SERVICE BRIEF

Fidelis CloudPassage Halo Server Secure™

With cloud data centers processing 94% of business workloads and the steady increase in dependence on multi-cloud environments[1], cloud security is a top concern among enterprise leaders. Security is noted as the most significant challenge in enabling a remote workforce and in keeping workloads safe in multi-cloud environments.

Today's workloads are designed for direct-to-customer interactions, big data analytics, rapidly opening new lines of business and new ways to market, and more. These workloads depend on the adoption of highly elastic, scalable, and performant cloud application stacks. Whether you're migrating existing workloads to the cloud, building new applications that take advantage of cloud agility, or you're a born-in-the-cloud business, only a cloud-focused security platform can protect your enterprise's most prominent workloads and data while keeping your employees and customers connected and secured.

Fidelis CloudPassage Halo Server Secure

Fidelis CloudPassage Halo Server Secure™ is the Cloud Workload Protection Platform (CWPP) service of the Fidelis CloudPassage Halo® platform. It automates security and compliance management for Linux and Windows servers across any mix of public, private, or hybrid cloud hosting environments. Fidelis 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.

Fidelis Server Secure is...

Lightweight

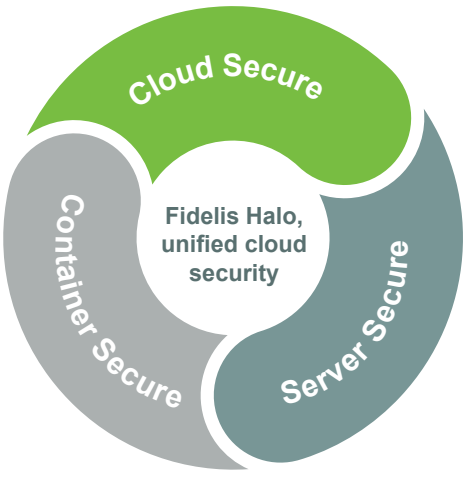
Requires no additional software to install or manage and protects your cloud workloads without increasing cloud budgets.

Automated

Self-installs after a simple cloud credentialing process to monitor for compliance, track security anomalies, and automatically alert and take actions based on your configuration preferences.

Unified

Provides uniform coverage for servers and workloads across any mix of public, private, hybrid, or multi-cloud hosting environments.



1 Cisco, " 2021 Global Networking Trends Report," https://www.cisco.com/c/en/us/solutions/enterprise-networks/2021-networking-report-preview.html

How Fidelis Server Secure CWPP Works

Fidelis Halo completely reinvents the architecture for agent-based server security, creating a uniquely streamlined, fast, and automated security solution that is made for the cloud. Fidelis Server Secure combines patented microagent technology and the Fidelis Halo Cloud centralized agent framework to provide maximum security and compliance coverage with minimum impact to your cloud resources. The platform's extreme scalability and dynamic operation allow it to keep up with rapid changes in the most dynamic of cloud implementations.

How Fast is Server Secure?

30 seconds
to register a Fidelis Halo microagent on IaaS, virtual machines, servers, and baremetal hosts.

90 seconds
to obtain a full inventory, evaluation, assessment, and instrumentation for ongoing monitoring across all registered microagents.

The Microagent of Microagents

At just 2 MB, with automated deployment, and built on an architecture that rarely needs updating, the Fidelis 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.

Secure

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

Proxy-aware

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

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.

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 Fidelis Halo Cloud.

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.

Comprehensive Workload Protection for Public, Hybrid, and Multi-Cloud Environments

Customizable policies and rules

Hundreds of pre-configured policies and tens of thousands of best-practice and compliance-based rules give you a strong foundation for cloud workload protection. You can select, clone, and customize policies and rules that govern common and required security controls, including configuration security management, file integrity management, log-based intrusion detection, network and firewall security, and special events monitoring.

A single source of truth

Simplify security management, gain powerful security intelligence, and accelerate investigation and remediation all through the Fidelis Halo Portal. This convenient, browser-based management portal provides access to configuration for all CWPP capabilities, including policy creation, alerting setup, report viewing, and user management. You can also use the Fidelis Halo Portal to investigate server-level intrusions, with overview screens and drill-down data for log monitoring, file and system integrity monitoring, indicator of threat and compromise detection, and more. And you can manage all your security investigations, remediation, and resolution through Fidelis Halo, making it a single source of truth for cloud security and compliance.

High-fidelity control over monitoring intervals

Stay ahead of your cloud workload security with monitoring that happens when and how you want. You can set monitoring intervals on a per-server basis or apply across a group of assets. During investigations and incident responses, you can run an ad-hoc scan that gives you actionable insight into log-based intrusion detection data, file and system integrity, anomalous network traffic, configuration drift, and more.

Improved communications between security and application owners

Automatically communicate critical server alerts to application owners as they are discovered for proactive, automated response to exposures, threats, and compliance issues. With automated cloud workload protection and best practice remediation advice delivered to your application owners, you foster better collaboration, accelerate communication, and dramatically reduce remediation times while improving response effectiveness.

Continuous compliance

Stop the eleventh-hour fire drills, put an end to pages-long security issue reports, and achieve a culture of continuous compliance. With automated CWPP, you'll manage server security and compliance across your entire infrastructure, at scale, with consistency and confidence. Fidelis Halo provides tamper-proof records of technical and operational compliance for all your workloads and servers. And it consolidates all security and compliance data in one place, from server population to configuration findings to historic and ongoing remediation efforts and records.

Endless Integration Possibilities

- **JSON** - All remediation data and policies are available via JSON for easy automation of consumption by downstream tools like SIEM, SOAR, GRC, operational workflow tools.
- **Deployment Scripts** - Microagents can be deployed by Chef, Puppet, Bash, and other common tools, by using included deployment automation scripts.
- **Server Images** - Microagents can be preconfigured and built into server images (e.g., AWS, AMIs) so security and compliance capabilities activate when your servers do.
- **CD Pipelines** - All Server Secure capabilities can be leveraged in CD pipelines using a Jenkins-native plugin.
- **CICD Tools** - A CICD SDK enables advanced integration with any CICD orchestration tool.

Easy integrations

Accelerate adoption and make cloud workload security a cross-cutting part of your corporate goals and culture by integrating with the tools your teams already use. All Fidelis Server Secure functions are available through the comprehensive Fidelis CloudPassage REST API and SDK to build security and compliance into operations instead of bolting security on after the fact. The Fidelis Halo API can be used to automate microagent deployment, integrate with other tools, or create new management tools.

Fidelis Server Secure Features

Configuration security monitoring

- Protect cloud workloads at the server and cloud service configuration level—the primary source for security holes in the cloud.
- Monitor the details of your configuration settings, system files, running processes, ownership, and permissions to ensure that no unauthorized changes are made that could compromise server security.
- Start with CSM policies built from best-practice configurations for operating systems and cloud services such as databases, web servers, docker, Kubernetes, and more.

File integrity monitoring

- Prevent file and registry tampering and quickly detect anomalies before they become security incidents.
- Automate server monitoring for changes to important system binaries, configuration files, and registry keys.
- Stay ahead of potential threats introduced by innocent changes or malicious activity including data changes, permission changes, and the addition or deletion of files, directories, and registry entries.
- Include file integrity monitoring as part of your continuous deployment pipeline.

Special events

- End alert fatigue by tracking the occurrences you want to track and quickly prioritizing events.
- Gain powerful flexibility over event logging and alerting with special events policies.
- Track unusual occurrences, including unexpected restarts, IP address changes, firewall reconfigurations, and more.
- Quickly determine security implications from special event alerts and easily prioritize events for evaluation and remediation.

Log-based intrusion detection

- Stay ahead of the threat and prevent front-page breaches with automated log-based intrusion detection that includes actionable alerts and intelligence.
- Monitor, collect, and alert on significant security-related events from server operating systems and running applications that could indicate misuse, misconfiguration, or compromise.
- Work with pre-built policies and customize your own to detect unwanted behavior, including suspicious login attempts, privileged changes, unauthorized changes or additions of user accounts, changes to policies, and the installation or removal of software.

Firewall and network

- Stop attacks before they get in the front door by securing your firewall, monitoring networks, and identifying suspicious traffic.
- Gather detailed information on both inbound and outbound TCP and UDP connections that occur on your servers.
- Identify connection patterns and detect suspicious connections quickly.
- Use firewall policies to automatically allow and block traffic to your servers' systems and workloads.

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