CloudPassage
A Fidelis Cybersecurity Company

DATA SHEET

UNIFIED SECURITY AND COMPLIANCE AUTOMATION FOR AMAZON WEB SERVICES

Fidelis CloudPassage Halo® is a unified cloud security platform that automates cloud security controls and compliance across servers, containers, and IaaS in any public, private, hybrid, and multi-cloud environment. Halo's extensive automation capabilities streamline and accelerate workflows between InfoSec and DevOps.

Halo's agentless technology supports services specific to the Amazon Web Services (AWS), as well as for Microsoft Azure and Google Cloud Platform (GCP). The same two Halo microagents—one for Windows, one for Linux—work seamlessly across cloud provider platforms to secure server workloads and containerized environments.

Automate Security for Amazon Web Services

The cloud is made for flexibility. As you move to AWS, your security platform shouldn't hold you back. Halo provides consistent visibility and control across all clouds, regardless of location or scale. With seamless API integration, you can automate security controls and protect your assets in AWS and beyond.

Deploy sensors within infrastructure

Halo instruments cloud service accounts, servers, containers, and image repositories, and integrates security into your CICD pipelines via existing automation processes (e.g., Chef, Puppet, AWS OpsWorks, AWS CloudFormation, Terraform).

Inventory cloud assets and services

Halo automatically maintains a detailed inventory of assets deployed in your AWS environments, including servers, containers, container images, serverless functions, storage objects, networking services, security credentials and policies, and more.

Continuously assess for issues

Halo detects dangerous misconfigurations that create exposures and policy violations that break compliance with deep, continuous assessment of cloud assets and services. Maintain continuous compliance with PCI DSS, CIS Benchmarks, SOC 2, GDPR, and more, as well as your own defined standards, with Halo.

Enable automated remediation

Halo automatically delivers exposure and issue data via existing DevOps workflows (e.g., REST API, Slack, Jira, SNS/SQS, Jenkins), enabling DevOps teams to automate issue remediation.

Verify, track, and monitor

Halo continuously monitors AWS assets and deployed workloads for new IaaS/PaaS inventory, configuration changes, newly disclosed vulnerabilities, indicators of threat, potential compromises, and deviations from configuration policies. Halo also automatically verifies and closes remediated issues, detects regressions, collects relevant system events, generates audit trails for compliance and investigation, and maintains KPI data.

Seamlessly integrate with DevOps

With Halo, you'll achieve greater efficiency, speed, and consistency by automating workflows and integrating with existing DevOps processes. Shift security left by injecting security assessments into CICD pipelines, create continuous compliance feedback for system owners, deliver remediation and incident response data using DevOps-native tools, respond to threats more quickly, and more.

True Cloud Agility with Unified Security

The Halo platform works seamlessly across any mix of public, private, hybrid, and multi-cloud environments. This means that security and compliance controls are portable, preventing lock-in and improving agility and efficiency. With Halo as your unified security platform, you can move assets as needed to support application requirements, and your security controls move with them—seamlessly.

Halo automates a broad range of security and compliance needs for cloud servers, IaaS and PaaS services, and containerized environments, along with protection for legacy virtual machines and bare-metal hosts.

Cloud Security Posture Management for AWS

The Halo Cloud Secure service supports CSPM for AWS IaaS accounts, services, and resources, including inventory and/or assessment. Attribute-based policy assignment automatically applies the CIS AWS Foundations Benchmark policy to all AWS projects. Users can create and customize policies as required.

- API Gateway
- CloudFormation
- CloudTrail
- EC2 instances, AMIs, security groups, and load balancers
- ECR repositories
- ECS clusters and containers
- EKS clusters
- Elastic Beanstalk
- IAM groups, users, roles, and policies
- KMS encryption keys
- Lambda functions
- RDS DB instances, snapshots, and security groups
- Route 53 hosted zones and domains
- S3 buckets
- VPC networks, ACLs, subnets, and peering connections

Cloud Workload Protection for AWS

The Halo Server Secure service provides inventory, assessment, event monitoring, and data collection for cloud-hosted servers and workloads, with comprehensive, customizable policy and rule templates and flexible policy management features.

Computing assets supported on AWS:

- Cloud Servers
- Windows and Linux Operating Systems
- Installed Applications
- User Accounts
- Processes
- Network Traffic

Container Security for AWS

Halo Container Secure secures your container images and runtimes, image registry platforms, Docker daemons, and orchestration software to ensure proper security and compliance. Comprehensive, customizable policies and rules support common Docker and Kubernetes standards such as CIS benchmarks.

Container technologies supported on AWS:

- Kubernetes (self-managed)
- Docker Enterprise
- Docker Community Edition
- Docker Private Registry
- Docker Trusted Registry
- JFrog Artifactory
- Docker Engine
- Containerd

ABOUT CLOUDPASSAGE

CloudPassage®, a Fidelis Cybersecurity® company, safeguards cloud infrastructure for the world's best-recognized brands in finance, e-commerce, gaming, B2B SaaS, healthcare, biotech, and digital media. Fidelis Cybersecurity combats the full spectrum of cyber-crime, data theft and espionage. As the leading innovator of Active XDR solutions, Fidelis helps organizations detect, respond and neutralize threats earlier and deploy deception technologies to stop adversaries before they advance across the IT environment. The CloudPassage Halo® platform unifies security and compliance across servers, containers, and IaaS resources across any mix of public, private, hybrid, and multi-cloud environments including Amazon Web Services, Microsoft Azure, and Google Cloud Platform. Fidelis Cybersecurity is trusted by Global 1000s and Governments as their last line of defense.

CloudPassage
A Fidelis Cybersecurity Company

Fidelis Cybersecurity | 1800.652.4020 | info@fidelissecurity.com