CloudPassage

PRODUCT BRIEF

HALO CLOUD SECURE

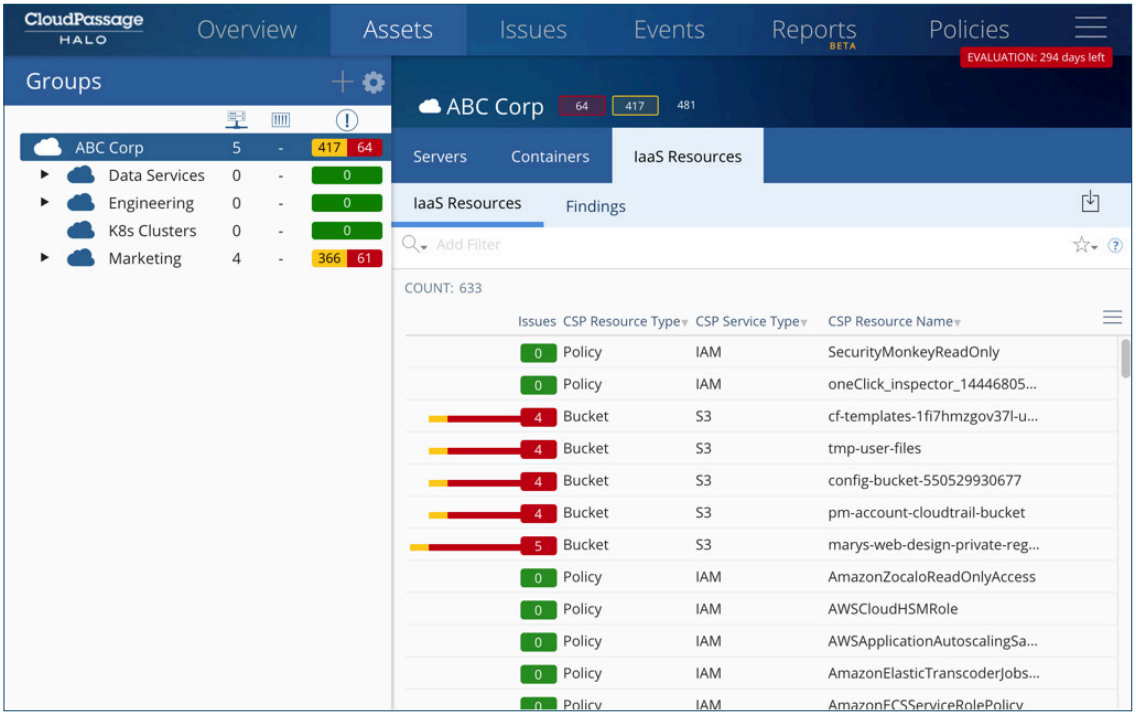
Public cloud use is on the rise. Cloud services are indisputably flexible, allowing for automated deployment of workloads, increased efficiency, and improved networking and vast scalability. However, security teams struggle to maintain security visibility of these dynamic computing environments due to decentralization of IT, the expanding cloud attack surface, and an ever-growing list of cloud service configuration options.

These challenges aren't going away. If you're a security practitioner today, you're bound to have a requirement for tracking fast-moving IaaS assets, their exposures, and related events that pertain to security and compliance. You need comprehensive visibility and security of your entire public cloud infrastructure.

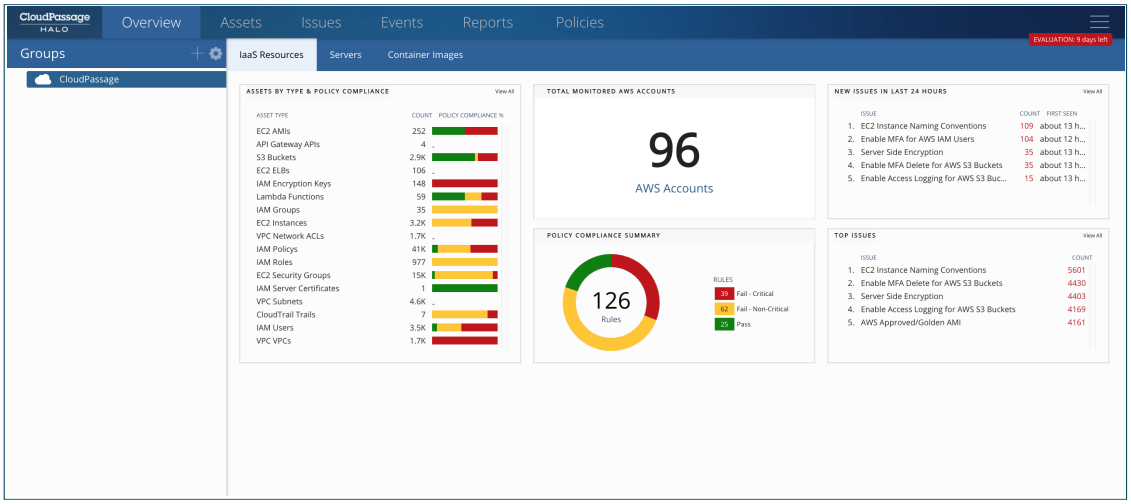
Solution: Halo Cloud Secure

Halo Cloud Secure is an automated public cloud infrastructure security solution that delivers comprehensive visibility, protection, and continuous compliance monitoring for compute, storage, database, networking, and identity services to reduce cyber risk. Unlike point solutions that provide limited coverage, Halo Cloud Secure finds critical risks other tools miss with the broadest and deepest coverage for AWS:

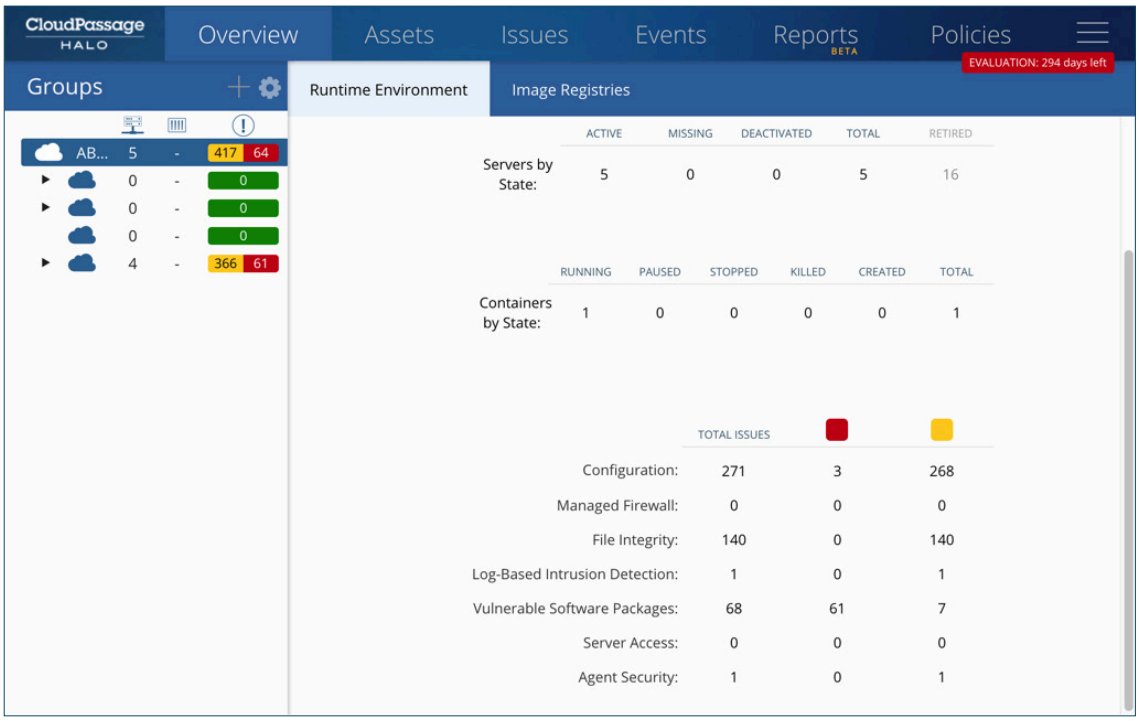
- Obtain single-point inventory and reporting of the security and compliance posture of public cloud infrastructure assets across every account in your organization.
- Quickly identify IaaS misconfigurations that expose your organization to cyber threats.
- Establish and maintain compliance with CIS Benchmarks and other best practices and regulations.
- Continuously monitor public cloud infrastructure assets for critical issues and compliance violations.



Quickly discover and inventory services and resources in use across any number of IaaS accounts in use in your organization for improved security visibility.



Reduce the attackable surface area of your IaaS deployments by identifying your most critical issues so you can remediate them.



CloudPassage offers broad security visibility coverage for support for virtual machines, containers, and serverless workloads in addition to IaaS services.

Benefits

Find critical risks other tools miss

Other tools only provide partial coverage for IaaS environments which can result in security blind spots and hidden risks. Halo Cloud Secure provides the broadest and deepest coverage for AWS all within a single, easy to use tool. Go beyond basic infrastructure security coverage by obtaining "inside-out" visibility of your server and container workloads as well as "outside-in" visibility of the infrastructure your workloads rely on. Quickly identify at-risk workloads that do not have essential security monitoring enabled.

Single pane of glass

Unlike solutions that provide a fragmented view of public cloud infrastructure services, Halo Cloud Secure provides a comprehensive, integrated view of IaaS services and resources from a single interface. Comprehensive visibility and security assessment of public cloud infrastructure assets in a single tool arms you with the contextual information needed to understand relationships between assets and better prioritize remediation steps to reduce risk.

Adapts to your environment

Focus on what matters and avoid wasting valuable human resources responding to low or non-existent risks. Halo Cloud Secure offers powerful policy customization so you can adapt the solution to your unique environment. Since not all IaaS accounts serve the same function, accounts may have differing security requirements. Tailor security policies to the unique requirements of each cloud account so you always receive alerts that are relevant and actionable.

Decrease exposure time

Enable fast and effective remediation by providing actionable information to the people who need it in an automated fashion. Automate remediation workflows by sending vulnerability and remediation information via Amazon SNS and other notification mechanisms.

Automated & integrated

CloudPassage enables DevSecOps with automated security workflows to maximize efficiency and effectiveness. Workflows in Halo Cloud Secure are available as REST-enabled API functions so your team can automate the CI/CD pipeline to improve operational agility.

Maintain continuous compliance

Achieve and maintain compliance by addressing policy requirements for CIS AWS Foundations Benchmark, HIPAA, ISO 27001, NIST 800-53, NIST 800-171, PCI DSS and SOC 2.

Features

- **Resource discovery & inventory:** Gain full-scope visibility of assets requiring protection at any given time, including contextual information such as owner and application name. Understand relationships between assets to prioritize issues.
- **CIS AWS Foundations Benchmark best practices:** Evaluate the hygiene of your AWS environment against the Center for Internet Security (CIS) AWS Foundations benchmark.
- **Advanced best practices:** Go beyond industry hygiene standards by leveraging comprehensive best practices developed by CloudPassage's security research team.
- **Rule customization:** Customize policy rules to suit your specific needs and unique environment. Customize rules by changing parameters and criticality, or by activating and deactivating rules for different environments.
- **Supports multiple accounts:** Assess the security and compliance state of multiple cloud service provider accounts using a single tool.
- **Customizable scan intervals:** Set scan intervals for your cloud service provider accounts on a per-service basis.
- **Ad-hoc account scanning:** Scan your cloud service provider account at any time to immediately get current information.
- **Server workload security:** Deploy agent-based security monitoring including software vulnerability assessment, configuration security monitoring, server account monitoring, and log-based intrusion detection.
- **Container workload security:** Deploy agent and agentless monitoring to secure your entire container environment including hosts, containers, and images in registries.
- **Find unmonitored instances:** Search for virtual machine instances that do not have essential security monitoring enabled.
- **Dashboard and reporting:** At-a-glance summary of your security and compliance state of your public cloud infrastructure. See an overview of assets by type and policy compliance status, and quickly find all of your newest and most critical issues—all in one place. View a list of all IaaS Resources and best practice findings and export information to CSV format for further analysis.
- **Messaging service integration:** Notify development and application owners as soon as vulnerable or non-compliant infrastructure is deployed. Send Amazon SNS topic notifications that include all of the necessary information including resource, owner, problem, and remediation details.

- **Unlimited users and API clients:** Provide the right level of access to anyone in your organization who needs it.
- **Data segregation by business unit:** Associate cloud service provider accounts with specific groups to manage user access to sensitive security and compliance data.
- **Multi-factor authentication (MFA):** Enable multi-factor authentication to protect user access to the Halo Portal.
- **Device authorization:** Provides browser fingerprinting to protect user access to the Halo Portal. When users access the Halo Portal from a new browser, they must pass an email verification.
- **IP address authorization:** Strengthen security by specifying which IP addresses may be used to sign-in to the Halo Portal. Restrict access to corporate IP addresses if desired.
- **SIEM integration:** Integrate Halo Cloud Secure with log-analysis and SIEM solutions to provide even more in-depth analysis.
- **SSO integration:** Streamline login to the Halo Portal by easily integrating Halo with any SAML compliant identity management system.

Free 15 Day Trial

Ready to gain comprehensive security visibility of your IaaS environment? Sign up for a free 15 day trial of Halo Cloud Secure today.

https://www.cloudpassage.com/freetrial

ABOUT CLOUDPASSAGE

Founded in 2010, CloudPassage® is a security pioneer awarded the first-ever patents for universal cloud infrastructure security and is a leading innovator in cloud asset visibility. CloudPassage Halo® is an award-winning security solution purpose-built for the cloud that helps customers automatically discover cloud assets, reduce their attack surface, and find and respond to critical risks other tools miss. It provides unrivaled visibility and continuous compliance for the cloud deployments of some of the world's most demanding IT shops in technology, finance, security, media, e-commerce, and hospitality. CloudPassage is backed by leading Silicon Valley firms Benchmark, Four Rivers Group, Lightspeed Venture Partners, Meritech Capital, Musea Ventures, Shasta Ventures, Sozo Ventures, and Tenaya Capital.

www.cloudpassage.com | 800.215.7404

CloudPassage