DATA SHEET

Fidelis CloudPassage Halo®

Safeguard Your Cloud Infrastructure

In today's fast-moving, highly scalable, hybrid- and multi-cloud environments, you need scalable and cost-effective cloud security platform that keeps up. Fidelis CloudPassage Halo® ensures security and compliance from the moment new IaaS, PaaS, servers, and containers come online, and continually thereafter, so security and

What is Fidelis Halo?

Fidelis Halo is a unified cloud security platform that continuously inventories, assesses, and monitors cloud accounts, assets, and infrastructure. With agentless cloud security posture management (CSPM) and patented, microagent-based cloud workload protection platform (CWPP) and container security, Fidelis Halo is a comprehensive solution. It identifies misconfigurations, alerts on compliance violations and vulnerabilities, detects indicators of threat, and provides best-practice remediation advice and automation scripts to achieve continuous compliance. Built on the cloud, for the cloud, Fidelis Halo provides full-lifecycle cybersecurity workflows that free staff from menial tasks and enables a true DevSecOps operating model. Fidelis Halo secures new infrastructure and assets automatically and migrates seamlessly between environments so security teams can confidently keep up with strategic cloud implementations.

Three Services. One Powerful

Fidelis Halo is a cost-effective Software-as-a-Service (SaaS) platform. It is comprised of three Fidelis Halo services— Fidelis Cloud Secure™, Fidelis Server Secure™, and Fidelis Container Secure™— that offload the "heavy lifting" of cloud security to the Fidelis Halo Cloud™ centralized agent framework. This powerful computing environment performs sophisticated analytics and evaluates all data collected by serverless API sensors and microagents, all without increasing your cloud budget or contending with your workloads for cloud resources.

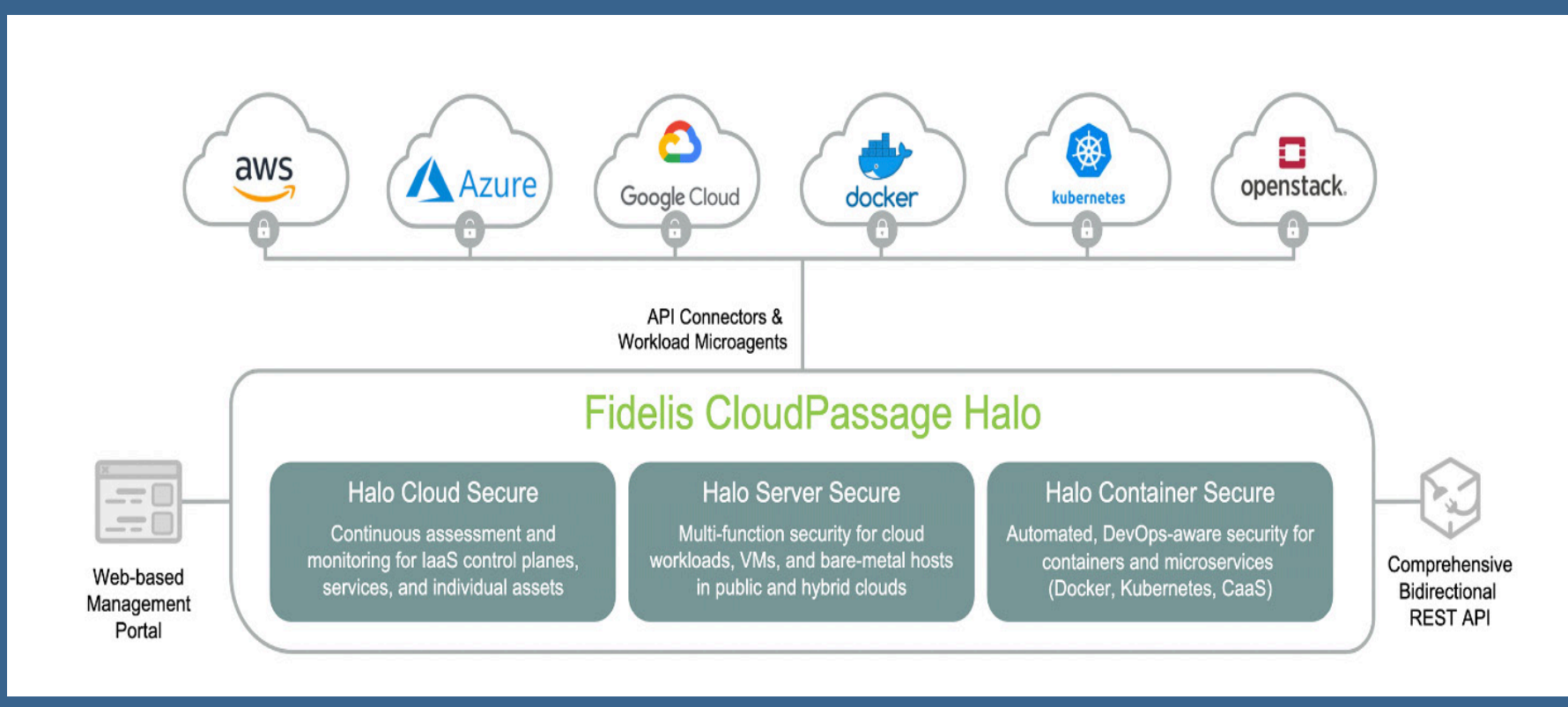
Fidelis Halo Platform Features

Whether you are using the comprehensive Fidelis Halo platform, or one or more services independently, Fidelis Halo provides core features that simplify management and operations.

- Enterprise access control: allows Fidelis Halo administrators to limit visibility for operators based on organizational business units, applications, or projects.
- Role-based access control: provides varying levels of permissions based on the roles of site administrator, group administrator, standard user, and auditor.
- Enterprise-class authentication: to configure password requirements, multi-factor authentication (MFA), and single sign-on (SSO), as well as restricting Fidelis Halo access to specific IP addresses.
- Activity auditing: records all user and API client activities for compliance and auditing purposes and stores historical information about Fidelis Halo logins, updates to settings, policy changes, and other activities.
- Unified view: of assets, security issues, events, and compliance findings all under a single pane of glass, with extensive search capabilities, including more than 40 data attribute filters that can be combined into powerful views.
- Contextual alerting: reduces alert fatigue by targeting users for email alerts based on issue criticality and asset owner.
- Customizable policy interface: starts with hundreds of policies and tens of thousands of rules, and allows security operators to customize from templates or apply new policies from scratch.
- Bi-directional REST API: automates security by managing Fidelis Halo through API endpoints for issues, events, assets, policies, users, administrative

Fidelis Halo Use Cases

- Digital Transformation
- New Cloud Development
- Cloud Bursting
- New Cloud Service Adoption
- DevSecOps/DevOps Integration
- Ransomware Protection
- Unified Security for AWS, Azure, and GCP
- Hybrid Environment Security



Agentless CPSM with Fidelis Cloud Secure

Fidelis Cloud Secure is the means to establish and maintain a strong IaaS and PaaS security posture automatically, and without agents.

- Automated discovery and inventory: within minutes of connection and continually thereafter, so you always know what you have in your cloud environments.
- Automated monitoring and assessment: to catch misconfigurations, configuration drift, and unauthorized changes in real-time across IAM services, virtual machine images, networks, storage services, database services, logging and monitoring services, serverless functions, key management services, DNS services, infrastructure-as-code services, API management services, web applications, certificate services, container registry services, container services, and managed Kubernetes services.
- Continuous compliance: with the latest CIS Benchmarks, evolving industry best practices, and regulatory compliance standards (i.e., PCI, HIPAA, SOX, etc.).
- Expert remediation advice: and automation scripts delivered directly to asset owners to accelerate manual fixes and enable automated remediation implementation.
- Remediation tracking: to track problems from the point of discovery through resolution and at each step in between.
- Integration with SIEM tools: for long-term storage and correlation of events from other devices.

Microagent-based CWPP with Fidelis

Fidelis Server Secure offers multi-function security for cloud workloads hosted on Windows and Linux servers, virtual machines (VMs), and bare-metal hosts in public, private, hybrid- and multi-cloud environments.

- Patented microagent technology: with just two agents— one for Windows and one for Linux—that use just 2MB of memory and negligible disk space, the Fidelis Halo microagent offers real-time security controls without inflating your cloud budget or contending for resources.
- Cloud server inventory and assessment: providing deep visibility and posture assessment of Windows and Linux server workloads across public, private, hybrid, and multi-cloud environments.
- Vulnerability assessment: keeps you ahead of Common Vulnerabilities and Exposures (CVEs) in server software, operating systems, and installed applications, so you can prioritize the most critical issues for remediation.
- File integrity monitoring: confirms the integrity of new workloads against their source images and detects unauthorized changes made to running workloads by checking important files and registry keys.
- Event monitoring: automatically monitors for and collects significant security-related events from operating systems and running applications to detect unwanted behavior such as attempted logins to immutable systems, “root” or “Administrator” login usage, privileged changes, changes to audit policies, installation or de-installation of software, and addition, deletion, or modification of user accounts.
- User account inventory and assessment: provides visibility into local user accounts on Windows and Linux workloads to uncover insecure configurations, discover unused accounts, and alert on users that belong to the wrong groups.
- User account integrity and event monitoring: to automatically ensure proper account configuration and alert on unauthorized changes and unwanted behaviors.
- Process discovery, monitoring, and management: to keep track of Windows and Linux processes, blacklist and whitelist processes, ensure proper port usage, and collect security-related events to detect unwanted behaviors.
- Network traffic discovery and visualization: discovers and inventories traffic to and from each workload and provides a visual map so you can quickly identify anomalous traffic.
- IaaS instance metadata collection: consolidates rich metadata for each IaaS asset into a single view.

Frictionless Container Security with Fidelis Container Secure

Fidelis Container Secure provides automated, DevOps-aware security for Docker, Kubernetes, and Container-as-a-Service (CaaS) environments.

- Microagent-based Coverage: using the same two microagents as Fidelis Server Secure, Fidelis Container Secure offers self-installing, low-maintenance, frictionless security controls for the complete container stack.
- Container registry security: provides inventory, assessment, vulnerability management, file integrity monitoring, and event monitoring for container registries.
- Container host security: provides visibility into container hosts, including Docker servers and Kubernetes nodes residing in IaaS and data center environments, and tracks configuration security, software inventory, software vulnerability, file integrity, security events, and network traffic.
- Container inventory: to automatically track Linux container workloads and determine which containers are actually in use, whether containers are based on the current image repository image, and whether they are “rogue”—meaning they came from an unknown image.
- Container software security: provides inventory, configuration assessment, and vulnerability assessment of container software to identify critical issues and prioritize remediation.

Fidelis Halo Advantages

Defense-In-Depth

Close gaps in the shared responsibility model, no matter which cloud providers you use, while extending the same layers of

Unified Control

Secure your complex environments with a unified set of security controls that cover asset discovery and inventory, vulnerability management, threat management, network security, and continuous compliance.

Security at any Scale

Scale your security dynamically and frictionlessly alongside your cloud footprint, keeping ahead of new workloads and assets, configuration changes, and containerized environments.

Flexible and Frictionless

Move security seamlessly and automatically with workloads, without any manual installation, reconfiguration, or tuning, so you can quickly pivot to take advantage

Seamless Integration

Accelerate and improve communication between SOC and DevOps teams and build a true DevSecOps environment, with automated alerts and remediation tracking

API-First Design

Integrated and automate any Fidelis Halo function into your workflows and tools with the comprehensive, bidirectional REST API.

About Fidelis Security®

Fidelis Security® is the industry innovator in proactive cyber defense, safeguarding modern IT for global enterprises with proactive XDR and CNAPP platforms. Fidelis Security consolidates IT security operations to shrink attack surfaces, automate threat detection, and accelerate analysis, forensics, and response so that organizations remain resilient through cyber-attacks and emerge stronger and more secure. Fidelis Security is trusted by top commercial, enterprise, and government agencies worldwide.
For more information, please visit: www.fidelissecurity.com

Contact us to learn more

www.fidelissecurity.com/contact
or scan the QR Code