CloudPassage

COMPANY OVERVIEW

How do you keep workloads secure in highly dynamic, highly automated compute environments? Traditional security products don't work well in these environments. They require too much manual effort to deploy and operate, and they don't provide fast feedback to developers.

CloudPassage has solved this problem. CloudPassage Halo is an automated security platform that delivers instant visibility and continuous protection in any combination of data centers, private clouds and public clouds. The platform is delivered as a SaaS application, so it's on-demand, fast to deploy, fully automated and works at any scale.

Customers

Capital One

Fidelity INVESTMENTS

GE

Sony Interactive Entertainment

xero

Problem

- IT security teams find that traditional security tools create too much friction in modern compute environments (e.g. devops, public or private cloud). Traditional tools require too much manual effort to deploy and configure, and they are too slow to monitor ephemeral workloads.
- Application developers waste time going back to fix vulnerabilities in applications that they released a long time ago. Traditional vulnerability assessment tools do not provide fast feedback.
- IT operations teams responsible for deploying applications into cloud environments like AWS EC2 waste time manually deploying, configuring, and managing security products that were not designed to integrate with automation tools such as Chef and Puppet.

Solution

- Halo is a security and compliance automation platform that was purpose-built to handle the highly fluid and scalable characteristics of modern compute environments and agile/DevOps toolchains.
- Halo leverages your existing automation tools. Halo microagents can be installed via scripts or orchestration tools such as Chef, Puppet, Jenkins, or Ansible.
- Halo can replace a broad range of traditional security controls. Halo controls are applicable to regulations such as in PCI, HIPAA, SOC2, SOX.

How we're different

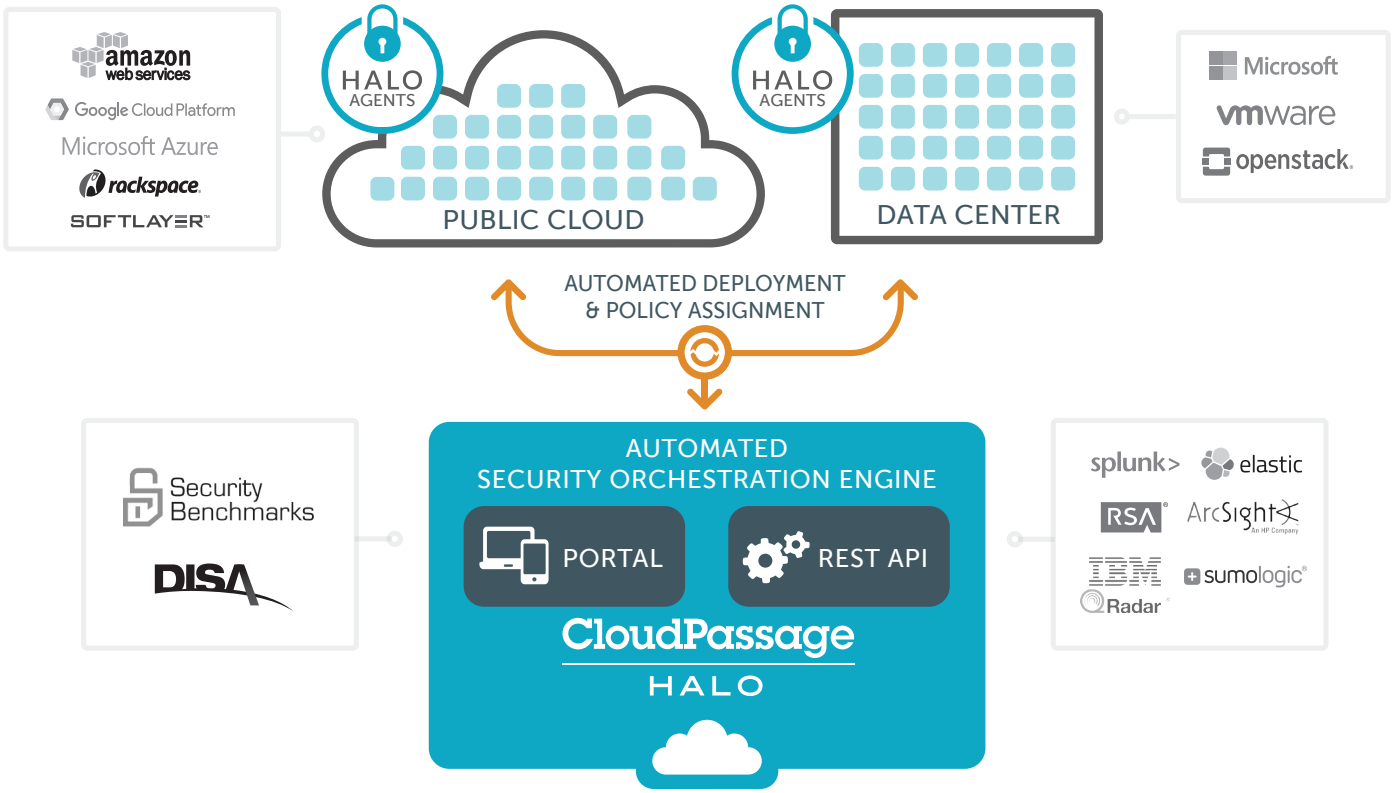
Halo is fast. Deployment can be totally automated via tools such as Chef, Puppet, Salt, Ansible, and Jenkins.

Halo is easy. Configuration benchmark policies can be configured with just a mouse click.

Halo is portable. It provides visibility in any environment—data centers, private clouds, public clouds and containers.

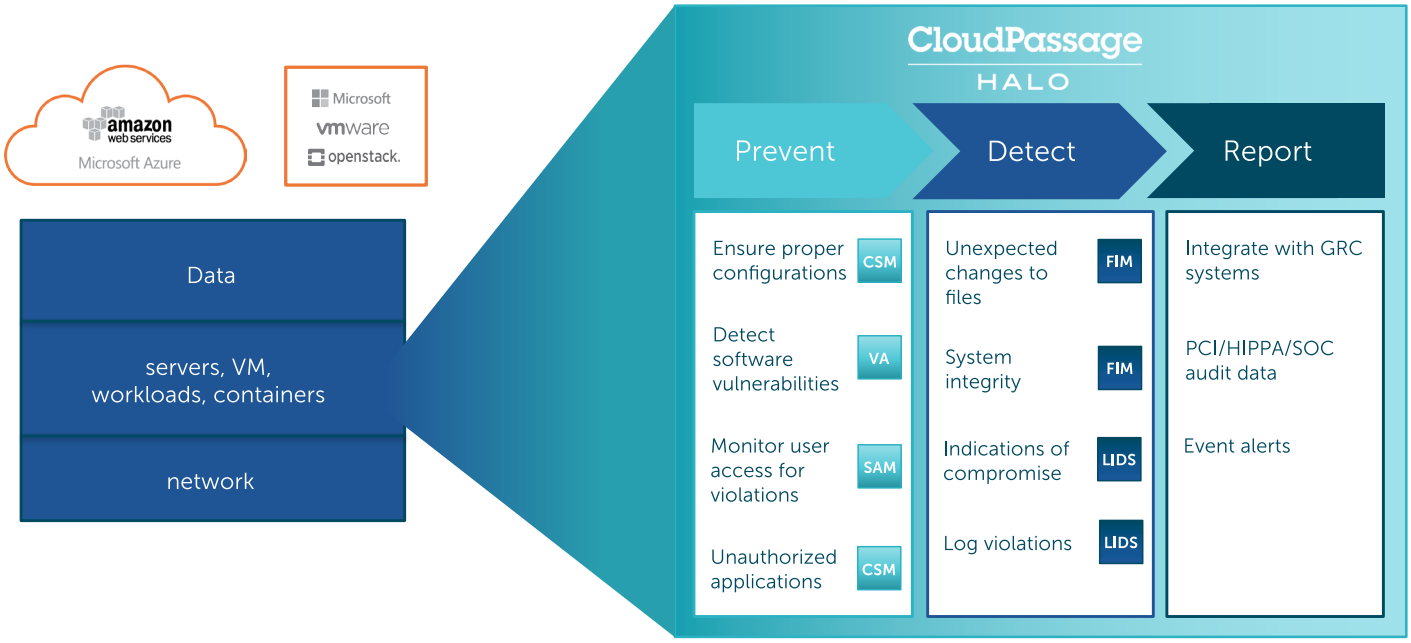
Halo agents are extremely lightweight. All security analytics are conducted on CloudPassage's servers, instead of your servers and cloud workloads.

Halo is a true SaaS solution. It scales on-demand. Our customers routinely deploy Halo to over 10,000 workloads in just a few days.



CloudPassage Halo

CloudPassage Halo protects workloads in any operating environment - public cloud or private data center. Halo is comprised of modules that can be purchased separately or in combination.



Configuration Security Monitoring (CSM)

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.

Software Vulnerability Assessment (SVA)

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.

Server Access Management (SAM)

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.

File Integrity Monitoring (FIM)

Protect the integrity of your cloud workloads by constantly monitoring for unauthorized or malicious changes to important system binaries or les. Automate creation of baseline records of new systems, then periodically re-scan each instance and compare the results to that baseline, with logging and alerting on drift.

Log-Based Intrusion Detection (LIDS)

Halo continuously monitors key server log les for events that should not happen; indicating misuse, miscon guration, or a compromise. When Halo detects a suspicious event, the details are collected and inserted into the Halo security events feed, and users are alerted to the suspicious activity.

ABOUT CLOUDPASSAGE

CloudPassage® Halo® is the world's leading automatedagile 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