DON'T LET SECURITY PUT THE BRAKES ON DEVOPS.

MOVE FASTER. SECURITY AUTOMATION & ORCHESTRATION AT DEVOPS SPEED.

THE PROBLEM

DevOps is built on principles of automation, rapid feedback, focus on testing throughout the process, collaboration, and consistent release practices. This provides a great opportunity for improved security, but it requires security tools that work well with pipeline-oriented DevOps processes.

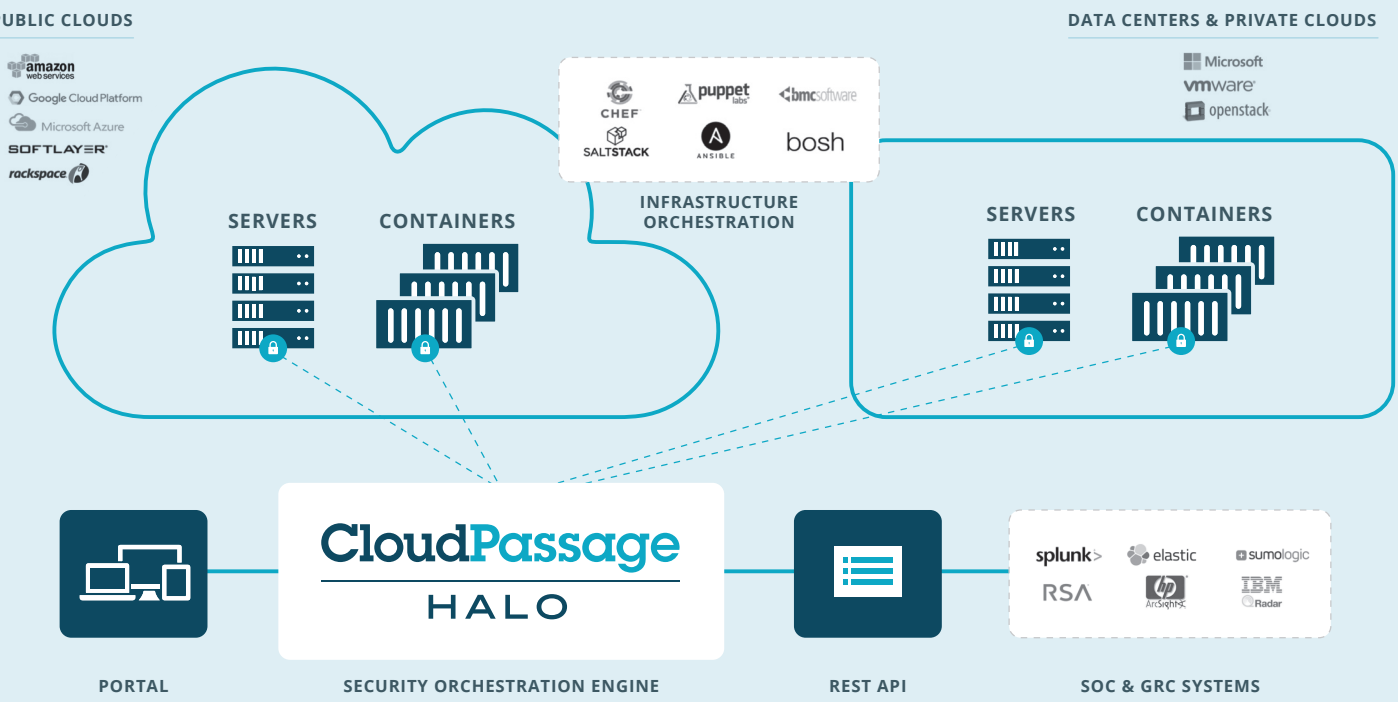
Traditional server security tools are not built for automated toolchains. They typically require manual configuration before they can be put into production. This slows down the DevOps cycle and increases the risk of configuration errors.

While some of the DevOps tool sets include basic configuration security checks, this feature by itself is just a small part of all the security controls that most enterprises need.

THE SOLUTION: CLOUDPASSAGE HALO

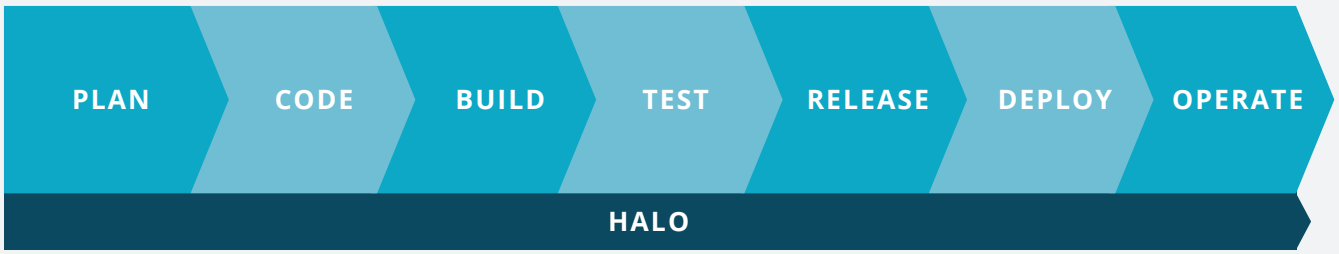
CloudPassage® Halo® solves these problems by integrating security right into the DevOps pipeline, ensuring every workload is protected from the start. Halo uses an ultra-lightweight agent that is installed automatically through your build management, configuration management and continuous integration tools like Jenkins, Chef, Puppet, Ansible, SaltStack or BOSH. The workloads can be anywhere: public cloud providers, private clouds or traditional data centers. And since Halo is delivered as a service, it deploys in minutes and scales on-demand.

With Halo, DevOps engineers can automatically verify new masters against security policies at build and test stages, and security teams get instant visibility to workloads from the moment they are deployed into staging and production. Halo lets you define security policies based on industry best practice templates. Policies are defined for logical server groups, so new workloads are automatically protected as soon as they are created, wherever they are.



Halo works across any cloud or virtual infrastructure: public, private, hybrid, multi-cloud or virtualized data center — including bare metal.

HALO AT BUILD AND AT RUN TIME



1

Plan
Define security policy and benchmarks for each workload group

2

Build & Test
Catch SVA & CSM issues, generate FIM baselines

3

Deploy
Apply production policies to systems automatically

4

Operate
Continuously feed Security Ops, Compliance and Governance

HOW HALO WORKS

AUTOMATED AGENT DEPLOYMENT

Halo ultra-lightweight agent that can be deployed automatically via scripts or popular orchestration tools that you are probably already using, such as Chef, Puppet, Ansible, SaltStack, Jenkins, BOSH, etc.

BROAD RANGE OF SECURITY CONTROLS

Halo provides foundational host security controls for Linux and Windows workloads and servers, including Software Vulnerability and Configuration Security management, Server Account Management and access controls, Host Firewall Orchestration and Traffic Discovery & Visualization, File Integrity Monitoring and Log-based Intrusion Detection.

AUTOMATED VISIBILITY

Halo agent automatically connects to the Halo Orchestration Engine every 60 seconds, giving you visibility to systems that are newly created or auto-scaled.

INSTANT SCALABILITY

Halo is delivered as a service so it can scale as rapidly as your IT automation systems can provision new workloads.

AUTOMATED POLICY ASSIGNMENT

Halo applies the appropriate policy to each system based on tags that define the application and operating system. These policies follow the workload no matter where the workload physically resides—data center, public cloud, private cloud.

FULL API

The CloudPassage Halo platform supports an open, RESTful API that makes it easy to integrate with a range of security and monitoring systems.

HOW HALO IS DIFFERENT

1

Halo is fast. Installation of agents can be totally automated.

2

Halo is portable. It works in any environment—data centers, private clouds and public clouds.

3

Halo agents are extremely lightweight. All security analytics are conducted on CloudPassage's servers, instead of your servers and cloud workloads.

4

Halo works with every kind of workload— servers, cloud workload instances, containers.

5

Halo is scalable. Our customers routinely deploy Halo to over 10,000 workloads in just a few days.

ABOUT CLOUDPASSAGE

CloudPassage® Halo® is the world's leading agile security platform that empowers our customers to take full advantage of cloud infrastructure with the confidence that their critical business assets are protected. Halo delivers a comprehensive set of continuous security and compliance functions right where it counts—at the workload. Our platform orchestrates security on-demand, at any scale and works in any cloud or virtual infrastructure (private, public, hybrid or virtual data center). Leading enterprises like Citrix, Salesforce.com and Adobe use CloudPassage today to enhance their security and compliance posture, while at the same time enabling business agility.

SB_DEVOPS_08112016