SOLUTION OVERVIEW

DON'T LET MANUAL PROCESSES HOLD UP COMPLIANCE

Continuous compliance monitoring for modern cloud environments.

CloudPassage

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. Traditional security controls were not designed for these new environments.

Here are specific examples of how legacy compliance tools are misaligned with modern compute environments like public cloud and container:

- Traditional network scanners do not operate continuously, thus, they can miss seeing workloads that spin up and down rapidly in the cloud. This gap can result in an audit failure.
- Security tools that are based on IP addresses require frequent adjustments as the IP addresses change in the cloud.
- Dealing with multiple reports from multiple tools--some of which may be based on IP addresses which change all the time--is difficult for auditors and wastes time.
- To get high-quality detections, network scanners require that credential-based authenticated scanning be performed on endpoints. But managing credentials is a laborious effort when systems are constantly changing.
- Coordinating scanning window permissions with cloud service providers is a labor-intensive task for IT security personnel

THE SOLUTION: CLOUDPASSAGE HALO

The CloudPassage® Halo® automated 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. 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 mandates, regardless of whether the systems are virtual machines, containers, or bare metal servers. Policies are automatically assigned to each workload based on the workload type, not the IP address. Halo automatically accommodates changes to IP addresses.

With open integration API's Halo can be integrated with any popular tooling, such as Jenkins for CI, Puppet for CD, and PagerDuty for alerting. Workflows can be automated enabling real time GRC dashboards such as Allgress or Archer. Setting up rich data feeds into any existing SIEM such as Sumo Logic or monitoring system like VictorOps is quick and straightforward.

	PCI	HIPAA	SOC2
Software vulnerability assessment	2.4, 6.1, 6.2	164.312(b)	7.2
Configuration security monitoring	2.1, 2.2, 3.6.5, 4.1, 6.1, 6.2, 6.3.1, 7.2.3, 8.2, 10.2, 10.4, 12.5.2, 12.10.5	164.312(b)	3.2, 3.3, 4.1, 5.8, 6.1, 6.2, 7.2, 7.3
Server account management	2.1, 6.3.1, 6.4, 8.1, 8.2, 8.5, 12.5.4	164.312(a)(1) 164.312(d)	5.6
Log-based intrusion detection	2.2.2, 2.3, 10.6, 11.4, 12.5, 12.10		3.2, 3.3, 4.1, 5.8, 6.1, 6.2, 7.2, 7.3
File integrity monitoring	2.2, 3.6.5, 6.3.1, 6.4.4, 11.5.1, 12.5.2, 12.10.5	164.312(b) 164.312(c)(1)	3.2, 3.3, 4.1, 5.8, 6.1, 6.2, 7.2, 7.3
Event logging and alerting	11.5, 12.5.2, 12.9.5	164.312(b)	3.3, 5.1, 6.1, 6.2, 7.2, 7.3

Halo provides a broad range of compliance controls to meet multiple regulations

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

SOFTWARE VULNERABILITY ASSESSMENT

Scan thousands of servers in minutes to maintain continuous exposure awareness in the cloud. Halo automatically scans for vulnerabilities in your software packages—across all of your environments.

LOG-BASED INTRUSION DETECTION

Halo continuously monitors key server log les for events that should not happen; indicating misuse, miscon guration, or a compromise, as required by many regulations.

CONFIGURATION SECURITY MONITORING

Evaluate servers against the latest configuration policies in seconds with almost no CPU utilization. Halo automatically monitors operating system and application configurations, processes, network services, privileges and more.

FILE INTEGRITY MONITORING

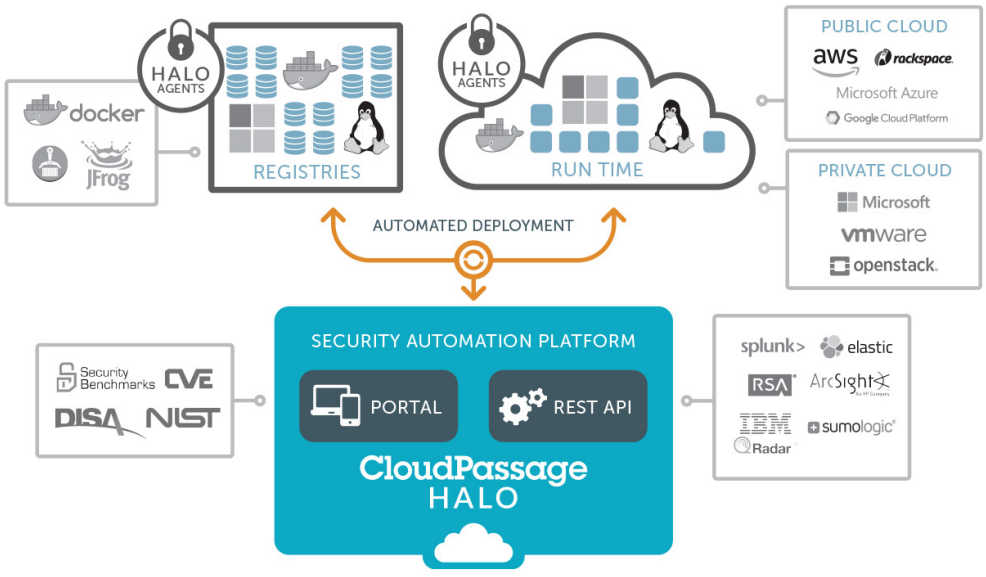
Protect the integrity of your cloud servers by constantly monitoring for unauthorized or malicious changes to important system binaries or files.

SERVER ACCOUNT MONITORING

Easily monitor and audit server accounts and access. Halo enables you to evaluate who has accounts on which servers, what privileges they operate under and how accounts are being used. You can monitor all your cloud servers through a single online management console.

EVENT LOGGING AND ALERTING

Detect a broad range of events and system states, alerting you when they occur.



HOW IT WORKS

Automated agent deployment

Halo uses a micro-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, Jenkins, etc.

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. This makes Halo agnostic to IP address changes.

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.

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

Founded in 2011, CloudPassage® was the first company to obtain a U.S. patent for universal cloud infrastructure security and has continued to innovate cloud security automation and compliance monitoring for application development and deployment. CloudPassage Halo® is an award-winning workload security automation platform, delivered as a service, that provides universal visibility and continuous protection for data centers, private/public clouds and containers. Halo deploys in minutes and scales effortlessly. The platform integrates with automation and orchestration tools such as Puppet and Chef, as well as CI/CD tools such as Jenkins. Today, CloudPassage Halo secures the infrastructure of leading global finance, insurance, media, ecommerce, high-tech service providers, transportation and hospitality companies.

CloudPassage

www.cloudpassage.com | 800.215.7404