YOUR SERVERS HAVE BEEN COMPROMISED. HOW CAN YOU TELL?

AUTOMATED COMPROMISE DETECTION — ANYWHERE, AT ANY SCALE.

THE PROBLEM

Once you have properly configured a server or cloud workload and hardened it against an attack, it's important to keep it that way. You need to be alerted if an important file changes, or a user account has been added, or an important function like the firewall has been turned off. Such a change might have been made unintentionally by someone on your staff, or it might have been made by a malicious attacker.

The high rate of change of modern server infrastructure poses a challenge. Many products on the market that monitor servers to detect when they have been compromised were designed for traditional data center environments. They utilize heavy agents which sap server resources. And they don't automatically deploy on new workloads the moment they are spun up. Each agent needs to be separately provisioned and configured. Security becomes a bottleneck, which slows down the business.

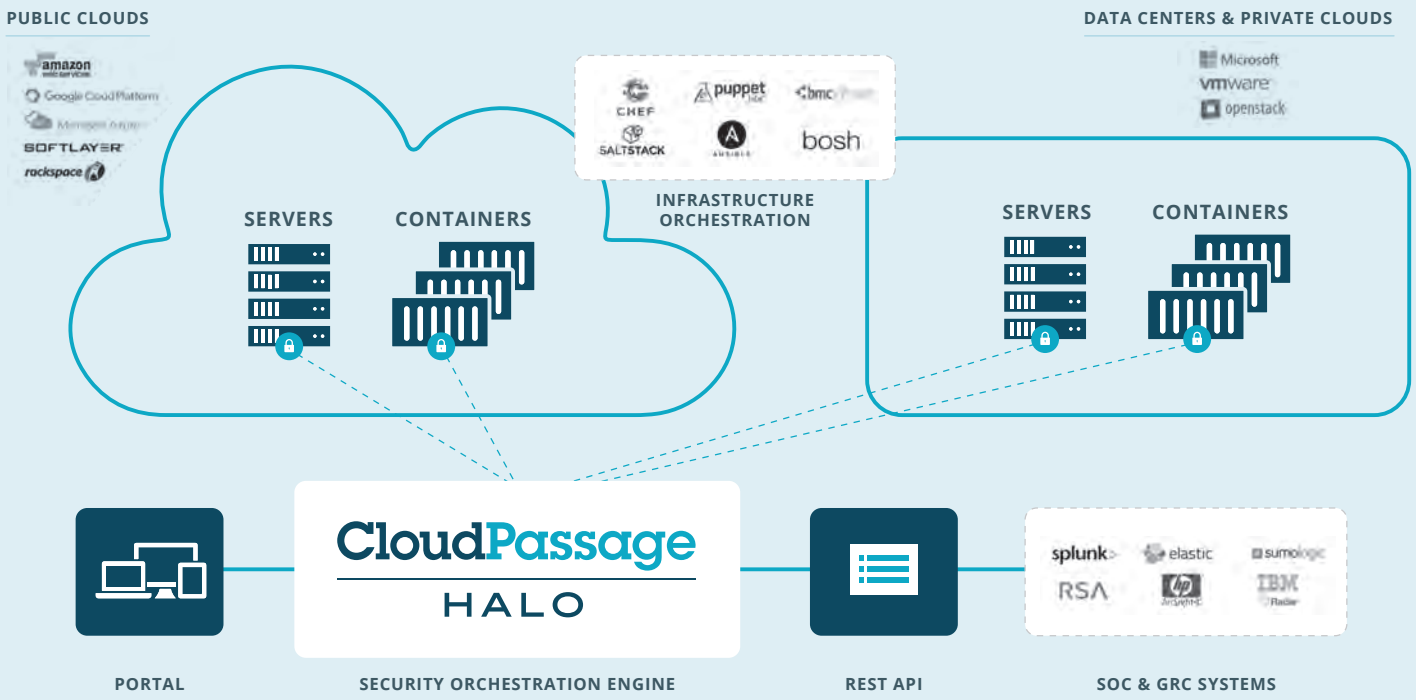
THE SOLUTION: CLOUDPASSAGE HALO

The CloudPassage® Halo® agile security and compliance platform is delivered as a service, so it works efficiently in modern compute environments. 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—including bare metal. With Halo, you have visibility to workloads from the moment they are created.

Halo includes file integrity monitoring (FIM) to detect if anything has changed on your servers and cloud workloads. Halo FIM has been optimized to work in both static and elastic environments. As each server is built, Halo can automatically create a baseline record of files and directories, which saves time and produces fewer false-positives than traditional FIM systems.

Halo also monitors server log files for important events that could indicate that your system has been compromised. A key advantage of log-based intrusion detection vs. other techniques is its light impact. Because only specific, high-value events are monitored by Halo, the massive gathering, storage, and analysis of voluminous events from hundreds or thousands of log files is avoided.

Halo includes a rich set of integration API's which can feed critical event data from Halo into your existing SIEM or other SOC monitoring systems.



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.

Verify system & data integrity
Apply and verify all required controls are in place.

Automate compliance workflows
Integrate with your existing tools and processes seamlessly.

Generate & track audit logs
Ensure all critical activities are archived and readily available.

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

Detect compromise
Scan all systems for signs that they have been compromised either because a file has been altered or an unexpected event has occurred.

Stay flexible
Deploy seamlessly across any cloud or virtual infrastructure.

HOW IT WORKS

FILE INTEGRITY MANAGEMENT
Monitor cloud workloads for unauthorized or malicious changes to important system binaries and configuration files, with full support for automation and multiple baselines.

LOG-BASED INTRUSION DETECTION
Halo includes pre-built log inspection policies that detect intrusions for a variety of operating systems (Linux, Windows). You can also easily add your own rules to the pre-built templates.

AUTOMATED AGENT DEPLOYMENT
Halo uses an ultra-lightweight agent that can be deployed automatically via automated scripts or via 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 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 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.

© 2016 CloudPassage. All rights reserved. CloudPassage® and Halo® are registered trademarks of CloudPassage, Inc.
SB_COMPROMISE_08112016