INSTANT VISIBILITY, CONTINUOUS PROTECTION

ON-DEMAND, AUTOMATED INFRASTRUCTURE SECURITY THAT WORKS ANYWHERE, AT ANY SCALE

THE SECURITY CHALLENGE

Enterprises are adopting next generation agile IT delivery models; the business benefits are simply too compelling to ignore. The new era of elastic IT resources is automated, on-demand, quick to deploy and self-provisioning, which drives tremendous agility, speed and efficiency.

But this transformation has put security organizations under intense pressure. Traditional security tools fail in these environments because they were architected in a world where rates of change were slow, control was centralized, IP addresses were fixed, and there was a well-defined perimeter. Trying to force-fit old security approaches could cost millions in breaches and operational delays. What's needed is a new approach that allows businesses the freedom to take full advantage of agile IT delivery models, while at the same time providing comprehensive protection of critical assets.

CLOUDPASSAGE HALO

CloudPassage® Halo® is the world's leading on-demand infrastructure security platform focused on protecting servers in any combination of data centers, private clouds and public clouds. Halo deploys in minutes and implements a comprehensive set of controls that continuously monitor the security posture of your servers and cloud workloads. Halo uses minimal system resources; so layered security can be deployed where it counts, right at every workload—servers, instances and containers. Since Halo is delivered as a service, it deploys in minutes and scales on-demand. Halo enables more than 100 leading enterprises like Citrix, Salesforce.com and Adobe to take advantage of modern infrastructure models that require automation, high rates of change and on-demand IT services.

VALUE...DELIVERED

- **Business Agility.** Halo is on-demand, always available & takes just minutes to set up.
- **Comprehensive Controls.** Achieve a broad range of control objectives all in one platform.
- **Instant Visibility.** Every workload, all the time, no matter where they are running.
- **Reduced Attack Surface.** Protect against lateral movement of threats with microsegmentation.
- **Speed.** Security baked into continuous development methods like DevOps.
- **Automated Compliance.** One click compliance monitoring & audit data.
- **Freedom of Choice.** Secure servers and virtual machines anywhere – data centers or cloud providers.
- **Integration.** Halo easily integrates with SIEM, access control, orchestration tools you use today.

THE HALO ON-DEMAND PLATFORM SOLVES REAL WORLD CHALLENGES

WORKLOAD PROTECTION

Halo reduces the software attack surface of your workloads by ensuring proper security configuration, discovering software vulnerabilities, and auditing remote access of each workload.

FAST MICROSEGMENTATION

Halo reduces your network attack surface by enabling microsegmentation through host firewall orchestration, traffic discovery and multi-factor network authentication. This reduces risk from lateral movement of threats – in any environment.

COMPROMISE DETECTION

Halo alerts you if any your workloads have been compromised by monitoring whether important binaries and configuration files have changed and by monitoring key server log files for suspicious events.

AUTOMATED COMPLIANCE

Halo lets compliance teams replace manual processes with full automation. Halo tracks the security posture of all assets in scope of regulations. This saves money, improves efficiency and enables continuous compliance.

SECURITY AT DEVOPS SPEED

Halo makes it easy to bake security right into the DevOps workflow, ensuring every workload is protected from the start. This allows businesses to securely embrace agile practices like DevOps and empowers security teams to move faster.

SECURITY FOR AWS EC2

Halo complements the security tools built into AWS EC2 with a broad range of workload security controls that allow you to protect your instances in AWS and other operating environments.

"CloudPassage is really an investment that will help us sell more efficiently. With CloudPassage we can show what we do for security and show how we prove it."

– MANNY LANDRON, SENIOR MANAGER, SECURITY & COMPLIANCE, CITRIX SYSTEMS

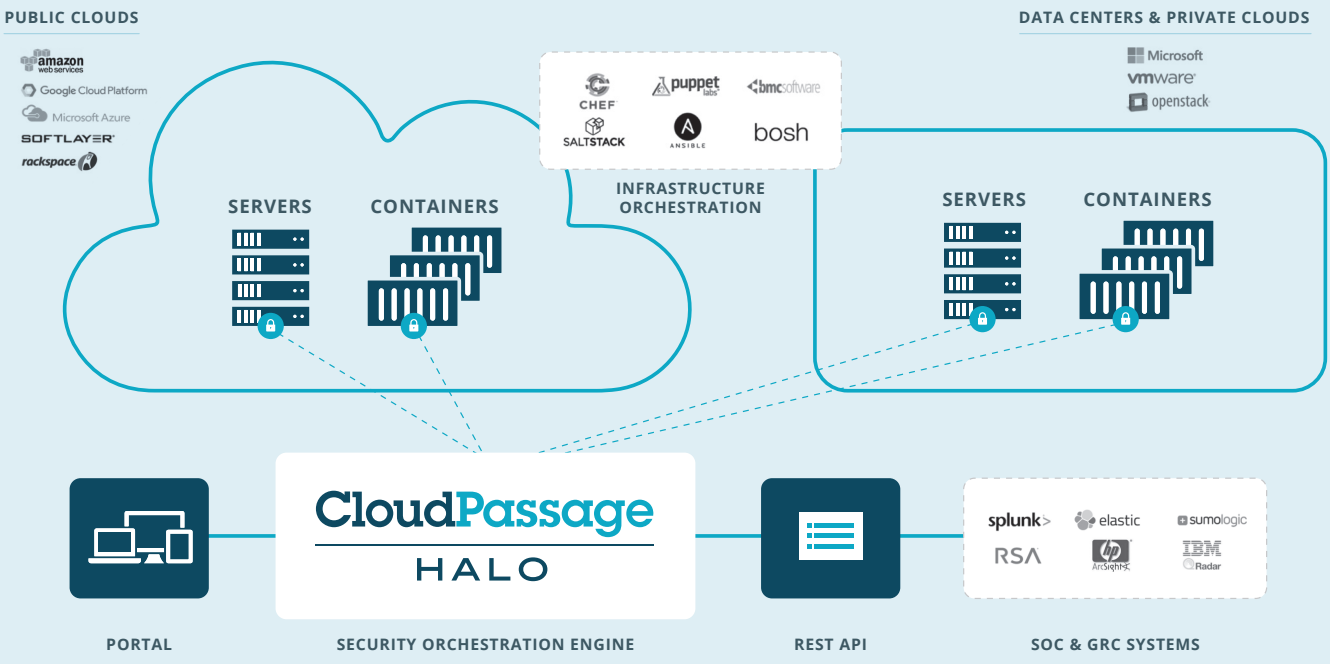
"Accelerating the security maturity of our acquired companies through the use of CloudPassage has been a huge benefit to reducing the friction of integrating new companies."

– PATRICK HEIM, CHIEF TRUST OFFICER, SALESFORCE.COM

HOW IT WORKS

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 define security policy through the Halo portal or API and can automate security provisioning by using popular orchestration tools such as Chef, Puppet, and others.

The ultra-lightweight Halo agent instruments workloads, wherever they are—in any combination of data centers, private cloud or public cloud. The agent picks up control commands from the Halo security orchestration engine and sends telemetry back to it. The security orchestration engine continuously analyzes information gathered, giving security and compliance organizations near real-time visibility into their security posture.



CLOUDPASSAGE HALO

CloudPassage Halo is a comprised of three packages that can be purchased separately or in combination.

1

HALO PROTECT

- Configuration Security Monitoring
- Software Vulnerability Assessment
- Server Access Management

2

HALO SEGMENT

- Traffic Discovery
- Workload Firewall Management
- Multi-Factor Network Authentication

3

HALO DETECT

- File Integrity Monitoring
- Log-Based Intrusion Detection

HALO SECURITY ORCHESTRATION PLATFORM

Security Events, Alerting, API, Portal, Policy Templates, Summary Dashboard

1

HALO PROTECT

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.

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.

SERVER ACCESS MANAGEMENT

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.

2

HALO SEGMENT

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.

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

Keep your server ports and IP addresses hidden and secure while allowing temporary on-demand access for authorized users. Halo supports secure remote network access using two-factor authentication (using one-time passwords via SMS or email or with YubiKey®) with no additional software or infrastructure.

3

HALO DETECT

FILE INTEGRITY MONITORING

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

Halo continuously monitors key server log files for events that should not happen; indicating misuse, misconfiguration, 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.

HALO SECURITY ORCHESTRATION PLATFORM

The CloudPassage Halo platform 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 integrations.

"Cloud computing is a cornerstone of Adobe's business strategy. Halo allows security teams to quickly attain visibility and control across cloud infrastructure environments."

- DAVE LENOE, DIRECTOR, SECURE SOFTWARE ENGINEERING, ADOBE

ABOUT CLOUDPASSAGE

CloudPassage® Halo® is the world's leading agile security platform that empowers our customers to take full advantage of cloud infrastructure with the confidence that their critical business assets are protected. Halo delivers a comprehensive set of continuous security and compliance functions right where it counts—at the workload. Our platform orchestrates security on-demand, at any scale and works in any cloud or virtual infrastructure (private, public, hybrid or virtual data center). 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.

Product_Overview_08112016