CloudPassage

TECHNICAL OVERVIEW

# HALO PLATFORM TECHNICAL OVERVIEW: SERVER SECURE

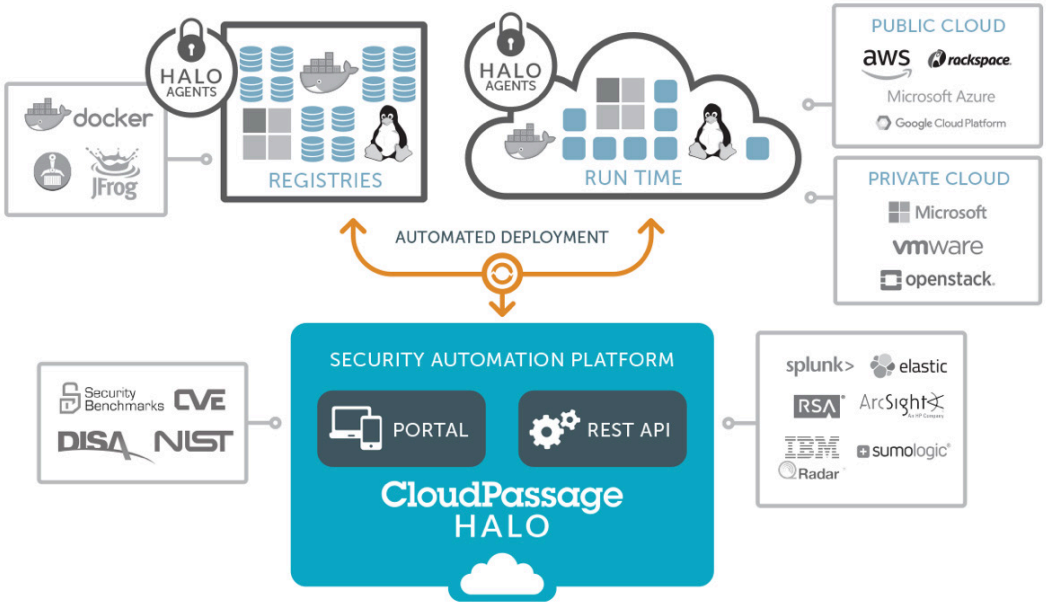
# OVERVIEW

CloudPassage Halo is purpose-built to provide your organization with the visibility, security, and compliance you need to deploy and run applications in modern hosting environments – without slowing you down.

Halo automates security and compliance within a dynamic, scalable platform that can be easily integrated with all of your existing tools. Halo is platform- and provider- agnostic, integrates with your existing infrastructure, and can be deployed in under an hour. Halo provides consistent security and compliance controls in any hosting environment – public, private, and hybrid.

Halo's architecture combines a cloud-based security automation platform, micro-agents, and a secure asynchronous messaging protocol to achieve continuous monitoring with minimal impact to monitored applications. Halo's analytics engine does the heavy lifting so that agents do not adversely impact the host.

Halo's quick deployment, broad spectrum of security controls, and deep automation free security personnel from mundane technical tasks– like cobbling together tools and provisioning policies for new resources– allowing your security team to focus on responding to exposures and improving overall posture.



# HALO SECURITY PLATFORM – WHAT IT IS, HOW IT WORKS

- Halo is delivered as a service. There are no appliances or management servers that you need to install on-premises. As a result, Halo can be up and running in minutes and scales on-demand.
- The Halo micro-agent is deployed to each workload including virtual machines, cloud instances, and hosts that service Docker containers. Because the micro-agent scans from within the host (and not over the network), thousands of workload configuration points can be assessed in minutes.
- Each Halo micro-agent communicates with the Halo security automation platform (each 60 seconds by default) to deliver workload state and behavior data and receive new scan commands. Since the agent initiates all communications, Halo works in any combination of data center environments and meets the security demands of even the most stringent enterprises.
- The Halo Portal provides a single management interface which allows analysts to assess compliance with security controls from a "single pane of glass" across all operating environments and compute resources.
- The Halo security automation platform analyzes the workload state information received from each agent to generate security intelligence based on user-configured policies. Security anomalies are logged, alerted, and viewable to analysts in the Halo Portal so that problems can be investigated and remediated. The workload-state information is used to deliver a broad spectrum of security controls including configuration security monitoring, file integrity monitoring, software vulnerability assessment, firewall management, log-based IDS, and server account monitoring. These controls are continuously monitored so analysts don't have to worry about manually scheduling and orchestrating security scans.
- The Halo REST API facilitates quick, easy integration with your existing systems such as Security Information and Event Monitoring (SIEM) tools like Sumo Logic, Splunk or ArcSight as well as Governance, Risk and Compliance (GRC) platforms like Archer. The use of open APIs also enables a high-speed DevOps automated workflow, weaving security into the fabric of the DevOps cycle from development through testing and deployment with tools such as Chef, Puppet, or Ansible.

# PLATFORM FEATURES

## Secure design and certifications

The Halo platform has been designed to meet the security requirements of the world's most demanding enterprises. All communications are initiated by the Halo micro-agent to the Halo security automation platform and are secured by https; the agent has no listening ports and there is no way for any entity to initiate communication to the agents or to intercept traffic– all databases used to store customer data are encrypted. CloudPassage Halo is operated under the ISO-27002 security standards and is audited annually against PCI Level 1 and SOC 2 standards. In addition, CloudPassage is listed in the CSA Security, Trust & Assurance Registry and has passed all of the requirements for being listed as FedRAMP Ready.

## Policy authoring

Halo includes policy templates based on industry best practices and benchmarks for file integrity monitoring, log-based intrusion detection, and configuration security monitoring. Templates based on DISA STIGs and Center for Internet Security (CIS) benchmarks are included for all supported operating systems. Administrators can copy and customize these templates or build entirely new policies with Halo's full-featured policy-authoring tools.

## Policy provisioning

Halo security policies are associated with logical application groupings. A tag is applied to each agent at deploy time, and when the agent "phones home" to the Halo security automation platform, the correct policies are applied to the agent.

## Analytics

Halo agents return telemetry and state information to the Halo security automation platform which analyzes the massive amount of data collected from thousands of agents, turning it into actionable intelligence which can be used by security analysts for remediation and risk professionals for compliance initiatives.

## Event Logging & Alerting

Halo produces security events when problems are found on monitored workloads. The platform allows administrators to define which security rules generate events, and define their criticality. Alerts can be generated for any event and delivered by email to the right users based on which group owns the affected workload.

Administrators can create exceptions so that certain events are suppressed while application owners remediate issues.

Events are also produced by users' and API clients' interactions within the Halo Portal. This ensures that all user activity is logged and a proper audit trail is maintained. These audit events are also configurable based on criticality.

A dynamic search interface allows users to review and search for events over a 90-day period.

Halo supports sending events to various SIEM and log collection tools via a connector which extracts events from the Halo REST API and forwards to the SIEM of your choice.

Halo event logging & alerting helps enterprises prove compliance with industry standards such as: PCI 11.5, 12.5.2, 12.9.5; HIPAA 164.312(b); and SOC2 3.3, 5.1, 6.1, 6.2, 7.2, 7.3.

## Issue tracking

The first time a security problem on a monitored workload is identified by the security automation platform, Halo creates an "Issue" which tracks the history of that problem on that workload. Analysts can use the issue to understand what the problem is, when it was first and last detected, how to remediate it, and how many other servers are affected by the same problem. When the problem is resolved by the person responsible for the affected server, on the next scheduled scan Halo will detect that the problem has been fixed and automatically mark the issue in Halo as resolved. Security analysts can generate reports of new and resolved issues on a regular basis.

## Role-based Access Control

Halo allows administrators to set the appropriate permissions for Halo Portal users and API clients based on predefined roles. Roles include administrator, standard, and auditor (read-only). In addition, administrators can set users' visibility based on an organizational hierarchy so that logical separation and data privacy can be achieved between various business units using the same Halo customer account. This allows large enterprises to leverage Halo with a single account across their entire organization, providing security personnel with high level views of the entire organization but limiting application owners to see only the data from assets for which they are responsible.

## Authentication

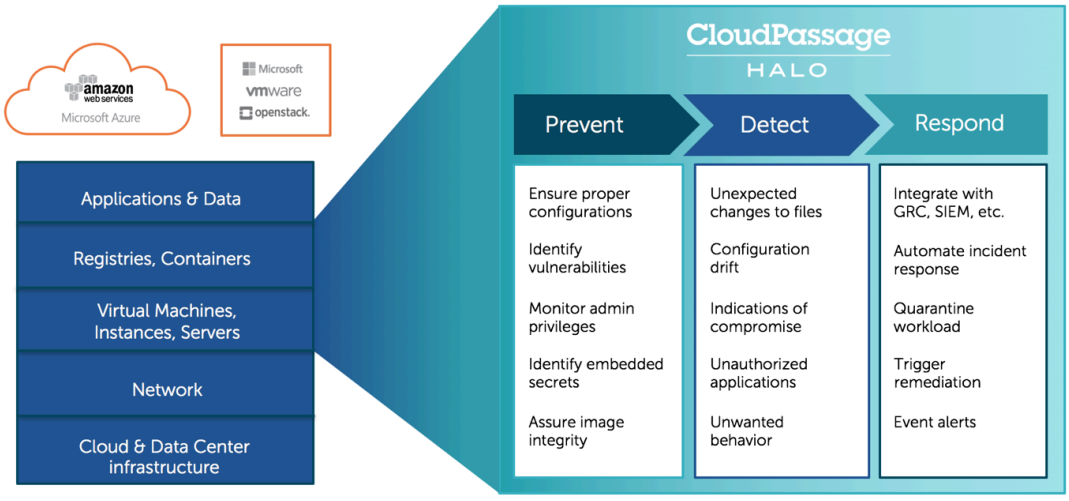
Halo allows administrators to customize the authentication methods performed when users access the Halo portal. Administrators can:

- Customize password complexity, password expiration, failed password lockout, and idle session timeout rules according to internal security standards.
- Set up multi-factor authentication using SMS codes, YubiKeys, or TOTP apps such as Duo and Google Authenticator.
- Configure Halo to accept authentication via any SAML 2.0 compliant Single Sign On (SSO) application.
- Enable browser fingerprinting so that users logging in with what appears to be a new browser must supply a code delivered by email.
- Limit access to the corporate network by defining a set of IP addresses from which users are allowed to log in.

# SERVER SECURE

## Summary/overview

Server Secure is a set of security controls delivered by the Halo platform which apply to virtual machines, host operating systems, and several very common application frameworks. The individual functions are described below. All functions are supported for both Linux and Windows.



# Configuration Security Monitoring (CSM)

Configuration security monitoring automatically and continuously monitors workload operating system and application configurations for adherence to security guidelines, best practices, and compliance regulations. Workloads are evaluated immediately upon startup and continuously at predefined intervals thereafter, with alerting and detailed reports on deviations from security policy. You can evaluate workloads against CIS benchmarks, DISA benchmarks, internal standards, image baselines, and industry best practices in seconds with almost no CPU utilization. In addition, you can use Server Secure to detect changes to security controls, running processes, user accounts, and installed software.

## Use cases

**OS Configuration Security & Compliance:** Evaluate workload operating systems against security best practices in order to reduce the software attack surface:

- CIS Benchmarks: AMZN Linux, Debian, Ubuntu, CentOS, RedHat Enterprise Linux, Oracle Linux, Microsoft Windows Server 2008 R2 – 2016, Docker Engine
- DISA STIGs: RedHat Enterprise Linux, Oracle Linux, Windows Server 2012

**Application Configuration Security & Compliance:** Evaluate applications against best practices in order to reduce the software attack surface:

- 1. Apache, HAProxy, Microsoft IIS, MongoDB, MySQL, Nginx, Postgres, WordPress

**Detect Configuration Drift:** Well-meaning users may put servers at risk by making configuration changes that undermine the security posture of the system. Server Secure can detect such changes by comparing servers to the benchmarks above.

**Detect Tampering:** In many cases, attackers will modify configuration parameters on the system. Because Server Secure monitors continuously for adherence to the assigned policies, such changes can be quickly detected and analysts can be alerted so that investigative steps can be taken.

**Software Whitelisting:** Server Secure lets you specify which processes and software packages are allowed to run on the workload, which are required to be running on the workload, and which are prohibited from running on the workload. For each process, the policy can specify which runtime parameters are allowed and the parameters of processes which are allowed or not allowed to run (e.g. bash running as root is not allowed). The policy can also specify the ports which are allowed for each process. And policies can be defined which specify which packages should be installed and which should not be installed.

## Feature highlights

- Built-in policy templates based on CIS benchmarks, DISA STIG benchmarks, and industry best practices
- For each scanned object, Server Secure detects whether it passed or failed, relative to the assigned policy.
- Remediation suggestions provided so analysts will know how to fix the problem.
- Continuous monitoring to detect changes to settings on an ongoing basis with no manual intervention
- Full-featured policy customization and authoring

**Confirm applications are running as the correct user:** Running applications as "root" and other over-privileged accounts frequently leads to system compromise as an attacker compromising the associated process can run commands as the application user account. Server Secure lets administrators specify that certain processes should always run as a specific user and to alert if the policy is violated.

**Evaluate operating systems and applications against internal security standards:** Many organizations have detailed security standards for server images. Server Secure's powerful configuration security authoring tool allows you to develop custom policies that you can apply to the images you create, and workloads you deploy. Server Secure's configuration policies are based on rules consisting of groups of checks against specific objects on the system. A few examples of how you can use Server Secure to example system objects are as follows:

- **Linux:** Because security parameters on Linux are largely file-based, many of the Server Secure checks for Linux focus on examining various aspects of user-specified file targets.
  - Check configuration files for specific parameters
  - Check files and directories for proper permissions
  - Check files for existence of specific string within file
  - Check for presence/absence of specific files, running processes, software, user accounts, listening ports
  - Check users' home directories for proper contents and permissions
  - Check users for proper group membership
  - Ensure geolocation of connected servers is expected
- **Windows:** Because security parameters on Windows are largely based on local security policies and registry settings, many of the CSM checks for Windows focus on examining those settings.
  - Confirm audit policies are properly set
  - Confirm local user rights assignments are properly set
  - Check values of specific registry keys
  - Check for presence of running service and process
  - Check for presence/absence of specific files, running processes, and services
  - Check for proper application of Windows Server local security policies including:
    - Account lockout duration
    - Account lockout threshold
    - Accounts: Administrator account status
    - Accounts: Guest account status

- Accounts: Rename administrator account
- Accounts: Rename guest account
- Audit account logon event
- Audit account management
- Audit directory service access
- Audit logon events
- Audit object access
- Audit policy change
- Audit privilege use
- Audit process tracking
- Audit system events
- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Network access: Allow anonymous SID/Name translation
- Network security: Force logoff when hours expire
- Password must meet complexity requirements
- Reset account lockout counter after
- Store passwords using reversible encryption

» **Regulatory compliance:** Server Secure's configuration security monitoring function helps you prove compliance with the following standards:

- PCI 2.1, 2.2, 3.6.5, 4.1, 6.1, 6.2, 6.3.1, 7.2.3, 8.2, 10.2, 10.4, 12.5.2, 12.10.5
- HIPAA 164.312(a)(1), 164.312(b), 164.312(e)(1)
- SOC2 3.2, 3.3, 4.1, 5.8, 6.1, 6.2, 7.2, 7.3.

## Software Vulnerability Assessment (SVA)

Server Secure software vulnerability assessment automatically and continuously scans for known vulnerabilities in software packages installed on your workloads. Workloads are evaluated immediately upon startup and continuously at predefined intervals thereafter, ensuring that any newly-discovered vulnerabilities since the previous scan are discovered without the need to manually schedule scans. Server Secure's reporting can base prioritization on CVSS score so that analysts will be quickly alerted to the most serious vulnerabilities.

## Feature highlights

- Support for both Linux and Windows
- Scans in seconds with no credentials or network traversal needed
- Generates inventory of installed software
- Identifies all CVEs associated to installed software
- Provides detailed CVE information from NIST
- SIEM integration

## Use-cases

**Software Inventory:** CIS Critical Control 2 indicates that you should proactively inventory, track, and correct all software on the network so that only authorized software is installed. This requires that at any time you can produce a report of all software installed on your workloads so that you can identify and remediate software that should not be present. Server Secure allows you to produce software inventories across your entire server environment on-demand. In response to new vulnerabilities found in software packages, analysts can query Server Secure to find all servers having a specific software and version - so they know their exposure even before formal CVEs are published.

**Vulnerability Assessment:** Most commonly used software packages have had vulnerabilities identified which could be used to gain control over the server or network. Leaving vulnerable software installed without remediation can result in system compromise. The trouble for administrators is keep track of and identifying all the vulnerable software in the network. Server Secure compares installed software packages to CVE data maintained by NIST in order to determine whether there are known vulnerabilities present, and alerts analysts to its presence so that they can be remediated effectively.

**Anomaly Detection:** One way to spot compromised or vulnerable systems is to find functionally equivalent servers that are not configured like their peers. For example, a compromised server may have software packages installed to facilitate moving data out of the network, which other servers having the same role do not have such software installed. For such systems which are not already identified by software whitelisting, analysts have the ability filter and soft software inventories by the number of servers having each installed software; when using this facility, anomalous systems quickly jump out.

**Meet regulations such as PCI, HIPAA, SOC2:** Server Secure's software vulnerability assessment function helps you meet a broad range of regulations and industry requirements such as:

» 1. PCI 2.4, 6.1, and 6.2.

» 2.HIPAA 164.312(b)

» 3.SOC2 7.2

# Server Account Monitoring (SAM)

Server Secure provides a complete inventory of local user accounts and groups on each workload. This capability allows analysts to provide inventories for compliance purposes, identify administrative accounts, identify accounts which are locked, be alerted when accounts are created, and other important use cases.

## Use-cases

**User Account Inventory:** The misuse of administrative privileges is a primary method for attackers to gain control over an application. As such, administrative privileges should be carefully guarded and only used when needed to achieve a task. Most servers need only a small set of privileged accounts in order to function and run applications correctly. Halo provides a complete inventory of local accounts configured on the system, with the ability to filter so that administrative accounts can be quickly identified. New user accounts are an alertable event so that analysts can quickly detect creation of new users on production systems. In many cases, attackers will duplicate UIDs and GIDs to subvert the system with secret "root" accounts. Typically such misconfigurations are indicators of compromise and each Halo scan will alert analysts to their presence. Typical questions analysts may need to ask for security and audit purposes:

- Provide and audit a list of all local accounts across the environment
- Provide a list of all administrative accounts
- Provide a list of all administrative accounts which have not logged in for n days
- Provide a list of all accounts with expired passwords
- Provide a list of all accounts with locked passwords

**Anomaly Detection:** One way to spot compromised or vulnerable systems is to find functionally equivalent servers that are not configured like their peers. For example, a compromised server may have user accounts configured to facilitate moving data out of the network, which other servers having the same role do not have configured. For such systems which are not already identified by user account whitelisting, analysts have the ability to filter user account inventories by servers that don't have identical software running when using this facility, anomalous systems quickly jump out.

**Meet regulations such as PCI, HIPAA, SOC2:** Server Secure's server account monitoring capability helps you meet several different kinds of regulations and industry requirements such as:

- 1. PCI 2.1, 6.3.1, 6.4, 8.1, 8.2, 8.5, 12.5.4
- 2.HIPAA 164.312(a)(1)
- 3.SOC2 5.6.

## Feature highlights

- Supports both Windows and Linux
- Easily produce inventories of specific categories of users such as those with sudo/ root, Administrator roles.
- Find outliers across the environment such as local accounts that exist on some servers but not others
- Alert when new local accounts are added
- 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

## Feature highlights

- Support for both Linux and Windows
- Detect changes to file contents, registry key contents, and permissions
- Leverage predefined policy templates based on industry best practices
- Compare any host to pre-existing baseline from source image
- Continuous monitoring for changes

# File Integrity Monitoring (FIM)

File integrity monitoring detects unintended or malicious changes to files, directories, and registry keys on monitored hosts. With Server Secure, you can determine whether deployed workloads start with integrity by automatically comparing new workloads to a baseline of the source image. Then, continuously scan the deployed workload to detect changes on an ongoing basis. Policy templates for supported operating systems make it easy to get started monitoring the right set of files without causing undue burden on the monitored systems.

## Use-cases

**Confirm integrity of new workloads as they are deployed:** Ever deployed a server to production and found out too late it was based on the wrong image? File integrity monitoring can detect such mistakes, intentional or not, by comparing deployed workloads to a known good baseline taken during the image creation process. When the workload is deployed, Halo can identify which baseline should apply and immediately scan it for integrity.

**Detect Tampering with running workload:** Attackers frequently replace system binaries and other important files with hacked versions that, when executed, elevate the attacker's privilege on the system. Halo's file integrity monitoring takes cryptographic checksums of files and registry keys to ensure that the files match a "known good" version of the file, thus detecting when files are modified and could represent a threat. Halo includes these predefined policy templates, based on industry best practices, to get you up and running quickly:

» RedHat, CentOS, Amazon Linux, Oracle Linux, Ubuntu, Windows 2008 R2 – 2016, RedHat, Ubuntu, Microsoft IIS, MongoDB, SQL Server, WordPress

**Meet regulations such as PCI, HIPAA and SOC2.** Server Secure's file integrity monitoring capability helps you meet several different kinds of regulations and industry requirements such as:

» 1. PCI 2.2, 3.6.5, 6.3.1, 6.4.4, 11.5.1, 12.5.2, 12.10.5

» 2.HIPAA 164.312(b)

» 3.SOC2 3.2, 3.3, 4.1, 5.8, 6.1, 6.2, 7.2, 7.3.

# Log-based Intrusion Detection (LIDS)

It is critically important to monitor log files for unwanted activity; but in modern computing environments, it is common for systems to be launched and decommissioned rapidly without establishing any log collection mechanism. Even if log collection is in place for such ephemeral systems, in many cases the destination is a SIEM tool or log management

system which is not configured to alert security personnel to unwanted activity. 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.

## Use-cases (these are just a few examples that should be of concern to security personnel on production systems)

- Detect attempted logins to "immutable" systems
- Detect attempted login as specific user such as "root" or "Administrator"
- Detect attempted changes to firewall policies
- Detect privilege changes
- Detect addition/deletion/modification of user accounts
- Detect changes to audit policies
- Detect modification of system time
- Detect installation / deinstallation of software
- Meet regulations such as PCI and SOC2. For example Halo LIDS meets or partially meets PCI 2.2.2, 2.3, 10.6, 11.4, 12.5, 12.10 and SOC2 3.2, 3.3, 4.1, 5.8, 6.1, 6.2, 7.2, 7.3.

## Feature highlights

- Support for both Linux and Windows
- Support for text-based log files and Windows event logs
- Captures original log entry for forensic analysis
- Built-in policy templates based on industry best practices
- Continuous monitoring to rapidly detect unwanted behaviors
- Full-feature policy customization and authoring
- SIEM integration

# ABOUT CLOUDPASSAGE

Founded in 2010, CloudPassage® was the first company to obtain a U.S. patent for universal cloud infrastructure security and has been a leading innovator in cloud security automation and compliance monitoring for high-performance application development and deployment environments. CloudPassage Halo® is an award-winning workload security automation platform that provides universal visibility and continuous protection for servers in any combination of data centers, private/public clouds and containers. The Halo platform is delivered as a service, so it deploys in minutes and scales effortlessly. Fully integrated with popular infrastructure automation and orchestration tools such as Puppet and Chef, as well as leading CI/CD tools such as Jenkins, Halo secures the enterprise where it's most vulnerable—application development and workload deployment. Today, CloudPassage Halo secures the critical infrastructure of many of the leading global finance, insurance, media, ecommerce, high-tech service providers, transportation and hospitality companies.

CloudPassage

**www.cloudpassage.com** | 800.215.7404