OVERVIEW

Security is a critical component for digital transformation, particularly since 76% of enterprises indicate they are using multiple IaaS providers. Cloud infrastructures offer increased agility, lower costs, and the flexibility needed to move with rapidly changing market conditions. However, these dynamic infrastructures also create new security challenges, including coverage gaps, loss of visibility, and unsustainable complexity. As companies transform their business systems and processes with cloud technologies, information security needs to be part of that transformation.

Fidelis CloudPassage Halo

Fidelis CloudPassage Halo® is a unified cloud security platform that automates security controls and compliance across any mix of public, private, hybrid, or multi-cloud environments. Halo is cloud-first and DevSecOps-ready, providing fast, scalable asset discovery and inventory, vulnerability assessment, security posture management, continuous compliance, and more. The Halo API enables integrations that streamline and accelerate communications and workflows between InfoSec and DevOps.

Halo is ideally suited for environments that are:

- **Distributed**: Secure application infrastructures across data centers and IaaS platforms and easily move workloads between cloud service providers without reconfiguration or relicensing.
- **Diverse**: Secure thousands of possible asset types and workloads, and use agentless connectors for IaaS and PaaS cloud security posture management.
- **Dynamic**: Accelerate security operations to keep up with rapidly changing application infrastructures and secure new resources as they are added, changed, or expanded.

Fidelis CloudPassage Halo Platform

![Diagram of Fidelis CloudPassage Halo Platform](image)

- **Minimal Footprint** – Conserves cloud budgets and simplifies operations with agentless CSPM and patented microagent-based CWPP and container security.
- **Built on Best Practices** – Delivers out-of-the-box policies and rules built on CIS benchmarks and industry best practices.
- **Immediately Beneficial** – Provides complete visibility and assessment of your IaaS environments in minutes from initial setup.
- **Single Pane of Glass** – Simplifies security operations with a single portal for policy creation, alerting setup, report viewing, and more.
- **Security at Scale** – Scales security to match your cloud footprint, regardless of how large or fast you grow.

![API Connectors & Workload Microagents](image)

![Comprehensive Bidirectional REST API](image)

HALO IS A SUPERIOR CHOICE FOR CLOUD SECURITY

Halo is built on the cloud, for the cloud, and designed to be a unified solution that extends the same cloud security coverage across all your environments. As a scalable, cost-effective SaaS platform, there are three services that comprise Halo:

- **Cloud Secure** provides Cloud Security Posture Management (CSPM) to continually inventory, assess, and monitor IaaS control planes and IaaS and PaaS services and assets.
- **Server Secure** delivers Cloud Workload Protection (CWPP) offering multi-function security for cloud workloads hosted on Windows and Linux servers, virtual machines (VMs), and bare-metal hosts in public and hybrid clouds.
- **Container Secure** provides automated, DevOps-aware security for Docker, Kubernetes, and Container-as-a-Service (Caas) environments.

Each of the Halo services can be used on its own or in combination with one another based on the needs of your unique environment. InfoSec can easily manage all Halo services and view security data for all connected cloud accounts and servers through the web-based Halo Portal.

THE HALO CLOUD-FIRST PLATFORM IS...

**UNIFIED**
Uses the same API, API connectors, microagents, console, policy engine, data model, and analytics engine across all Halo services to provide unified security controls across your entire infrastructure.

**AUTOMATED**
Deploys and operates itself, with full-lifecycle workflows and API endpoints for vulnerability, threat, and compliance management, to free staff from menial tasks and accelerate DevSecOps adoption.

**PORTABLE**
Works seamlessly across any mix of public, private, hybrid, and multi-cloud environments, typically with zero changes to your configuration.

**COMPREHENSIVE**
Includes asset discovery, inventory, assessment, remediation assistance, threat detection, microsegmentation, traffic discovery, and continuous compliance.

**FAST**
Configures and deploys easily as a fully self-contained, turnkey SaaS solution, so you can be up and running or add new cloud service provider accounts in minutes.

**INTEGRATED**
Integrates with a comprehensive set of security tasks into the tools and workflows your teams already use, including SIEM, SOAR, DevOps tools, and more.

**SCALABLE**
Scales elastically, automatically scaling up when workloads increase, and down when workloads decrease.

**COST-EFFECTIVE**
Offers simple, flexible, and competitive pricing for predictable budget forecasting and improved economics over time.

SECURITY AS A SERVICE WITH THE HALO CLOUD

The Halo Cloud centralized agent framework is a powerful computing environment that performs sophisticated analytics and evaluates all data collected by serverless API sensors and microagents. It performs all your “heavy lifting” for you, preserving your server resources and performance for your workloads.
CLOUD SECURE
CSPM for AWS, Azure, and GCP

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

Cloud Secure is the means to establish and maintain a strong IaaS and PaaS security posture automatically. In just minutes from initial setup, and continually thereafter, 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, Cloud Secure finds critical risks other tools miss, with CSPM coverage for Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

SUPPORTED IaaS AND PAAS RESOURCES
Cloud Secure delivers extensive cloud resource inventory and assessment through a comprehensive set of controls and features, including:

<table>
<thead>
<tr>
<th>AWS</th>
<th>Azure</th>
<th>GCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>• API Gateway</td>
<td>• Active Directory</td>
<td>• Cloud Identity and Access Management (IAM)</td>
</tr>
<tr>
<td>• CloudFormation</td>
<td>• Application Gateway, App Service routing and load balancing services</td>
<td></td>
</tr>
<tr>
<td>• CloudTrail</td>
<td>• Azure Compute</td>
<td>• Virtual Private Cloud (VPC)</td>
</tr>
<tr>
<td>• EC2 instances, AMIs, security groups, and load balancers</td>
<td>• Azure IAM guest users</td>
<td>• Compute Engine</td>
</tr>
<tr>
<td>• ECR repositories</td>
<td>• Key Vault encryption key service</td>
<td>• Cloud Storage</td>
</tr>
<tr>
<td>• ECS clusters and containers</td>
<td>• Azure Monitoring Service</td>
<td>• Cloud Logging</td>
</tr>
<tr>
<td>• EKS clusters</td>
<td>• SQL Servers</td>
<td>• Cloud Monitoring</td>
</tr>
<tr>
<td>• Elastic Beanstalk</td>
<td>• Azure Storage</td>
<td>• Cloud Key Management Service (KMS)</td>
</tr>
<tr>
<td>• IAM groups, users, roles, and policies</td>
<td>• Azure Virtual Network load balancers, security groups, and network watcher</td>
<td></td>
</tr>
<tr>
<td>• KMS encryption keys</td>
<td>• Azure Functions</td>
<td>• Cloud DNS</td>
</tr>
<tr>
<td>• Lambda functions</td>
<td>• Azure Web Apps</td>
<td>• App Engine</td>
</tr>
<tr>
<td>• RDS DB instances, snapshots, and security groups</td>
<td>• ACR</td>
<td>• Big Query</td>
</tr>
<tr>
<td>• Route 53 hosted zones and domains</td>
<td>• AKS</td>
<td></td>
</tr>
<tr>
<td>• S3 buckets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• VPC networks, ACLs, subnets, and peering connections</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SERVER SECURE
Cloud Workload Protection for Public, Hybrid, and Multi-Cloud Environments

Halo Server Secure is the Cloud Workload Protection Platform (CWPP) service of the Halo platform. It automates security and compliance management for Linux and Windows servers across any mix of public, private, or hybrid cloud hosting environments. Server Secure addresses the security and compliance demands of cloud-hosted servers and workloads, giving rich context across diverse and distributed environments, and opening the door to consistent, automated remediation. It establishes, maintains, and automates workload protection across even the most dynamic enterprise computing environments.

Server Secure combines patented microagent technology and the Halo Cloud platform centralized agent framework to provide maximum security and compliance coverage with minimum impact to your cloud resources. The platform’s extreme scalability allows it to keep up with rapid changes in the most dynamic of cloud implementations.

THE MICROAGENT OF MICROAGENTS
At just 2 MB, with automated deployment, and built on an architecture that rarely needs updating, the Server Secure microagent is a gamechanger for automated cloud security. With only two microagents to manage—one for Linux, and one for Windows that work across cloud providers and the data center—your security persists through OS patches without reinstallation or agent updates.

HIGHLY EFFICIENT CODE
Requires no additional installations of software or Java runtimes. The slim resource requirements of the agent don’t get in the way, slow you down, or inflate your cloud budget.

PROXY-AWARE
Requires no network changes. Simply point Halo at the server you want to secure, and it works within your existing network configuration.

COMMAND AND CONTROL PROTOCOL
Works on a command-and-control protocol, meaning that all communications from the agent are unidirectional, only communicating from the agent to the Halo Cloud.

SECURE
Installs on each cloud server via configuration through the Halo Portal. It exposes no management or communication interfaces and is not network accessible, which minimizes the possibility of tampering.

DESIGNED FOR HOSTILE ENVIRONMENTS
Ensures that messages between the agent and the Halo Cloud maintain authenticity, confidentiality, and integrity through patented cryptographic controls at the payload and network levels.

MAINTAINS ITS OWN HEALTH
Assesses each microagent hourly to proactively detect signs of tampering. Network traffic and data access are also monitored for signs of malicious activity.
CONTAINER SECURE
Security for Docker, Kubernetes, and the CICD Pipeline

Halo Container Secure is the container security service of the Halo platform. Container Secure answers the complex challenges of container security in the cloud by automating security and compliance for Docker, Kubernetes, and continuous-delivery pipeline infrastructure. It works as a standalone service or in concert with Halo’s server and cloud security services.

Container Secure provides security and compliance automation for containerized applications running in public, private, hybrid, or multi-cloud hosting environments. It validates security across the entire infrastructure stack for containers, including registries, pre-production images, run-time environments, and DevOps toolchains, and it provides advanced threat detection by alerting on the presence of rogue containers.

**KEEP PACE WITH RAPIDLY CHANGING ENVIRONMENTS**
Automatically discover, inventory, and evaluate containerized environments and assets, including container instances, host systems, image repositories, IaaS accounts, and CaaS from AWS, Azure, and GCP.

**STAY AHEAD OF EMERGING THREATS**
Automatically detect Docker host and Kubernetes node intrusions through log monitoring, file and system integrity monitoring, and intrusion detection. You can also quarantine suspected rogue containers within seconds of detection.

**ACHIEVE SECURITY INTEGRATION WITH DEVOPS**
Shift security left and make DevOps a force multiplier for security with the immediate delivery of vulnerability and exposure issues to system owners via REST API integrations and message queues.

**PROTECT CONTAINERIZED APPLICATIONS FROM THE HOST UP**
Detect vulnerabilities in host operating systems, container runtimes, orchestration configurations, unpatched packages, access privileges, security control configurations, network services, process whitelists/blacklists, and more.

**REDUCE THE ATTACK SURFACE IN CONTAINERIZED ENVIRONMENTS**
Continually monitor container stacks to detect new vulnerabilities and exposures introduced by innocent changes or malicious activity, expose rogue containers in real-time, and accelerate remediation to thwart attacks before they do damage to your enterprise.

**ACHIEVE SECURITY INTEGRATION WITH DEVOPS**
Integrate with DevOps tools to provide alerts in real-time. DevOps teams receive best-practice remediation guidance with every alert, delivered through the tools they already use, including Jira, Slack, and ServiceNow.

**SECURE THE COMPLETE CONTAINER STACK**
- Container Instances
- Kubernetes
- Container Runtimes
- Host System
- Image Repository
- IaaS Account
HALO PLATFORM FEATURES

Comprehensive, Flexible Policies and Rules
Accelerate your cloud security strategy with 175+ policies and 20k+ rules that can be cloned, customized, and applied based on asset groups and attributes.
- Policies and rules based on Center for Internet Security (CIS) Benchmarks, PCI, HIPAA, SysTrust/SOC 2, and industry best practices
- Continually updated with changing benchmarks, regulations, and best practices
- Fully customizable rules
- JSON import and export of rules available
- Simplified update process for new and updated rules
- Ready for integration with version control and policy management tools
- Hierarchical cloud asset modeling for access control and simplified policy assignment
- Attribute-based policy management for Configuration Security Management (CSM), File Integrity Management (FIM), and Log-based Intrusion Detection (LIDS) policies

Patented Architecture
The patented, battle-tested and industry-proven Halo platform is unique among cloud security platforms.
- Simplified microagents—one for Windows and one for Linux—are only 2 MB in size
- CSPM runs on API connectors for agentless coverage
- Centralized agent framework reduces resource requirements
- Negligible processing impact on system resources

Single Source of Truth
End operational fatigue and gain access to seamless functionality and security intelligence within a single platform.
- Data is aggregated, normalized, and enriched across cloud service providers, assets, and resources
- Interactive dashboards and reports of accounts, resources, and assets give policy and compliance status to simplify issue tracking and audit compliance
- Drill-down reports contain detailed information needed for remediation and audit
- All Halo data can be exported to CSV for use in external reporting tools and analysis applications
- Tamper-proof records of technical and operational compliance for your IaaS environments

Remediation Guidance
Empower all remediation team members, including asset owners, SOC teams, and operations to accelerate remediation efforts with best-practice advice and API endpoints for policies and rules.
- Security alerts can be sent directly to asset owners
- Up-to-date remediation advice included with every alert
- Remediation steps provided in plain text and JSON format for manual or automated remediation
- Remediation status updates in real time based on actions taken by system owners

Secure
Halo is a secure service, maintaining read-only access to your cloud accounts and providing industry-leading security for Halo user management and portal authorization and access.
- Built-in SAML 2.0 integration capabilities streamline logins to the Halo Portal
- Multi-factor authentication, including browser fingerprinting and email verification
- Login restriction by individual IP addresses or IP ranges
- Group-based access control to manage user access to sensitive security and compliance data

Complete Security Monitoring Control
Rely on granular control over cloud security monitoring to make incident investigation and response a matter of minutes and hours instead of days and weeks.
- Configurable monitoring intervals on a per-service basis
- Ad-hoc snapshot capability for incident investigation
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. CloudPassage extends Fidelis Cybersecurity capabilities in the cloud. 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.

Copyright © 2002-2021 Fidelis Cybersecurity, Inc. All rights reserved.