CloudPassage

CASE STUDY

XERO CHOOSES CLOUDPASSAGE HALO FOR WORKLOAD SECURITY AT DEVOPS SPEED

Executive summary

Xero chose CloudPassage Halo to protect their workloads running in AWS EC2 and to help them meet compliance requirements. They chose Halo because the product was highly automated, integrated with their rapid DevOps production pipeline, and provided a broad range of important security controls.

About Xero, Inc.

Xero develops cloud-based accounting software for small and medium-sized businesses. They have over 860,000 subscribers in more than 180 countries, and their software accounts for over $1 trillion of incoming and outgoing transactions per year.

Challenges

In 2014, after several years of strong growth, Xero knew that they needed some new technologies to support their next wave of growth. Specifically, Xero needed technologies that would enable:

- **Fast scalability.** They needed an operating environment that could scale up and down as market demand for Xero's SaaS-based accounting software changed.
- **Fast infrastructure deployment.** They wanted to reduce the amount of time it took them to build new IT infrastructure, from weeks (to purchase and deploy new hardware) to minutes.
- **Automated security.** They needed a security system that would integrate with their DevOps processes and tools and which could also be managed by the actual developers who were writing Xero's accounting software products.

"The old adage was 'You can go fast, or you can be secure'. Now that we have CloudPassage Halo, we can be both fast and secure."

Xero solved the first two challenges by moving their IT infrastructure from a traditional outsourced datacenter environment to a public cloud environment—Amazon Web Services.

Xero found the last challenge was a bit harder to solve. Most IT security products on the market would not perform efficiently in a fast-pace DevOps environment. Xero's lead security architect, Aaron McKeown, wanted to provide Xero's DevOps teams with a set of strong security controls that could be baked into their DevOps processes, not bolted on after the fact.

So McKeown set out to find a security system that was fully automated. By 2014, all product teams at Xero had been transformed into agile product development teams. They were able to run so fast that they were able to release over 800 new features within a single year. Keeping up with this pace required a security system that could be automated as part of Xero's continuous integration and continuous deployment (CI/CD) processes. Xero's typical practice was to recycle compute resources (hosts) for any change, including software releases. This means each AWS EC2 instance had a typical lifespan of 24 to 48 hours. They needed a fully automated security system that could protect every AWS EC2 instance from the moment it was created to the moment it was destroyed, all while maintaining a complete audit trail of all of it.

Visibility was also very important to McKeown. Xero had over 45 different AWS accounts, hundreds of developers, thousands of servers, and things that changed daily, hourly, or even sometimes within minutes.

Aaron McKeown said: "Our developers go fast. My job is to provide security that goes just as fast, because otherwise it would be a bottleneck and would slow the business down."

In addition to speed and automation, McKeown was looking for a security system that aligned with the following operating principles:

- **Security on demand.** McKeown wanted a security product that aligned with the pay-for-what-you-use pricing model that AWS charged them for compute resources.
- **Full API access.** McKeown wanted to enable the CI/CD tools that the DevOps teams were using. He wanted the variety of their chosen tools to be able to automate not just the installation of the security agents onto new workloads but also configuration of the security policies themselves. McKeown did not want to have to tell Xero's DevOps teams that they would have to log into a separate security console to make manual changes to policies or administrative commands.
- **Connectivity** to other tools that Xero operated such as their security information and event management (SIEM) system.

How CloudPassage helped

After a lengthy search for the right security tool, McKeown chose CloudPassage Halo. Halo met all of McKeown's requirements, and then some. Built for speed, Halo is fully automated, everything from installation of agents all the way through to policy assignment, alerting ,and reporting.

- **Instant scalability.** Halo's architecture supports elastic operating environments and can scale just as fast as your operations teams can deploy new workloads.
- **Full API access.** McKeown was able to realize his dream that developers would never need to log into the Halo security console. All operations could be done programatically through the API.
- **Broad range of security controls.** Halo includes several different kinds of security controls that allowed McKeown to minimize the software attack surface, reduce the network attack surface, ensure that Xero's workloads have not been compromised, and maintain compliance with PCI data regulations.
- **SIEM integration.** Halo is able to transmit all of the information that it learns about the security posture of Xero's workloads to Xero's SIEM which is Splunk.

> "At Xero we operate in an agile environment, things move quickly and there is a great deal of change so it's important to monitor, detect, and defend at the Host level. Halo is central to our overall security architecture and strategy."

"Elasticity and automation are key. We recycle our servers frequently and the security automation tooling needs to be able to handle that, Halo meets that requirement."

- **Integrates with DevOps.** Because Halo is completely automated, the DevOps workflow that allow Xero to achieve competitive strategic advantage remain unencumbered.

Results

- **Halo is easy to use.** Working with CloudPassage, the Cloud Security Team at Xero quickly built up knowledge of the Halo platform, which was then turned into patterns and reference materials for the Xero product team. As a result, Halo was deployed as standard for all EC2 instances.
- **Xero has expanded the scope of deployment.** Initially, Halo was deployed to core platform systems, but as product teams migrated to AWS the scope of deployment was increased.
- **Xero worked closely with CloudPassage to build a strong relationship** and to achieve the outcome they needed. This was a shared journey for Xero and CloudPassage.

ABOUT CLOUDPASSAGE

Founded in 2010, 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 cloud security and compliance automation platform that provides universal visibility and continuous protection for infrastructure, servers, and containers in multi-cloud environments. 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.

CloudPassage

www.cloudpassage.com | 800.838.4098