AUTOMATED SECURITY FOR AMAZON EC2
Planning your organization’s move to the cloud is far from easy, and requires a great deal of time, effort, and strategic thought. Many organizations will not transition completely to a cloud environment, living in a hybrid state of on-premises and cloud for an extended period of time, and in some cases permanently. No matter where your data center resides, security is a primary concern. As organizations plan and eventually make their move to the cloud, security becomes an even higher priority. The Gartner report titled, “Market Guide for Cloud Workload Protection Platforms,” comments:

“Cloud workloads have different requirements for security than end-user facing endpoints, and the adoption of hybrid private/public cloud computing models compound the differences. CISOs should deploy products specifically designed for the protection of hybrid cloud workloads.”

Security products designed for existing and legacy on-premises data centers are unable to keep up with the rapid pace of innovation required by modern agile business practices such as DevOps. For this reason, Amazon Web Services (AWS) has leveraged its abilities (and those of AWS Partner Network (APN) Security Partners) to create a new generation of security services purpose-built to provide security in the cloud. CloudPassage Halo has taken that a step further by providing an on-demand infrastructure security service focused on protecting servers in any combination of on-premises, private clouds, and your AWS workloads.
In the AWS Shared Responsibility Model, security is a collaborative effort between AWS and you, the customer. AWS provides the secure infrastructure and services for you to develop and run your applications. Assuring the security of your application stack is your responsibility.

This means managing and protecting your applications by applying security policies to the workloads themselves to satisfy your security objectives and compliance requirements such as PCI DSS, SOC2, HIPAA/HITECH, and FISMA.
Cloud security at AWS is the highest priority. As an AWS customer, you will benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations. In fact, according to a recent IDC White Paper, “Assessing the Risk: Yes, the Cloud Can Be More Secure Than Your On-Premises Environment,” you can, and probably will, be more secure on the AWS Cloud than on-premises if you leverage a properly designed security program like CloudPassage Halo.

An advantage of the AWS Cloud is that it allows customers to scale and innovate, while maintaining a secure environment. Customers pay only for the services they use, meaning that you can have the security you need, but without the upfront expenses, and at a lower total cost of ownership than in an on-premises environment. Security built to keep up with the pace of innovation in modern IT is a requirement of any organization utilizing the cloud.

CloudPassage Halo is a security and compliance automation infrastructure that provides the enhanced security required by the AWS Shared Responsibility Model. As an AWS Security Competency Partner, CloudPassage has demonstrated success in building products and solutions on AWS to support customers. Halo gives you instant visibility into, and continuous protection for, your workloads across AWS public cloud or virtual private cloud, as well as hybrid cloud environments.
Solving Modern Data Center Challenges

The Visibility Challenge
Modern infrastructure environments are highly elastic, dynamic and automated, but maintaining continuous visibility into your data center, cloud instances, and workloads can be a daunting task. Traditional security tools simply don’t work well in these environments because they aren’t agile enough, require lots of manual change control, don’t scale, and don’t automatically deploy as systems spin up.

The CloudPassage Halo infrastructure works seamlessly in any combination of dynamic compute environments: data centers, private cloud, and public cloud. Halo is delivered as a service, so it’s on demand, fast to deploy, fully automated, and works at any scale.

The Lateral Challenge
The same modern, agile infrastructure environments are also putting a huge strain on network security teams as they struggle with blind spots and threats missed by the perimeter. As networks get flatter, east-west traffic is increasing, which makes it difficult to detect lateral threats. New workloads are added and retired dynamically, change control is challenging, and maintaining granular firewall rules and security policies is a time consuming process. Expanding onto the AWS Cloud can break traditional tools, as virtualized security appliances lack dedicated hardware acceleration, limiting scalability and performance. And virtualized endpoint security tools have a large footprint, imposing a heavy burden on each workload. As a result, many IaaS workloads are inadequately protected.

The CloudPassage Halo agile security and compliance infrastructure solves these challenges by reducing the attack surface through microsegmentation, host firewall orchestration, traffic discovery, and layered protection at every server. Policies that control east-west traffic between groups of servers can be easily customized for your AWS environment. A single user interface makes it fast and easy to spot problems and drill down to the appropriate level of detail needed to remediate.
The Compliance Challenge

The rapid pace at which organizations are migrating from traditional servers to the agile, elastic infrastructure of the cloud seems to increase daily. Implementing continuous monitoring and logging, while maintaining an accurate inventory of systems, can be a seemingly daunting task, at first glance.

The CloudPassage Halo infrastructure solves these challenges by automating many of the currently manual processes related to compliance. For example, Halo automatically gathers and presents information required for PCI compliance audits, dramatically simplifying audit readiness and enabling organizations to adopt a “compliance in motion” strategy.

The DevSecOps Challenge

The rise of continuous development and deployment methods, like DevOps, have brought speed and quality benefits, but they have inadvertently posed significant tests to security organizations. Applying security policies based on static parameters and making manual rule adjustments just before production leaves little time for provisioning the policies.

This impacts release quality, increases risk of errors and slows down the DevOps cycle. Trying to use DevOps tools to provision security can leave companies exposed since these tools lack critical controls and don’t integrate with the rest of the security infrastructure.

CloudPassage Halo on AWS solves these challenges by giving security and DevOps teams an agile security and compliance infrastructure that bakes security right into the deployment/provisioning process, ensuring that new workloads, instances, and containers are protected from the start.
CloudPassage Halo is purpose-built for agile IT environments, working anywhere, on-demand, and at any scale. Halo is delivered as a metered service, deploys in minutes, scales on-demand, and eliminates costly, error-prone manual processes by baking security directly into your workloads. Its library of ready-to-use security policies gives you a head start on meeting your security objectives and compliance requirements.

The Halo REST API makes it easy to integrate with your existing security tools and extends your security investments.

The CloudPassage Halo Toolbox provides examples of scripts and integrations developed by our customers, our partners, and CloudPassage. These include archival, audit, automation deployment, and integration tools.
The Power of Halo for AWS

Instant visibility and continuous protection for AWS workloads.

Automated provisioning of security for faster deployment and automatic scalability.

Faster time to value and reduced operational overhead.

REST API for easy integration with AWS and existing tools.
Orchestration services

CloudPassage Halo is built on the principles of abstraction, automation, orchestration, automatic scalability and API enablement — all essential capabilities required for securing dynamic cloud infrastructure. Customers have the option to set up automated, hands-free security provisioning through the Halo portal or by using other popular orchestration tools.

Integrations

The CloudPassage Halo infrastructure supports an open, RESTful API that makes it easy to integrate with a range of security and operational solutions. Check our website for the latest list of tested integrations.
Enhanced Security Controls for Data on AWS

**Configuration Security Monitoring:** Continuously monitor the configuration of your server instances and detect any drift from your standards and policies. With almost no CPU utilization, Halo automatically monitors operating systems, application configurations, processes, network services, privileges and more.

**Workload Firewall Management:** Easily deploy and manage dynamic host firewall policies across all environments. Build firewall policies from a simple web-based interface, and assign them to groups of servers. Changes to host firewalls are orchestrated automatically based on policies as new servers are added, retired, or as IP addresses change.

**Multi-Factor Network Authentication:** Further harden your server instances by only allowing temporary, on-demand access for authorized users. Halo supports secure remote network access using two-factor authentication without requiring any additional software or infrastructure.

**File Integrity Monitoring:** Protect your instance integrity by continuously monitoring for unauthorized or malicious changes to important system binaries, configuration files, and any other file. Halo automatically creates a baseline record of the “clean” state of new systems, then periodically re-scans each instance and compares the results to that baseline. Any differences are logged and reported.
Enhanced Security Controls for Data on AWS

**Server Access Management:** Monitor your server instances through a single management console to easily identify invalid or expired accounts, plus evaluate who has accounts on which servers, what privileges they operate under and how accounts are being used.

**Log-Based Intrusion Detection:** Halo LIDS continuously monitors important server log files for suspicious events and activities that might indicate misuse, misconfiguration, or even a compromise. When LIDS detects a suspicious event, details are inserted into the Halo security events feed, and administrators are alerted to the suspicious activity.

**Event Logging & Alerting:** Easily detect and manage a broad range of events and system states. Halo enables you to watch system logs, define events and their severity level, and instantly send alerts to enable a fast response time.

**Traffic Discovery:** Discover and visualize the IP connection patterns and listening ports of your workloads and servers, both between Halo-protected systems as well as connections to and from remote systems. Traffic Discovery helps you create dynamic firewall policies with confidence, ensuring that you are not blocking desirable traffic.

**Software Vulnerability Assessment:** Scan thousands of server instances in minutes and with almost no overhead on your network bandwidth to maintain continuous exposure awareness in the AWS Cloud. Halo can automatically scan your entire environment for vulnerabilities in your packaged software.
Getting Started

• CloudPassage AWS solution page
• CloudPassage on AWS Marketplace

About AWS:
For 10 years, Amazon Web Services has been the world’s most comprehensive and broadly adopted cloud platform. AWS offers over 70 fully featured services for compute, storage, databases, analytics, mobile, Internet of Things (IoT) and enterprise applications from 33 Availability Zones (AZs) across 12 geographic regions in the U.S., Australia, Brazil, China, Germany, Ireland, Japan, Korea, and Singapore. AWS services are trusted by more than a million active customers around the world – including the fastest growing startups, largest enterprises, and leading government agencies – to power their infrastructure, make them more agile, and lower costs.

To learn more about AWS, visit http://aws.amazon.com

About CloudPassage:
CloudPassage® Halo® is one of the world’s leading agile security platform that provides instant visibility and continuous protection for servers in any combination of data centers, private clouds and public clouds. The Halo platform is delivered as a service, so it deploys in minutes and scales on-demand. Halo uses minimal system resources; so layered security can be deployed where it counts, right at every workload – servers, instances and containers.

To learn more about CloudPassage, visit www.cloudpassage.com