CloudPassage

SOLUTION BRIEF

CLOUDPASSAGE HALO INTEGRATION WITH SUMO LOGIC

Automated security for workloads, containers, and servers

Introduction

CloudPassage® Halo® automates workload security and compliance from development to deployment across clouds and data centers, servers, and containers – at speed and scale. Halo instruments a broad set of security controls to secure all types of servers and workloads including virtual machines, containers, public and hybrid clouds (AWS, Azure, Google Compute Engine, etc.).

CloudPassage and Sumo Logic have partnered to deliver a real-time security analytics and incident response solution for modern compute environments. Through this integration, IT Ops, DevOps, and security teams can share a comprehensive, real-time view of their security and compliance postures while rapidly detecting and containing attacks by correlating CloudPassage data with other data streams in Sumo Logic, including threat intelligence data.

Business challenge

Every business is becoming a software business. To gain market advantage, enterprises are adopting high-velocity application development and deployment technologies and processes such as DevSecOps, containers, and public cloud. In this new model, on-demand elasticity, scalability, and resiliency play a huge role. Unfortunately, traditional security, compliance and monitoring tools don't work well in these modern environments. They slow down the business and frustrate every stakeholder.

The solution: Sumo Logic + CloudPassage

Sumo Logic and CloudPassage have partnered to provide an advanced security monitoring and closed loop incident response solution for modern compute environments. CloudPassage Halo has been specifically designed to secure workloads in high-velocity environments such as DevOps, containers, and public or private clouds. Sumo Logic can ingest logs from CloudPassage Halo and correlate those logs with other sources such as threat intelligence, infrastructure, and application logs. The result is more complete situational awareness into security and compliance posture while removing blind spots.

Benefits

Both CloudPassage Halo and Sumo Logic are delivered as SaaS applications, so they are on-demand, fast to deploy, fully automated, and work at any scale. Benefits of the joint integration include:

- **Stronger security**

CloudPassage provides comprehensive security assessments for cloud based workloads. This security assessment includes evaluating cloud workloads for known vulnerabilities, monitoring the OS and application for configuration hardening standards, file system monitoring, and more. IT security managers can integrate this data into their Sumo Logic deployment and identify exposures and threats in their cloud environments. Additionally, this integration can help them detect "indicators of compromise" (IOC) for their cloud workloads.

- **Continuous compliance**

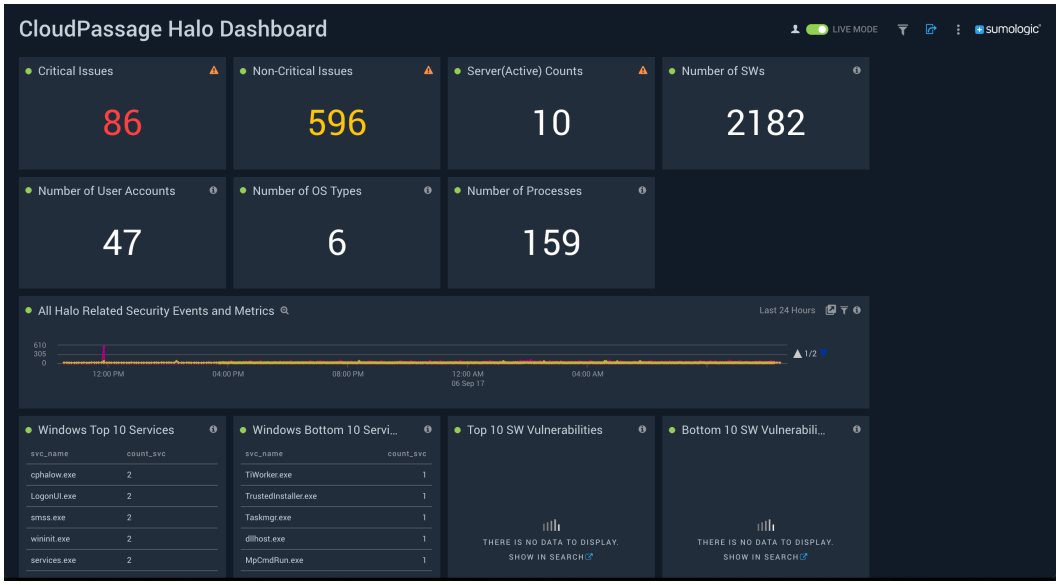
CloudPassage enables continuous compliance for both stateful long running workloads and stateless, ephemeral workloads. Halo can detect and provide the security status of workloads and containers within 90 seconds of spinning up, providing critical protection for elastic resources.

- **Enhanced DevOps**

The combination of operational and security data from Sumo Logic with workload security data from CloudPassage is now available via a single pane of glass to multiple stakeholders. CloudPassage provides fast feedback to developers early in the CI/CD pipeline regarding software vulnerabilities, which saves time and money.

- **Faster incident response**

A single system for continuous intelligence into your machine data with on-demand elasticity Sumo Logic can be a single source of truth for operations, security, and developer teams. It reduces incident response time as well as risk of data breach by analyzing logs and surfacing indicators of compromise using machine learning operators. Faster detection translates into faster containment and eradication of malware and ransomware.



ABOUT CLOUDPASSAGE

Founded in 2011, CloudPassage® was the first company to obtain a U.S. patent for universal cloud infrastructure security and has been a leading innovator in cloud security automation and compliance monitoring for high-performance application development and deployment environments. CloudPassage Halo® is an award-winning workload security automation platform that provides universal visibility and continuous protection for servers in any combination of data centers, private/public clouds and containers. The Halo platform is delivered as a service, so it deploys in minutes and scales effortlessly. Fully integrated with popular infrastructure automation and orchestration tools such as Puppet and Chef, as well as leading CI/CD tools such as Jenkins, Halo secures the enterprise where it's most vulnerable—application development and workload deployment. Today, CloudPassage Halo secures the critical infrastructure of many of the leading global finance, insurance, media, ecommerce, high- tech service providers, transportation and hospitality companies.

ABOUT SUMO LOGIC

Sumo Logic is the leading cloud-native, machine data analytics platform that delivers continuous intelligence across the entire application lifecycle and stack. More than 1,500 customers around the globe rely on Sumo Logic for the analytics and insights to build, run and secure their modern applications and cloud infrastructures. With Sumo Logic, customers gain a service-model advantage to accelerate their shift to continuous innovation, increasing competitive advantage, business value and growth.

CloudPassage

www.cloudpassage.com | 800.215.7404