SERVICE BRIEF

Fidelis CloudPassage Halo Cloud Secure™

Public cloud use is on the rise, with over half of today's enterprises running more than 40% of their workload in the cloud[1]. The flexibility of cloud services allows for automated deployment of workloads, increased efficiency, and improved networking, and vast scalability. However, security practitioners have to track fast-moving IaaS assets, their exposures, and related events that pertain to security and compliance, and they struggle to maintain visibility and control. New security concerns, including expanded cloud attack surfaces, varying shared security responsibilities with public cloud providers, and an ever-growing list of cloud service configuration options add to the mounting concerns that information security teams deal with every day.

Fidelis CloudPassage Halo Cloud Secure

Fidelis CloudPassage Halo Cloud Secure™ is the Cloud Security Posture Management (CSPM) service of the Fidelis CloudPassage Halo® platform. It automates security and compliance management for critical assets hosted in public clouds, both as a standalone service or in concert with Fidelis Halo's server and container security capabilities.

Fidelis Cloud Secure is the means to establish and maintain a strong IaaS and PaaS security posture automatically. Upon initial setup, and continually thereafter, Fidelis Cloud Secure gives you full visibility into the security and compliance posture of your entire cloud environment. It keeps pace with the fast rate of change in dynamic cloud resources and opens the door to consistent, automated remediation workflows. Unlike point solutions that provide limited coverage of a single service or provider, Fidelis Cloud Secure finds critical risks other tools miss, with CSPM coverage for Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

Fidelis Cloud Secure is...

Agentless

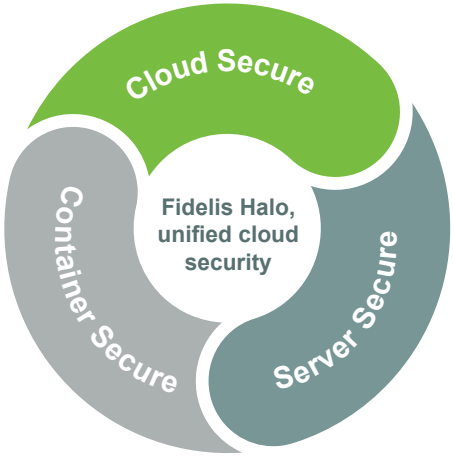
The API connector architecture means there's nothing to install, and no service degradation – the negligible processing impact doesn't get in the way or inflate your cloud budget.

Automated

The fully automated SaaS solution provides a full inventory, evaluation, and assessment of all your cloud assets, along with a prioritized issue list and best-practice remediation advice within minutes of setup.

Simplified

The read-only connection between Fidelis Halo and your cloud accounts is easily managed through the Fidelis Halo Portal, a single-pane-of-glass interface for complete CSPM configuration and control.



1 Cloud Security Alliance, "State of Cloud Security Concerns, Challenges, and Incidents," 30 March 2021, https://cloudsecurityalliance.org/artifacts/state-of-cloud-security-concerns-challenges-and-incidents/

Fast, Automated Security and Compliance in the Public Cloud

Traditional security platforms cannot keep up with the ephemeral nature of cloud computing. Fidelis Cloud Secure runs as an agentless service—and that makes it fast— to keep up with dynamic hybrid and multi-cloud environments at scale. Fidelis Cloud Secure connects to your cloud provider IaaS resources and PaaS services through their native APIs to discover, inventory, assess, and monitor cloud assets for security and compliance issues. The Fidelis Halo API connectors collect and stream data to the efficient, transparently scalable Fidelis Halo Cloud, which uses its own resources to analyze data and alert you in real-time of any risks or threats to your cloud security.

Find critical risks other tools miss

Automatically discover and inventory all IaaS resources and PaaS services attached to your cloud provider account for comprehensive infrastructure visibility across your AWS, Azure, and GCP environments, and receive continual assessments to check for policy compliance and best-practice configurations.

Reduce risk through automated monitoring

Continually monitor cloud accounts, assets, and events to detect security and compliance risks introduced by newly provisioned assets, innocent changes, or malicious activity.

Eliminate alert fatigue

Avoid wasting valuable human resources responding to false alarms and low or non-existent risks and allow Fidelis Halo to automatically detect and track remediation efforts and report resolved issues.

Control security monitoring timing

Fine-tune your continuous monitoring by asset type so you can closely monitor your high-value assets. Your security teams can also run ad-hoc scans at any time, without interrupting scheduled scans, to gather data for event and anomaly investigations.

Decrease exposure time

Enable fast and effective remediation by automating actionable alerts, delivered to the people who need them. Automate remediation workflows by sending detailed vulnerability information and remediation guidance and scripts.

Improve operational efficiency

Immediately deliver security issues to system owners to maximize the efficiency and effectiveness of your remediation process. Workflows in Fidelis Cloud Secure are available as REST-enabled API functions so your team can integrate directly with existing DevOps tools and processes to improve operational agility.

Maintain continuous compliance

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

How Fidelis Cloud Secure Works

Cloud Security Posture Management (CSPM) is imperative to finding and closing gaps, illuminating exposures, and tracking and remediating security and compliance events and issues.

Fidelis Cloud Secure is an automated CSPM service that provides continuous inventory, evaluation, and assessment of your entire infrastructure, including your public cloud assets, at any scale. With proxy-aware, native API connectors, Fidelis Cloud Secure is an agentless service that delivers extensive cloud resource inventory and assessment through a comprehensive set of controls and customizable policies and rules.

Supported IaaS and PaaS resources

AWS	Azure	GCP
• 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	• Active Directory • Application Gateway, App Service routing and load balancing services • Azure Compute • Azure IAM guest users • Key Vault encryption key service • Azure Monitoring Service • SQL Servers • Azure Storage • Azure Virtual Network load balancers, security groups, and network watcher • Azure Functions • Azure Web Apps • ACR • AKS	• Cloud Identity and Access Management (IAM) • Virtual Private Cloud (VPC) • Compute Engine • Cloud Storage • Cloud Logging • Cloud Monitoring • Cloud Key Management Service (KMS) • Cloud DNS • App Engine • Big Query

Integrate CSPM with your security tools

Fidelis Cloud Secure works with tools that security teams rely upon for day-to-day activities while offering nearly limitless integration possibilities across your organization. With Fidelis Cloud Secure, you can shift left and automate security assessments by integrating with common CICD tools and integrate with SIEM tools to aggregate and analyze security posture management data. You can also communicate misconfigurations and vulnerabilities directly with asset owners via common messaging, ticketing, and task management tools. And you can secure your Fidelis Halo environment while streamlining access for security teams by integrating with identity management tools, including Ping Identity, Centrify, and Okta.

Fidelis Cloud Secure Features

Resource discovery and 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.

Advanced best practices

- Go beyond industry hygiene standards by leveraging comprehensive best practices developed by the Fidelis CloudPassage security research team.

Comprehensive, flexible policies and rules

- Start from preconfigured, security and compliance rules that support IaaS and PaaS assets on AWS, Azure, and GSP.
- Customize rules by changing parameters and criticality, or by activating and deactivating rules for different environments.

Customizable and ad-hoc security monitoring

- Set monitoring intervals for your cloud service provider accounts on a per-service basis.
- Scan your cloud service provider account at any time to immediately get current information.

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.

Find unmonitored instances

- Search for virtual machine instances that do not have essential security monitoring enabled.

Dashboard and reporting

- Get an at-a-glance summary of the 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.

Proxy-aware connections

- Simplify management with Fidelis Cloud Secure's proxy-aware API connectors that require no changes to your network environment.

SIEM integration

- Integrate Fidelis Cloud Secure with log-analysis and SIEM solutions to provide even more in-depth analysis.

Multi-factor authentication (MFA)

- Enable multi-factor authentication to protect user access to the Fidelis Halo Portal.

SSO integration

- Streamline login to the Fidelis Halo Portal by easily integrating Fidelis Halo with any SAML compliant identity management system.

Single pane of glass

- Unify cloud inventory, evaluation, and assessment across even the most diverse and dynamic clooud environments under a single pane of glass.

Device and IP authorization

- Rely on browser fingerprinting to protect user access to the Fidelis Halo Portal.
- Enforce email verification when users access the Fidelis Halo Portal from a new browser.
- Strengthen security by specifying which IP addresses may be used to sign in to the Fidelis Halo Portal.
- Restrict access to corporate IP addresses if desired.

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 deep, dynamic visibility and asset discovery, 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