CloudPassage

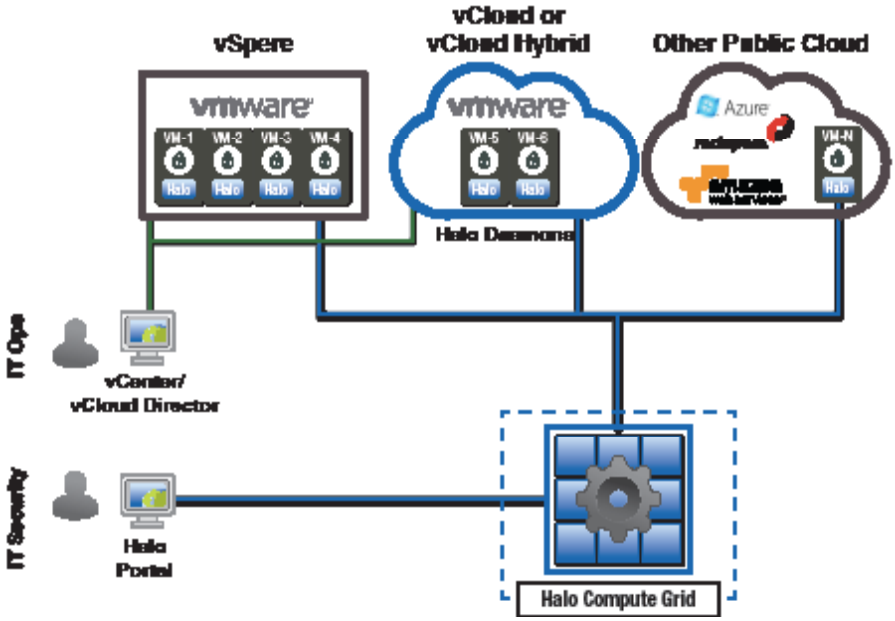
Automated Security and Compliance.

Preserves the Agility of Your VMware Environments.

SECURING YOUR VMWARE INFRASTRUCTURE

Cloud computing and software-defined datacenters (SDDC) are driving business agility, operational efficiency and infrastructure utilization to the next level. Enterprise technology leaders broadly rely on VMware™ and its vCloud suite to deliver on the promise of SDDC.

However, in this dramatically more dynamic environment, infrastructure teams struggle to make security and compliance work without compromising fundamental cloud benefits such as agility and efficiency. Traditional infrastructure security tools depend on fixed topology, static configurations, defined perimeters, and specialized hardware – all nearly impossible to satisfy in true SDDC and cloud environments. The software-defined datacenter, whether built strictly using VMware or combining other virtualization and cloud platforms, is the brave new world of IT but organizations need a security and compliance solution that can keep up with this paradigm shift in computing.



HALO'S UNIQUE DIFFERENTIATORS

Automates security acrossheterogeneous cloud, software-defined, and traditional datacenter environments

- Security purpose-built for dynamicSDDC and cloud infrastructure
- Security that protects acrossmultiple cloud, virtual, and baremetal instances
- Portable security for any cloudplatform or service provider

Enables operations to quicklyprovision resources for users

- Software-as-a-Service solutionthat is up and running in minutes
- Accelerated provisioning with directcloud application stack integration
- Security automation that growsand changes with your cloud

Provides continuous security and compliance controls

- Patented architecture and command and control system
- Automated controls to meet compliance needs (e.g. PCI-DSS, HIPAA, SOC2)
- Group-based security and compliance policy management
- Easy integration to SIEM systems such as Splunk, HP/ArcSight, and SumoLogic
- Easy integration with cloud management tools such as RightScale, Chef and Puppet

CloudPassage

AUTOMATED SECURITY AND COMPLIANCE, CONTINUED.

CLOUDPASSAGE HALO: SECURITY AND COMPLIANCE THAT WORKS IN ANY CLOUD OR SOFTWARE-DEFINED DATA CENTER

CloudPassage Halo was purpose-built to automate security and compliance for any cloud or SDDC infrastructure. Halo is a cloud-powered solution based on a rapidly deployable, highly automated, and easy-to-integrate orchestration platform. This platform enables Halo to deliver security that matches new operationally agile models while providing critical protection, visibility, and control needed for security and compliance assurance. Halo is also highly portable, protecting your VMware environments as well as other SDDC, public cloud, and even traditional datacenter environments. Halo has exceptionally low impact on infrastructure resources, and is non-intrusive to VMware and other hypervisors.

BENEFITS OF HALO

Halo enables the key tenets of the software-defined datacenter:

Optimized Resource Utilization: Uses a lightweight daemon with a near-zero footprint (across memory, CPU and I/O) that allows increased guest density compared to traditional heavy agents or hypervisor-based security products

Visibility: Halo provides security and operations teams with consistent visibility and compliance across all infrastructure environments

Automation: Applies automated security and compliance purpose built for any cloud or software-defined data center, leveraging group-based policy management that can automatically secure thousands of systems

On-demand Provisioning: Automatically deploys as part of the cloud application stack in real time as cloud servers are created

Elasticity: Employs a grid computing architecture to issue commands and policy updates to the in-guest agents, ensuring security and compliance are maintained as servers are cloned, reactivated, and moved

HOW IT WORKS

Halo is an easily deployed Software-as-a-Service solution that takes less than ten minutes to get up and running. Halo's grid computing architecture delivers multiple security capabilities with minimal impact to server performance and resources.

The Halo Daemon is a lightweight, secure software component that runs as a service on each cloud virtual guest. It collects data using cloud-aware protocols and takes actions based on pre-configured or customized security policies.

HALO'S UNIQUE DIFFERENTIATORS, CONTINUED

Saves on costs and resources

- Hourly utility pricing with discounted prepayment options
- Near-zero resource footprint that provides increased VMconsolidation ratios, saving on CAPEX and OPEX
- Automated security controlsthat save management time
- Automated compliance controlsthat help ensure successful audits

CLOUDPASSAGE HALO:

- First and only solutionpurpose-built for high-scale cloud infrastructure
- Architecture patented April 2013
- Thousands of production deployments
- 2,500+ protected cloud servers per month
- 400,000+ scans performed per month
- 1.2 million+ alerts generated per month

CLOUDPASSAGE HALO: KEY SECURITY FEATURES

- Configuration Security Monitoring
- Software Vulnerability Assessment
- File Integrity Monitoring
- Dynamic Firewall Automation
- GhostPorts Two-factor Authentication
- Account Management
- Event Logging and Alerting
- REST API Access

CloudPassage

AUTOMATED SECURITY AND COMPLIANCE, CONTINUED.

The Halo Grid is a cloud-based compute grid that provides analytics for hundreds (if not thousands) of important security factors based on data collected by the Halo Daemons. The Halo Grid does the "heavy lifting" for the Daemons to preserve virtual guest resources and performance.

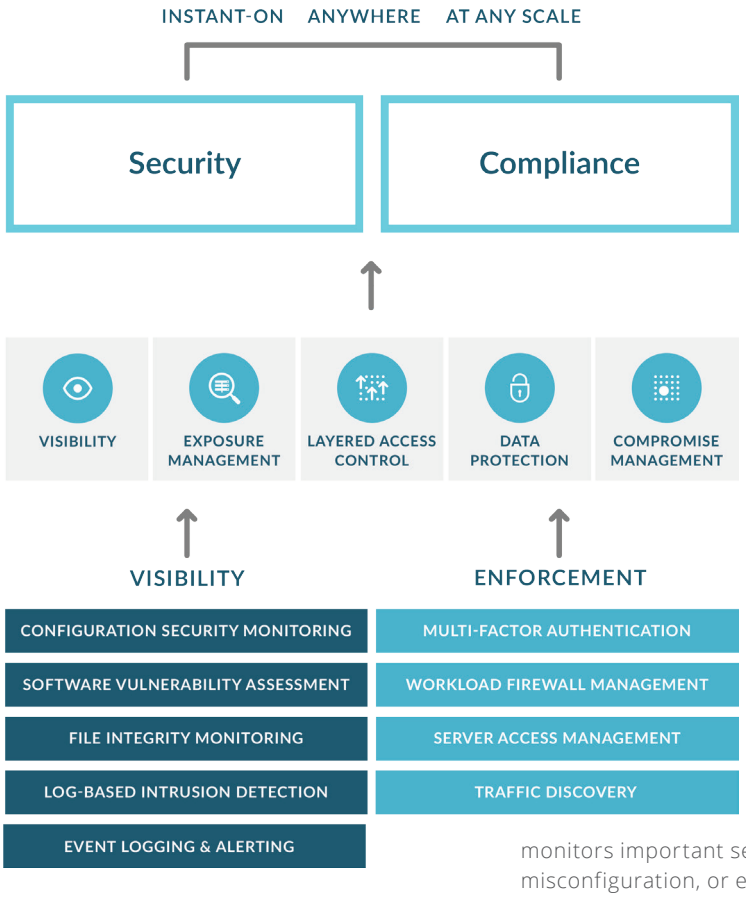
The Halo Portal is the "single pane of glass" used to manage all Halo product capabilities across all servers—cloud, virtual, and traditional hardware.

PROTECT YOUR VMWARE SERVERS TODAY

VMware gives organizations the flexibility to implement software-defined datacenters and cloud models that address their unique business needs. CloudPassage provides a patented, next-generation security solution purpose-built to secure you across these environments. Secure your software-defined datacenter and other cloud deployments as they develop while continuing to protect your current investments—all with one automated approach to server security and compliance.

"Within cloud and SDDC environments, it's easy to forget that you're creating, managing and cloning real systems, each with real vulnerabilities. Halo's extensive automation addresses that problem."

Wendy Nather, 451 research



ABOUT CLOUDPASSAGE

CloudPassage® Halo® is 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. 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. Headquartered in San Francisco, California, CloudPassage is backed by Benchmark Capital, Lightspeed Venture Partners, Meritech Capital Partners, Tenaya Capital, Shasta Ventures, Musea Ventures and other leading investors.

FEATURES

- **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 packaged software—across all of your environments.
- **Server Access Management:** Easily identify invalid or expired accounts. Evaluate who has accounts on which servers, what privileges they operate under and how accounts are being used. Monitor all your servers through a single online management console.
- **File Integrity Monitoring:** Protect the integrity of your servers by constantly monitoring for unauthorized or malicious changes to important system binaries and configuration files. 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.
- **Log-Based Intrusion Detection:** Halo LIDS continuously monitors important server log files for events that should not happen; indicating 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.
- **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 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.
- **Event Logging & Alerting:** Easily manage and detect a broad range of events and system states. Halo enables you to define which events generate logs or alerts, whether they are critical and who will receive them.

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 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 tested integrations.