anchore

Case Study

infoblox

Infoblox, a leader in Enterprise DDI (DNS, DHCP, IPAM), required a reliable container vulnerability scanning and management solution to scale the program to 150 applications developed by 600+ engineers. Product security and compliance are critical business functions at Infoblox. The trust created by these teams are foundational to business success and continuity.

Infoblox

Santa Clara, CA

www.infoblox.com

Industry: Network software

Segment: Enterprise DDI

Challenges

- Shift left security at scale; vulnerability detection & management to prevent vulnerabilities from entering production
- Resourcing challenge; Automation needed to scale 15 Security FTEs to meet output of 600+ Engineering FTEs
- Meet and maintain compliance certifications (FedRAMP moderate, SOC 2, StateRAMP, ISO 27001)
- Enterprise integration into existing pipeline and infrastructure (e.g., Amazon EKS, Harbor registry, Jenkins CI, etc.)

Solutions

Anchore Enterprise secures the software supply chain with:

- Container image scanning with low false positives
- Vulnerability and CVE Management
- Native integrations with Amazon EKS, Harbor and Jenkins
- FedRAMP, SOC 2, StateRAMP, and ISO compliant platform

Results

- 75% reduction in time for manual vulnerability detection tasks
- 55% reduction in hours allocated to retroactive remediation of vulnerabilities
- 60% reduction in hours spent on compliance tasks
- Empowered product security team to adopt proactive—shift left—security posture

Introduction

Infoblox, a leading provider in the enterprise DDI (DNS, DHCP, and IP Address Management) space, has been pioneering the DDI segment for over 25 years. The enterprise DDI space is crucial for managing and automating network services, ensuring seamless and secure network operations. Infoblox manages over 150 applications in production environments. With multiple deployments per day, this leads to 1000s of containers per month that need to be scanned for vulnerabilities; On top of that, they operate both a commercial and high compliance environment (e.g., FedRAMP, etc).

AWS Services:

- **EKS**
- **RDS**
- **IAM**
- **S3**
- **ELB**
- **ECR**

Technology Stack:

- **Helm**
- **GitHub**
- **Jenkins**
- **Spinnaker**
- **FluxCD**
- **KubeVela**
- **Harbor**

Challenge

Shift left at scale

The Infoblox Product Security team faced a significant challenge due to the lack of an existing vulnerability detection and management program. Previously, apps were deployed to production without any knowledge of potential vulnerabilities or manually reviewed after the deployment.

Scaling security with low false positive rate

Given the scale of the software development program at Infoblox (i.e., 1000s of containers built monthly), manual scanning and review was not a viable strategy. Furthermore, the product security team, consisting of only 15 full-time employees (FTE), was vastly outnumbered by the 600 FTEs in engineering, resulting in a 40:1 ratio. This disparity made it essential to have a vulnerability scanning tool with a low false-positive rate to scale the vulnerability management program effectively.

Scaled security without friction

The existing development tools and infrastructure, such as Amazon EKS, Harbor registry, and Jenkins CI, required a solution that could seamlessly integrate without disrupting the current DevOps workflows.

"When I first started, I was manually searching GitHub repos for references to vulnerable libraries but it was impossible to tell whether the codebase was a test repo, staging or not even in use. Anchore's SBOM inventory gave us certainty that a vulnerability was actually in production and needed to be fixed."

Sukhmani Sandhu, Product Security Engineer

Automation was necessary to manage the high volume of applications and deployments, ensuring vulnerabilities were detected and managed efficiently.

Compliance at scale

Another layer of complexity was added by the need to acquire and maintain multiple compliance certifications, including FedRAMP Moderate, SOC 2, StateRAMP, and ISO 27001. Infoblox required a secure and compliant vulnerability management system to meet existing compliance requirements and facilitate the attainment of new certifications. Not only did the organization prioritize these business critical certifications but the security team was charged with meeting these new requirements without dropping any of their existing responsibilities. They needed a solution that could not only meet compliance but allow the team to scale their efforts.

Solution

To address these challenges, Infoblox chose Anchore Enterprise as their container vulnerability scanning and management solution.

Save time - more signal and less noise

Anchore Enterprise's low false-positive rate was a critical factor in this decision, enabling the product security team to scale their efforts effectively despite the 1000s of containers being deployed every week. Every false positive eliminated means less time wasted by the Product Security team and more time dedicated to remediating actual threats to the organization.

Less fire fighting in production

Centralized vulnerability and CVE management, allowed the Product Security team to proactively remediate vulnerabilities when a container image is checked-in to the container registry, Harbor. This early detection was a significant step in Infoblox's shift-left strategy for product security. On top of this, developers from the engineering organization began to self-serve AnchoreCTL in order to scan their source code for vulnerabilities while they were authoring it. This helped Infoblox catch vulnerabilities even before the source code was sent to Jenkins for the build process.

Enterprise integration with DevOps speed

Anchore Enterprise seamlessly integrated with Infoblox's existing software development infrastructure and tooling, including Amazon EKS, Jenkins CI, and Harbor. This integration ensured that the new vulnerability management processes did not disrupt the current workflows and still allowed the product security team to scale their vulnerability detection and management efforts in the high-output DevOps engineering environment.

FedRAMP, SOC 2 and ISO compliance in rapid deployment environment

Additionally, Anchore Enterprise helped Infoblox achieve and maintain compliance certifications, such as FedRAMP Moderate, SOC 2, StateRAMP, and ISO 27001. Not only does Anchore Enterprise meet existing compliance standards, it helps Infoblox meet compliance controls, specifically the NIST 800-53 control family (RA-5). Infoblox was able to take advantage of both of these benefits by choosing Anchore Enterprise for vulnerability scanning and compliance certification. All of this while not adding friction to the high-speed development cadence and speeding up the compliance process.

"We're not trying to waste our team or other team's time. We don't want to report vulnerabilities that don't exist. A low false-positive rate is paramount. FedRAMP is very stringent and we don't want to create more work for ourselves given our limited resources."

Chris Wallace, Product Security Engineering Manager

Results

Anchore Enterprise transformed Infoblox's product security program by enabling the team to scale their efforts, automate compliance and maintain the speed of deployments.

- **75% reduction in time for manual vulnerability detection tasks**
- **55% reduction in hours allocated to retroactive remediation of vulnerabilities**
- **60% reduction in hours spent on compliance tasks**

By reducing the amount of time spent on manual security and compliance tasks, Infoblox opened the product security team up to focus on higher value initiatives like automating policy and remediation.

Developers self-adopted scanning tools during development, removing vulnerabilities before they entered the build pipeline. This proactive approach led to a 55% reduction in hours allocated to retroactive remediation. Both teams could now manage risk collaboratively, knowing about vulnerabilities before applications were pushed to production.

During incident response, a centralized inventory of all SBOMs enabled quick searches in Anchore Enterprise, reducing the need for extensive codebase searches. This automation reduced manual vulnerability detection time by 75%.

Additionally, the automation of compliance reporting artifacts resulted in a 60% reduction in hours spent on compliance tasks, dramatically improving how quickly compliance could be certified and the number of hours needed to meet the compliance requirements.

"We effectively had no tooling before Anchore. Everything was manual. ***We reduced the amount of time on vulnerability detection tasks by 75%****."*

Chris Wallace, Product Security Engineering Manager

About Anchore

Anchore enables organizations to speed digital transformation and reduce risks by streamlining the development of secure and compliant cloud-native applications. Anchore's solutions integrate with existing DevOps toolchains to automate security and compliance checks throughout the software development lifecycle. Organizations can reduce costs and accelerate time to market by remediating security and compliance issues early and continuously. Headquartered in California with offices also in Boston and the UK, Anchore's customers include large enterprises and government agencies that require secure and compliant cloudnative applications.

anchore

sales@anchore.com

anchore.com