PROTECT SERVERS AND CLOUD-BASED WORKLOADS FROM ATTACK

AUTOMATED PROTECTION — ANYTIME, ANYWHERE.

THE PROBLEM

To protect servers and cloud-based workloads from attack, enterprise security managers must:

- Have visibility to all important workloads, no matter where they are located
- Ensure that the workloads are properly configured
- Ensure that no major software vulnerabilities exist in the operating system or application framework
- Carefully manage who can login to each workload and what functions they can perform

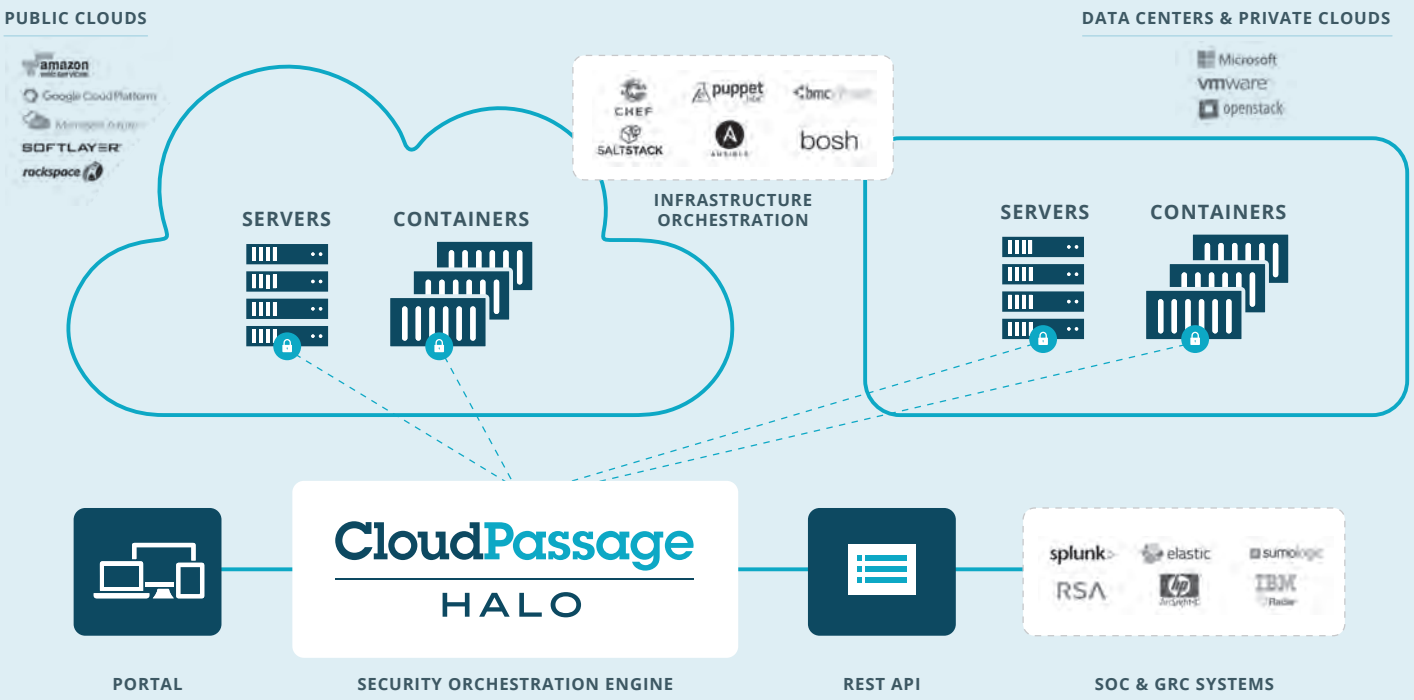
These things are hard to do in modern compute environments that are highly elastic, dynamic and automated. Why? Because traditional security tools use heavy agents which sap server resources, and they need to be manually deployed and configured on new systems as they are spun-up or auto-scaled. Security systems that use external scans are also problematic because they need to be coordinated with cloud providers.

THE SOLUTION: CLOUDPASSAGE HALO

The CloudPassage® Halo® agile security and compliance platform solves all of these challenges. Halo is unique because it provides continuous visibility and protection delivered as a service, so it's on-demand, fast to deploy, fully automated and works at any scale. Halo uses an ultra-lightweight agent that can be deployed automatically on servers in any infrastructure: public, private, hybrid, multi-cloud or virtualized data center.

CloudPassage Halo automatically applies your security policies based on the workload type, regulation category or sensitivity of the data. Halo scans for software vulnerabilities against a number of sources, including the National Institute of Standards and Technology (NIST) database of Common Vulnerabilities and Exposures (CVE). Halo assesses the configuration of your workloads by comparing them to standard benchmarks from the Internet Security (CIS) Benchmarks and Defense Information Systems Agency (DISA). You can also develop your own custom configuration checks using Halo's built-in policy editor. Halo can scan thousands of servers and cloud-based workloads in minutes to maintain continuous exposure awareness in the cloud.

With open integration APIs, the security posture data flows to popular GRC systems and workflows can be automated, and setting up rich data feeds into any existing SIEM or monitoring systems is quick and straightforward.



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

THE POWER OF HALO

Get instant visibility
Workloads are tracked and reported on instantly and automatically.

Reduce costs & improve efficiency
Eliminate manual processes — streamline and automate workflows.

Leverage industry best practices
Apply templates from CIS and DISA for configuration security.

Automatically discover vulnerabilities
Scan all systems for software vulnerabilities at a cadence that works for you.

Consolidate multiple products
Combat tool fatigue with a single platform that can replace point products.

Scale on demand
Non-intrusive, agent-based model scales without breaking a sweat.

Stay flexible
Deploy seamlessly across any cloud or virtual infrastructure.

HOW IT WORKS

AUTOMATED AGENT DEPLOYMENT

Halo uses an 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.

AUTOMATED VISIBILITY

Halo agent automatically connects to the Halo Orchestration Engine every 60 seconds, giving you instant visibility to systems as they are 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.

BROAD RANGE OF PRE-BUILT CONFIGURATION CONTROLS

Halo includes pre-built configuration policies spanning a wide range of operating systems (Linux, Windows) and applications. Configuration policies include benchmarks from Center for Internet Security (CIS) and Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs).

SOFTWARE VULNERABILITY ASSESSMENT

Halo scans for vulnerabilities in your packaged software rapidly and automatically, across all of your cloud environments – precisely where traditional vulnerability scanning products are unable to operate effectively. With Halo, thousands of workloads can be assessed in minutes, helping you to maintain continuous exposure awareness in the cloud.

SERVER ACCESS MANAGEMENT

Halo evaluates who has accounts on which servers, what privileges they operate under, and how accounts are being used. Halo provides a single online management console where you can monitor your servers in public, private and hybrid cloud environments. The convenient user interface makes it easy for you to identify accounts that should have been removed.

FULL API

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

HOW IT 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 is comprehensive.** It includes a broad range of security controls at both the host and the network levels.
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.