anchore

Case Study

IRON BANK

Iron Bank is a program within the Department of Defense (DoD) that enables easier adoption of DevSecOps solutions and provides transparency into containerized software throughout the DoD. It provides Platform One and any DoD agency with a hardened and centralized container image repository that supports the end-to-end lifecycle needed for secure and dynamic software development.

Iron Bank at a Glance

San Antonio, Texas

https://p1.dso.mil/ironbank

Industry: US Military

Challenges

- Provide DoD agencies with hardened components for downstream software applications
- Fulfill extremely rigorous security standards that ensure the safety and integrity of military systems
- Low deployment frequency and policy compliance due to constantly changing security threats
- High toil on false positives

Solutions

Anchore Enterprise secures the software supply chain of Iron Bank with:

- An on premise and distributed container image scanner
- A turnkey SBOM generation and management solution
- Automated policy engine that evaluates and enforces security standards and compliance

Results

- Reduced false positives on customer deployments without requiring administration changes or software updates
- Delivered accurate SBOMs with improved mapping to vulnerabilities for hardening of downstream applications
- Jointly developed a codified custom policy to enforce the DoD Container Hardening requirements
- Enabled the systematic distribution of an always up-to-date Iron Bank DoD policy bundle to downstream users and projects

Introduction

Iron Bank is Platform One's hardened container image repository that supports the end-to-end lifecycle needed for modern software development. Iron Bank runs on Cloud One, a DoD multi-cloud ecosystem, which runs in AWS GovCloud. Iron Bank centralizes infrastructure tools and standardizes application hardening throughout the DoD to create a proactive security stance that protects modern military infrastructure, equipment, and the military workforce.

AWS Services

- **GovCloud**

Challenge

Iron Bank faces the complex task of balancing deployment velocity, software, and policy compliance (according to the DoD Container Hardening Guide), all while maintaining rigorous security standards and adapting to new security threats. The Iron Bank development team is responsible for the integrity and security of 1,800 base images that are provided to build and create software applications across the DoD.

I ron Bank not only provides all software components that are used for Platform One but also distributes them across the DoD. It's imperative that they can efficiently scan images and simultaneously adhere to rigorous security standards that guarantee the safety and integrity of military systems.

Another challenge is addressing false positives effectively. Due to the high volume of images and vulnerability management the team needs to process, false positives are time intensive and can cause significant toil.

"Even though security is important for all organizations, the stakes are higher for the DoD. What we need is a repeatable development process. It's imperative that we have a standardized way of building secure software across our military agencies."

Camdon Cady
Chief Technology Officer at Platform One

Solution

Anchore's engineering team was deeply embedded with the Iron Bank infrastructure and development team to improve and maintain critical components in the DevSecOps pipeline. This supported the Iron Bank team in getting hardened containers into the Iron Bank.

Custom policy for app checks and open source containers

Since the IronBank inception in 2020, Anchore Enterprise has been the software supply chain security tool of choice. After the first iteration of Iron Bank infrastructure, Anchore started scanning container images and implemented a custom policy pack to check all images for compliance against DoD's Container Hardening Guide requirements. This custom policy encompasses general security best practices within containers as well as application specific checks for a set of open source containers maintained by the Iron Bank team.

Lower false positives with the exclusion feed

In collaboration with the Iron Bank team, Anchore developed the exclusions feed to remove findings that were known false positives. The exclusion feed reduces the security assessment load on the Iron Bank team while addressing false positives seamlessly.

At the writing of this case study, the exclusion feed captured over 12,000 known false positives.

Since 2020 the following joint engineering efforts between Iron Bank and Anchore resulted in:

- **Time-based Allowlisting** - expire allowlisted findings after a defined period of time using Anchore policy
- **Content Hints** - add or override container software content to improve vulnerability scanning coverage for Platform One
- **Binary Content Type** - install checks for software binaries outside of a package manager to increase coverage of scans
- **False Positive Management** - correct false positives through a fast-feedback mechanism
- **Clamav Support** - more thorough container scanning of all artifacts through integrated malware scanning
- **Image Ancestry Comparison** - provide rich content while determining image ancestry, informing vulnerabilities and policy evaluations inherited from previous layers
- **Windows Image Scanning** - scan Windows based container images

> "People want to be security minded, and they want to do the right thing. And what they really want is tooling that helps them to do that with all the necessary information in one place. That's why we looked to Anchore for help."
>
> Camdon Cady
> Chief Technology Officer at Platform One

Results

Anchore Enterprise provided Iron Bank with quality vulnerability and compliance findings to ensure that container images go through a standardized and efficient process that adheres to the DoD's Container Hardening Guide.

Streamlines process for accurate vulnerability scanning and compliance

Anchore Enterprise empowered Iron Bank to create a standardized and efficient process for container scanning that adheres to the DoD's Container Hardening Guide and delivers quality vulnerability and compliance findings.

SBOM Hints and Corrections to increase accuracy

To address false positives and misidentified components in a streamlined and repeatable workflow, Anchore developed and delivered two custom capabilities, SBOM Hints and SBOM Corrections. SBOM Hints and SBOM Corrections allow Iron Bank customers to adjust metadata in order to create a more accurate generation of SBOMs and improved mapping to vulnerabilities.

Time savings and reduced overhead with exclusion feed

The Anchore Vulnerability Feed enabled the Iron Bank team to reduce the occurrence of false positives and incomplete data in public feeds. To launch the vulnerability feed, the Iron Bank team handed Anchore a list of 10,000 false positives for analysis and inclusion. Iron Bank customers now benefit from live updates that immediately reduce false positives without any need for administration changes or software updates. This is made possible through the continuous monitoring and updating of the data feed. For example, all Iron Bank customers can request an assessment of potential false positives through the Anchore support portal to add new data to the feed.

In addition, Anchore enabled support for time-based allowlisting, now Iron Bank can expire allowlisted findings after a defined period of time using the Anchore policy engine.

From 2020 until today Anchore has provided ongoing support to the engineering team at Iron Bank, like providing them with custom DoD policy packs. The collaboration between Iron Bank and Anchore continues to expand and advance towards the shared goal of protecting modern military infrastructure, equipment and workforce.

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

© 2024 Anchore, Inc. All rights

sales@anchore.com

anchore.com