SOLUTION OVERVIEW

CLOUD WORKLOAD SECURITY

Bottom line: If you're in IT today, you're already in the cloud.

CloudPassage

As technology becomes an increasingly important element of business success, the adoption of highly elastic, highly scalable, and highly performant application stacks is no longer a choice – it's a necessity. The majority of new applications built for today's enterprises are typically developed and deployed on public clouds such as Amazon Web Services (AWS) and Microsoft Azure. These apps are predominantly new web apps or analytics apps – designed for direct-to-customer interactions, big data analytics, or for rapidly opening new lines of business/new ways to market — IoT, mobile, etc.

These cloud-native, "modern" applications have some foundational characteristics:

- Unlike your legacy apps, these applications are "assembled" from stateless microservices packaged in ephemeral virtual machines or containers and a combination of data, messaging and/or notification services
- The application is deployed through an automated CI/CD pipeline. They utilize infrastructure automation and orchestration tools to speed deployment without manual intervention - think Infrastructure-as-code/automated everything. Unlike your legacy apps which were released once in few months these "modern" applications change several times a week if not daily.
- The application is often hosted on modern but shared infrastructure like public clouds.

And if you're not there yet – you will be

For many enterprises, the cloud is a more aspirational goal. Rather than starting fresh with new apps, they are focused on migrating existing apps from their on-prem data center (could be virtualized infrastructure, colo or any dedicated infrastructure) or from a shared service environment to the public cloud. This has significant cost savings benefits in terms of facilities, personnel, and energy – not to mention the convenience of adding new resources on-demand.

KEY SECURITY & COMPLIANCE CHALLENGES

The attack surface has expanded

Until now, the standard approach for protecting an enterprise's most prominent applications has been to host them in a siloed (virtualized) infrastructure with network perimeter security around it. This is a flawed approach even when applied to relatively static and predictable private data center environments. In the public cloud this approach is suicidal. In a shared infrastructure, besides securing your perimeter, you have to secure each host, cloud resource for your application.

Security can't keep up

Unlike legacy apps, a cloud-hosted application is designed for higher rates of change. The application scales up and down automatically based on load; new features and functionality is delivered weekly if not daily; and the app itself is typically deployed automatically. A manual security approach that is bolted on at the end of the deployment cycle, while appropriate for legacy apps in data center, will not be able to keep up with modern applications running on modern infrastructure or the DevOps teams charged with their creation, care, and feeding.

Compliance is even more complex

The combination of a new and expanded attack surface, the change rate inherent in the application development, deployment, and environment, and the lack of a dedicated and parameterized infrastructure causes new compliance challenges that you will have to adapt to.

THE 4 KEY STEPS FOR MASTERING THESE CHALLENGES

There are 4 key steps for properly securing your cloud workloads without sacrificing speed, flexibility, or overall manageability.

1. Secure the core

Go from a perimeter-security-and-soft-core approach to a harden-the-core approach: Secure your applications by hardening every single node of your application. Broadly speaking, the attack surface of an application is largely composed of its data and the commands in and out as well as the code that actually processes the data and its associated commands. Here are some practical guidelines for reducing the attack surface for your applications:

- **Vulnerability scanning:** Make sure your application nodes are free of known vulnerabilities. More than 80% of cyberattacks can be prevented by good cybersecurity hygiene and the first step towards that is keeping your servers free from any critical vulnerabilities.
- **Secure configuration:** Poorly configured applications or operating system controls allow attackers to take control of your system and propagate to other systems and environments.

Define policies for hardened and secure configurations and ensure your applications are compliant with these policies. Leverage CIS benchmarks (industry standard or your own internally developed rules).

- **Access control:** Lock down access control privileges for your application systems. Follow the principle of least privilege. Discourage root or sudo access for any personnel. MFA is highly recommended

2. Continuously monitor for IoCs and policy violations

It's no longer appropriate to set policies, controls, and checks and then move on. In the cloud, you must continuously monitor your systems, since vulnerabilities can be introduced and exploited within seconds – with potentially disastrous results.

In the public cloud you now must continuously scan for:

- New vulnerabilities announced since your servers were initially deployed.
- Critical vulnerabilities that are still not patched
- Configuration policy violations
- File system integrity violations
- Monitor load balancer logs, applications logs, database transaction logs, network flow logs for any unwanted or non-compliant activity
- Unauthorized access to root level accounts

3. Shift left

Move your control implementation and security audits to be as early as possible in your development/deployment cycles. In a public cloud infrastructure it takes minutes– if not seconds – for a poorly secured server to become compromised. Therefore, it is definitely best practice for your application nodes to be secured prior to deployment in production environments. You wouldn't

deploy your application without completing your functional, integration, and user acceptance testing (UAT). Add security and compliance assessment to you test matrix early and prevent huge problems later.

4. Automate Everything – Especially Security

Business and development teams are both moving fast. They have automated deployments for the full application stack, including the underlying infrastructure. The build and testing of these applications have also been automated. In this automated world, security testing, implementation, and monitoring, have to all be automated. In the absence of security automation, businesses have to face a trade off between security vs time to market. Which is really not a trade off at all when you consider the risk and damage to a business's reputation and customer trust that a security breach can cause.

HALO: MASTERING THE 3 CHALLENGES – AUTOMATICALLY

Halo is the industry-leading solution for cloud workload security. It not only offers the most comprehensive set of automated security and compliance monitoring capabilities, but also enables them from a highly automated, scalable, and mature cloud-scale platform.

1. Halo assesses your workload attack surface

- Halo automatically identifies vulnerable packages in both your Linux and Windows servers.
- Halo enables you to define and monitor your configuration hardening standards. Halo comes with several policy templates that you can clone and customize to your specific organization's needs. Leverage our out of the box integration with industry leading configuration management tools for automated remediation of policy violations.
- Halo manages and monitors your local access controls on each server.

2. Halo detects policy violations and undesirable activities

Halo employs a continuous monitoring model and will detect any configuration drift or changes in your workload attack surface.

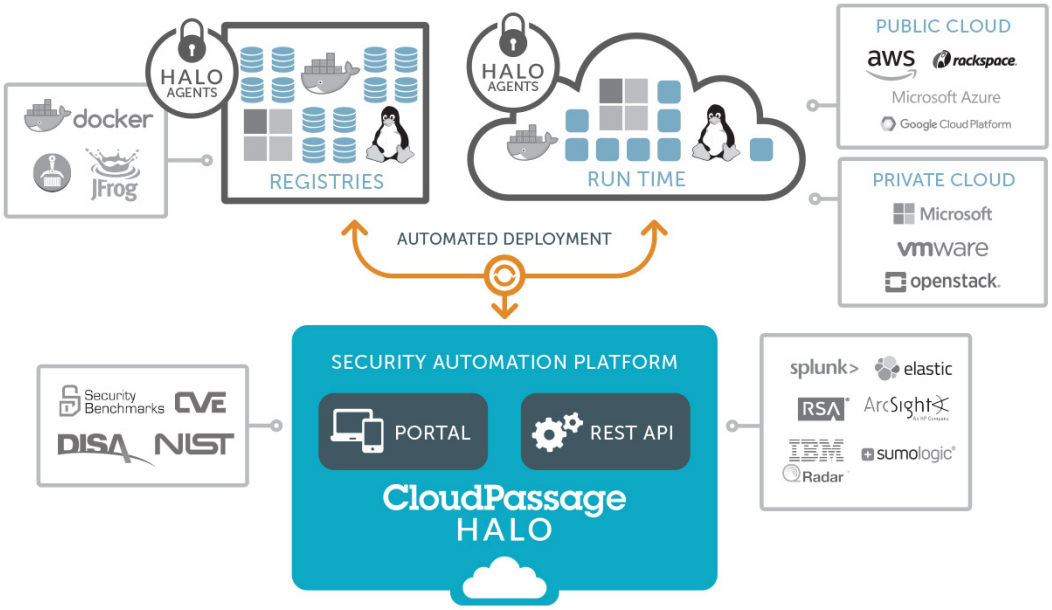
Halo also includes a comprehensive set of host based intrusion detection capabilities, watching as well as alerting on several critical aspects of your server workloads including:

- File system integrity
- Investigating and auditing various log file for security-related events of interest.
- Privileged access auditing and monitoring
- Network traffic flow monitoring

3. Halo automates security

Halo's security automation capabilities allow you to:

- Automate security assessment as part of infrastructure provisioning. A thin micro-agent inserted into a gold image or deployed in servers using a client's existing deployment processes will deliver a comprehensive assessment in less than 90 seconds.



- Automate security workflows and implement a closed-loop security model. Halo comes with full REST APIs, which can be used to integrate security events and alerts into your existing SIEM or orchestration workflows. Halo implements a continuous monitoring model and automatically resolves issues that have been successfully remediated.

Now application owners do not have to chose between speed and security. They can have both.

WHAT'S UNIQUE ABOUT HALO'S SOLUTION?

- **Comprehensive security capabilities** – while many vendors claim to provide a full stack of security monitoring and alerting tools, only Halo delivers fully integrated functionality across the development and deployment stack. Rather than purchasing and integrating multiple modules Halo delivers single agent/single console visibility to the critical security functionality that enables you detect, protect, and remediate threats and vulnerabilities to your cloud infrastructure at speed and at scale.
- **Infrastructure agnostic** – Halo supports the full cloud application stack. This is critical as today's modern cloud applications are assembled from multiple services – orchestrated and managed by multiple services running in a multiplicity of environments. Halo delivers visibility across all levels of the stack. More importantly Halo is the only cloud security solution in the market that can be used both for virtualized

and container/microservices environments. As containers become an increasingly popular way to develop, package, and deploy apps, proper security hygiene is as critical for those environments as it is for virtualized ones. While many vendors can claim to support different public cloud vendors such as AWS or Azure, only Halo can deliver visibility and control across the entire cloud application stack – including containers and microservices.

- **Halo was built for DevSecOps.** Halo offers one of the industry's most complete REST API enabling enterprise security, IT, and DevOps teams to seamlessly integrate security into their DevOps processes, CI/CD toolchains, and infrastructure automation solutions. Halo also features a Python SDK that acts as a wrapper to the REST API. It handles authentication, pagination and decreased snowflakes by promoting reusable code. The API itself is fully bi-directional. It can use data from Halo to integrate with third-party products (e.g. open a ticket in Jira or ServiceNow, export data to common SIEMs or create an Ansible playbook to remediate vulnerable packages). Halo is also used by DevOps teams to automate configuration security monitoring scans in their build pipeline. Finally, the API can pull data into Halo such as security policies, e.g. a file integrity or configuration security policy.

ABOUT CLOUDPASSAGE

Founded in 2011, CloudPassage® was the first company to obtain a U.S. patent for universal cloud infrastructure security and has continued to innovate cloud security automation and compliance monitoring for application development and deployment. CloudPassage Halo® is an award-winning workload security automation platform, delivered as a service, that provides universal visibility and continuous protection for data centers, private/public clouds and containers. Halo deploys in minutes and scales effortlessly. The platform integrates with automation and orchestration tools such as Puppet and Chef, as well as CI/CD tools such as Jenkins. Today, CloudPassage Halo secures the infrastructure of leading global finance, insurance, media, ecommerce, high-tech service providers, transportation and hospitality companies.

www.cloudpassage.com | 800.215.7404

CloudPassage