anchore

CASE STUDY

Ocrolus Elevates Security Posture With Container Vulnerability Scanner & Increases Overall SRE Team Productivity

INTRODUCTION

Named the 30th fastest-growing private software company in America on the Inc. 5000, Ocrolus' fintech intelligence automation platform analyzes financial documents with more than 99 percent accuracy for customers in the banking and financial services sector, while transforming documents into actionable data.

Since its founding in 2014, Ocrolus has experienced impressive growth and revenue gains, which have allowed it to expand service offerings to include built-in fraud detection and analytics, that enable its customers to make smarter and faster business decisions with unprecedented precision.

OCROLUS AT A GLANCE

New York, New York | www.ocrolus.com

INDUSTRY	FinTech | Infrastructure | Data Intelligence
CHALLENGES	• Organization compliance policies • Default-deny whitelisting process • Lack of insight for audit & non-technical teams • Container vulnerability scanning
SOLUTIONS	• Automate whitelisting • Complete vulnerability & compliance reporting • Improve stakeholder accessibility
RESULTS	• Transparent communication around compliance • Visibility on reporting for auditors • Increased productivity through automation • Customer requirements satisfied

Challenge

Ocrolus' site reliability engineering (SRE) team is responsible for adhering to the organization's compliance policies to ensure specific security and auditable controls around the software development lifecycle. This encompasses code review, security scanning as part of development and continuous monitoring of production.

Observing strict compliance protocols to secure personal and financial identifiable information, as well as provide visibility to the internal compliance department on security outputs was imperative. Equally important was the ability to provide transparency around the SRE team's whitelisting process, while maintaining visibility to other Ocrolus business groups that weren't directly involved with solution implementation. And lastly, needing continuous scanning on newly published vulnerabilities for deployed applications was critical.

> ***"Anchore has brought a tremendous amount of value to Ocrolus."***

Solution

A longtime open-source Anchore Engine user, the Ocrolus SRE team recognized the tremendous value that Anchore Engine brought to the organization early on. The team's decision to upgrade to Anchore Enterprise was spurred by the need for transparent communication with organizational stakeholders around compliance; and by the importance to increase productivity and streamline other processes, such as whitelisting, among others.

Adding the full-service capabilities of Anchore Enterprise to the Ocrolus environment was an effortless and seamless process. The simplicity of implementation was based on:

- Easy access to documentation, which resulted in effortless onboarding.
- Product communication served in familiar language for DevOps teams.
- Zero custom tooling requirements needed for system setup.

Anchore's straightforward user interface gave auditors instant access to information when they needed it. By clicking the compliance tab, compliance data was presented that was digestible and timely. For non-technical users at Ocrolus, this solution established confidence in the SRE team and the system.

Results

Post-implementation, the SRE team was able to empower audit team members by inviting and training them with the Anchore Enterprise platform for on-demand access to security and vulnerability reporting. Through the Anchore user-interface, non-technical colleagues have greater insight into projects, which built trust with the overall system.

SRE team resource constraints were lifted and productivity dramatically improved by reducing dependencies on a single individual to provide answers to audit questions. Furthermore, other processes, like whitelisting, were made more efficient. In particular, Anchore Enterprise made image whitelisting easier helping the SRE team improve its operational efficiency.

In addition, Anchore Enterprise prevented false-negatives from vulnerability scans, which saved the SRE team time and money. Without false negatives, the focus was shifted to fixing true vulnerabilities to improve its enterprise performance and application security architecture.

With Anchore Enterprise, the organization was able to meet and exceed customer container security requirements to win new logos and business. Having Anchore Enterprise in place allowed Ocrolus to achieve customer expectations around container security scanners and demonstrate a strong security posture in the fintech space.

> ***"Based on the amount of time our team has saved, Anchore Enterprise has paid for itself 20 times over."***

~10 HOURS

Average Time Saved (Monthly)
Responding to Audit Requests

5 HOURS

Average Time Saved (Monthly)
Whitelisting Applications

10 MINUTES

Start to Finish Configuration
ACL SAML

> *"Implementing application-specific whitelists take less time to implement with Anchore Enterprise user interface than a global whitelist manually in Anchore Engine."*

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