TECHNICAL BRIEF

CloudPassage

The Halo cloud security platform was purpose-built to provide your organization with the critical protection, visibility and control needed to assure cloud security—without the fixed perimeters of legacy security.

OVERVIEW

The Halo cloud security platform was purpose-built to provide your organization with the critical protection, visibility and control needed to assure cloud security—without the fixed perimeters of legacy security.

Halo automates security and compliance in an easily integrated and scalable platform. Halo's centralized grid computing architecture is platform- and provider-agnostic, integrates with your existing infrastructure, and can usually be deployed in under an hour. Halo provides consistent security and compliance controls across clouds and data centers alike.

Halo's architecture combines a cloud-based security analytics engine, lightweight agents, and a secure asynchronous messaging protocol for continuous command-and-control and monitoring. This architecture enables the Halo platform to deliver a wide range of software-defined security and compliance capabilities for application workloads.

Halo's quick deployment, broad control consolidation, legacy solution enablement, and deep automation free security personnel from mundane technical tasks—allowing security staff to focus on more strategic needs.

HALO FEATURES

REST API: Halo's REST API provides full automation of your cloud deployments and lets you integrate your security platform with your other systems. Once installed, Halo can automatically monitor security compliance rules across thousands of systems.

Halo Integrations: Halo has proven, functioning integrations with solutions in the log-analytics and GRC space (such as Splunk, Sumo Logic, ArcSight, Archer, enVision) and with SAML-based single-sign-on identity providers (such as OneLogin, Okta, and others).

Compliance Automation: Halo is designed to support the dynamic nature of how workloads initiate, network, and cycle. With the ability to track and log dynamic workflow, state and changes across multiple cloud environments the Halo cloud security platform provides ease of compliance without sacrificing progress.

CloudPassage Certifications: CloudPassage Halo is operated under the ISO-27002 security standards and is audited annually against PCI Level 1 and SOC 2 standards.

Metered Billing: Halo uses metered usage-based billing that maps directly to Halo Agent usage, ensuring that security and compliance cost reflects actual use.

HALO CLOUD SECURITY PLATFORM

- The Halo Agent is deployed on each protected workload (e.g., cloud instances, virtual machines, hardware workloads)
- Each Halo Agent heartbeats to the Halo Security Analytics Engine (each 60 seconds by default) to deliver workload state and behavior data and collect new commands
- The Halo Security Analytics Engine analyzes workload state, behaviors and relationships plus issues additional data collection requests or security commands based on user-configured policies
- The Halo platform includes a number of functional Control and Telemetry Modules such as configuration security monitoring, file integrity monitoring, software vulnerability scanning, firewall management, secure server access, and event logging and alerting
- The Halo Portal provides a single point of central management for deployments
- The Halo API Gateway provides a rich set of REST endpoints for integration of third-party security solutions

FEATURE HIGHLIGHTS

- Scans both Linux and Windows hosts
- Many built-in policy templates
- Compliance-specific policies included
- Remediation suggestions provided
- Policies fully customizable
- Event reports and SIEM integration

CONFIGURATION SECURITY MONITORING

Configuration security monitoring allows you to automatically monitor workload operating system and application configurations, processes, network services, privileges, and more. Evaluate new and reactivated workloads against the latest configuration policies in seconds with almost no CPU utilization.

Built-In Policy Templates

Linux	
Amazon Linux	nginx
Apache	PostgreSQL
Cassandra	Red Hat Enterprise Linux
CentOS	Ubuntu
Debian	Verify Retirement of Encryption Keys
Fedora	Verify Time Server Settings
HAProxy	Verify Use of Strong Crypto
MongoDB	WordPress
MySQL	

Windows
Microsoft IIS
Microsoft SQL Server
Windows Server 2008 R2
Windows Server 2012
WordPress

Configuration Scanning Checks

Linux	
Configuration file setting	Home directory has no device files
Directory ACL	Home directory has no setgid files
Directory group ownership	Home directory has no setuid files
Directory user ownership	Home directory-correct group owner
File ACL	Home directory-correct user owner
File group ownership	Network service accessibility
File presence	Network service processes
File setgid	No recent account login
File setuid	Password is not username
File user ownership	Process group ownership
Group GID	Process presence
Group has password	Process user ownership
Group members	Recent account login
Home dir. files-correct group owner	String presence
Home dir. files-correct user owner	User account UID
Home dir. files-safe PATH stmts.	User group membership
Home dir. files-valid umask cmds.	User has password
Home directory exists	World-writable dirs.-sticky bit set
Home directory file presence	

Windows*
Advanced Audit Policy Setting
File presence
Local Security Policy setting
Local User Rights Assignment
Registry Key Value Setting
Service Started

*Many of the Windows checks are composites; one Windows check can perform the equivalent of multiple Linux checks

FILE INTEGRITY MONITORING

Protect the integrity of your workloads by using file integrity monitoring to continually check for unauthorized or malicious changes to important system binaries and configuration files. File Integrity Monitoring first saves a baseline record of the “clean” state of your workload systems. It then periodically re-scans each workload instance and compares the results to that baseline. Any differences detected are logged and reported to the appropriate administrators.

FEATURE HIGHLIGHTS

- Scans both Linux and Windows hosts
- Many built-in policy templates
- Compliance-specific policies included
- Remediation suggestions provided
- Policies fully customizable
- Event reports and SIEM integration

Built-In Policy Templates

Linux	
Amazon Linux	Monitor Changes to SETUID Files
Apache	Monitor Privilege Escalation
Cassandra	nginx
CentOS	PostgreSQL
Debian	Red Hat Enterprise Linux
Fedora	Ubuntu
HAProxy	WordPress
MongoDB	WordPress

Windows
dMicrosoft IIS
Microsoft SQL Server
Windows Server 2008 R2
Windows Server 2012
WordPress

FEATURE HIGHLIGHTS

- Scans Linux and Windows hosts
- Generates complete inventory of installed software
- Detailed CVE information from NIST
- Improved accuracy from third-party feeds and proprietary research
- Event reports and SIEM integration

SOFTWARE VULNERABILITY ASSESSMENT

Halo software vulnerability assessment scans for vulnerabilities in your packaged software rapidly and automatically, across all of your cloud environments–precisely where traditional software scanning products are unable to operate effectively. With Halo, thousands of workload configuration points can be assessed in minutes, helping you to maintain continuous exposure awareness in the cloud.

The primary source of vulnerability data is the NIST NVD (National Vulnerability Database). This is supplemented with data from OS vendor security advisories and bulletins and internal research and testing from the CloudPassage security team.
NIST vulnerability data is updated on a daily cycle and OS vendor and internal research data is updated on a monthly cycle.

FEATURE HIGHLIGHTS

- Protects Linux and Windows hosts
- Tight access control through policies customized for each workload group
- Controls inbound and outbound traffic
- Works with Secure Server Access to ensure secure access for workload admins
- Automatically updates as other hosts are brought up or down
- Generates alerts on unauthorized firewall modification

FIREWALL POLICY AUTOMATION

Use the firewall automation module of Halo to deploy and manage dynamic firewall policies across public, private, and hybrid cloud environments. Build firewall policies from a simple web-based interface, and assign them to groups of workloads. Policies update automatically within seconds of workload additions, deletions and IP address changes.

FEATURE HIGHLIGHTS

- Strong security, multi-factors authentication for accessing any of your hosts (Windows or Linux)
- Convenience of two methods of multi-factor authentication
- Server ports are invisible and closed until opened after users authenticate
- Access is time-limited, restricted to IP address of the authenticated user, for specifically defined ports
- Full auditing and alerting capabilities of Secure Server Access activation and deactivation

SECURE SERVER ACCESS

Halo Secure Server Access enables secure remote network access using two-factor authentication via SMS to a mobile phone, or using a YubiKey® with no additional software or infrastructure. Keep your workload ports hidden and secure from the rest of the world while allowing temporary access on demand for authorized users only.

FEATURE HIGHLIGHTS

- Central management of all local accounts on all Linux hosts across our clouds
- Tracks login activity
- Displays UID and GID info, root permissions, sudo privileges, SSH information
- Easy to compare all accounts on one host or one account across all hosts
- Supports creating, editing, deleting accounts

SERVER ACCOUNT MANAGEMENT

With workload account management, you can evaluate who has accounts on which workloads, what privileges they operate under, and how accounts are being used. Halo provides a single online management console where you can monitor your workloads in public, private and hybrid cloud environments. The convenient user interface makes it easy for you to identify accounts that should have been removed.

FEATURE HIGHLIGHTS

- Security events from scans, workload events, and user-related audit events logged
- Logging can be turned on or off on a per-event basis
- Events can trigger alerts to individuals based on workload group and event criticality
- Reports available filtered by time range, event type, and other criteria
- Automatically exported events can be integrated into SIEM or log-analysis tools

EVENT LOGGING AND ALERTING

The Halo security logging and alerts capabilities detect a broad range of events and system states, alerting you when they occur. The platform allows users to define which events generate logs or alerts, whether they are critical, and who will receive them.

Auditable and Alertable Events

API Key Management	
API key created	API key modified
API key deleted	API secret key viewed

Configuration Security Scanning Management	
Configuration policy assigned	Configuration policy imported
Configuration policy created	Configuration policy modified
Configuration policy deleted	Configuration policy unassigned
Configuration policy exported	

Server Events	
Configuration rule matched	Server firewall modified
Daemon compromised	Server IP address changed
File integrity object signature changed	Server missing
File integrity object added	Server restarted
File integrity object missing	Server retired
Local account created (Linux only)	Server shutdown
Local account deleted (Linux only)	Server un-retired
Log-based intrusion detection rule matched	Vulnerable software package found
Multiple root accounts detected (Linux only)	

File Integrity Scanning Management	
Automatic file integrity scan schedule modified	File integrity policy assigned
Automatic file integrity scanning disabled	File integrity policy created
Automatic file integrity scanning enabled	File integrity policy deleted
File integrity baseline	File integrity policy exported
File integrity baseline deleted	File integrity policy imported
File integrity baseline expired	File integrity policy modified
File integrity baseline failed	File integrity policy unassigned
File integrity baseline invalid	File integrity re-baseline
File integrity exception created	File integrity scan failed
File integrity exception deleted	File integrity scan requested
File integrity exception expired	

Firewall Management	
Halo firewall policy assigned	Network service added
Halo firewall policy created	Network service deleted
Halo firewall policy deleted	Network service modified
Halo firewall policy modified	Server firewall restore requested
Halo firewall policy unassigned	

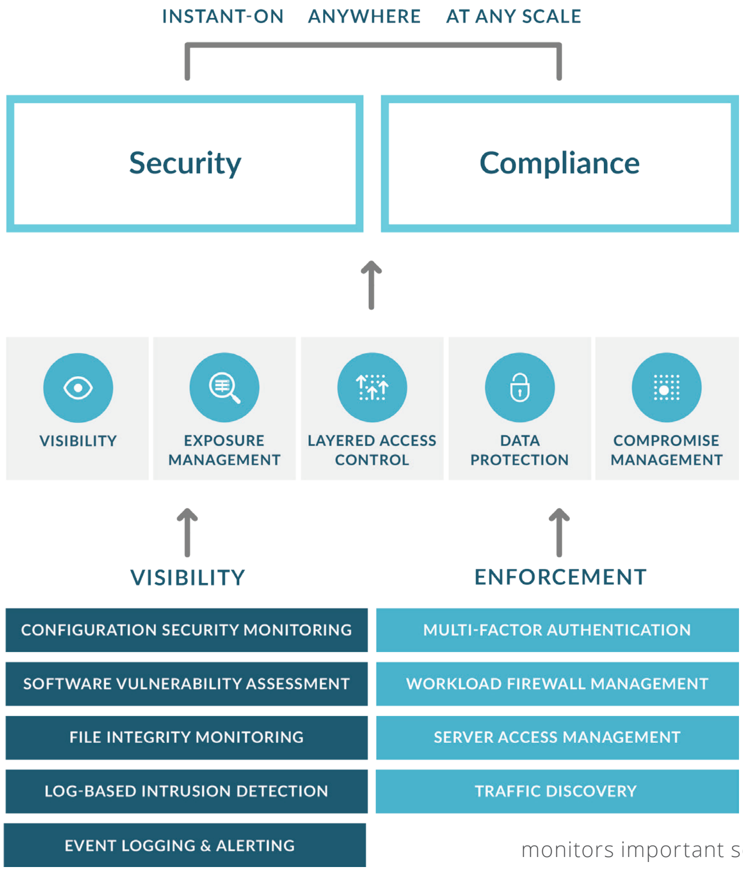
GhostPorts	
Ghostports login failure	Ghostports provisioning
Ghostports login success	Ghostports session close

Halo Daemon Management	
Daemon settings modified	Server deleted
Daemon version changed	Server moved to another group
New server	

Halo Users and Authentication	
Authorized IPS modified	Halo user account locked
Halo authentication settings modified	Halo user account unlocked
Halo login failure	Halo user activation failed
Halo login success	Halo user added
Halo logout	Halo user deactivated
Halo password authentication settings modified	Halo user deleted
Halo password changed	Halo user modified
Halo password recovery request failed	Halo user re-added
Halo password recovery requested	Halo user reactivated
Halo password recovery success	Master account linked
Halo session timeout	SMS phone number verified
Halo session timeout modified	

Log-based Intrusion Detection Systems (LIDS) Management	
disabled	deleted
enabled	exported
assigned	modified
created	unassigned

Uncategorized
Portal audit policy modified



INSTANT-ON ANYWHERE AT ANY SCALE

Security | Compliance

VISIBILITY | EXPOSURE MANAGEMENT | LAYERED ACCESS CONTROL | DATA PROTECTION | COMPROMISE MANAGEMENT

VISIBILITY
- CONFIGURATION SECURITY MONITORING
- SOFTWARE VULNERABILITY ASSESSMENT
- FILE INTEGRITY MONITORING
- LOG-BASED INTRUSION DETECTION
- EVENT LOGGING & ALERTING

ENFORCEMENT
- MULTI-FACTOR AUTHENTICATION
- WORKLOAD FIREWALL MANAGEMENT
- SERVER ACCESS MANAGEMENT
- TRAFFIC DISCOVERY

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.