anchore

CASE STUDY

Scanning at Scale Brings Container Security Issues to the Forefront

INTRODUCTION

Established in 2010, CloudBees is a provider of continuous integration/continuous delivery (CI/CD) tools for customers in the commercial and public sectors. Based on Jenkins open source, CloudBees CI is considered an industry-standard in the DevOps community.

CloudBees has about 500 employees worldwide, most of whom work remotely. The product development (engineering and product management) organization is about 167 employees. Product security and Jenkins security are two separate teams in this organization.

The product security team builds libraries or tools for other teams to consume and easily integrate into their pipelines. By lowering the effort needed to integrate scanning in their environment, teams could incorporate it easily into their toolchains and development life cycles.

CLOUDBEES AT A GLANCE

San Jose, CA | www.cloudbees.com

INDUSTRY Software

CHALLENGES
- Industry concerns around container security in Docker images
- Wanted a solution that enabled their security team to resolve Docker container security issues proactively
- CloudBees allows their teams to be flexible in their choice of parent Docker images, thus wanted more governance to ensure security

SOLUTIONS
- Provide container governance across projects
- Lower the effort to integrate container scanning in the DevOps toolchain
- All CloudBees products that generate Docker container images have to use Anchore Enterprise as per internal corporate policy

RESULTS
- New container governance model for the company born from a greenfield project
- Improved transparency into container security and compliance issues in their container supply chains corporate-wide
- Capability to support customers who work in government, financial services, healthcare, and other industries with compliance mandates

Challenge

Several CloudBees customers raised concerns about the dire state of security within their Docker container images. Thus it became essential for them to have a policy feature to secure their container images. During this time, CloudBees began working with the United States Department of Defense (DoD), which currently uses Anchore Enterprise. The DoD requested CloudBees to validate their solutions against their policies proactively.

At a corporate level, CloudBees wanted to implement consistent standards for Docker container security across different products. Teams had been choosing their own parent Docker images, which had the potential to grow into a security challenge of its own.

The team decided that a best-in-class solution was necessary because CloudBees engineering management wanted to keep the product development organization focused on delivering innovation for CloudBees customers - not reinventing a wheel that was already well-made. This consideration made their "build vs. buy" decision easy.

"Scanning at scale can surface issues and help to identify things such as prioritizing specific scans over others for immediate examination."

Solution

Many on the CloudBees team were Anchore open source users and knew of its efficacy. These engineers advocated for an Anchore Enterprise solution. Their positive Anchore open source experience, the product's ease of use, and a common customer in the US DoD made Anchore Enterprise a natural choice. The Anchore Policy Engine was also attractive to the CloudBees team.

The key criteria for selecting Anchore Enterprise was its policy engine and the role-based access control (RBAC) provided within the solution. Additionally, CloudBees requires that all software vendors possess a well-made API to integrate third-party tools into software pipelines.

CloudBees considered a solution from Twistlock before selecting Anchore Enterprise. However, Anchore Enterprise made better sense and was more suited to the use-cases at hand.

Results

All CloudBees software delivery pipelines that generate Docker container images now have to use Anchore Enterprise, per internal product security policy. Findings are consolidated in a central vulnerability repository for teams to triage, review, and fix within internal SLA time.

Both security and policy findings that Anchore identifies are automatically uploaded with the help of CloudBees internal tooling to DefectDojo, an open-source application vulnerability management tool in which CloudBees is actively involved.

CloudBees experienced a rise in the number of scan findings, showing the power of deep scanning using Anchore Enterprise. This new level of transparency into their container security positions allows them to remediate critical issues more quickly than before using Anchore Enterprise.

Implementing Anchore Enterprise was a greenfield project for CloudBees. It led to a new Docker image governance model that reduced base images to better secure products that their developers build with containers.

CloudBees is now using Anchore Enterprise to bake in the right policies to support their customer needs across many different industries and government.

About Anchore

Based out of Santa Barbara, California, and Northern Virginia, Anchore provides a set of tools that provide visibility, transparency, and control of your container environment. Anchore aims to secure container workloads at scale without impacting deployment velocity. Our Anchore Professional Services team helps users leverage Anchore to analyze, inspect, scan, and apply custom policies to container images within custom CI/CD pipelines.

anchore

info@anchore.com

anchore.com