



SOLUTION OVERVIEW

---

# DON'T LET MANUAL PROCESSES HOLD UP COMPLIANCE

---

Automated compliance  
— anytime, anywhere.

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

- Strong access controls
- Server access monitoring
- Configuration security monitoring
- Software vulnerability assessment
- File integrity management
- Log-based intrusion detection

## THE PROBLEM

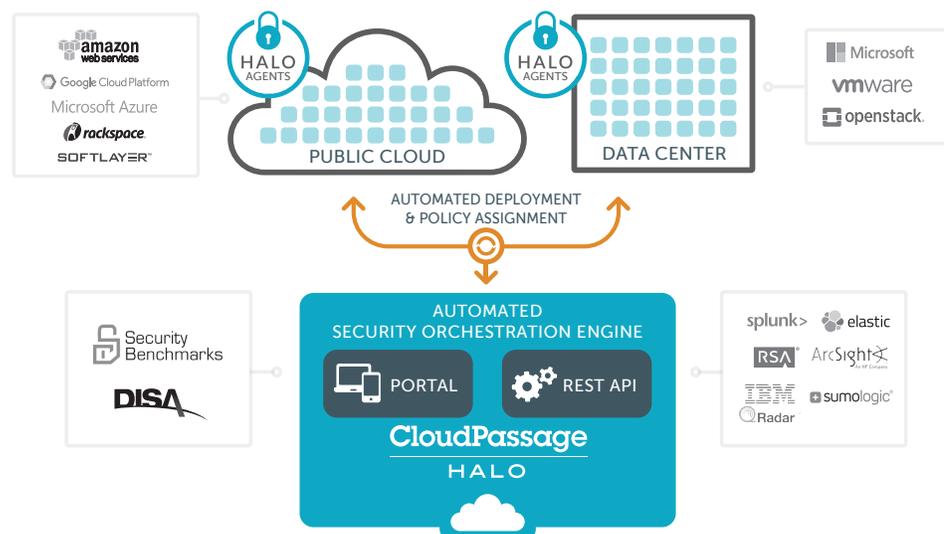
Enterprises that are subject to regulations such as PCI, HIPAA, SOC2, SOX have traditionally used a variety of IT controls to prove compliance with these regulations. While each regulation is different, the typical requirements include strong access controls, continuous monitoring and logging, and an accurate inventory of systems where sensitive data resides.

Unfortunately, the rapid migration from traditional servers to Infrastructure-as-a-Service in private and public clouds is putting a huge strain on enterprise compliance efforts. Neither the network controls nor the host-based controls are designed for these new environments. Traditional network firewalls have policies defined with specific source and destination IP addresses, which does not mesh well with the dynamic IP addressing used in cloud environments. And traditional host-based security systems are slow to deploy; they can not keep up with the rapid server provisioning that is a characteristic of cloud environments.

## THE SOLUTION: CLOUDPASSAGE HALO

The CloudPassage® Halo® agile security and compliance platform solves all of these challenges. Halo works across any cloud or virtual infrastructure: public, private, hybrid, multi-cloud or virtualized data center — including bare metal. It's unique because the platform provides continuous visibility and enforcement delivered as a service, so it's on-demand, fast to deploy, fully automated and works at any scale.

With CloudPassage Halo, you can track and report on all systems that fall under compliance regulations. The policies are automatically assigned based on the workload type, regulation category or sensitivity of the data. With open integration API's, the relevant data flows to popular GRC systems and workflows can be automated, and setting up rich data feeds into any existing SIEM or monitoring systems is quick and straightforward.



# 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.

Halo works across any cloud or virtual infrastructure: public, private, hybrid, multi-cloud or virtualized data center — including bare metal

## HOW HALO IS DIFFERENT

1

### Halo is fast.

Installation of agents can be totally automated.

2

### Halo is portable.

It works in any environments—data centers, private clouds and public clouds.

3

### Halo agents are extremely lightweight.

All security analytics are conducted on CloudPassage's servers, instead of your servers and cloud workloads.

4

### Halo is comprehensive.

It includes a broad range of security controls that map to compliance requirements.

5

### Halo is scalable.

Our customers routinely deploy Halo to over 10,000 workloads in just a few days.

# HOW IT WORKS

## Automated agent deployment

Halo uses an ultra-lightweight agent that can be deployed automatically via automated scripts or via popular orchestration tools that you are probably already using, such as Chef, Puppet, Ansible, Salt, Jenkins, BOSH, etc.

## Automated visibility

Halo agent automatically connects to the Halo Orchestration Engine every 60 seconds, giving you visibility to systems that are newly created or auto-scaled.

## Instant scalability

Halo is delivered as a service so it can scale as rapidly as your IT automation systems can provision new workloads.

## Automated policy assignment

Halo applies the appropriate policy to each system based on tags that define the application and operating system. These policies follow the workload no matter where the workload physically resides—data center, public cloud, private cloud.

## Broad range of compliance controls

Halo controls are directly applicable to many of the data privacy regulations included in PCI, HIPAA, SOC2, SOX. Controls span server access, workload configuration, software vulnerability assessment, file integrity management, and host-based log storage and analysis.

## Full API

The CloudPassage Halo platform supports an open, RESTful API that makes it easy to integrate with a range of security and operational solutions.

# 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.

[www.cloudpassage.com](http://www.cloudpassage.com) | 800.215.7404

**CloudPassage**

© 2017 CloudPassage. All rights reserved. CloudPassage® and Halo® are registered trademarks of CloudPassage, Inc. SB\_COMPLIANCE\_04272017