but can also use access control features of the Windows 10 operating system or HP features to do so.

8.1.4 Remove/disable inactive user accounts within 90 days. 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. 8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts. 8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. 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.		Requirements 8.1.1 through 8.1.8. HP BIOSphere tool protects access to the BIOS at the hardware level, including the setting up and management of user credentials for BIOS access. HP Sure Admin provides functionality for setting up secure access to the BIOS for either local or remote administration using RSA public key cryptography rather than passwords, which are often exposed in BIOS administration.	
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. 8.2.1 Using strong cryptography, render all authentication credentials (such as	HP BIOSphere HP Client Security Manager HP MIK HP Sure Admin	HP is not responsible for setting up authentication credentials, per PCI DSS, but provides tools for setting up password parameters to meet PCI DSS Requirements 8.2.1 through 8.2.6, including password length, complexity. HP BIOSphere tool protects access to the BIOS at the hardware level, including the setting up and management of passwords for BIOS access. HP Sure Admin provides functionality for setting up secure access to the BIOS for either local or remote	The merchant is responsible under PCI DSS for setting up passwords to meet Requirement 8.2.1 through Requirement 8.2.6 but can also use password control features of the Windows 10 operating system or HP features to do so.

passwords/phrases) unreadable during transmission and storage on all system components. 8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys. 8.2.3 Passwords/passphrases must meet the following: Require a minimum length of at least seven characters. Contain both numeric and alphabetic characters. Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above. 8.2.4 Change user passwords/passphrases at least once every 90 days. 8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used. 8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.		administration using RSA public key cryptography rather than passwords, which are often exposed in BIOS administration. The HP MIK can also be used to configure the above security features.	
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	HP Client Security Manager	HP is not responsible or required to set up multi-factor authentication, if required by the customer. However, the HP Client Security Manager has tools	The merchant is responsible under PCI DSS for setting up multi-factor authentication, if needed for Requirements 8.3.1 and 8.3.2 but can use features in the HP

8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access. 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.		for configuring multi-factor authentication, including PINs, cards and biometrics, if necessary	Client Security Manager to do so.
9.5 Physically secure all media.	Biometric & NFC Chassis Locks Encryption-capable MSRs Intrusion Sensors Port Disablement	Not Applicable Physical security is always the responsibility of the merchant in PCI DSS. However, HP POS Systems have physical security safeguards that can assist the customer with their PCI DSS compliance. HP POS Systems have locks, sensors, biometrics and port disablement available to physically lockdown and prevent access to the device itself.	The merchant is responsible under PCI DSS for providing physical security for the CDE. However, the merchant can use the physical security tools provided with the HP POS System to aid in meeting PCI DSS compliance for this requirement.
9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	HP Secure Erase	HP Secure Erase provides for the secure destruction of media, including media with credit card data. HP Secure Erase uses the industry standard NIST SP800-88 Rev 1 for secure destruction of electronic media.	The merchant is responsible under PCI DSS for providing secure destruction of card data on electronic meda. However, the merchant can use HP Secure Erase provided with the HP POS System to aid in meeting PCI DSS compliance for this requirement.
10.3 Record at least the following audit trail entries for all system components for each event:	HP Endpoint Security Controller HP Sure Run HP Sure Sense	HP POS Systems provide two types of logging that can assist the customer with meeting this requirement of PCI DSS.	The merchant is responsible under PCI DSS for providing logging. However, the merchant can use the logging tools provided with the HP POS

10.3.1 User identification 10.3.2 Type of event 10.3.3 Date and time 10.3.4 Success or failure indication 10.3.5 Origination of event 10.3.6 Identity or name of affected data, system component, or resource 10.5 Secure audit trails so they cannot be altered. 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.	HP Sure Start	HP Sure Run feature within the HP Endpoint Security Controller enforces logging at the hardware level. HP Sure Run logs all its activity to Windows Event Log. HP Sure Sense provides monitoring of security alerts and logs them to its Alert Log. It uses deep learning to develop models for logging potential malware attacks. Both the Alert Log provided by the HP POS System and Windows Event Log can assist the customer with meeting the PCI DSS requirements for logging. HP Sure Start logs activity at the BIOS level for BIOS protection. The HP MIK can also be used to configure the above security features.	System with HP Sure Run, HP Sure Sense and HP Sure Start to aid in meeting PCI DSS compliance for this requirement.
11.4 Use 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 in the cardholder data environment, and alert personnel to suspected compromises. 11.5 Deploy a change-detection mechanism (for example, file-	HP BIOSphere HP Endpoint Security Controller HP Image Assistant HP Sure Click HP Sure Run HP Sure Start	HP POS Systems provide monitoring of systems and processes through the HP Endpoint Security Controller to assist the customer in meeting this PCI DSS requirement. HP BIOSphere monitors if the BIOS has been altered, similar to the file-integrity monitoring (FIM). HP Image Assistant monitors a system image for issues similar to the file-integrity monitoring (FIM), HP Sure Run monitors vital Windows processes and provides alerts of changes to key system files, similar to the file integrity	The merchant is responsible under PCI DSS for system monitoring, such as intrusion detection and file integrity monitoring. However, the merchant can use the intrusion detection and monitoring tools provided with the HP POS System with HP BIOSphere, HP Image Assistant, HP Sure Click, HP Sure Run and HP Sure Start to aid in meeting PCI DSS compliance for this requirement.

integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.		monitoring (FIM) and intrustion detection required by PCI DSS. HP Sure Start does the same at the BIOS level for BIOS protection by providing alerts of attempted attacks. HP Sure Click checks for untrusted files the user may open, such as Word, PDF or e-mail documents, and runs them in a separate and isolated virtual machine (VM) to prevent malicious access to other parts of the system. HP Sure Click also provides a secure browser that blocks malicious web attacks by monitoring for attempts to download untrusted files and malware via the browser. The HP MIK can also be used to configure the above security features.	
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: -Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum -Specific incident response procedures -Business recovery and continuity procedures	HP Sure Recover	Not Applicable HP is only deploying its hardware and not acting as either a merchant or service provider and, as a result, not in PCI DSS scope to require issuing an incident response plan. HP Sure Recover feature could be considered part of a business continuity or incident response plan to assist a merchant with their PCI DSS, which provides the capability to automatically and securely restore the software image to the HP POS System as needed.	The merchant deploying the HP POS Systems is responsible for providing an incident response plan as part of its PCI assessment.

-Data backup processes -Analysis of legal requirements for reporting compromises -Coverage and responses of all critical system components Reference or inclusion of incident response procedures from the payment brands.			

ASSESSOR COMMENTS

The assessment scope put a significant focus on validating the use of the HP POS Systems in a PCI DSS environment, specifically to include its impact on all the PCI DSS requirements. HP POS Systems, when properly implemented following guidance from HP, can be utilized to meet the technical portions of several PCI DSS requirements for a merchant or a service provider. However, as most computing environments and configurations vary drastically, complete compliance with PCI DSS is a combination of multiple elements of people, process and technology.

It should not be construed that the use of HP POS Systems guarantees full PCI DSS compliance, as disregarding PCI requirements and security best practice controls for systems and networks inside or outside of PCI DSS scope can introduce many other security or business continuity risks to merchants and service providers. Security and business risk mitigation should be any merchant's goal and focus for selecting security controls.

TESTING ENVIRONMENT AND PROCEDURES

The assessment used the following testing methods to assess the potential PCI DSS coverage of the HP POS Systems:

1. The HP Engage One Pro was installed in accordance with vendor guidelines in a closed private network connected by an Ethernet cable. The device had no wireless access of interface. The installation resembled how a kiosk might be set up in a merchant environment.
4. The device consisted only of the operating system and HP software. Since the scope of the assessment was only the device and the HP software, no credit card payment application, or any other third-party software, was installed on the device.
5. The following security features were run, and their configurations and menus were observed on the device:
    a. HP BIOSphere
    b. HP Sure Admin
    c. HP Sure Click

    d. HP Sure Run
    e. HP Sure Sense
    f. HP Sure Start
6. The HP Smart Dock was run on the HP Engage Go and was used to do the following:
    a. Add users and groups
    b. Set password parameters
    c. Add a PIN for multi-factor authentication
7. Reviewed Alert Logs from HP Sure Sense and Windows Event Logs
8. Reviewed the security settings for the web browser through HP Secure Click
9. Reviewed the password settings in the config file generated by HP BIOSphere
10. Ran the HP Engage Console web application on a separate web browser not on the device:
    a. Added devices, including the HP Engage One Pro and HP Engage Go tablet
    b. Add users and configured PCI-compliant passwords
    c. Reviewed other available settings for remotely configuring the devices
11. Reviewed documentation for HP Sure Recover and HP Secure Erase
12. Matched each of the observed features with PCI DSS requirements that might be applicable.

CONCLUSIONS

Coalfire conducted a thorough analysis of the impact on compliance for the Payment Card Industry Security Standards Council (PCI SSC) standard (PCI DSS) and found that the implementation of the HP POS Systems security features have sufficient controls to assist customers of HP with meeting the applicable PCI DSS requirements when deployed in a merchant cardholder data environment (CDE). Ultimately, it is still the responsibility of the customer to ensure PCI DSS requirements are fully met and configured for all in-scope devices and applications installed on the HP POS Systems.

In summary, HP only provides hardware with pre-installed software and is neither a merchant nor a service provider, which would be in scope for PCI DSS. The HP POS System implemented in a merchant network does not store, process or transmit card data itself. Installation of the HP software and features on the device does not adversely impact the status of PCI DSS compliance for a merchant. It should be seen as a configuration management and hardening mechanism a merchant or service provider can use to support PCI DSS compliance in an often complex use case. In fact, many features of the HP POS Systems easily support compliance with PCI DSS requirements and assists organizations with both a more secure and cost-effective solution.

REFERENCES

HP Wolf Security website - https://www.hp.com/us-en/security/endpoint-security-solutions.html

Documentation provided by HP:

HP BIOSphere Whitepaper - https://h20195.www2.hp.com/v2/getpdf.aspx/4AA7-2634ENW.pdf

HP Client Security Getting Started Guide - http://h10032.www1.hp.com/ctg/Manual/c04597082

HP Engage Console User Guide - http://h10032.www1.hp.com/ctg/Manual/c06697512.pdf

HP Secure Erase Whitepaper - https://www8.hp.com/h20195/v2/GetPDF.aspx/4AA7-2608ENW.pdf

HP Smart Dock User Guide - http://h10032.www1.hp.com/ctg/Manual/c06172126

HP Sure Admin Infosheet - https://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA7-7978ENW

HP Sure Admin Whitepaper - https://h20195.www2.hp.com/v2/getpdf.aspx/4AA7-7307ENW.pdf

HP Sure Click Infosheet - https://www8.hp.com/h20195/v2/getpdf.aspx/4AA7-2638ENW.pdf

HP Sure Click Whitepaper - https://h20195.www2.hp.com/v2/getpdf.aspx/4AA7-4555ENW.pdf

HP Sure Recover Infosheet - https://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA7-2564ENW

HP Sure Recover Whitepaper - https://www8.hp.com/h20195/v2/GetPDF.aspx/4AA7-4556ENW.pdf

HP Sure Run Infosheet - https://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA7-2563ENW

HP Sure Run Whitepaper - https://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA7-2200ENW

HP Sure Sense User Guide - http://h10032.www1.hp.com/ctg/Manual/c06379792

HP Sure Sense Whitepaper - https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-6875ENW

HP Sure Start Infosheet - https://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA7-2562ENW

HP Sure Start Whitepaper - https://www8.hp.com/h20195/v2/GetPDF.aspx/4AA7-6645ENW.pdf

Hardware Reference Guide - http://h10032.www1.hp.com/ctg/Manual/c06171330

- HP Engage Go Convertible System
- HP Engage Go Mobile System
- HP Engage Go Dock

Maintenance & Service Guide - http://h10032.www1.hp.com/ctg/Manual/c06189743

- HP Engage Go Convertible System
- HP Engage Go Mobile System
- HP Engage Go Dock

PCI Data Security Standard, v3.2.1 – https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

APPENDIX A: PCI REQUIREMENTS COVERAGE MATRIX

PCI DSS REQUIREMENTS

NOTE: The below requirements and configurations apply only to the HP POS Systems. All backend and virtual environments in the merchant environment hosting the HP POS System must be configured for PCI DSS compliance.

HP POS FEATURE	APPLICABLE PCI REQUIREMENT	HOW FEATURE SUPPORTS PCI COMPLIANCE
Biometric & NFC **Chassis Locks** **Encryption-capable MSRs** **Intrusion Sensors** **Port Disablement**	9.5 (physically secure media)	These devices are all hardware tools that provide security for physical access to the devices. In the event the device hosts payment software storing card data on the HP POS System, these physical controls protect the device in a manner that can assist the customer meet the applicable PCI DSS requirement for physical security controls.
HP BIOSphere	6.1 (vulnerability management) 6.2 (patch management) 8.2.x (unique user IDs) 11.5 (FIM)	1) Allows setting up user credentials in the BIOS to assist the customer meet the requirement for user authentication parameters. 2) Monitors if the BIOS has been altered, similar to the file-integrity monitoring (FIM) required by PCI DSS. 3) Can be configured to identify vulnerabilities and check for BIOS updates through Windows Update.
HP Client Security Manager	6.1 (vulnerability management) 6.2 (patch management) 8.1.x (unique user IDs) 8.2.x (password parameters) 8.3.x (multi-factor authentication)	1) Provides password provisioning for assisting in setting up unique user IDs. 2) Allows for configuration of passwords to assist in setting up meeting the PCI DSS requirement for password parameters. 3) Can be configured to identify and implement security updates and patches on software installed on the HP POS System.
HP Endpoint Security Controller	5.1 (anti-virus) 5.2 (anti-virus monitored to verify always running) 10.3.x (logging) 10.5 (secure audit trails) 10.6 (log reviews) 11.4 (intrusion detection) 11.5 (FIM)	Umbrella for the following HP security features either installed or available for the HP POS Systems: HP Sure Click HP Sure Run HP Sure Start
HP Engage Console	2.1 (default passwords) 7.2 (access controls)	This is a tool that is the user interface for providing access contorls and access to the following other

		security features on the HP POS System and would assist the customer with meeting the PCI DSS requirements for their respective features: HP Secure Erase HP Sure Recover HP Sure Run
HP Image Assistant	11.5 (FIM)	Monitors a system image for issues, including security, similar to the file-integrity monitoring (FIM), required by PCI DSS.
HP Manageability Integration Kit (MIK)	5.1 (anti-virus) 7.2 (access controls) 8.2.x (password parameters) 10.3.x (logging) 11.4 (monitoring)	An HP tool for integrating HP features, such as the following for HP POS Systems: HP Sure Recover HP Sure Run HP Sure Sense HP Sure Start Manageability Integration Kit BIOS Configuration Microsoft Device Guard These HP tools aid overall PCI DSS applicable requirements compliance.
HP Secure Erase	3.1 (data deletion) 9.8.2 (electronic media destruction)	Provides for the secure deletion of card data and secure destruction of media with data in assisting the customer with the PCI DSS requirement for the secure destruction of credit card data.
HP Smart Dock (Only on HP Engage Go and HP Engage Go 10)	7.2 (access controls)	Provides for setting up privileged user accounts with specific access on a need-to-know basis, as required by PCI DSS for user groups.
HP Sure Admin	8.1.x (unique user IDs) 8.2.x (password parameters) 8.3.x (multi-factor authentication)	1) Provides for secure authentication that can assist the customer in meeting the PCI DSS requirement for access controls, including multi-factor authentication, if necessary. 2) Provides for BIOS protection of authentication credentials from theft or tampering, as required by PCI DSS.
HP Sure Click	3.1 (data protection) 11.4 (monitoring) 11.5 (FIM)	1) Monitors for untrusted files that the user might open, similar to the FIM required by PCI DSS and assisting the customer with meeting the PCI DSS requirement for FIM. 2) Provides for a secure browser that monitors downloaded files and blocks potential malicious web attacks via those files, again like a FIM.
HP Sure Recover	12.10.1 (continuity)	Automatically and securely restores the software image to the HP POS System as needed, which could be part of a business continuity or incident response plan required by PCI DSS.

HP Sure Run	5.1 (anti-virus) 5.2 (anti-virus current) 5.3 (anti-virus always running) 6.1 (vulnerability management) 6.2 (patch management) 10.3.x (logging) 11.4 (monitoring) 11.5 (FIM)	1) Monitors key system processes, such as anti-virus software. However, HP Sure Run must be enabled by an admin in the HP Client Security Manager to prevent it from being disabled. 2) It works with anti-virus software, which the customer may have already deployed for assisting in meeting PCI DSS requirements for anti-virus software. 3) It logs and monitors changes to system processes and alerts the user of unusual or mailicious activity and blocks attempts by malware to stop or disable system processes, similar to the FIM required by PCI DSS. 4) Protects processes that check for vulnerabilities and implements corresponding patches.
HP Sure Sense	5.1 (anti-virus) 5.2 (anti-virus current) 5.3 (anti-virus always running) 10.3.x (logging 10.5 (secure audit trails) 10.6 (log reviews)	Uses deep-learning models to prevent malware attacks, like a PCI-compliant anti-virus solution, and provides logs of security alerts in a PCI-DSS-compliant manner.
HP Sure Start	5.1 (anti-virus) 5.3 (anti-virus always running) 10.3.x (logging) 11.4 (intrusion detection)	1) Provides protection similar to anti-virus software. 2) Provides logging and monitoring of mailicious activity, similar to that required by PCI DSS.

ABOUT THE AUTHOR

Joel Dubin | Senior Consultant

Joel Dubin (jdubin@coalfire.com) is a Senior Consultant and Application Security Specialist with Coalfire. Joel has several years of experience working as a QSA and PA-QSA helping clients develop systems and software for use in PCI DSS environments and has authored and spoken on multiple security topics including application security, cyber risk management, secure software development, and PCI DSS and PA-DSS compliance. He holds a CISSP, QSA, and PA-QSA.

ABOUT THE REVIEWER

Bhavna Sondhi | Principal

Bhavna Sondhi is the practice subject matter expert for the solution validation team at Coalfire. Bhavna performs advisory work and assessments for various PCI compliance frameworks and authors technical white papers. Bhavna joined Coalfire in 2013 and brings over 14 years of software engineering and information security experience to the team. Her software engineering experience plays a vital part in ensuring that the teams recognize the importance of secure code development and information security within their operational practices.

Published July 2021.

ABOUT COALFIRE

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 16 years and has offices throughout the United States and Europe. Coalfire.com