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. Fidelis Halo's extensive automation capabilities streamline and accelerate workflows between InfoSec and DevOps.

Fidelis 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 Fidelis 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. Fidelis 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

Fidelis 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

Fidelis 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

Fidelis 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 Fidelis Halo.

Enable automated remediation

Fidelis 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

Fidelis 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. Fidelis 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 Fidelis 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.

* All Fidelis CloudPassage Halo services, including Halo Cloud Secure, Halo Server Secure, and Halo Container Secure, support all international AWS, GCP, and Azure regions.

True Cloud Agility with Unified Security

The Fidelis 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 Fidelis Halo as your unified security platform, you can move assets as needed to support application requirements, and your security controls move with them—seamlessly.

Fidelis 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 Fidelis 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 Fidelis 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, including Amazon Linux 2
- Installed Applications
- User Accounts
- Processes
- Network Traffic

Container Security for AWS

Fidelis 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 Fidelis Cybersecurity

Fidelis Cybersecurity, the industry innovator in proactive cyber defense solutions, safeguards modern IT environments with unparalleled detection, deception, response, cloud security, and compliance capabilities. We offer full visibility across hybrid environments via rich, dynamic cyber terrain mapping and multi-faceted context and risk assessment. These features help minimize attackable surface areas, automate exposure prevention, threat detection, and incident response, and provide the context, accuracy, speed, and portability security professionals need to find and neutralize adversaries earlier in the attack lifecycle. With Fidelis, organizations emerge stronger and more secure. Fidelis is trusted by many top commercial, enterprise, and government agencies worldwide. For more information, please visit **www.fidelissecurity.com**

Fidelis Cybersecurity