SERVICE BRIEF

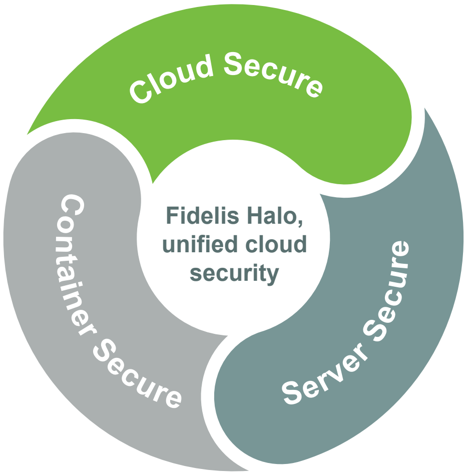
Fidelis CloudPassage Halo Container Secure™

Containerized development using technologies like Docker and Kubernetes is gaining rapid adoption across organizations. While containers provide a significant gain in productivity, agility, and efficiency for DevOps team, they represent an entirely new attack surface and unique set of security challenges that traditional security tools aren't designed to solve. And since containers are only as secure as the host themselves, CIS Benchmark for Docker and NIST SP800-190 also require organizations to secure the Docker host. InfoSec needs a new type of security platform that can keep the entire container stack secure without becoming a bottleneck to rapid application development and deployment.

Fidelis CloudPassage Halo Container Secure

Fidelis CloudPassage Halo Container Secure™ is the container security service of the Fidelis CloudPassage Halo® platform. Fidelis 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 Fidelis Halo's server and cloud security services.

Fidelis 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.



Fidelis Container Secure is...

Agile

Provides visibility and context in even the fastest moving, ephemeral containerized environments so you can reduce risk, close security gaps, and detect rogue containers before they become breach entry points.

Comprehensive

Secures every layer of the container stack, from the IaaS account to the container instance and at every level in between, including image repositories, host systems and OS, container runtimes, and Kubernetes.

Automated

Continually monitors container environments to detect new vulnerabilities and exposes introduced by innocent changes or malicious activites, and enables automated remediation driven by InfoSec or DevOps teams.

Automate Security for Docker, Kubernetes, and the CICD Pipeline

Fidelis Halo automates key security and compliance functions through a set of customizable policies and technical rules that support common Docker and Kubernetes standards, including CIS benchmarks. These policies and rules are used to determine if container-related assets are compliant with best-practice security controls.

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.

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

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.

Automate remediation assistance

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.

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.

Secure the Complete Container Stack

Container Instances Kubernetes Container Runtimes	Collect detailed configuration and status information about container instances, Kubernetes services, and container runtimes. The collected information is evaluated against policies for security, best practices, and compliance to detect deviations. The results are available via the Fidelis Halo GUI or REST API.
Host System	Automate server instrumentation to implement a variety of security controls including discovery/inventory, vulnerability management, system hardening, system integrity monitoring, drift detection, runtime security events, and audit data collection.
Image Repository	Inventory, evaluate, and assess image registries and repositories and assess container images at rest for vulnerabilities so you can catch and remediate violations in both active and to-be-deployed workloads.
IaaS Account	Monitor your IaaS and PaaS accounts to automate security controls for hosts, registry services, IAM, and any other resource that supports your containerized environment.

How Fidelis Container Secure Works

Deploys in minutes

Fidelis Container Secure is a fully self-contained, turnkey SaaS solution that deploys very quickly. You'll be fully operational within minutes from initial account creation, including a full inventory, evaluation, and assessment of container instances, runtimes, and image repositories. Ongoing inventory and assessments of container hosts and guest instances take less than 90 seconds, and new microagents on Docker hosts and servers can be registered in less than 30 seconds.

Configures quickly with customizable policies and rules

Fidelis Halo's library contains common best-practice and compliance policies and rules for containers, Kubernetes, Docker hosts, runtime environments, and more that can be quickly applied as-is or cloned and customized into your environment. All rules are based on Center for Internet Security (CIS) Benchmarks, PCI, HIPAA, SysTrust/SOC 2, and best practices as determined by the Fidelis Halo Threat Intelligence team. Rule updates happen automatically, keeping your containerized environments secure as new threats emerge and cloud security best practices change.

Connects using patented microagent technology

The 2 MB Fidelis Halo microagent—one for Windows, and one for Linux—secures your containerized environments through a simple policy assignment in the Fidelis Halo Portal. Microagents can be installed directly as software on the container host environment or as a running container. The Kubernetes-native DaemonSet support automates deployment of the Fidelis Halo microagent on every Kubernetes node for easy security management, and the SaaS-based Fidelis Halo Cloud does the heavy lifting for the microagent. Each monitored node is monitored against its container image database and applied policies and rules to uncover known vulnerabilities and violations.

Shifts security left

Fidelis Container Secure natively connects with common continuous delivery pipeline tools, including Jenkins, to integrate security assessments into the development process. It can also be integrated with nearly any DevOps tool using the bi-direction REST API, including Jira, jFrog Artifactory, and more, to include system owners as active participants in your enterprise security strategy.

Automates Container Security

Registry connectors scan container images at rest and plugins and integrations track images in motion. As changes are committed, images are moved toward production, and container instances spin up, Fidelis Container Secure is there, alerting on anything that violates your configured policies and rules.

Provides a single source of truth

The Fidelis Halo Portal and API streamline security management by consolidating all configuration, management, alert, and response under a single platform, no matter how diverse your containerized environment. Through the portal, you can create policies for your containerized application infrastructures and apply them uniformly across any number of cloud service providers, cloud accounts, virtual machines, or bare metal hosts. With the API, you can configure alerts to route directly to asset owners to accelerate incident response and get ahead of emerging threats. And all data is maintained as a comprehensive view in a single portal, with interactive dashboards and reports that include prioritized issues and alerts.

> Fidelis Container Secure answers the complex challenges of container security in the cloud by automating security and compliance for Docker, Kubernetes, and continous-delivery pipeline infrastructure.

Fidelis Container Secure Features

Continuous image assurance

- Scan images across registries for software vulnerabilities.
- Scan images pushed to registries.
- Pass/fail builds via integration with CI tools automatically.

Runtime configuration assessment

- Get detailed configuration information such as capabilities, container namespaces, security options, and more.
- Detect rogue containers instantiated from unauthorized/unknown images.
- Detect privileged, writable, and interactive containers.

Docker host and daemon security monitoring and management

- End alert fatigue by tracking the occurrences you want to track and quickly prioritizing events.
- Detect indications of intrusion and compromise on hosts.
- Automate file integrity monitoring for containers at rest and runtime.
- Segment your container host network to reduce the risk of lateral movement.

Deep visibility and compliance

- Summarize findings across servers and containers with automated dashboards.
- Inventory all containers and servers they are running on automatically, including organizational units.
- Track containers through its lifecycle, including Docker events.
- Export identified issues to meet compliance requirements.

Container host security

- Protect both servers and containers with a same platform.
- Detect vulnerabilities and configuration issues with the host operating systems, cloud asset configurations, host access, networks, and more.

Supported Technologies

Container Runtime Engine	Docker CE, Docker EE, Containerd
Infrastructure	Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, OpenStack, Virtual Machines (VMware, etc.) Rackspace, bare metal.
Image Registry	Docker Private Registry, Amazon EC2 Container Registry (ECR), jFrog Artifactory
Container Host OS	Amazon Linux, Ubuntu, CentOS, RHEL, Debian, CoreOS
Image Base	OS Ubuntu, CentOS, RHEL, Debian, Alpine
CICD Integration	Jenkins, Bamboo, TeamCity, Circle CI, Travis CI and more
Other Integrations	Rest API, SIEM (SumoLogic, Splunk, etc.) Messaging (Slack), Ticketing (JIRA), and more

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**