CloudPassage

CloudPassage Halo Agent in Audit Mode

Protect cloud computing with continuous visibility, oversight and audit controls. Gain immediate and direct views into the security and compliance state of workloads.

VISIBILITY IS VITAL FOR BUSINESS COMPLIANCE

The incredibly dynamic nature of modern software-defined data centers and cloud infrastructure poses real security challenges for organizations that cannot afford data breaches of any kind. Without near real-time visibility into the security and compliance state of virtualized workloads and servers, enterprises are not able to address risk properly. Furthermore, the unsettling fact is that traditional security tools, often tied to the underlying hardware or perimeters, are not ready for the high rates of change, transient nature, and diversity of IaaS, private cloud and softwaredefined environments. CloudPassage Halo overcomes these obstacles. With the Halo agent configured to be in audit mode, continuous visibility is achieved across any environment, including public cloud, private cloud and hybrid environments. With one solution, security, audit and compliance professionals can now gain oversight of the inventory of cloud assets as well as the software deployed on them.

Centralized Security and Oversight

Halo provides one centralized view across diverse environments. With the CloudPassage Halo agent in audit mode, security and compliance teams can assess risk, provide security exposure management, be alerted to integrity issues and detect intrusions—all from a single easy-to-use platform. Security teams can now provide business value with guidance on best practices and alert operations on issues based on vendors, type of infrastructure at play, and business use of the workload. Security teams can also be proactive in determining the best business use cases for new investments in cloud infrastructure and services. Halo enables business to make the best of resources and infrastructure services while protecting the workloads and minimizing risk. Within minutes, Halo can provide detailed reporting for hundreds to thousands of servers. These reports give security teams the information needed to address misconfigurations, vulnerabilities and abnormalities across the infrastructure environment.

HIGHLIGHTS:

- Obtain clear visibility and accountability of workloads across cloud environments.
- View and sample security and compliance information without impacting operations.
- Assess risk and compliance regardless of vendor or hypervisor, unconstrained by where workloads are sourced or located.

HALO AGENT IN AUDIT MODE PROVIDES:

- File Integrity Monitoring
- Configuration Security Monitoring
- Software Vulnerability Assessment
- Log-Based Intrusion Detection

CloudPassage

AUTOMATED SECURITY AND COMPLIANCE, CONTINUED.

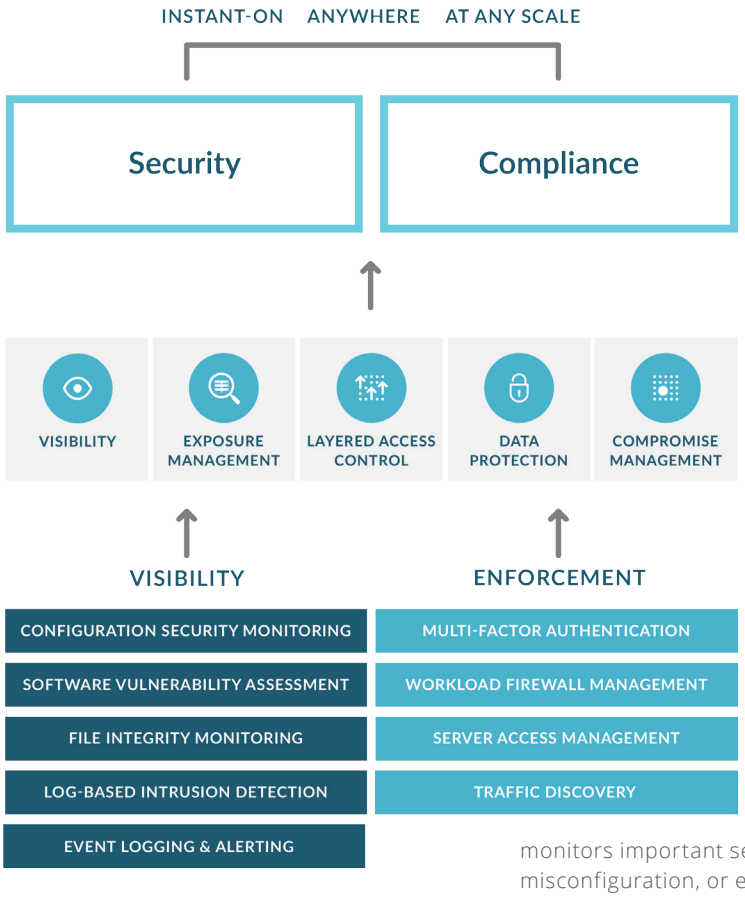
Easy Operational and Lifecycle Management

Halo's unique platform, service and agent require no additional overhead to manage. The lightweight agent easily integrates with cloud and data center orchestration tools like Chef and Puppet, allowing it to be directly incorporated into daily operations. Security and operations teams can rest assured that the Halo agent in audit mode will not cause performance issues, manipulate or change any configurations or settings for user accounts or firewalls. This makes Halo a great tool for internal or external audit and compliance teams to get direct access to run reports, quickly identify systems running software with vulnerabilities, sample system configurations, assess privileged user accounts, and refine security and compliance policies.

Because of the patented design, new instances or clones of existing workloads will automatically be tracked when the Halo agent is present. Security policies will be inherited from the parent or clone workload, with updates applied every 60 seconds from the Halo platform automatically. This means that security or compliance professionals do not need to worry about a new cloud instance spinning up as they will have the ability to track and provide server inventory of cloud workloads, including deployed software.

Value from a Software-Defined Platform

Halo was purpose-built for cloud and software-defined datacenters, and provides the broadest coverage in the most efficient manner. The Halo REST API gives enterprises the ability to create their own programmable security and to highly automate their cloud infrastructure and software-defined data center operations. The security intelligence and data collected by the Halo platform is a powerful way for enterprises to enhance their security, compliance and internal IT processes. For example, collected security and audit information can be exported to third-party products such as SIEMs, log managers and IT GRC tools. Going beyond traditional security log monitoring, Halo agent in audit mode can provide notifications when specific errors or faults are registered in application logs.



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.

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.

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.