

HP Addendum to VMware Solution Guide for Payment Card Industry Data Security Standards



HP Addendum to VMware Solution Guide for Payment Card Industry Data Security Standards



Table of Contents

1. INTRODUCTION	3
2. CLOUD COMPUTING	6
3. OVERVIEW OF PCI AS IT APPLIES TO CLOUD/VIRTUAL ENVIRONMENTS	10
4. HP PCI COMPLIANCE SOLUTIONS.....	12
5. HP PCI REQUIREMENTS MATRIX (OVERVIEW)	14

1. Introduction

Merchants and service providers who transmit, store or process payment card information are required to meet all 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.

This paper examines the capabilities of the following seven HP products in achieving Payment Card Industry (PCI) Data Security Standard (DSS) compliance, and describes how these products align to the PCI compliance controls:

- 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 Next Generation Intrusion Protection System (NG IPS) & vController+vFW
- HP WebInspect

ATALLA
DATA SECURITY

ArcSight

DVLabs

FORTIFY

hp TippingPoint

VMware

Compliance and security continue to be top concerns for organizations which plan to move their environment to cloud computing. VMware helps organizations address these challenges by providing bundled solutions (suites) that are designed for specific use cases. These use cases address questions like “How to be PCI compliant in a VMware Private Cloud” by providing helpful information for VMware architects, the compliance community, and third parties.

The PCI Private Cloud Use Case is comprised of five VMware Product Suites - vSphere, vCloud, vCenter Operations (vCOPs), vShield, and View. These product suites are described in detail in this paper. The use case also provides readers with a mapping of the specific PCI controls to VMware’s product suite, partner solutions, and organizations involved in PCI Private Clouds. While every cloud is unique, VMware and its partners can provide a solution that addresses over 70% of the PCI DSS requirements.

Figure 1: VMware Partner Integration

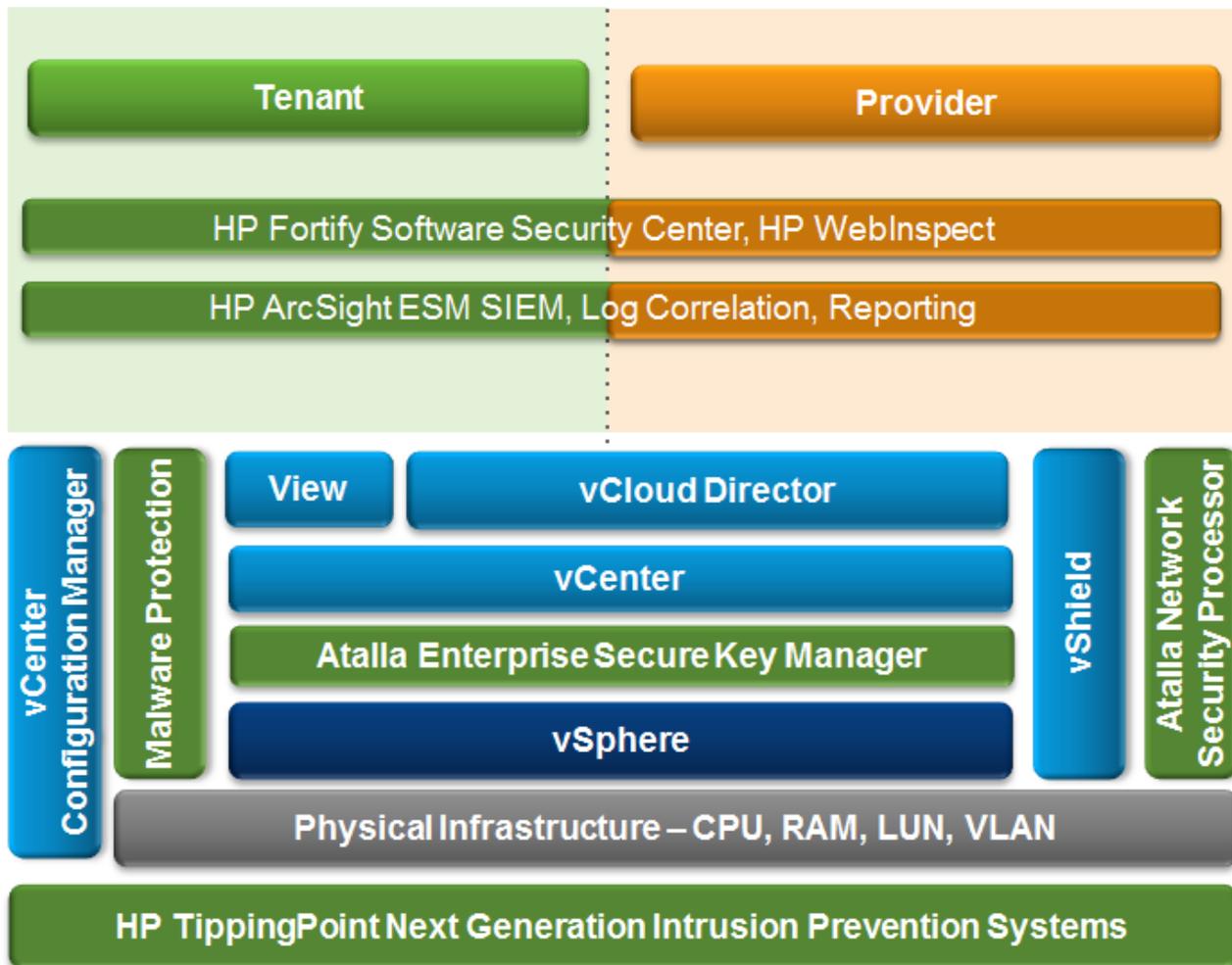
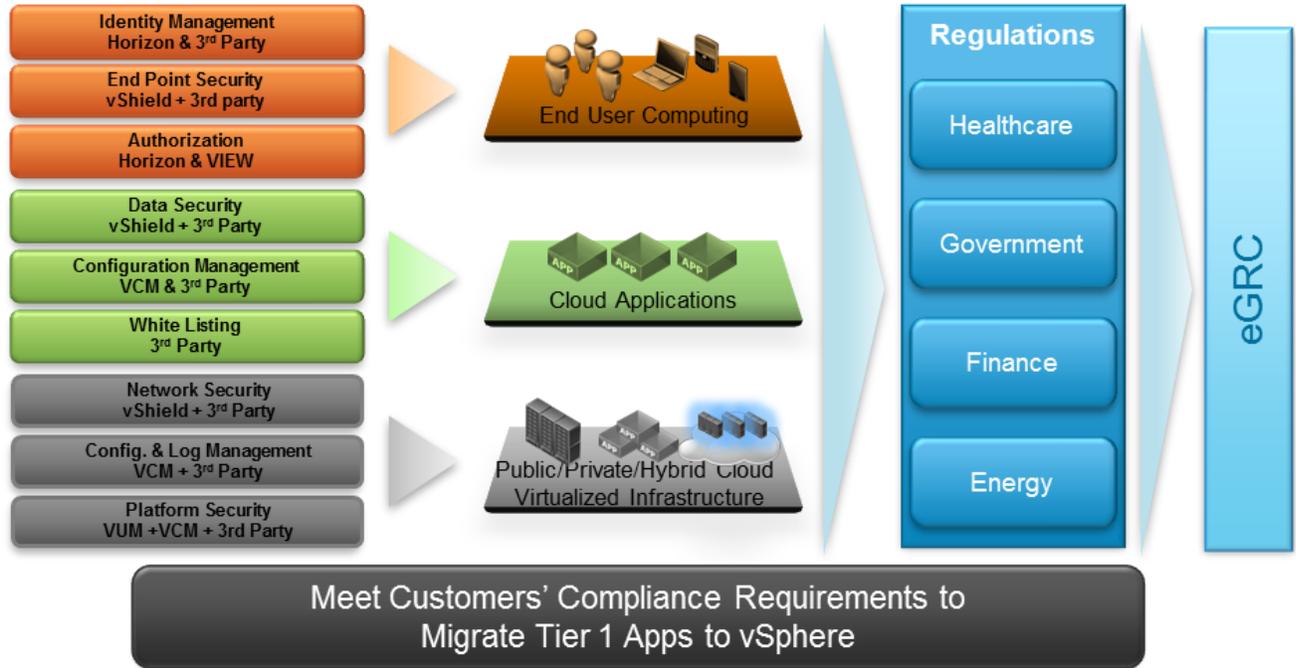


Figure 2: Help Meet Customers' Compliance Requirements to Migrate Tier 1 Apps to vSphere



2. Cloud Computing

Cloud computing and virtualization have continued to grow significantly every year. There is a rush to move applications and even whole datacenters to the “cloud”, although few people can succinctly define the term “cloud computing.” There are a variety of different frameworks available to define the cloud, and their definitions are important as they serve as the basis for making business, security, and audit determinations. VMware defines cloud or utility computing as the following (<http://www.vmware.com/solutions/cloud-computing/public-cloud/fags.html>):

“Cloud computing is an approach to computing that leverages the efficient pooling of on-demand, self-managed virtual infrastructure, consumed as a service. Sometimes known as utility computing, clouds provide a set of typically virtualized computers which can provide users with the ability to start and stop servers or use compute cycles only when needed, often paying only upon usage...”

There are commonly accepted definitions for the cloud computing deployment models and there are several generally accepted service models. These definitions are listed below:

- Private Cloud – The cloud infrastructure is operated solely for an organization and may be managed by the organization or a third party. The cloud infrastructure may be on-premise or off-premise.
- Public Cloud – The cloud infrastructure is made available to the general public or to a large industry group and is owned by an organization that sells cloud services.
- Hybrid Cloud – The cloud infrastructure is a composition of two or more clouds (private and public) that remain unique entities, but are bound together by standardized technology. This enables data and application portability; for example, cloud bursting for load balancing between clouds. With a hybrid cloud, an organization gets the best of both worlds, gaining the ability to burst into the public cloud when needed while maintaining critical assets on-premise.
- Community Cloud – The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (for example, mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party, and may exist on-premise or off-premise.

To learn more about VMware’s approach to cloud computing, review the following:

- <http://www.vmware.com/solutions/cloud-computing/index.html#tab3> - VMware Cloud Computing Overview
- <http://www.vmware.com/cloud-computing/cloud-architecture/vcat-toolkit.html> - VMware’s vCloud Architecture Toolkit

When an organization is considering the potential impact of cloud computing to their highly regulated and critical applications, they may want to start by asking:

- Is the architecture a true cloud environment (does it meet the definition of cloud)?
- What service model is used for the cardholder data environment (SaaS, PaaS, IaaS)?
- What deployment model will be adopted?
- Is the cloud platform a trusted platform?

The last point is critical when considering moving highly regulated applications to a cloud platform. PCI does not endorse or prohibit any specific service and deployment model. The appropriate choice of service and deployment models should be driven by customer requirements, and the customer's choice should include a cloud solution that is implemented using a trusted platform.

VMware is the market leader in virtualization, where virtualization is the key enabling technology for cloud computing. VMware's vCloud Infrastructure Suite is the trusted cloud platform that customers use to realize the manifold benefits of cloud computing including safely deploying business critical applications.

To get started, VMware recommends that all new customers undertake a compliance assessment of their current environment. VMware offers free compliance checkers that are based on VMware's vCenter Configuration Manager solution. Customers can simply point the checker at a target environment and execute a compliance assessment request. The resultant compliance report provides a detailed rule by rule indication of pass or failure against a given standard. Where compliance problems are identified, customers are directed to a detailed knowledge base for an explanation of the rule violated and information about potential remediation. To download the free compliance checkers click on the following link:

<https://my.vmware.com/web/vmware/evalcenter?p=compliance-chk&lp=default&cid=7018000000MJsMAAW>

Figure 3. HP and VMware Cloud Partnership

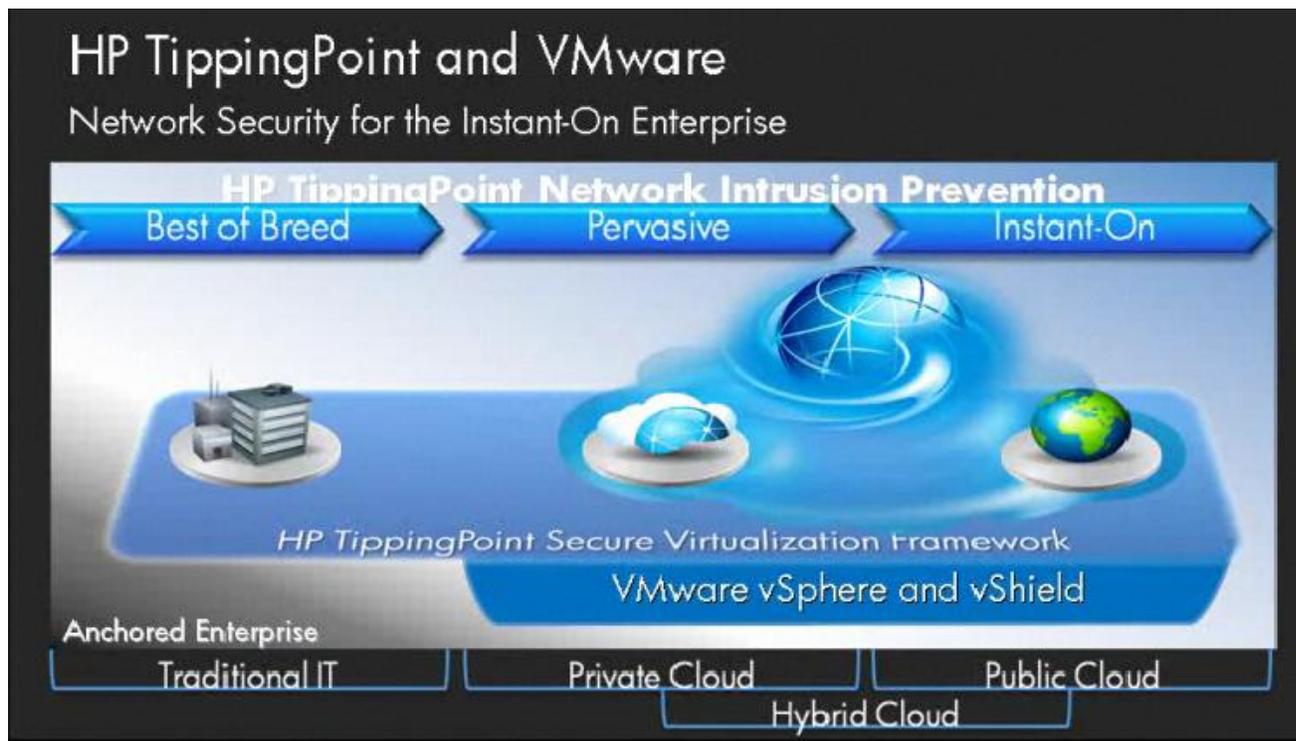


Figure 4: VMware Cloud Computing Partner integration

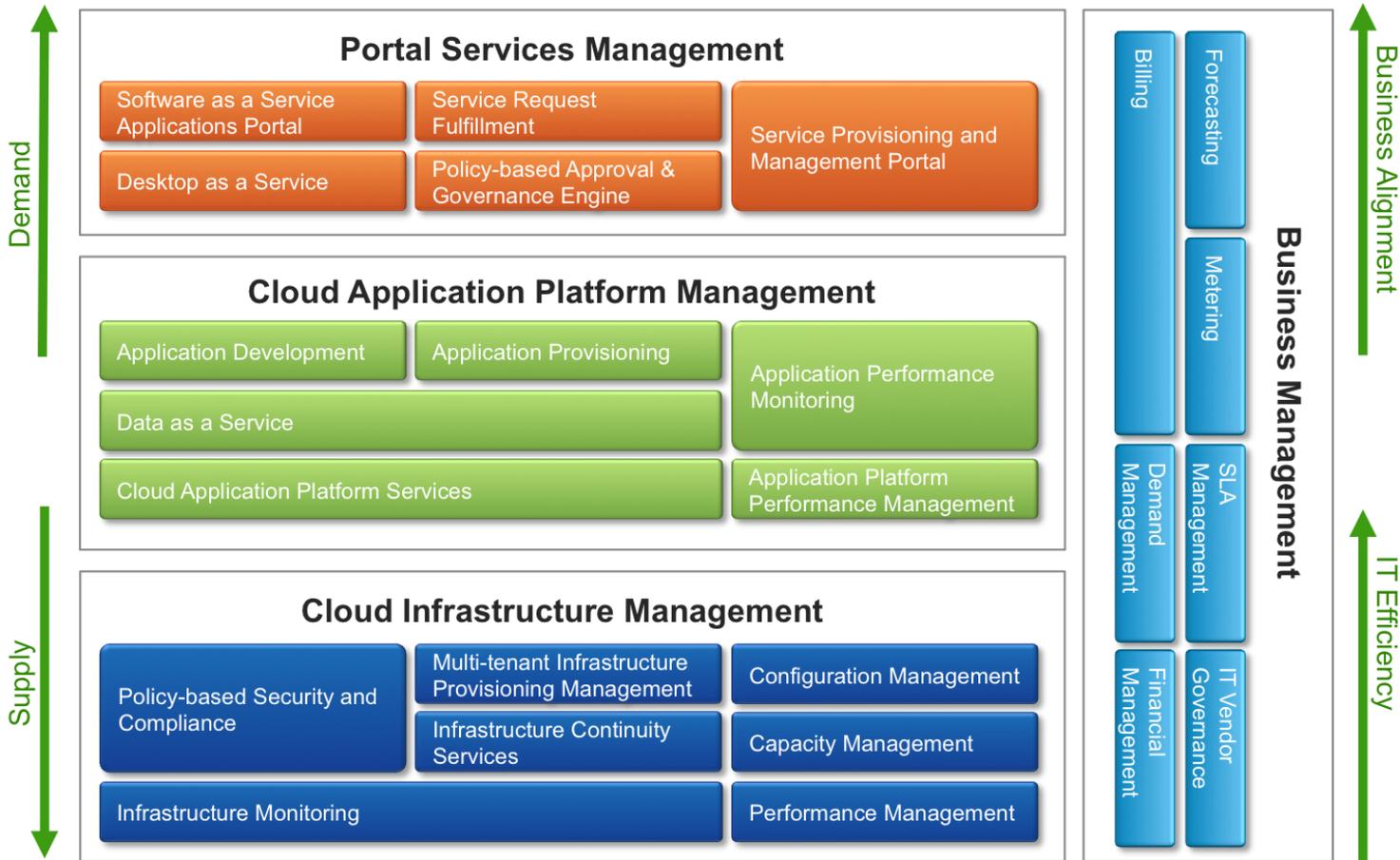
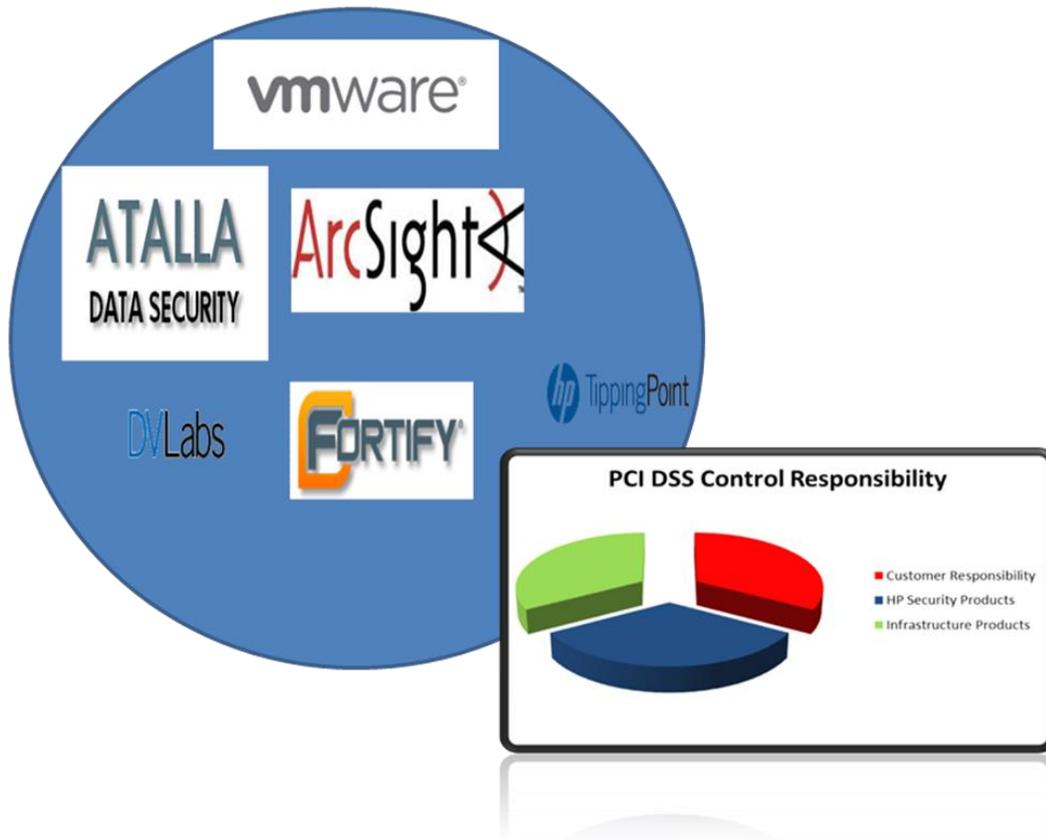


Figure 5: HP Cloud Computing Partner integration

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. 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.

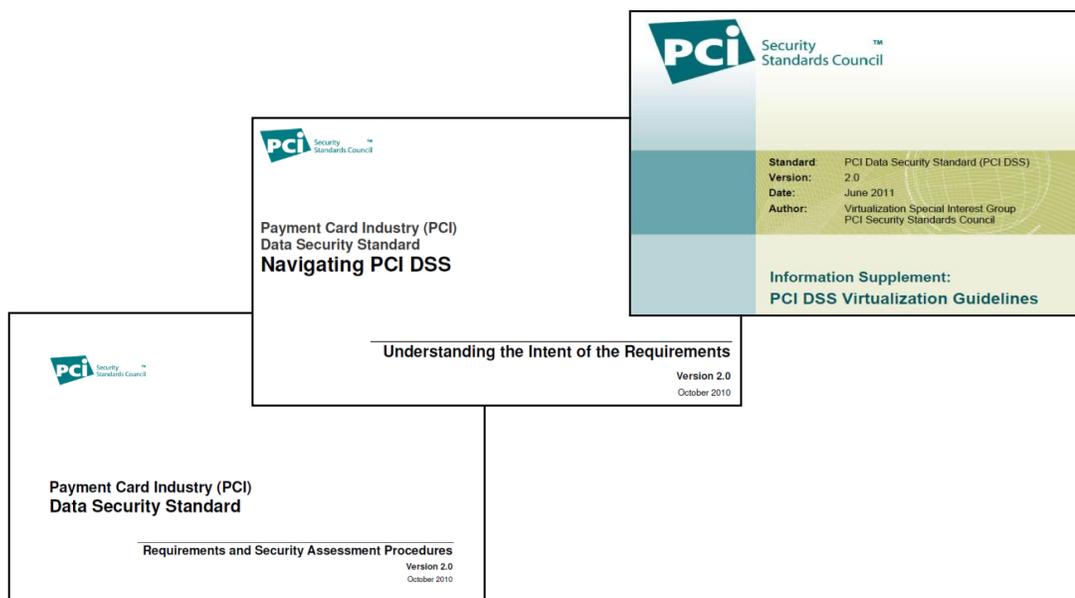


3. Overview of PCI as it applies to Cloud/Virtual Environments

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 through their Operating Regulations that any merchant or service provider must be PCI compliant. Merchants and service providers are required to validate their compliance by assessing their environment against nearly 300 specific test controls outlined in the PCI Data Security Standards (DSS). Failure to meet PCI requirements may lead to fines, penalties, or inability to process credit cards in addition to potential reputational loss.

The PCI SSC specifically began providing formalized guidance for cloud and virtual environments in October 2010. These guidelines were based on industry feedback, rapid adoption of virtualization technology, and the move to cloud. Version 2.0 of the Data Security Standard (DSS) specifically mentions the term “virtualization” (previous versions did not use the word “virtualization”). This was followed by an additional document explaining the intent behind the PCI DSS v2.0, “Navigating PCI DSS”. These documents were intended to clarify that virtual components should be considered as “components” for PCI, but did not go into the specific details and risks relating to virtual environments. Instead, they address virtual and cloud specific guidance in an Information Supplement, “PCI DSS Virtualization Guidelines,” released in June 2011 by the PCI SSC’s Virtualization Special Interest Group (SIG).

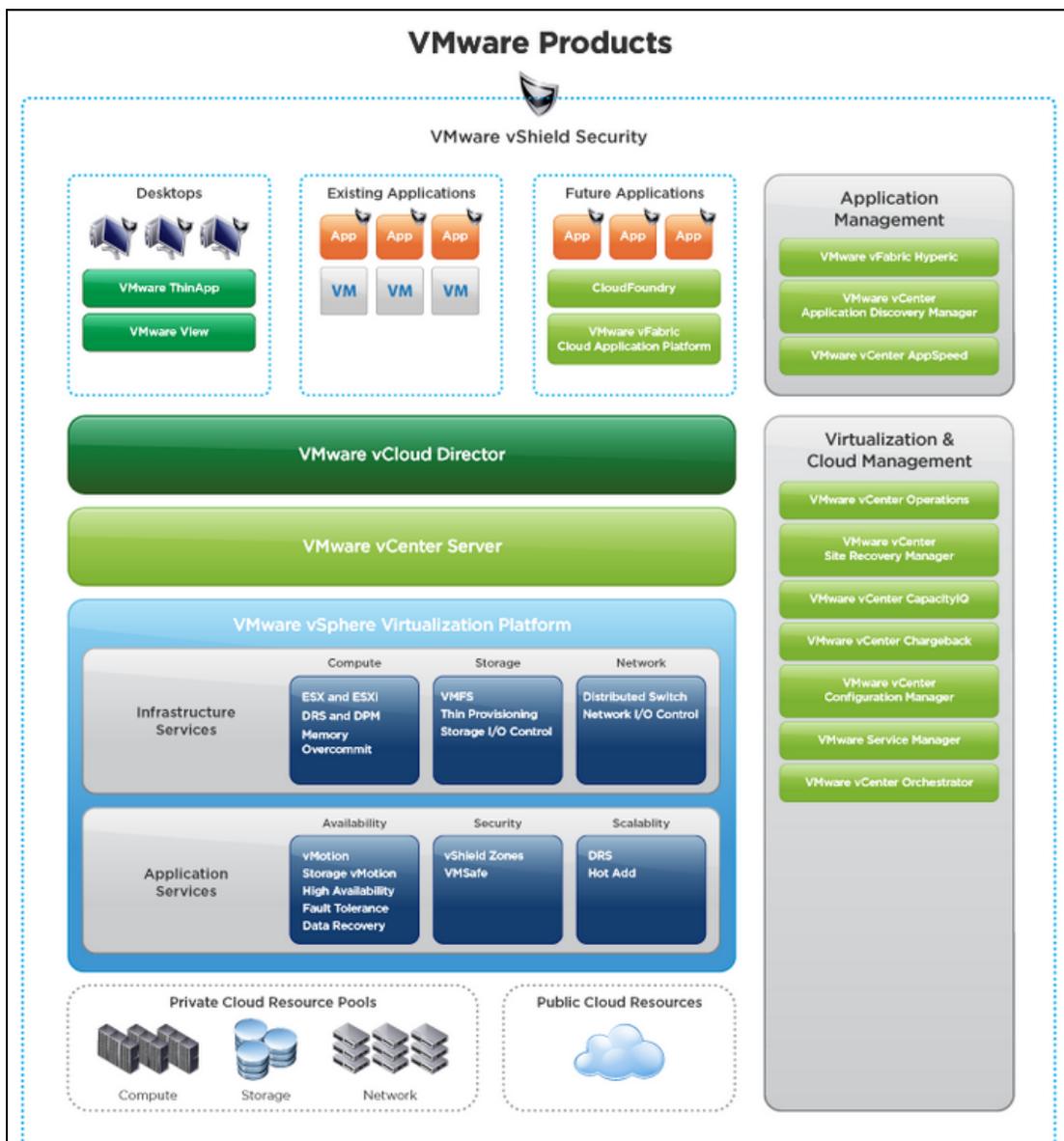
Figure 6: Navigating PCI DSS



The virtualization supplement was written to address a broad set of users (from small retailers to large cloud providers) and remains product agnostic (no specific mentions of vendors and their solutions).

* VMware solutions are designed to help organizations address various regulatory compliance requirements. This document is intended to provide general guidance for organizations that are considering VMware solutions to help them address such requirements. VMware encourages any organization that is considering VMware solutions to engage appropriate legal, business, technical, and audit expertise within their specific organization for review of regulatory compliance requirements. It is the responsibility of each organization to determine what is required to meet any and all requirements. The information contained in this document is for educational and informational purposes only. This document is not intended to provide legal advice and is provided "AS IS". VMware makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Nothing that you read in this document should be used as a substitute for the advice of competent legal counsel.

Figure 7: VMware PCI Compliance products



4. HP PCI Compliance Solutions

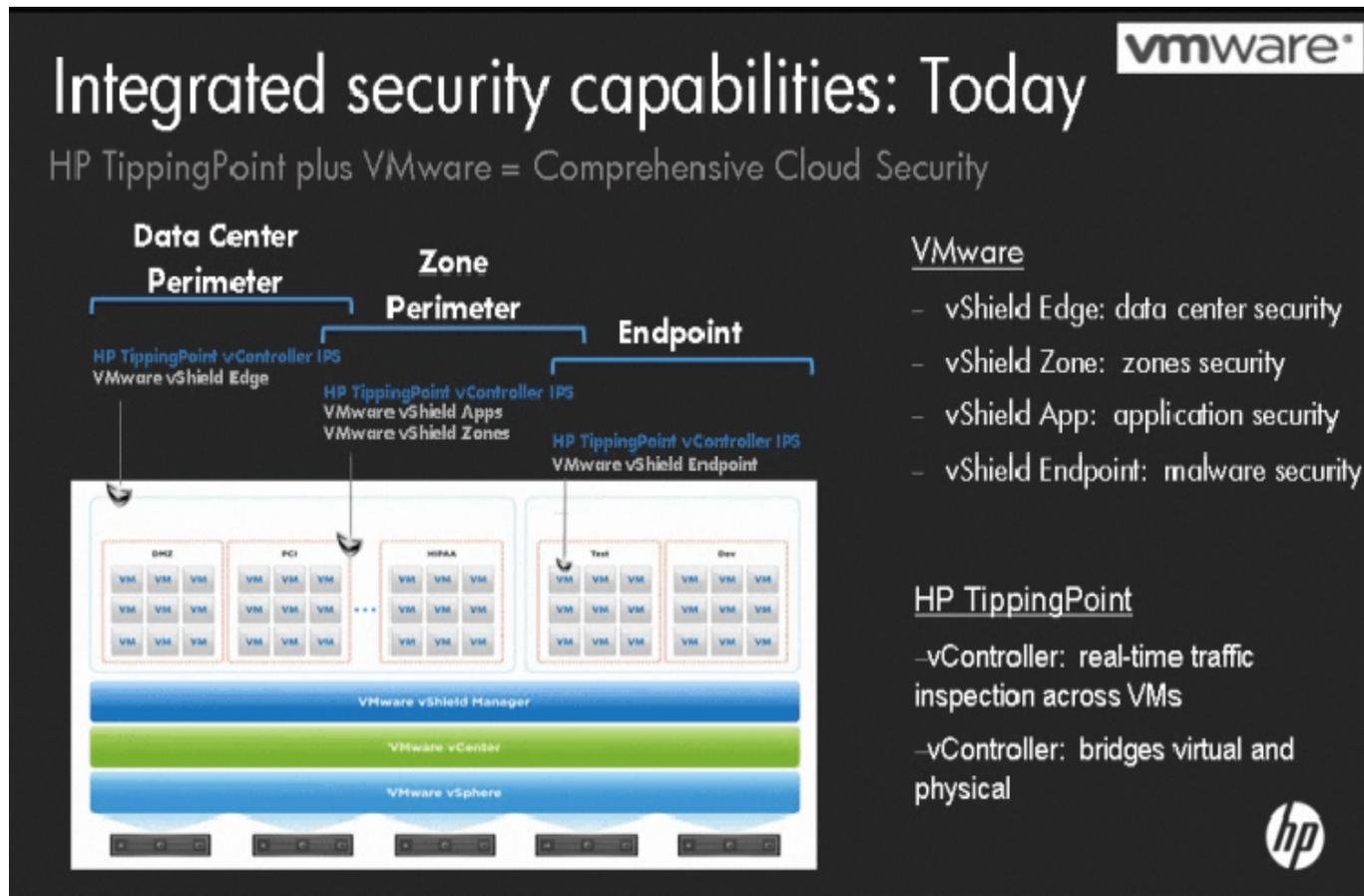
The table below is divided by solution that may contain several components as explained in the description.

Table 1: HP Solutions

Solution	Description
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.
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.
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 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, HP ArcSight IdentityView, and HP ArcSight ESM.
HP TippingPoint Next Generation Intrusion Prevention Systems (NG IPS) & vController+vFW	The HP Next Generation Intrusion Prevention System (NG IPS) provides proactive network security through inline, real-time protection of network traffic and data centers. The NG 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 NG IPS consists of the following systems: Security Management System (SMS) Client, Security Management System (SMS) Server, Intrusion Prevention System Device(s), Threat Management Center (TMC) Digital Vaccine(r), Virtual Management Center (VMC), and vController and/or vController+vFW
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.

Figure 8: Diagrammatic Representation of HP PCI suites

HP TippingPoint, ArcSite, Fortify, Atalla and TS Services have the broadest technology solution for PCI compliant virtualization running VMware TippingPoint, ArcSite, Fortify, and Atalla have created a combined reference design that customers can adapt quickly to their VMware environments.



5. HP PCI Requirements Matrix (Overview)

Table 2: PCI DSS Requirements Matrix

PCI DSS REQUIREMENT	NUMBER OF PCI 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	HP TIPPINGPOINT NEXT GENERATION INTRUSION PREVENTION SYSTEMS (NG IPS) & VCONTROLLER R+VFW	HP WEBINSPECT	COLLECTIVE TOTAL CONTROLS ADDRESSED BY HP PRODUCTS
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	25				9	11		14
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	24		1		3	6		6
Requirement 3: Protect stored cardholder data	33	14	13		1			19
Requirement 4: Encrypt transmission of cardholder data across open, public networks	9	1			1			1
Requirement 5: Use and regularly update anti-virus software or programs	6				3			3
Requirement 6: Develop and maintain secure systems and applications	32			15	2	2	9	17
Requirement 7: Restrict access to cardholder data by business need to know	7		6		1	7		8
Requirement 8: Assign a unique ID to each person with computer access	32		18		6	17		19
Requirement 9: Restrict physical access to cardholder data	28		1					1
Requirement 10: Track and monitor all access to network resources and cardholder data	29		22		20	19		26
Requirement 11: Regularly test security systems and processes.	24				2	1		3
Requirement 12: Maintain a policy that addresses the information security for all personnel.	40				1			1
Requirement A.1: Shared hosting providers must protect the cardholder data environment	8				2	1		3
TOTAL	297	15	61	15	51	64	9	121
Note: Control totals do not add up to 297 due to overlapping features of HP products.								

PCI Cloud Compliance Stack Details

The following matrix maps the PCI DSS controls to the functionality of the HP PCI Cloud Compliance Stack.

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.

Table 3: Applicability of PCI Controls to Atalla Network Security Processor (NSP) PCI Requirements Matrix

PCI DSS V2.0 APPLICABILITY MATRIX		
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	<p>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.</p> <p>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.</p> <p>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.</p> <p>All configuration actions are logged for audit trail from initial installation.</p>
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.



Atalla Enterprise Secure Key Manager (ESKM) PCI Requirements Matrix

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.

Table 4: Applicability of PCI Controls to Atalla Enterprise Secure Key Manager (ESKM)

PCI DSS V2.0 APPLICABILITY MATRIX		
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	<p>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.</p> <p>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</p>



PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	CONTROLS ADDRESSED	DESCRIPTION
		<p>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 guarantees that keys are not associated to user accounts for either data encrypting or key encrypting keys.</p> <p>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.</p> <p>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.</p> <p>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.</p>
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,	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



PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	CONTROLS ADDRESSED	DESCRIPTION
	8.5.14, 8.5.15, 8.5.16	<p>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.</p> <p>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.</p>
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	<p>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.</p> <p>ESKM also runs a digital signature verification of its internal software at power up or restart to ensure the integrity of the software.</p>



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 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.

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

Table 5: Applicability of PCI Controls to HP Fortify Software Security Center

PCI DSS V2.0 APPLICABILITY MATRIX		
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



PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	CONTROLS ADDRESSED	DESCRIPTION
		<p>based on industry standards and best practices and that information security is included throughout the development life cycle.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>HP Fortify RTA provides the capabilities to block traffic at the application layer and meet PCI requirements as a web application firewall.</p>



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.

Table 6: Applicability of PCI Controls to HP ArcSight ESM Compliance Insight Package for PCI

PCI DSS V2.0 APPLICABILITY MATRIX		
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.



PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	CONTROLS ADDRESSED	DESCRIPTION
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,	<p>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.</p> <p>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,</p>



PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	CONTROLS ADDRESSED	DESCRIPTION
	10.7	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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</p>



PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	CONTROLS ADDRESSED	DESCRIPTION
		<p>date and time stamps are collected and correlated for all audit trail events.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
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.



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(r) – 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.

Table 7: Applicability of PCI Controls to HP TippingPoint Intrusion Prevention Systems (IPS) & vController+vFW

PCI DSS V2.0 APPLICABILITY MATRIX		
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)	<p>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</p> <p>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.”</p>
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).



PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	CONTROLS ADDRESSED	DESCRIPTION
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.



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.

Table 8: Applicability of PCI Controls to HP WebInspect.

PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	CONTROLS ADDRESSED	DESCRIPTION
<p>Requirement 6: Develop and maintain secure systems and applications</p>	<p>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</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>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</p>



PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	CONTROLS ADDRESSED	DESCRIPTION
		<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>



Acknowledgements:

VMware would like to recognize the efforts of the VMware Center for Policy & Compliance, VMware Partner Alliance, and the numerous VMware teams that contributed to this paper and to the establishment of the VMware Compliance Program. VMware would also like to recognize the Coalfire Systems Inc. VMware Team www.coalfire.com/Partners/VMware for their industry guidance. Coalfire®, a leading PCI QSA firm, provided PCI guidance and control interpretation aligned to PCI DSS v. 2.0 and the Reference Architecture described herein.

The information provided by Coalfire Systems and contained in this document is for educational and informational purposes only. Coalfire Systems makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained herein.

About Coalfire®

Coalfire Systems 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, San Francisco, Seattle and Washington, D.C., and completes thousands of projects annually in retail, financial services, healthcare, government and utilities. Coalfire® has developed a new generation of cloud-based IT GRC tools under the Navis™ brand that clients use to efficiently manage IT controls and keep pace with rapidly changing regulations and best practices. Coalfire's solutions are adapted to requirements under emerging data privacy legislation, the PCI DSS, GLBA, FFIEC, HIPAA/HITECH, NERC CIP, Sarbanes-Oxley and FISMA. For more information, visit www.coalfire.com.

