Coalfire
IT Audit and Compliance

hp | Enterprise Security

ATALLA DATA SECURITY

ArcSight

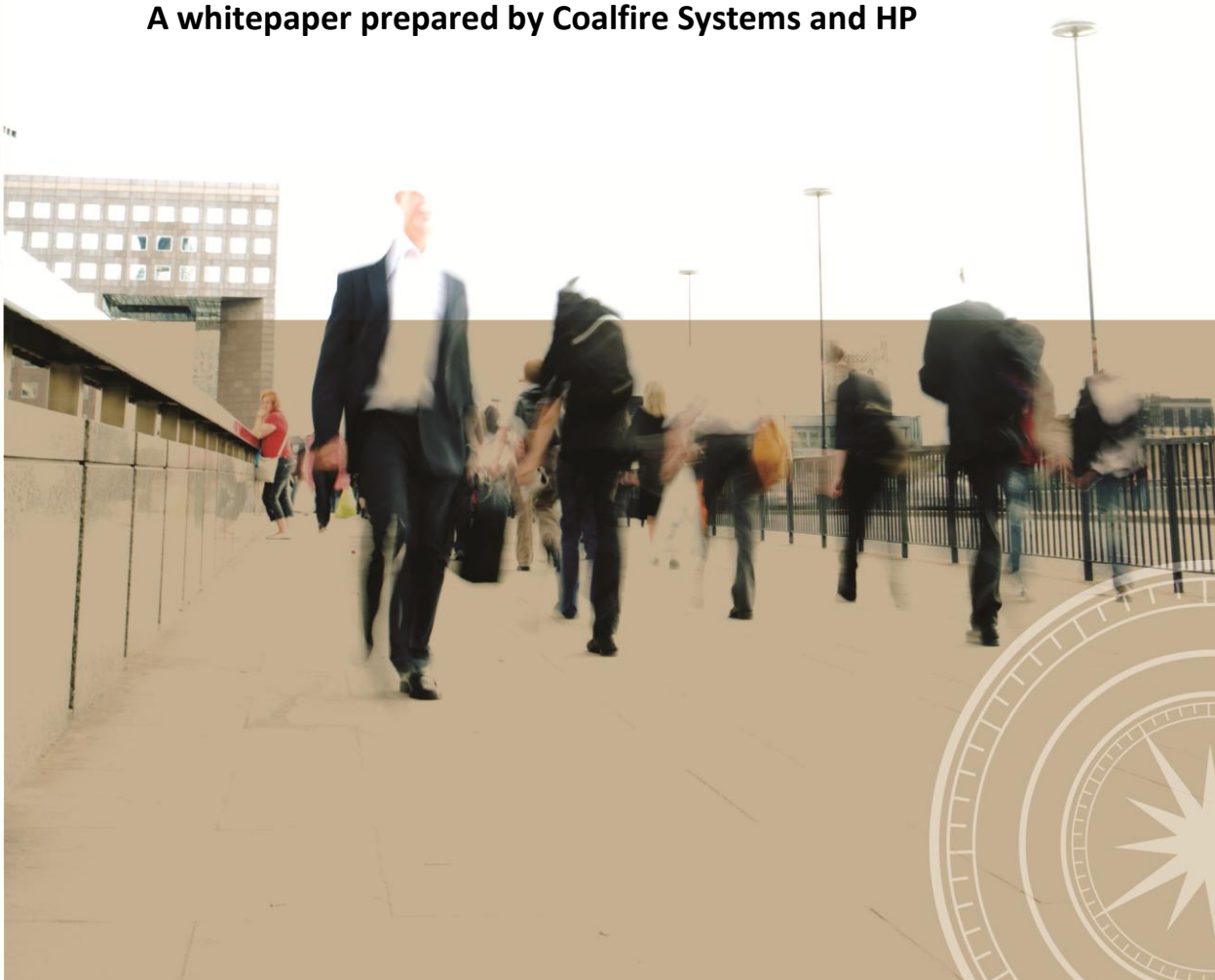
DVLabs

FORTIFY

hp TippingPoint

# *Solutions to Meet Your PCI Compliance Needs*

**A whitepaper prepared by Coalfire Systems and HP**



# Table of Contents

## Executive Summary

Security and regulatory compliance become business inhibitors for many organizations. Hewlett-Packard (HP), a global leader in information technology, has taken a leadership role in solving organizations' challenges by bringing to the market selected products designed to assist organizations in achieving their security and regulatory compliance goals. This paper examines the capabilities of seven HP products in achieving Payment Card Industry (PCI) Data Security Standard (DSS) compliance.

The following HP products underwent a capabilities review in alignment with PCI DSS version 2.0 by a PCI Qualified Security Assessor (QSA):

- Atalla Network Security Processor (NSP)
- Atalla Enterprise Secure Key Manager (ESKM)
- HP Fortify Software Security Center
- HP ArcSight ESM Compliance Insight Package for PCI
- TippingPoint Intrusion Protection System (IPS) & vController+vFW
- HP WebInspect

This is the first phase in a project in which the overall goal is to validate the ability of selected HP and VMware products to meet PCI DSS requirements and provide customers with the necessary guidance to implement the solutions in creating a PCI compliant architecture.

## The Payment Card Industry Data Security Standard

The PCI Security Standards Council (SSC) was established in 2006 by five global payment brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. The payment brands require any merchant or service provider that transmits, stores or processes payment card information comply with the current version of the PCI DSS. In order to achieve PCI compliance, merchants and service providers must validate their compliance by assessing their environment against nearly 200 specific controls outlined in the PCI DSS, and a passing grade requires every control requirement to be in place. Failing to achieve PCI compliance can lead to fines, penalties or inability to process payment card transactions.

The PCI DSS has twelve general requirements outlined as follows:

| PCI Data Security Standard – High Level Overview | |
|---|---|
| **Build and Maintain a Secure Network** | 1. Install and maintain a firewall configuration to protect cardholder data<br>2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| **Protect Cardholder Data** | 3. Protect stored cardholder data<br>4. Encrypt transmission of cardholder data across open, public networks |
| **Maintain a Vulnerability Management Program** | 5. Use and regularly update anti-virus software or programs<br>6. Develop and maintain secure systems and applications |
| **Implement Strong Access Control Measures** | 7. Restrict access to cardholder data by business need to know<br>8. Assign a unique ID to each person with computer access<br>9. Restrict physical access to cardholder data |
| **Regularly Monitor and Test Networks** | 10. Track and monitor all access to network resources and cardholder data<br>11. Regularly test security systems and processes |
| **Maintain an Information Security Policy** | 12. Maintain a policy that addresses information security for all personnel |

Achieving PCI compliance is not a simple task. It is difficult for many organizations to navigate the current landscape of information systems and adequately fulfill all PCI DSS requirements. There are few systems adequately assessed and documented by an independent third-party to determine how the systems fulfill various PCI DSS requirements. HP, working with VMware, is continuing its leadership role in the industry by providing reference architectures, services and products from the data center to the cloud to help clients meet their compliance needs.

## PCI SSC Virtualization and Cloud Guidance

The PCI SSC has recently released guidance for organizations and Qualified Security Assessors (QSAs) on the controls required to properly secure virtual systems and meet PCI compliance requirements. Both the "Payment Card Industry (PCI) Data Security Standard – Requirements and Security Assessment Procedures v2.0" and "Navigating PCI DSS – Understanding the Intent of the Requirements v2.0" address virtualization, but it is the "Information Supplement: PCI DSS Virtualization Guidelines, June 2011" that provides the greatest amount of detail with respect to PCI DSS requirements.

The general guidance provided by the information supplement is as follows:

*There are four simple principles associated with the use of virtualization in cardholder data environments:*

- *If virtualization technologies are used in a cardholder data environment, PCI DSS requirements apply to those virtualization technologies.*
- *Virtualization technology introduces new risks that may not be relevant to other technologies, and that must be assessed when adopting virtualization in cardholder data environments.*
- *Implementations of virtual technologies can vary greatly, and entities will need to perform a thorough discovery to identify and document the unique characteristics of their particular virtualized implementation, including all interactions with payment transaction processes and payment card data.*
- *There is no one-size-fits-all method or solution to configure virtualized environments to meet PCI DSS requirements. Specific controls and procedures will vary for each environment, according to how virtualization is used and implemented.*

The paper goes on to further state:

*In order for in-scope and out-of-scope VMs to co-exist on the same host or hypervisor, the VMs must be isolated from each other such that they can effectively be regarded as separate hardware on different network segments with no connectivity to each other. Any system components shared by the VMs, including the hypervisor and underlying host system, must therefore not provide an access path between the VMs.*

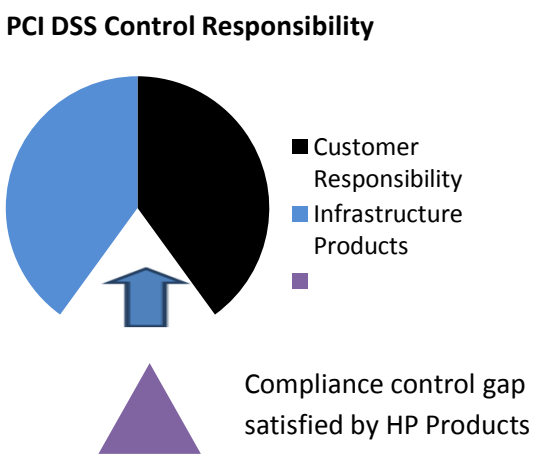
*PCI Council Information Supplement – Virtualization (June, 2011)*

The above guidance provides a means by which to assess the controls, but it does not eliminate the compliance challenges organizations must overcome when utilizing virtual technologies.

## HP – Providing Software to Meet PCI Compliance Needs

Merchants and service providers who transmit, store or process payment card information are required to meet all of the 200 PCI DSS controls in order to fulfill the compliance standard for accepting payment cards. HP is working with VMware to provide solutions that help clients achieve their PCI compliance requirements with a robust set of security products, complemented by their Technology Consulting integration capabilities and key partners.

HP Technology Consulting provides an integrated architecture framework that includes VMware and HP products as well as other partner products that allow customers to meet PCI DSS control requirements. The successful integration with infrastructure products will provide customers with a guide to successfully navigate the compliance landscape.




HP solutions documented in this study help customers meet 110 of 200 PCI DSS controls. The other controls must be met by infrastructure and other products, as well as by the customer. Some controls such as penetration testing, policies, and procedures cannot be met by a software or hardware solution and will always be the responsibility of the customer. Other controls may be supported by additional products and services.

HP aims to identify the gap that HP and VMware products can fill and create a seamless, integrated architecture with other products that allow customers to meet PCI DSS control requirements. The successful integration with infrastructure products will provide customers a guide to successfully navigate the compliance landscape.

To assist its customers in their mission for compliance, HP engaged Coalfire to validate its products within their PCI compliance framework and how their products align to the PCI compliance controls. This initiative is being conducted in two phases. The first is this position paper in which Coalfire assesses HP's products through available documentation and interviews to evaluate the solutions chosen against the PCI DSS control requirements.

The second phase will consist of deploying the HP solutions in a dedicated lab environment and through a third party assessment conducted by Coalfire, validate the ability of the HP solutions to meet PCI DSS requirements.

***The goal of the overall project is to validate the ability of selected HP products to meet PCI DSS requirements and provide customers with the necessary guidance to implement the solutions creating a compliant architecture.***

## Identified HP Solutions

Coalfire reviewed the following HP-identified product solutions and their ability to meet associated PCI DSS requirements:

- Atalla Network Security Processor (NSP)
- Atalla Enterprise Secure Key Manager (ESKM)
- HP Fortify Software Security Center
- HP ArcSight ESM Compliance Insight Package for PCI
- TippingPoint Intrusion Protection System (IPS) & vController+vFW
- HP WebInspect

The above products meet specific needs of the customer as they seek compliance with PCI requirements. Together they address 110 of the 200 identified PCI DSS controls as well as help enable the customer to more easily meet additional controls.

## HP Solutions Mapped to PCI Controls

The table below shows the PCI controls addressed by the selected HP products.

| HP Solution | Solution Description | PCI Controls Met |
|---|---|---|
| **Atalla Network Security Processor (NSP)** | The Atalla Network Security Processor (NSP) devices provide hardware based cryptographic processing for payment data information both for local storage and transmission over the network. | 3.2, 3.2.1, 3.2.2, 3.2.3, 3.4, 3.5, 3.5.1, 3.5.2, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.6, 3.6.7, 4.1 |

| | | |
|---|---|---|
| **Atalla Enterprise Secure Key Manager (ESKM)** | The Atalla Enterprise Secure Key Manager is a pre-configured and hardened security server that provides unified services for creating, protecting, and delivering cryptographic keys to data encryption devices and applications across distributed enterprise IT infrastructures. The Atalla Enterprise Secure Key Manager (ESKM) works in conjunction with HP StorageWorks encrypting devices or HP NonStop server encryption options to provide management for cryptographic keys. For the purposes of this document, the ESKM capabilities are referenced and compared to Payment Card Industry (PCI) requirements outlining the protection of stored cardholder data. | 2.1, 3.4, 3.4.1, 3.5.1, 3.5.2, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.2, 7.2.3, 8.1, 8.2, 8.4, 8.5.1, 8.5.3, 8.5.4, 8.5.5, 8.5.6, 8.5.8, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15, 8.5.16, 9.10.2, 10.1, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.4 |
| **HP Fortify Software Security Center** | The HP Fortify Software Security Center is a suite for automating software security assurance programs and consists of the following HP solutions: HP Fortify Static Code Analyzer (SCA), HP Fortify Real-Time Analyzer (RTA) and the HP Fortify Software Security Center server.<br><br>**HP Fortify Static Code Analyzer (SCA)** –SCA is static analysis solution that includes a set of software security-analyzers that search for violation of security specific coding rules and guidelines in a variety of languages. The security code analyzers include Data Flow, Control Flow, Semantic, Structural, Configuration, and Buffer providing the ability to assist in remediating more than 500 categories of vulnerabilities.<br><br>**HP Fortify Real-time Analyzer (RTA)** – The HP Fortify RTA operates in the same manner as its name suggests: it monitors the code as it operates in production. Defending against evolving logic based attacks, the HP Fortify RTA provides a real-time view into how a deployed application is being attacked and allows personnel to view the attacker (based on IP address and domain name), what part of the application is under attack, and the execution of the | 6.3, 6.3.1, 6.3.2, 6.4.4, 6.5, 6.5.1, 6.5.2, 6.5.3, 6.5.4, 6.5.5,6.5.6, 6.5.7, 6.5.8, 6.5.9, 6.6 |

| | | |
|---|---|---|
| | attack.<br><br>**HP Fortify Software Security Center Server** - Provides a means of integrating analysis data from multiple Fortify analysis agents and enables you to focus and tailor data so that each contributor to the enterprise's Secure Development Lifecycle can focus their efforts most efficiently. | |
| **HP ArcSight ESM Compliance Insight Package for PCI** | Automatically collects information from various system components covered under PCI DSS 2.0 and provides an intelligent layer of analysis & reporting on the ArcSight ESM platform. The HP ArcSight ESM Compliance Insight Package for PCI consists of the following:<br><br>**HP ArcSight PCI Logger –** The PCI Logger is an all-in-one log collection, storage and analysis solution for cost-effective automation of PCI audits and proactive protection of cardholder data.<br><br>**HP ArcSight IdentityView -** HP ArcSight IdentityView enriches log events with user information, and as a result, organizations get a complete picture of user activity, including monitoring high risk privileged and shared accounts.<br><br>**HP ArcSight ESM** – ESM analyzes and correlates every event that occurs across the IT infrastructure – every login, logoff, file access, database query, firewall traversal, email/web gateway access etc. – to deliver accurate prioritization of security risks and compliance violations. | 1.1.6, 1.2, 1.2.1, 1.2.2, 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.5, 2.1, 2.2.2, 2.4(A1.2 and A1.3), 3.3, 4.1, 5.1, 5.1.1, 5.2, 6.4, 6.5, 7.1, 8.5.1, 8.5.4, 8.5.5, 8.5.9, 8.5.13, 8.5.16, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.5.1, 10.5.2, 10.5.3, 10.5.4, 10.5.5, 10.6, 10.7, 11.1, 11.2, 12.3.3 |
| **HP TippingPoint Intrusion Prevention Systems (IPS) & vController+vFW** | The HP Intrusion Prevention System provides proactive network security through inline, real-time protection of network traffic and data centers. The IPS platform's architecture offers deep packet inspection of network traffic and its modular software design enables the addition of valuable network protection services to its proven intrusion prevention solution. The TippingPoint IPS consists of the following systems:<br><br>**Security Management System (SMS) Client –** | 1.1.1, 1.1.4, 1.1.5, 1.2.1, 1.2.2, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.7, 2.1, 2.2, 2.2.2, 2.2.3, 2.3, 2.4(A1.1), 6.1, 6.6, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3, 8.1, 8.2, 8.3, 8.4, 8.5.1, 8.5.3, 8.5.4, 8.5.5, 8.5.8, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15, 8.5.16, 10.1, 10.2.1, 10.2.2, 10.2.3, 10.2.4, |

| | | |
|---|---|---|
| | Provides services and functions to monitor, manage, and configure the entire TippingPoint system.<br><br>**Security Management System (SMS) Server** – Management platform that provides centralized administration, configuration, monitoring, and reporting for TippingPoint IPS Devices. The SMS server will provide device status and monitoring, IPS networking and policy configuration, filter customization, as well as filter and software distribution.<br><br>**Intrusion Prevention System Device(s)** – Detects and blocks malicious network traffic according to security policy and the TippingPoint Digital Vaccine (DV). IPS devices are optimized to provide high resiliency, high availability security for the perimeter, data center, network core and remote branch offices and are capable of protecting network segments from both external and internal attacks.<br><br>**Threat Management Center (TMC)** – Centralized service center that monitors global threats and distributes up-to-date attack filter packages (Digital Vaccine), software updates, and product documentation.<br><br>**Digital Vaccine(r)** – A subscription service that provides updated filter packages and the security intelligence needed for protecting your network.<br><br>All these systems combine to create the TippingPoint Intrusion Prevention System. HP also provides solutions specifically designed for VMware environments associated with the TippingPoint IPS, HP vController and vController + Firewall. The HP vController products provide a software solution that enables network traffic within a VMware-based virtual environment to be inspected and filtered by an HP TippingPoint Intrusion Prevention System (IPS). The vController solution is comprised of the following components: | 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4, 10.4.1, 10.4.2, 10.4.3, 11.4 |

| | | |
|---|---|---|
| | • **Virtual Management Center (VMC)** – acts as the vController management application. Used to connect VMC clients.<br>• **vController and/or vController+vFW** – deployed on each VMware hypervisor which hosts a virtual machine whose network traffic is to be inspected and secured by vController or vController + Firewall. | |
| **HP WebInspect** | HP WebInspect is an application security testing software used to assess the security of web applications required to ensure secure SDLC of payment card applications. | 6.5.1, 6.5.2, 6.5.3, 6.5.4, 6.5.6, 6.5.7, 6.5.8, 6.5.9, 6.6 |

## Conclusion

Hewlett-Packard recognizes the challenges organizations face in meeting PCI DSS requirements. By standardizing an approach and framework to compliance and ultimately working with partner solutions, HP provides customers with proven solutions and methods that address their compliance needs. HP's holistic approach will provide management, IT architects, administrators, and auditors with greater transparency into the risks, solutions and mitigation strategies to meet PCI DSS compliance.

### About Coalfire

Coalfire is a leading, independent information technology Governance, Risk and Compliance (IT GRC) firm that provides IT audit, risk assessment and compliance management solutions. Founded in 2001, Coalfire has offices in Dallas, Denver, Los Angeles, New York, and Seattle and completes thousands of projects annually in retail, financial services, healthcare, government, and utilities. For more information, visit www.coalfire.com.

## Appendices

# Secure Card Information Storage

## Atalla Network Security Processor (NSP)

**Atalla Network Security Processor (NSP)** - The Atalla Network Security Processor (NSP) devices provide hardware based cryptographic processing for payment data information both for local storage and transmission over the network. The matrix below details the PCI requirements impacted by utilizing the Atalla NSP.

| PCI DSS v2.0 Applicability Matrix – Atalla NSP | | |
|---|---|---|
| **Requirement** | **Controls Addressed** | **Description** |
| **Requirement 3:** Protect stored cardholder data. | 3.2, 3.2.1, 3.2.2, 3.2.3, 3.4, 3.5, 3.5.1, 3.5.2, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.6, 3.6.7 | The Atalla Network Security Processor (NSP) device is a PCI-PTS validated Host Security Module (HSM). It provides hardware-based cryptographic processing for the support of financial applications. The NSP may be used to encrypt cardholder and other sensitive data. In order to meet PCI-PTS requirements, the NSP operates within its own key management domain. Keys are generated within the NSP, loaded manually through the SCA, or received as cryptograms from another PCI-PTS device.<br><br>There is no persistent storage of any working keys or sensitive authentication data. The Atalla NSP does not store any information after processing the transactions.<br><br>All configuration and security policy management are managed under dual control using the Secure Configuration Assistant (SCA). Security Administrators are authenticated using FIPS 140-2 level 3 smartcards.<br><br>All configuration actions are logged for audit trail from initial installation. |
| **Requirement 4:** Encrypt transmission of cardholder data across open, public networks. | 4.1 | When used in conjunction with terminals that are equipped with the ability to encrypt sensitive cardholder data, the NSP is used to manage the keys and support host applications requiring sensitive data in the clear or as a pass-through operation. |

# Secure Card Information Storage

## Atalla Enterprise Secure Key Manager (ESKM)

**Atalla Enterprise Secure Key Manager (ESKM)** - The Atalla Enterprise Secure Key Manager is a pre-configured and hardened security server that provides unified services for creating, protecting, and delivering cryptographic keys to data encryption devices and applications across distributed enterprise IT infrastructures. The Atalla Enterprise Secure Key Manager (ESKM) works in conjunction with HP StorageWorks encrypting devices or HP NonStop server encryption options to provide encryption key management for cryptographic keys. For the purposes of this document, the ESKM capabilities are referenced and compared to Payment Card Industry (PCI) requirements outlining the protection of stored cardholder data.

The matrix below details the PCI requirements impacted by utilizing the Atalla Enterprise Secure Key Manager.

| PCI DSS v2.0 Applicability Matrix – Atalla Enterprise Key Manager (ESKM) - Storage | | |
|---|---|---|
| **Requirement** | **Controls Addressed** | **Description** |
| **Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters. | 2.1 | Atalla Enterprise Secure Key Manager (ESKM) supports administrator password complexity requirements and expiration policies. Newly enrolled ESKM administrators are assigned a temporary password which must be changed during their initial logon. |
| **Requirement 3:** Protect stored cardholder data. | 3.4, 3.4.1, 3.5.1, 3.5.2, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8 | Atalla Enterprise Secure Key Manager (ESKM) provides the capability of managing encryption keys used for storing data at rest and in transit and works in conjunction with HP StorageWorks encrypting devices or HP NonStop server encryption options to provide keys for AES, DEA, DES and Triple DES algorithms. Key generation and retrieval for the keys to devices that store PAN data. ESKM keeps all records and auditing logs for changes and accesses to the keys used by the encryption devices.<br><br>Atalla Enterprise Secure Key Manager (ESKM) offers a complete management console capable of either integrating with a Light-weight Directory Authentication Protocol (LDAP) structure for authentication purposes or maintaining local user and group accounts and permissions. In the event a customer chooses to implement a full disk encryption data protection scheme, accounts utilized for logical access must be managed independently of the native operating system storing the encrypted data. To provide further defense-in-depth, the Atalla ESKM provides options to require multiple credentials to implement critical actions such as substitution and retirement of encryption keys. The use of these features guarantee that keys are not associated to user accounts for either data encrypting or key encrypting keys.<br><br>Atalla Enterprise Secure Key Manager provides access management through multiple layers of authentication and access control. Provisions for LDAP and local user account management are provided. Group permissions and authorization policies provide further granularity for restricting access to cryptographic keys and ESKM security |

| | | |
|---|---|---|
| | | administrators do not have access to the keys themselves. When ESKM is used for key generation and retrieval, a separate access control mechanism is inserted for management. Keys are tied to encryption devices and media, not user accounts.<br><br>All keys are stored encrypted at rest, even inside the ESKM devices and ESKM is equipped to securely export keys to external ESKMs by backup, exchange of media, and restore. All data encrypting keys and key encrypting keys are exchanged via secure socket layer (SSL)/transport layer security (TLS) session to prevent clear text transmission of keys between encryption devices in the environment.<br><br>Clients enrolled for access to keys from ESKM are only devices or machine users, not people. Key values are never accessible by human operators. Enrolled devices are only granted access to keys that they are enrolled or authorized to access and keys are only sharable between devices if they are specifically configured into a key sharing group. |
| **Requirement 7:** Restrict access to cardholder data by business need to know. | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.2, 7.2.3 | Access to the ESKM is managed either through the management console, Command Line Interface via SSH, or directly using the serial console. ESKM administrators have no access to key values or encrypted cardholder data. |
| **Requirement 8:** Assign a unique ID to each person with computer access. | 8.1, 8.2, 8.4, 8.5, 8.5.1, 8.5.3, 8.5.4, 8.5.5, 8.5.6, 8.5.8, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15, 8.5.16 | Access to the ESKM is managed either through the management console GUI via SSL/TLS, Command Line Interface via SSH, or directly using the serial console. All logins require passwords which support alpha-numeric values, may be as long as 30 characters in length and support password expirations, history, and other PCI DSS password requirements. Shared ESKM administrator IDs or passwords are neither required nor recommended. ESKM administrator privileges may be assigned on a fine-grained level so that each administrator role has only the permissions and capabilities required for that role.<br><br>Atalla Enterprise Secure Key Manager (ESKM) supports administrator password complexity requirements and expiration policies. Newly enrolled ESKM administrators are assigned a temporary password which must be changed during their initial logon. |
| **Requirement 9:** Restrict physical access to cardholder data. | 9.10.2 | Atalla Enterprise Secure Key Manager (ESKM) works in conjunction with HP StorageWorks encrypting devices to provide keys for AES, DEA, DES and Triple DES data encryption algorithms to prevent loss or leakage without access to the encryption keys. To fully satisfy Requirement 9.10.2, the organization implementing Atalla's ESKM must provide evidence of proper configuration of encryption and storage methods as well as secure key management practices. |
| **Requirement 10:** Track and monitor all access to network resources and cardholder data. | 10.1, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.4 | The ESKM creates and maintains various logs to capture all administrative actions, network activity, cryptography key requests, and system events among other items. Logs may be digitally signed for tamper detection/evidence and can be configured to transfer to a centralized logging server for monitoring/reporting and protected there.<br><br>ESKM also runs a digital signature verification of its internal software at power up or restart to ensure the integrity of the software. |

# Secure Card Application Development

## HP Fortify Software Security Center

The HP Fortify Software Security Center is a suite for automating software security assurance programs and consists of the following HP solutions: HP Fortify Static Code Analyzer (SCA), HP Fortify Real-Time Analyzer (RTA) and the HP Fortify Software Security Center server.

**HP Fortify Static Code Analyzer (SCA)** – SCA is a static analysis solution that includes a set of software security analyzers that search for violation of security specific coding rules and guidelines in a variety of languages. The security code analyzers include Data Flow, Control Flow, Semantic, Structural, Configuration, and Buffer providing the ability to assist in remediating more than 500 categories of vulnerabilities.

**HP Fortify Real-time Analyzer (RTA)** – The HP Fortify RTA operates in the same manner as its name suggests: it monitors the code as it operates in production. Defending against evolving logic based attacks, the HP Fortify RTA provides a real-time view into how a deployed application is being attacked and allows personnel to view the attacker (based on IP address and domain name), what part of the application is under attack, and the execution of the attack.

The Payment Card Industry requires that organizations who develop software applications as part of their process to process, transmit, or store credit card data do so based on industry best practices for security throughout the software development lifecycle. HP Fortify Software Security Center allows organizations to meet some of these requirements.

| PCI DSS v2.0 Applicability Matrix - HP Fortify Software Security Center | | |
|---|---|---|
| **Requirement** | **Controls Addressed** | **Description** |
| **Requirement 6:** Develop and maintain secure systems and applications. | 6.3, 6.3.1, 6.3.2, 6.4.4, 6.5, 6.5.1, 6.5.2, 6.5.3, 6.5.4, 6.5.5, 6.5.6, 6.5.7, 6.5.8, 6.5.9, 6.6 | The HP Fortify Software Security Center provides an organization tools to assure software application development aligns with the requirements in the Payment Card Industry (PCI) Data Security Standard (DSS). The primary capabilities include analyzing project source code, augmenting internal processes to test newly compiled source code and monitoring project code as it operates in production to identify potential security vulnerabilities. To fully satisfy Requirement 6.3, the organization utilizing HP Fortify Software Security Center must provide documented software development processes. These processes must demonstrate they are based on industry standards and best practices and that information security is included throughout the development life cycle.<br><br>HP Fortify Software Security Center provides project code review during three stages. The first is a static source code review, which attempts to identify coding errors with the Static Code Analyzer (SCA). The second stage utilizes the HP Fortify SecurityScope and HP WebInspect to support internal testing procedures of newly compiled source code. The third stage of code review provides monitoring the code during operation to identify weaknesses and potential attack vectors that may arise from breach attempts and code updates. Per the DSS requirements, |

| | | |
|---|---|---|
| | | automated code review is good, but should not be relied upon as the "sole means of code review." To fully satisfy Requirement 6.3.2, the organization utilizing HP Fortify Software Security Center must provide evidence of code review activities prior to releasing the code to production.<br><br>HP Fortify Software Security Center provides automated application security testing for vulnerabilities, including OWASP Top 10 Web Application Vulnerabilities and assists in secure code training for developers. HP Fortify SCA is capable of automating the security testing process in testing for the OWASP Top 10 Vulnerabilities from several years (2004, 2007, 2010) and deliver reports accordingly. In addition, HP Fortify RTA assists in preventing the exploitation of any code by monitoring the code as it is in production.<br><br>HP Fortify SCA acts as a security code analyzer which can be utilized to test public-facing web applications. Its ability to leverage multiple algorithms meets the requirement to automatically scan for application vulnerabilities.<br><br>HP Fortify RTA provides the capabilities to block traffic at the application layer and meet PCI requirements as a web application firewall. |

# Card Processing Platform Security Logging & Monitoring

## HP ArcSight ESM Compliance Insight Package for PCI

The HP ArcSight ESM Compliance Insight Package for PCI automatically collects information from various system components covered under PCI DSS 2.0 and provides an intelligent layer of analysis & reporting on the ArcSight ESM platform. The HP ArcSight ESM Compliance Insight Package for PCI consists of the following:

**HP ArcSight PCI Logger** – The PCI Logger is an all-in-one log collection, storage and analysis solution for cost-effective automation of PCI audits and proactive protection of cardholder data.

**HP ArcSight IdentityView** - HP ArcSight IdentityView enriches log events with user information, and as a result, organizations get a complete picture of user activity, including monitoring high risk privileged and shared accounts.

**HP ArcSight ESM** – ESM analyzes and correlates every event that occurs across the IT infrastructure – every login, logoff, file access, database query, firewall traversal, email/web gateway access etc. – to deliver accurate prioritization of security risks and compliance violations.

The following matrix describes PCI DSS controls that are addressed by the HP ArcSight ESM Compliance Insight Package for PCI.

| PCI DSS v2.0 Applicability Matrix - ArcSight Logger, ArcSight IdentityView, and ArcSight ESM | | |
|---|---|---|
| **Requirement** | **Controls Addressed** | **Description** |
| **Requirement 1:** Install and maintain a firewall configuration to protect cardholder data. | 1.1.6, 1.2, 1.2.1, 1.2.2, 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.5 | As logging and monitoring software, the ArcSight ESM Compliance Package can provide management tools to assist in meeting firewall configuration requirements through alerts and reporting. The system is able to alert personnel in the event of firewall configuration changes, show external systems that are communicating directly with systems within the Cardholder Data Environment (CDE), and many other useful reports to simplify controls for an organization. |
| **Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters. | 2.1, 2.2.2, 2.4 (A1.2, A1.3) | As logging and monitoring software, the ArcSight ESM Compliance Package can provide management tools to assist in meeting system configuration requirements through alerts and reporting. The system is able to alert personnel in the event of any default account in use that would provide additional assurance to an organization as part of their security hardening process. |
| **Requirement 3:** Protect stored cardholder data. | 3.3 | As logging and monitoring software, the ArcSight ESM Compliance Package can provide management tools to assist in meeting stored encryption requirements through alerts and reporting. The system is able to provide various alerts to personnel, such as any apparent credit card number sent in clear text or the use of a system's default account, to provide additional assurance to an organization as part of their security hardening process. |

| | | |
|---|---|---|
| **Requirement 4:** Encrypt transmission of cardholder data across open, public networks. | 4.1 | As logging and monitoring software, the ArcSight ESM Compliance Package can provide management tools to assist in meeting secure transmission requirements through alerts and reporting. The system is able to alert personnel and report on any PCI systems that are communicating using unencrypted data. |
| **Requirement 5:** Use and regularly update anti-virus software or programs. | 5.1, 5.1.1, 5.2 | As logging and monitoring software, the ArcSight ESM Compliance Package can provide management tools to assist management in ensuring anti-virus is running and up to date through alerts and reporting. |
| **Requirement 6:** Develop and maintain secure systems and applications. | 6.4, 6.5 | As logging and monitoring software, the ArcSight ESM Compliance Package can provide management tools to assist the change management process through alerts and reporting. |
| **Requirement 7:** Restrict access to cardholder data by business need to know. | 7.1 | As logging and monitoring software, the ArcSight ESM Compliance Package can provide management tools to assist in enforcing access controls by providing a report of all personnel that accessed the Cardholder Data Environment. |
| **Requirement 8:** Assign a unique ID to each person with computer access. | 8.5.1, 8.5.4, 8.5.5, 8.5.9, 8.5.13, 8.5.16 | As logging and monitoring software, the ArcSight ESM Compliance Package can provide management tools to assist in enforcing access controls and authentication management. Reports consisting of password changes, and account lockouts by both system and user are available. |
| **Requirement 10:** Track and monitor all access to network resources and cardholder data. | 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.5.1, 10.5.2, 10.5.3, 10.5.4, 10.5.5, 10.6, 10.7 | ArcSight ESM utilizes correlated user entitlements to log information and Netflow data to attribute any access to cardholder data to a specific person. This attribution is done even if a shared account has been used or access occurred from a dynamic IP address. To fully satisfy Requirement 10.2.1, the organization implementing ArcSight ESM must provide evidence of all access to cardholder data being logged and correlated to specific persons.<br><br>ArcSight Logger shows all successful logins to systems performed by default administrative users. Logger shows the system to which the login was attempted, the number of times the attempt happened, and the last time it happened. Administrative users are defined as admin, administrator, root, superuser, super. The default administrative user names should be changed to the actual administrator names after implementation. To fully satisfy Requirement 10.2.2, the organization implementing ArcSight Logger must provide evidence of all activity in the cardholder data environment has been logged and correlated to specific administrators.<br><br>ArcSight Logger is supplied with a report capable of showing the clearing of windows audit logs, which should usually not be done and could indicate a security problem. To fully satisfy Requirement 10.2.3, the organization implementing ArcSight Logger must provide evidence that access to audit logs has been logged and audit logs are being generated.<br><br>ArcSight ESM tracks and correlates all unsuccessful login attempts to systems monitored. Alerts may be set after an identified number of unsuccessful login attempts. Full audit trails are provided for all failed login attempts. To fully satisfy Requirement 10.2.4, the organization implementing ESM must provide evidence detailing audit trails for invalid login attempts.<br><br>Logger provides reporting that shows attempts to create files. It displays the machine on which the file creation attempt occurred, the outcome of the attempt, the user involved, the name of the file, and how many times the attempt happened. To fully satisfy Requirement 10.2.7, the organization implementing ArcSight Logger must provide evidence detailing the report available in Logger has been activated and is providing evidence as expected. |

| | | |
|---|---|---|
| | | ArcSight Logger provides a report titled "User Logins – All" that details all non-administrative users who attempted to log into a system. The report is sorted first by zone and then by time. A non-administrative user is one whose user name is not Admin, Administrator, root, superuser, or super. This list should be changed according to the actual administrative names after installation. To fully satisfy Requirement 10.3.1, the organization implementing Logger must provide evidence detailing the report available in Logger has been activated and is providing evidence as expected.<br><br>ArcSight Logger captures date and time information for all events captured by the system. ESM provides a report that shows all ArcSight SmartConnectors that report inaccurate times. This might be an indication of clocks that are not synchronized with each other in the logging infrastructure and thus affect the credibility of data access reports. To fully satisfy Requirement 10.3.3, the organization implementing ArcSight Logger must provide evidence detailing the report available in Logger has been activated and is providing evidence as expected and that date and time stamps are collected and correlated for all audit trail events.<br><br>All events captured by ArcSight ESM detail the success or failure of the attempted activity. This data is provided for login attempts, account creation attempts, file access, and file creation, deletion and modification. To fully satisfy Requirement 10.3.4, the organization implementing ESM must provide evidence detailing success or failure indications for all audit trail events.<br><br>All events captured by ArcSight ESM include the name of the object accessed, created, modified or deleted as well as the account that attempted the access. An example of this data being captured is available in the "File Creation Attempts Report". To fully satisfy Requirement 10.3.6, the organization implementing ESM must provide evidence detailing names of objects are detailed when events affecting the object are captured.<br><br>Using PCI Reports available in ArcSight Logger, the "File Manipulations – All" reporting is capable of identifying any failed or successful access to log data. To fully satisfy Requirement 10.5.5, the organization implementing Logger must provide evidence proving that log data may not be altered without system administration being aware of the change.<br><br>ArcSight Logger provides PCI Alerts (real time) and PCI Reports (on demand) to facilitate log review and reaction to security events and vulnerabilities identified. To fully satisfy Requirement 10.6, the organization implementing Logger must provide evidence detailing the use of PCI Alerts and PCI Reports in ArcSight Logger. The evidence provided must clearly show daily review by personnel. |
| **Requirement 11:** Regularly test security systems and processes. | 11.1, 11.2 | ArcSight ESM has the ability to centralize and correlate reports if a wireless analyzer is also being used. |
| **Requirement 12:** Maintain a policy that addresses information security for all personnel. | 12.3.3 | ArcSight Logger is able to provide a list of all systems that are logging and forwarding logs for the Cardholder Data Environment. |

# Card Processing Portfolio Attack Defense

## HP TippingPoint Intrusion Prevention Systems (IPS) & vController+vFW

The HP Intrusion Prevention System provides proactive network security through inline, real-time protection of network traffic and data centers. The IPS platform's architecture offers deep packet inspection of network traffic and its modular software design enables the addition of valuable network protection services to its proven intrusion prevention solution. The TippingPoint IPS consists of the following systems:

**Security Management System (SMS) Client** – Provides services and functions to monitor, manage, and configure the entire TippingPoint system.

**Security Management System (SMS) Server** – Management platform that provides centralized administration, configuration, monitoring, and reporting for TippingPoint IPS Devices. The SMS server will provide device status and monitoring, IPS networking and policy configuration, filter customization, as well as filter and software distribution.

**Intrusion Prevention System Device(s)** – Detects and blocks malicious network traffic according to security policy and the TippingPoint Digital Vaccine (DV). IPS devices are optimized to provide high resiliency, high availability security for the perimeter, data center, network core and remote branch offices and are capable of protecting network segments from both external and internal attacks.

**Threat Management Center (TMC)** – Centralized service center that monitors global threats and distributes up-to-date attack filter packages (Digital Vaccine), software updates, and product documentation.

**Digital Vaccine (DV)** – A subscription service that provides updated filter packages and the security intelligence needed for protecting your network.

All these systems combine to create the TippingPoint Intrusion Prevention System. HP also provides solutions specifically designed for VMware environments associated with the TippingPoint IPS, HP vController and vController + Firewall. The HP vController products provide a software solution that enables network traffic within a VMware-based virtual environment to be inspected and filtered by an HP TippingPoint Intrusion Prevention System (IPS). The vController solution is comprised of the following components:

- **Virtual Management Center (VMC)** – acts as the vController management application. Used to connect VMC clients.
- **vController and/or vController+vFW** – deployed on each VMware hypervisor which hosts a virtual machine whose network traffic is to be inspected and secured by vController or vController + Firewall.

These solutions associated with the vController solution are designed to increase the security and enable customers to meet requirements to logically segment virtual machines within a virtual architecture.

Overall, the HP TippingPoint Intrusion Prevention System (with vController+vFW for VMware environments) provides a tool to segment virtual machines within a VMware environment and a comprehensive IPS system while enabling organizations to also address many other PCI DSS requirements.

| PCI DSS v2.0 Applicability Matrix - HP TippingPoint Intrusion Prevention Systems (IPS) & vController+vFW | | |
|---|---|---|
| **Requirement** | **Controls Addressed** | **Description** |
| **Requirement 1:** Install and maintain a firewall configuration to protect cardholder data. | 1.1.1, 1.1.4, 1.1.5, 1.2.1, 1.2.2, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.7 | VMC provides the capability for IT personnel to establish and manage firewall configurations for the virtual firewalls implemented on VMs. VMC firewall management allows for the description of groups, roles, and responsibilities and also the ability to document the business justification for permitted ports, protocols, and services. |
| **Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters. | 2.1, 2.2, 2.2.2, 2.2.3, 2.3, 2.4(A1.1) | HP TippingPoint IPS and VMC require the changing of local Administrator default passwords and are designed to provide IPS protection upon installation. Organizations are expected to tune IPS devices to meet their operational needs<br><br>Within a VMware environment, vController+vFW provides the ability to effectively segment VMs located on the same hypervisor. From the Navigating the DSS v2.0 document, "Where virtualization technologies are used, each virtual component (e.g. virtual machine, virtual switch, virtual security appliance, etc.) should be considered a 'server' boundary. Individual hypervisors may support different functions, but a single virtual machine should adhere to the 'one primary function' rule." |
| **Requirement 6:** Develop and maintain secure systems and applications. | 6.1, 6.6 | The SMS monitors the TMC for appropriate patches and allows for organizations to meet required patching requirements for HP TippingPoint IPS. |
| **Requirement 7:** Restrict access to cardholder data by business need to know. | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3, | HP TippingPoint provides three distinct User Roles by default with which personnel are granted access: Operator, Administrator, and Super-User. Higher granularity role-based access controls may be granted above and beyond the 3 default roles. Access to HP TippingPoint devices can be managed through Microsoft Active Directory or RADIUS (best practice). |
| **Requirement 8:** Assign a unique ID to each person with computer access. | 8.1, 8.2, 8.3, 8.4, 8.5.1, 8.5.3, 8.5.4, 8.5.5, 8.5.8, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15, 8.5.16 | HP TippingPoint provides three distinct User Roles by default with which personnel are granted access: Operator, Administrator, and Super-User. Upon initial login to the system, the local Super User is forced to choose a password that conforms to a password complexity policy. Access to HP TippingPoint devices can then be managed through Microsoft Active Directory or RADIUS (best practice) and password requirements may be enforced to meet PCI requirements. VMC also meets PCI requirements for administration and password requirements, but cannot be managed through Active Directory. |

| | | |
|---|---|---|
| **Requirement 10:** Track and monitor all access to network resources and cardholder data. | 10.1, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4, 10.4.1, 10.4.2, 10.4.3 | Logging and auditing requirements are best met through the use of an additional product such as ArcSight ESM that will centralize and collect logs for all systems. HP TippingPoint is able to track PCI DSS required events such as administrator access, access to cardholder systems, among the other required events and then export logs from its IPS devices to the SMS Server. The SMS Server provides a centralized interface for a HP TippingPoint deployment, including the vController+vFW. The SMS provides the capability to limit the access to applicable logs through a least privilege methodology. |
| **Requirement 11:** Regularly test security systems and processes. | 11.4 | HP TippingPoint is an IPS device that meets the standards of the PCI DSS requirements for an IPS. |

# Web-based Secure Card Application Vulnerability Testing

## HP WebInspect

**HP WebInspect** - HP WebInspect is an application security testing software used to assess the security of web applications and web services. The Payment Card Industry requires that organizations regularly conduct vulnerability scans of their environment, and HP WebInspect enables an organization to meet many of these requirements.

| PCI DSS v2.0 Applicability Matrix - HP WebInspect | | |
|---|---|---|
| **Requirement** | **Controls Addressed** | **Description** |
| **Requirement 6:** Develop and maintain secure systems and applications. | 6.5.1, 6.5.2, 6.5.3, 6.5.4, 6.5.6, 6.5.7, 6.5.8, 6.5.9, 6.6 | HP WebInspect provides a toolset that includes multiple parameter injection engines, including SQL injection, capable of identifying vulnerabilities created by injection based flaws. To fully satisfy Requirement 6.5.1, the organization utilizing HP WebInspect must provide evidence of scanning activities being conducted during the development and test phases as a tool to identify coding vulnerabilities.<br><br>Parameter overflow attack vulnerability detection is included in the HP WebInspect product. Identifying an application's capability of handling unexpected and extremely large amounts of data during testing will prevent buffer overflow attacks being released into production code. To fully satisfy Requirement 6.5.2, the organization utilizing HP WebInspect must provide evidence of scanning activities being conducted during the development and test phases as a tool to identify coding vulnerabilities.<br><br>Methods of identifying insecure communications employed by HP WebInspect include checking that secure pages require the use of SSL for connectivity, the level of SSL certificate accepted by the web server meets industry standards, masking of password fields for authentication mechanisms is enabled, authentication content sent unencrypted is identified, and authentication data in query strings is not sent. To fully satisfy Requirement 6.5.4, the organization utilizing HP WebInspect must provide evidence of scanning activities being conducted during the development and test phases as a tool to identify coding vulnerabilities.<br><br>HP WebInspect has functionality for "policy" usage when scanning web applications. Policies are collections of vulnerability checks and attacks used to identify weaknesses in the web application. HP WebInspect comes with pre-configured policies and the ability to customize scans targeted to specific application types or functions. Samples of policy types include SQL Injection, Critical and High vulnerabilities, and OWASP Top 10 Application Security Risks. To fully satisfy Requirement 6.5.6, the organization utilizing HP WebInspect must provide evidence of scanning activities being conducted during the development and test phases as a tool to identify coding vulnerabilities.<br><br>HP WebInspect provides a web fuzzer tool capable of generating cross-site scripting attacks to test web |

| | | |
|---|---|---|
| | | applications. The web fuzzer utilizes a text file containing paragraphs constructed to test cross-site scripting susceptibility. To fully satisfy Requirement 6.5.7, the organization utilizing HP WebInspect must provide evidence of scanning activities being conducted during the development and test phases as a tool to identify coding vulnerabilities.<br><br>There are a number of checks utilized by HP WebInspect to test for improper access control. The checks include verifying that administration sections require authentication, verifying that authentication mechanisms utilize encrypted connections, and checking that passwords are masked when entered. To fully satisfy Requirement 6.5.8, the organization utilizing WebInspect must provide evidence of scanning activities being conducted during the development and test phases as a tool to identify coding vulnerabilities.<br><br>HP WebInspect provides a test for cross-site request forgery that attempts to identify whether the web application is attempting to protect a specific location. Once a protected location has been identified, an emulated CSRF attack is generated to determine If the application is vulnerable. To fully satisfy Requirement 6.5.9, the organization utilizing HP WebInspect must provide evidence of scanning activities being conducted during the development and test phases as a tool to identify coding vulnerabilities.<br><br>The HP WebInspect tool set provides a feature for automatic updates of the vulnerability summary and remediation database called “Smart Update”. An organization utilizing the Smart Update feature of HP WebInspect will have an up to date report of potential vulnerabilities after running checks and testing. To fully satisfy Requirement 6.6, the organization utilizing HP WebInspect must provide evidence of scanning activities being conducted on an ongoing basis to identify coding vulnerabilities. |