CloudPassage

HALO IN ACTION – COMPLIANCE

DON'T LET LEGACY SECURITY TOOLS HOLD UP PCI COMPLIANCE IN THE CLOUD

Automated PCI compliance
— anytime, anywhere.

THE PROBLEM

Online commercial transactions will hit an estimated $2.35 trillion by 2017, according to eMarketer in their "Worldwide Retail Ecommerce Forecast". Coincident with this explosive growth has been the widespread adoption of cloud-based IT infrastructures that are able to handle the high volume of transactions that online and mobile commerce create.

Traditionally, enterprises have deployed a variety of IT controls to comply with the PCI DSS regulation – strong access controls, vulnerability assessment, file integrity monitoring, log monitoring, and other controls. This patchwork of controls works fine when all the card data resides in a traditional data center environment, but it breaks down in Infrastructure-as-a-Service (IaaS) environments such as Amazon Web Services (AWS). Traditional security controls are not fundamentally designed to operate efficiently in these new environments. When you try to operate traditional PCI security controls in IaaS environments, you encounter the following problems:

- Traditional host-based security products and log management products are slow to deploy and require manual effort to configure. This positions the security team as a bottleneck to the speed and agility that businesses expect from modern cloud environments and agile/DevOps organizations.
- Traditional controls do not operate continuously, therefore they can miss seeing short-lived workloads. For example, network scanning products that are based on periodic scanning windows (weekly or monthly) can completely miss seeing workloads that come and go within that time period. This would likely cause an auditor to flag these controls as being inadequate.
- Coordinating scanning permissions with cloud service providers (e.g. AWS) is a labor-intensive task for IT security personnel.
- Deploying traditional network scanners in the cloud – configuring each one for a specific IP range, and then adjusting them if/when your network changes – cannot be performed fast enough in the time windows required to ensure adequate protection.
- To get high-quality detections, network scanners require credential-based authenticated scanning to be performed on endpoints. But managing credentials is a significant effort when systems are constantly changing and credentials are constantly updated throughout the environment.

THE SOLUTION: CLOUDPASSAGE HALO

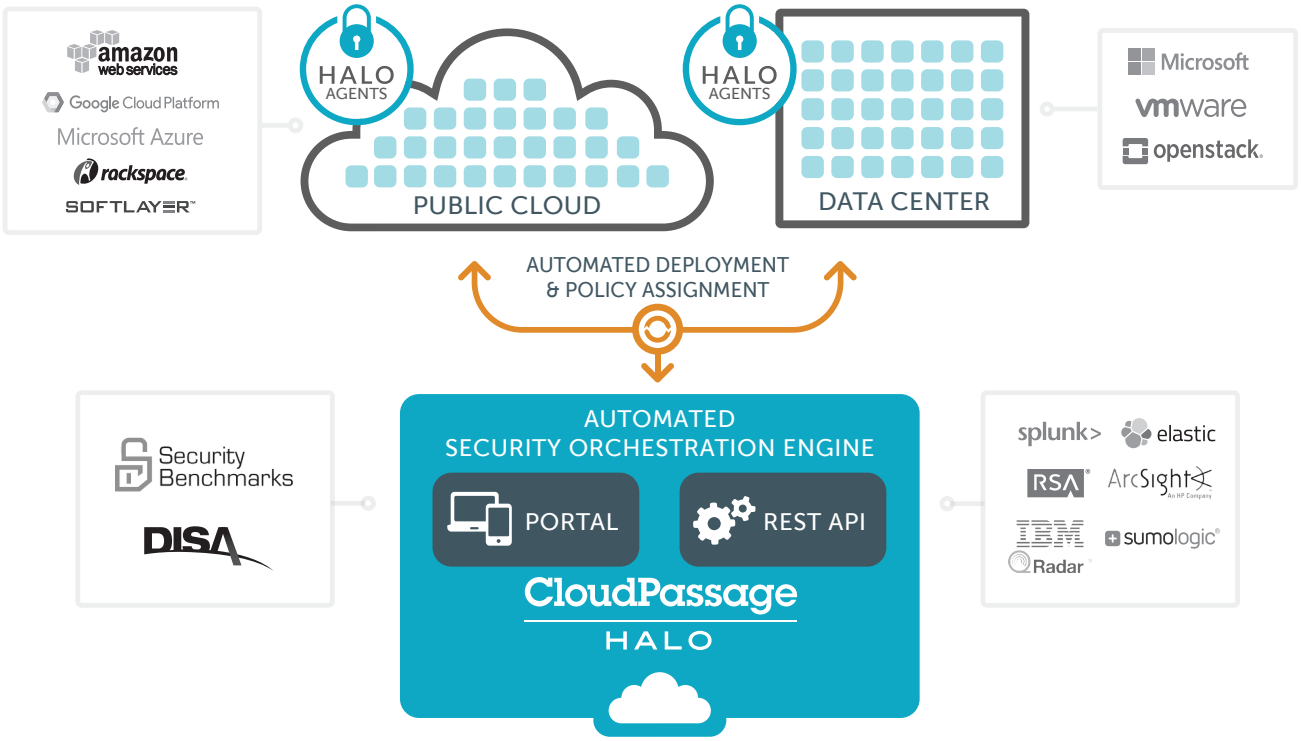
The CloudPassage® Halo® automated security and compliance platform solves all of these challenges. Halo provides businesses the easiest, most automated way to ensure compliance with the Payment Card Industry Data Security Standard.

Halo works across any cloud or virtual infrastructure: public, private, hybrid, multicloud or virtualized data center — including bare metal. Halo aligns directly with the critical needs of today's commerce-focused enterprise: delivered on-demand, fast to deploy, fully automated, and works at any scale.

- **Halo is continuous.** The Halo microagent can continuously monitor workloads that spin up and down rapidly in the cloud. Fresh information can be gathered from your entire environment in a matter of minutes.
- **Halo is a 100% SaaS-based product.** Halo's cloud-optimized architecture provides IT security managers a real-time, holistic view of their security posture and provides auditors a complete set of data from which to base a PCI audit—without the use of appliances or scanners.
- **Halo leverages a lightweight onboard microagent** which results in high-quality information without the need to manage credentials to the endpoints.
- **Halo is fast to deploy and easy to manage.** Installation of the microagent is totally automated. Halo integrates with DevOps tools such as Chef, Puppet, Salt, and Ansible.
- **Halo is portable.** If workloads move or IP addresses change, Halo policies automatically follow the workload.
- **Halo is audit-friendly.** Halo provides information based on the workload type, not the IP address which may frequently change in IaaS environments. Halo also includes open integration APIs to allow data to flow into popular GRC systems and SIEM systems.

Halo provides a broad range of controls that are required to prove compliance with PCI DSS requirements, including:

- Software vulnerability assessment
- Configuration security monitoring
- Server access monitoring
- File integrity management
- Log-based intrusion detection
- Software and hardware inventory



THE POWER OF HALO

GET INSTANT VISIBILITY

Workloads are tracked and reported on instantly and automatically.

REDUCE COSTS & IMPROVE EFFICIENCY

Eliminate manual processes — streamline and automate workflows.

VERIFY SYSTEM & DATA INTEGRITY

Apply and verify all required controls are in place.

AUTOMATE COMPLIANCE WORKFLOWS

Integrate with your existing tools and processes seamlessly

GENERATE & TRACK AUDIT LOGS

Ensure all critical activities are archived and readily available.

SCALE ON DEMAND

Non-intrusive, agent- based model scales without breaking a sweat.

STAY FLEXIBLE

Deploy seamlessly across any cloud or virtual infrastructure.

Here is how Halo controls replace traditional controls for PCI compliance:

Traditional controls	Halo controls
Network intrusion prevention	Halo includes log-based intrusion detection and file integrity management which can take the place of traditional network intrusion prevention
File integrity monitoring	Halo includes file integrity management
Software vulnerability management	Halo includes software vulnerability assessment
Configuration management	Halo includes configuration security monitoring
Strong access control	Halo includes server account management

Here is how Halo helps you meet each of the twelve PCI DSS requirements:

Goal 1: Build and maintain a secure network and systems

PCI DSS requirement	CloudPassage Halo coverage
Install and maintain a firewall configuration to protect cardholder data	*SUPPORTS SOME REQUIREMENTS* Halo can ensure that local firewall software is installed and configured correctly. In addition, Halo is compatible with any existing network firewalls or cloud-based zoning mechanisms that a customer may be using to support PCI requirements.
Do not use vendor-supplied defaults for system passwords and other security parameters	*DIRECTLY SATISFIES REQUIREMENTS* Server and application configuration scanning is a core Halo feature. This functionality is capable of identifying default OEM and cloud provider configuration options, including those that create security vulnerabilities. Two common examples of serious deficiencies in default configurations include Linux servers created with no root account password and servers with no password expiration controls. Halo provides out-of-the-box, customizable templates that alert to default and weak security parameters for servers and applications services. In addition to identifying poor default security configurations, Halo's configuration scanning provides ongoing assurance of system and application configuration compliance, with historical reporting that makes generating audit-related data fast and simple.

Goal 2: Protect cardholder data

PCI DSS requirement	CloudPassage Halo coverage
Protect stored cardholder data	*SUPPORTS SOME REQUIREMENTS* This requirement is very broad, including a number of data management, authentication and encryption requirements. CloudPassage Halo supports implementation of these requirements through management of encryption mechanisms and associated keys. Halo's configuration scanning functionality can continuously monitor for presence and configuration of encryption functions and access restrictions to cryptographic keys. This monitoring can be performed for operating system, application, and database platforms.
Encrypt transmission of cardholder data across open, public networks	*SUPPORTS SOME REQUIREMENTS* This requirement is really twofold: ensuring encryption of cardholder data in transit, and ensuring that cardholder data is never transmitted in the clear. Halo supports verification of correct configuration, as well as the explicit absence of unwanted data transmission facilities like FTP servers. As mentioned above, Halo's configuration scanning functionality can continuously monitor configurations for services capable of transmitting cardholder data. For example, web server configurations can be scanned to ensure that only HTTPS protocols are enabled. Another example is scanning of services listening on the network for FTP and other non-encrypted data transmission facilities. Given the typical scale of cloud-deployed applications, automation of these scans means saving extensive time and energy in manual verification and collection of data required for audits.

Goal 3: Maintain a vulnerability management program

PCI DSS requirement	CloudPassage Halo coverage
Protect all systems against malware and regularly update antivirus software or programs	*SUPPORTS SOME REQUIREMENTS* Halo does not provide antivirus capability, but does provide secondary controls to ensure that antivirus software is current, correctly configured, and maintains integrity. The configuration scanning capabilities in Halo provide the ability to ensure that antivirus software is present, the correct version, and active on the system. Specific configuration parameters, scan scheduling, and presence of memory-resident antivirus processes can all be continuously monitored. Halo's file integrity monitoring capability ensures that anti-virus binaries and signature data files have not been tampered with and therefore can provide accurate results.
Develop and maintain secure systems and applications	*DIRECTLY SATISFIES REQUIREMENTS* This requirement is one of the most broad in the PCI DSS, impacting nearly every area of information technology development and operation. It's also one of the areas where Halo adds very high value to cloud-based deployments. Halo provides functions to develop and maintain secure servers and applications. The software vulnerability scanning directly addresses requirements 6.1 and 6.2. Halo can also scan and monitor web server and application stack configurations to ensure resistance to application-level attacks, supporting requirement 6.6. Halo's file integrity monitoring and configuration scanning tools directly support requirements in sections 6.3 and 6.4. Collectively, Halo includes insight into known vulnerabilities; ability to enforce secure authentication and logging; ensure ongoing secure configurations; proper maintenance of accounts; monitoring of change control process and environments; and auditing of system and application changes.

Goal 4: Implement strong access control measures

PCI DSS requirement	CloudPassage Halo coverage
Restrict access to cardholder data by business need to know	*DIRECTLY SATISFIES REQUIREMENTS* This section requires implementation of access controls on a need-to-know basis and includes a number of reporting and verification requirements. Halo was specifically designed to implement these functions across large numbers of cloud servers. Halo's system configuration scanning and server account management features address the majority of server-level access control requirements in section 7. Halo also provides a centralized view of server accounts and their privileges across cloud hosting environments.
Identify and authenticate access to system components	*DIRECTLY SUPPORTS SOME REQUIREMENTS* This requirement entails maintenance of individual accounts on servers for anyone requiring access. These requirements include user authentication, provisioning, and password management practices. Halo Server Account Management addresses some of these needs. Halo Server Account Management provides web or API interfaces for management of accounts on cloud servers. Accounts can be created, modified, disabled and deleted; capabilities include password construction enforcement, secure password reset, and distribution of server authentication certificates. Halo also allows monitoring for account usage, abandoned accounts, and modifications to account security parameters.
Restrict physical access to cardholder data	*NO REQUIREMENTS COVERAGE* Halo does not address physical security requirements. Physical security is the responsibility of the owner/operator of the cloud environment in question. Service-level agreements and audit reports from the provider typically satisfy requirements where servers are hosted with external cloud service providers.

Goal 5: Regularly monitor and test networks

PCI DSS requirement	CloudPassage Halo coverage
Track and monitor all access to network resources and cardholder data	*DIRECTLY SATISFIES REQUIREMENTS* CloudPassage Halo directly satisfied fulfillment of multiple server-related requirements in this area of the PCI DSS. In addition to the access management capabilities explained in Requirement 8 (above), Halo provides extensive usage monitoring, logging and alerting capabilities. Some examples of server states and events that can be monitored include account usage, file ACL states, and process effective rights. These capabilities also provide extensive automated recordkeeping that saves time and effort in audit-related data collection.
Regularly test security systems and processes	*DIRECTLY SATISFIES REQUIREMENTS* This section requires that vulnerability scans are conducted regularly and whenever changes to the environment occur (e.g. new system components, changes in topology, firewall rule modifications, product upgrades). In dynamic cloud environments, these kinds of changes are constant meaning that continuous vulnerability monitoring is required. The requirements in section 11 also include intrusion detection monitoring and alerting at critical points in the infrastructure, such as on application and database servers. The standard also contains an explicit requirement for file-integrity monitoring tools that alert personnel to unauthorized modification of critical system files, configuration files, or content files. Halo addresses the need for vulnerability scans with Security Configuration Monitoring and Security Vulnerability Scanning features. Pre-defined templates provide deep configuration security policies for servers and application components, providing continuous monitoring that's automatically enabled whenever new cloud servers are deployed. Vulnerability scanning utilizes industry-standard software vulnerability signatures to monitor for known security issues in packages used by servers and applications. Halo's File Integrity Monitoring feature directly satisfies the PCI DSS requirement for detecting and alerting unexpected changes to critical system files. As with all Halo features, deployment of FIM controls is automatic for new servers deployed in cloud environments. In addition to immediate alerting, Halo provides a historical record of FIM scans and issues which speeds data collection needed at audit time.

Goal 6: Maintain an information security policy

PCI DSS requirement	CloudPassage Halo coverage *DIRECTLY SATISFIES REQUIREMENTS*
Maintain a policy that addresses information security for all personnel	Section 12 of the PCI DSS requirements is extensive. The key requirement that drives a need for Halo's deep security automation is 12.2, which calls for daily operational security procedures that are consistent with requirements in this and other sections. This single requirement creates dozens of day-to-day operational tasks that demand automation to achieve compliance in dynamic cloud environments. Halo was explicitly designed to automate deployment and operation of a broad range of controls in rapidly changing public, private and hybrid cloud hosting environments. Halo's extensive capabilities for automating day-to-day security operations is summarized in the sections above, and is extensively documented in resources on the CloudPassage website.

ABOUT CLOUDPASSAGE

CloudPassage® Halo® is the world's leading automated agile security platform that orchestrates security on-demand, at any scale and works in any cloud or virtual infrastructure (private, public, hybrid or virtual data center). Halo delivers a comprehensive set of continuous security and compliance functions right where it counts—at the server, VM, container, or workload. Our platform empowers our customers to take full advantage of cloud infrastructure with the confidence that their critical business assets are protected. Leading enterprises like Citrix, Salesforce.com, and Adobe use CloudPassage today to enhance their security and compliance posture, while at the same time enabling business agility.

CloudPassage

www.cloudpassage.com | 800.215.7404