

DEVELOPMENT AT MACH SPEED

How Anchore and Red Hat teamed up to build a DevSecOps pipeline for the Department of Defense

The United States Department of Defense (DoD) is taking a completely new approach to building, deploying, and operating software.

On the way out: slow-moving, waterfall-driven development processes that result in monolithic, hard to manage applications. They have come to the conclusion that the traditional way of delivering software is expensive and inflexible, and the situation for today's warfighters demands maximum efficiency. There are too many lives at risk if the DoD fails to innovate, and too much geopolitical competition.

Advanced enterprises solve this problem through the implementation of cloud-native technologies such as Kubernetes and the implementation of DevOps practices. Using this combination of tools and tactics, software can be delivered in much smaller components and updated frequently. This results in a very quick pace of development, and allows for frictionless reuse of components between teams and communities. Automated build, integration, and deployment can reduce the lead time to deliver warfighter capabilities from months to minutes.

The DoD needs to deliver software to the warfighter at the speed of operations, so they have built a new platform and software supply chain to remove bottlenecks on their cloud-native journey. The foundation of this platform is an automated DevSecOps pipeline that bakes in automated security and compliance checks before delivering to a CNCF compliant Kubernetes cluster. This allows them to build and consume software at the pace required to maintain their competitive edge. However, even though security is important for all enterprises, the

Automated build, integration, and deployment can reduce the time from invention to production - from months to minutes.

stakes are higher for the DoD. So while they could build on commercial best practices, there are several additional steps required to meet security standards. There is also a need to deploy in a standardized way across various disparate environments, from traditional on-premise environments to special regions of public cloud and even small footprints at the tactical edge.

Over the past 12-months, Anchore and Red Hat have worked side by side to develop and implement an automated process for hardening and securing containerized software within the United States Air Force. Anchore is the only container security vendor providing hands-on support as part of the U.S. Department of Defense DevSecOps Platform (DSOP) initiative. The beating heart of the DSOP initiative is a powerful Kubernetes cluster that can run on any infrastructure. In many cases, including this one, the Kubernetes cluster is powered by Red Hat OpenShift. This paper, based on hands-on experience working with our government partners in the U.S. Department of Defense and United States Air Force, provides valuable insight and guidance on best practices for secure, high-velocity software delivery.

Audience

This paper is for security teams, DevSecOps engineers, and information system security leaders who would like to learn from the steps the DoD has taken to establish high-velocity development and deployment of new services in a context where security can have life-or-death consequences. Over the past decade, the Federal Government has issued numerous executive orders and memorandums that task IT leaders to efficiently transform software development using DevOps and DevSecOps deployment models at their various agencies. We aim to provide an overview of this transformation, showing how it can be done at scale within large enterprises.

Purpose

The purpose of this paper is to understand the importance of adopting and utilizing approved hardened containers in the US Government. This paper will describe the hazards of historical DoD software deployment lifecycles and how the United States Air Force migrated away from risky development practices, relying on hardened containers running on Kubernetes as the backbone to the success of its DevSecOps Platform. Our goal is to document the USAF DevSecOps model, describe the container-hardening process currently used by USAF, and demonstrate to federal audiences how they can instantiate or augment their own DevSecOps pipelines using DoD-approved, hardened containers.

Problem Statement

The DoD, similar to other large enterprises, faces the complex task of balancing deployment velocity, compliance and security. However, they are unique from other large enterprises in that the applications they build and maintain are military systems where human lives are at stake 24/7/365.

In the past, software development at the DoD used a traditional “waterfall” development methodology with a heavy emphasis on planning and requirements gathering. As a result, the pace of innovation was slow. Both private and public industries have moved to more iterative, agile development models due to several factors. Not only are these new methodologies quicker, they also incorporate end-user buy-in from an early stage. Often, the waterfall methodology can result in a product that does not adapt to rapidly-changing requirements and operational conditions.

For those who use traditional waterfall processes, compliance often becomes a game of catch-up. When development moves slowly, security teams often rush to validate software within contract deadlines. Additionally, once a program has exhausted its budget in the development phase, it is faced with the burden of obtaining a DoD Authority to Operate (ATO). This can take at least 9 months, causing the technology that was leading-edge at the inception of the program to become out of date.

For those who use traditional waterfall processes, compliance often becomes a game of catch-up.

The economic and programmatic risks of the waterfall delivery lifecycle are clear, but the cybersecurity risks are even more detrimental. By following the model prescribed above, software teams are locked into older, often deprecated software that can't be effectively hardened or protected. As a result, they are leaving systems open to hundreds - or even thousands - of vulnerabilities within outdated software that is no longer being maintained. Worse, these teams are often locked into contracts with third parties who deliver software slowly and make it extraordinarily challenging to stay on top of emerging vulnerabilities.

As security teams work to protect government systems, they lack the full breadth of options within the marketplace that can help them gain the upper hand against adversaries. Software designed and consumed by the DoD needs to be developed at a higher velocity, with greater efficiency, and with a focus on security in order to maintain dominance in the current cybersecurity landscape.



DevSecOps at the Department of Defense

DevSecOps is quickly becoming an optimal mode of operation for consumers of container-based technologies, from early adopters to long-time users. As enterprises move towards more agile development by implementing modern DevOps, the rate of change increases and attack surfaces become more fragmented and dynamic. The integration of security into each stage of the software development life cycle, a practice known as DevSecOps, is now critical for organizations operating in today's cloud-native environments.

The DoD codified their new approach to software creation and management in the DevSecOps Reference Design. This document, hosted at software.af.mil and linked from the [Anchore Federal](#) web page, contains a roadmap for various defense agencies and programs to dramatically overhaul the traditional waterfall software development practices in common use. It has resulted in the creation of a new platform for DevSecOps known as Platform One.

In their [DevSecOps Reference Design](#), the DoD defines DevSecOps as “a collection of software-integrated tools, services, and standards that enable partners and programs to develop, deploy, and operate applications in a secure, flexible and interoperable fashion”. Championed by Nicolas Chaillan, Chief Software Officer of the United States Air Force (USAF), the DoD DevSecOps Initiative is charged with creating a platform that can be easily reused and implemented across all branches of the DoD.

For more information on the mission of Platform One, view [this video](#) created by members of the Platform One team.

Separating itself from DoD operational systems of the past, this new Reference Design prescribes comprehensive use of industry standards such as Open Container Initiative (OCI) containers and Kubernetes to develop and deploy software. The use of containers deployed on Red Hat OpenShift is familiar to the teams at Anchore and Red Hat, as it is the same approach taken by many of the Fortune 500 enterprises we support. Containers offer multiple advantages of particular interest to the Department of Defense. These include:

01 Velocity: Provisioning containers is extremely fast when compared to virtual machines or bare-metal systems. An operator can deploy, scale up, scale down, and destroy a container workload easily, and each operation takes a matter of seconds.

02 Cost-efficiency: Containers allow for better allocation of computing resources for specific workloads with minimal overhead. They run on readily-available, standard hardware that can be sized to support a variety of requirements and are lower cost than traditional scale-up systems.

03 Immutability: Once a container image is created, a hash is created that ensures it can be uniquely identified and cannot be altered as it proceeds through the development and deployment process.

04 Scalability: Containerized applications and environments horizontally scale with ease, reducing the costs associated with discrete hardware. Individual services can be managed and scaled separately, helping to realize a core benefit of microservices architectures.

05 Consistency: Platforms like Kubernetes offer a consistent control plane for applications, reducing operational costs and increasing agility. Applications are defined, deployed, and managed using a single operational toolset.

06 Control: Container images are layered, building upon base images that provide basic environments for applications to run within. This allows the DoD to approve and reject base images based on security best practices, providing fine-grained control over the software that is deployed.



Establishing Continuous Security

Platform One includes a prescribed set of software and capabilities known as the Sidecar Container Security Stack (SCSS), which ensures a high level of runtime security. The SCSS model offers the ability to deliver correlated and centralized logs, fully-integrated container security, whitelisting, Role-Based Access Control (RBAC), continuous monitoring, signature-based scanning based on Common Vulnerabilities and Exposures (CVEs), and policy enforcement.

Continuous monitoring and scanning of runtime systems is a critical part of a comprehensive security strategy, but it is not enough. After all, a vulnerability discovered in a running application has already created an opportunity for an opponent to inflict damage. That's why Platform One includes processes that harden software containers before they are deployed in a mission setting. These hardening steps are integrated into the development pipeline and performed by Anchore and the Platform One team. Platform One will ultimately make hundreds of approved, hardened containers available for use.

Working in collaboration with the USAF, Anchore has developed custom policy checks for all images in the pipeline to harden them to meet the security and compliance baselines of the DoD. These policies were implemented by Anchore engineers, who work within the Platform One team to validate new images and deliver them into the DoD Centralized Artifact Registry, also known as "Iron Bank".

Continuous
monitoring and
scanning of
runtime systems
is a critical part of
a comprehensive
security strategy,
but it is not enough.

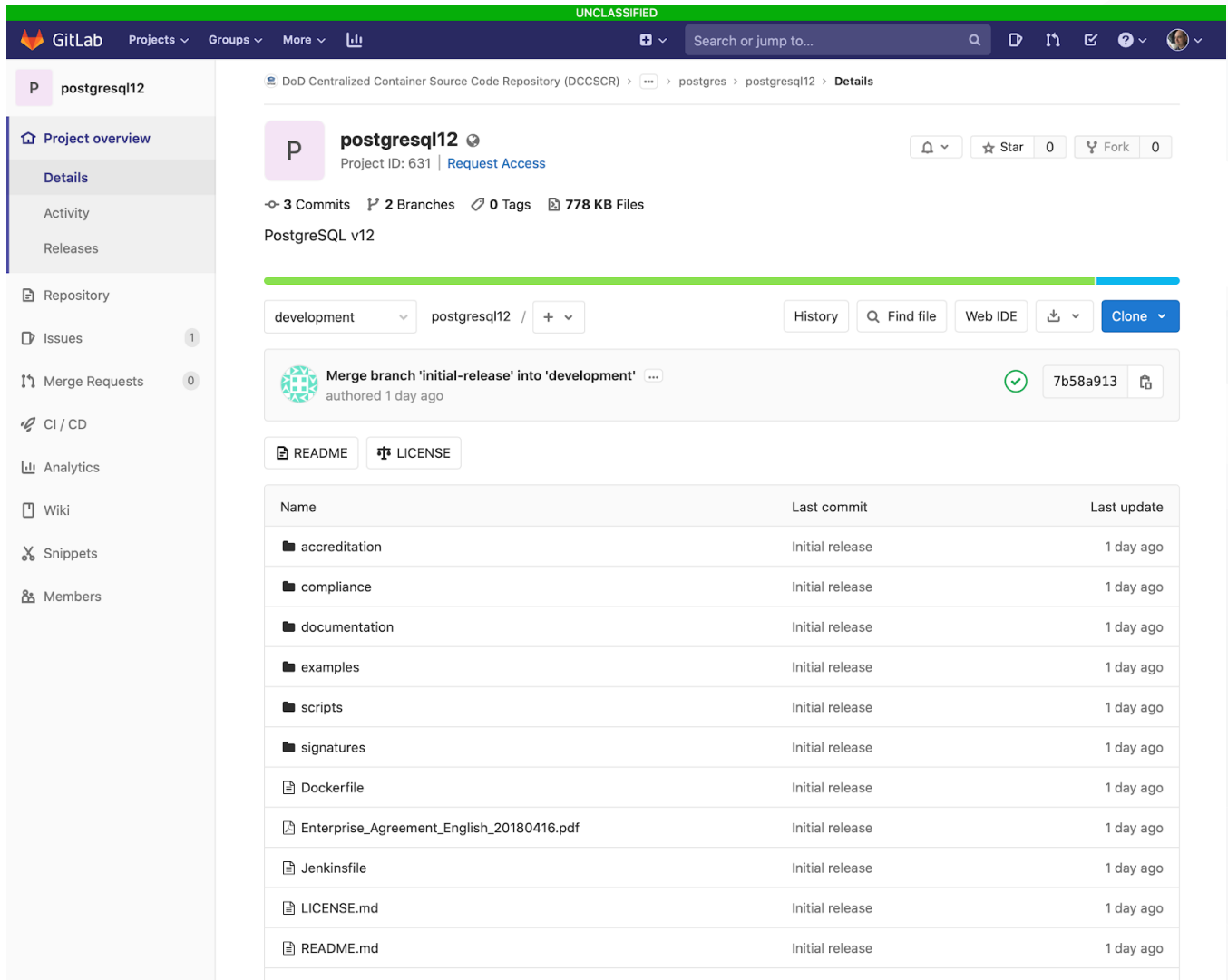
The DevSecOps Reference Design specifies three main categories of container images that will be hardened and maintained:

- » **Container images used to power** the DevSecOps platform, including: CI/CD systems, code and artifact repository platforms, and tools for developers and operators
- » **Sidecar Container Security Stack containers** to be used in runtime environments for continuous monitoring and scanning of container security
- » **Common containers to be used** as a baselines for software development by engaged agencies and programs

The container hardening process also applies to common containers from third party Independent Software Vendors (ISVs) looking to provide software to the DoD. In order to do so, ISVs will be required to interact with several key infrastructure services: Repo One and Iron Bank. More information about these services can be found in the following sections.

The Container Hardening Process

The container hardening process is initiated with a code push into the DoD Centralized Container Source Code Repository, also known as [Repo One](#).



Above: Example ISV project in Repo One

This repository is used to store the instruction files required to build container images (the “Dockerfiles”), along with their associated checksums and various forms of documentation. Anchore and Red Hat work together closely within the Platform One team to manage Repo One, with the ultimate goal of bringing over 170+ container images into the hardening pipeline. Anchore is a key contributor on the Platform One Container Hardening Team, which validates containers for use.

As part of the onboarding process, the Platform One team grants permissions which will allow an ISV to create a project and submit merge requests for review. Once a merge request has been submitted containing a new container image, the Container Hardening Team performs build, test, and validation steps specified in the DoD Container Hardening Guidelines document.




ISVs can find detailed information in the [vendor contributors guide](#) that can help them understand the process and get started.

A hardened container image is one that adheres to the container format published by the OCI and is made compliant with the DoD Container Hardening Security Requirements Guide. The container hardening process consists of a Jenkins job that pulls the Dockerfile from Repo One, builds an OCI-compliant container image, and pushes that image to the Repo One image registry. This automatically triggers the container scanning pipeline. The DSOP team validates that the ISV has staged their files correctly in Repo One [by following the contributor onboarding process](#). Once validated and merged into the proper branch, an automatic pipeline job is triggered to kick off the image build and scanning processes.

The Container Hardening Team uses Anchore and OSCAP to automatically review the compliance and security baseline of the container image following the build process. Anchore performs a series of policy specific and best-practice checks on every image built in our pipeline which is explored further below. The container hardening pipeline consists of Anchore and OpenSCAP. These tools each perform different functions, and enforce container image security best practices in unique ways.

Anchore is a policy-based container workflow platform that analyzes container images, maintains a centralized bill of materials, and continuously scans for known vulnerabilities and policy violations. One of the key purposes of Anchore is to mitigate insider threat within the DevSecOps lifecycle by detecting unapproved changes to Dockerfiles.

One of the key purposes of Anchore is the mitigation of insider threat within the DevSecOps lifecycle by [detecting unapproved changes to Dockerfiles](#).



It is important to detect when a developer intentionally makes changes to a Dockerfile that are erroneous or malicious.

For example, an insider could edit a Dockerfile and cause it to make an external call to a malicious database, or download and execute a malicious Java archive. These examples can be automatically detected and stopped with Anchore using a set of flexible policies that govern the contents of Dockerfiles. This prevents malicious Dockerfiles from becoming deployable images inside an operational environment.

Once an image is built, it can contain a large amount of third party operating system packages and language artifacts like Ruby GEMs, Java JARs, Python packages, and npm modules. Anchore also performs policy checks on the contents of container images after they have been built, providing automatic application-level enforcement. Compliance requirements on software configuration, such as those required by various Security Technical Implementation Guides (STIGs), can be enforced using Anchore's policies. For example, the STIG that provides guidance on using a PostgreSQL database requires specific lines to exist in the configuration file. Anchore can validate configuration files through policy rules that, in the case of this example, ensure that certain lines exist. If they don't, it can prevent the image from proceeding to the next stage of the development pipeline.

OpenSCAP serves two distinct purposes. First, it performs scanning to ensure that the application that runs within a container is configured in accordance with published policy. Second, it evaluates container images against the Red Hat OVAL feed to ensure that it does not contain vulnerabilities without corresponding patches installed. The OVAL feed from Red Hat provides information on every known vulnerability that affects Red Hat Enterprise Linux, including UBI containers, as well as any mitigations or patches that are available to address exploits. OpenSCAP generates reports that reflect the overall health of the container in which an application will be run or developed.

One container hardening has been successfully completed, all scanning results and the images themselves are uploaded to the Iron Bank.

IRON BANK SINGLE SIGN ON

Log In

Username or email

Password

[Forgot Password?](#)

[Log In](#)

New user? [Register](#)

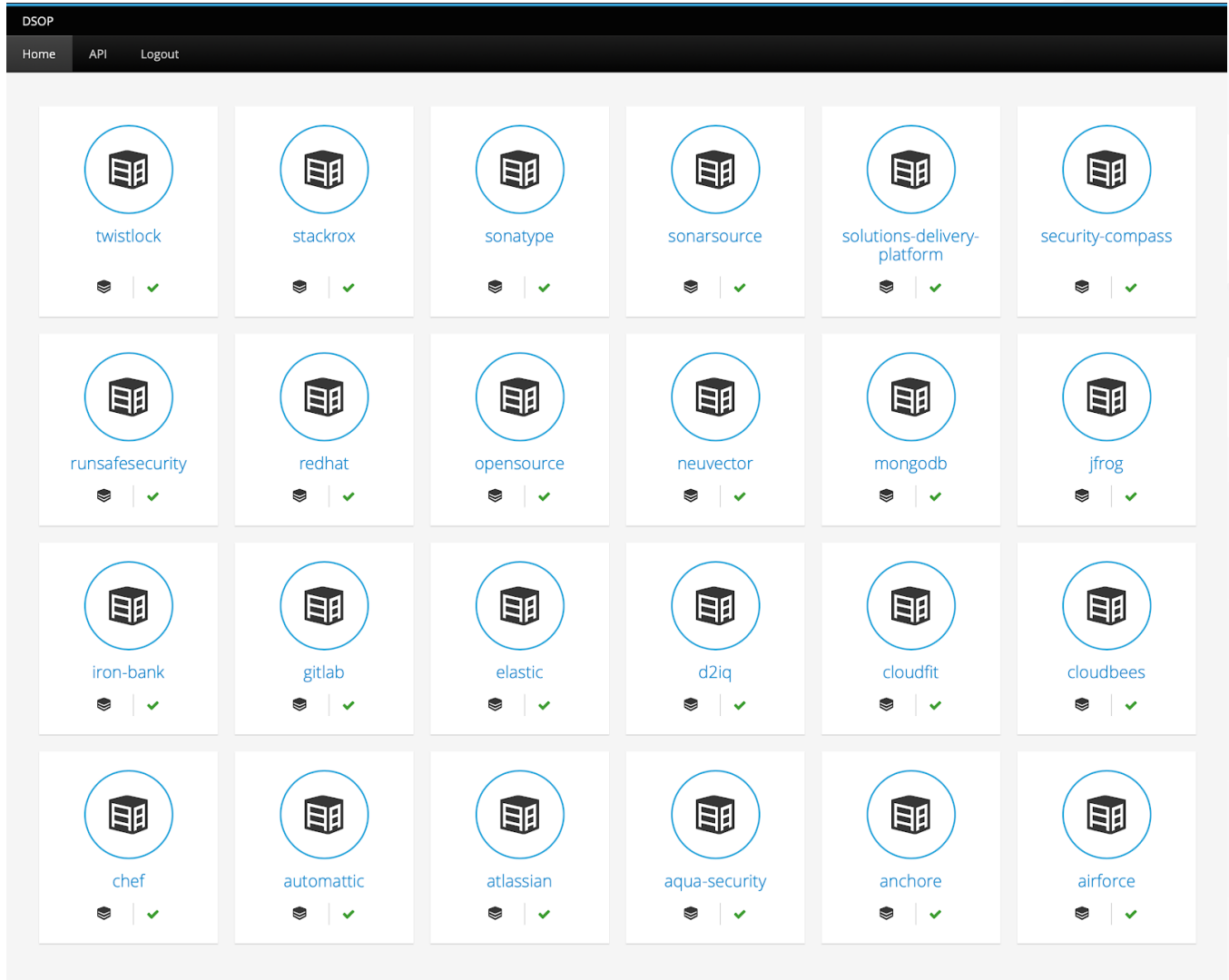
Above: the Iron Bank login screen

Iron Bank: A Stronghold For Hardened Container Images

The Iron Bank is an artifact repository that holds all hardened container images produced by the Platform One software factory. These container images have all been validated against DoD security and compliance policies defined in the DoD Container Hardening Security Requirements Guide. They have also been comprehensively analyzed by Anchore, which identifies known vulnerabilities and unsafe practices in OS & non-OS packages, libraries, licenses, binaries, credentials, secrets, and metadata.

For end users, creating an account with Iron Bank to download hardened container images is a quick and painless process that takes only a few seconds. Once authenticated, Iron Bank displays a dashboard that contains the images available for use, their approval status, and the scanning reports generated by Anchore, OpenSCAP, and the runtime scanning tools within the SCSS.

Iron Bank also shows a list of vendors whose container images are available, which grows daily as new software is hardened to the DoD standard.



Above: the list of vendors in the Iron Bank, as of this writing

By drilling down on a particular container image, users can view specific instructions for downloading and sideloaded the image into their own repository.

opensource/nodejs/nodejs Artifacts

Container Approval Status: pendingapproval

Verifying Image Instructions:

1. Save key to file (call it public.asc)
2. Import key with: `gpg --import public.asc`
3. Create a personal gpg key if not yet created
4. Trust the imported public key: `gpg --sign-key test_dod@redhat.com`
5. Download the image manifest (manifest.json), and PGP signatures (nodejs.sig and signature.sig) below
6. Verify manifest with: `gpg --verify signature.sig manifest.json`
7. Verify image with: `gpg --verify nodejs.sig nodejs`
8. Verify that the sha tag matches the signed manifest.json entry for the manifest-digest:
sha256:063cf4306024ccced50ae205dd734abbbf4855ac38ae4af74f4adac727b19b98
9. Hash the image to verify that the result matches the sha256 checksum entry in manifest.json: `sha256sum nodejs-12.16-reports-signature.tar.gz`

Downloading and Running the image:

1. Find the SHA tag for run below: ex:
sha256:063cf4306024ccced50ae205dd734abbbf4855ac38ae4af74f4adac727b19b98
2. Retrieve the image by downloading it: `nodejs`
3. Load the image into local podman registry: `podman load -i ./nodejs`
4. Run the image with: `podman run nexus-docker-secure.levelup-nexus.svc.cluster.local:18082/opensource/nodejs/nodejs:12.16`

Run for 4 using with tag:12.16

SHA tag - sha256:063cf4306024ccced50ae205dd734abbbf4855ac38ae4af74f4adac727b19b98

Image scanned - [nodejs-12.16.tar](#)

Image manifest - [manifest.json](#)

PGP Signature - [signature.sig](#)

Version Documentation - [documentation.json](#)

Tar of reports and signature - [nodejs-12.16-reports-signature.tar.gz](#)

Tool reports:

OpenSCAP - [Compliance](#), [OVAL](#)

TwistLock - [TwistLock](#)

Anchore - [Gates](#), [Security](#)

Summary Report - [Summary](#)

Full Report - [All Scans rolled up into one Excel File](#)

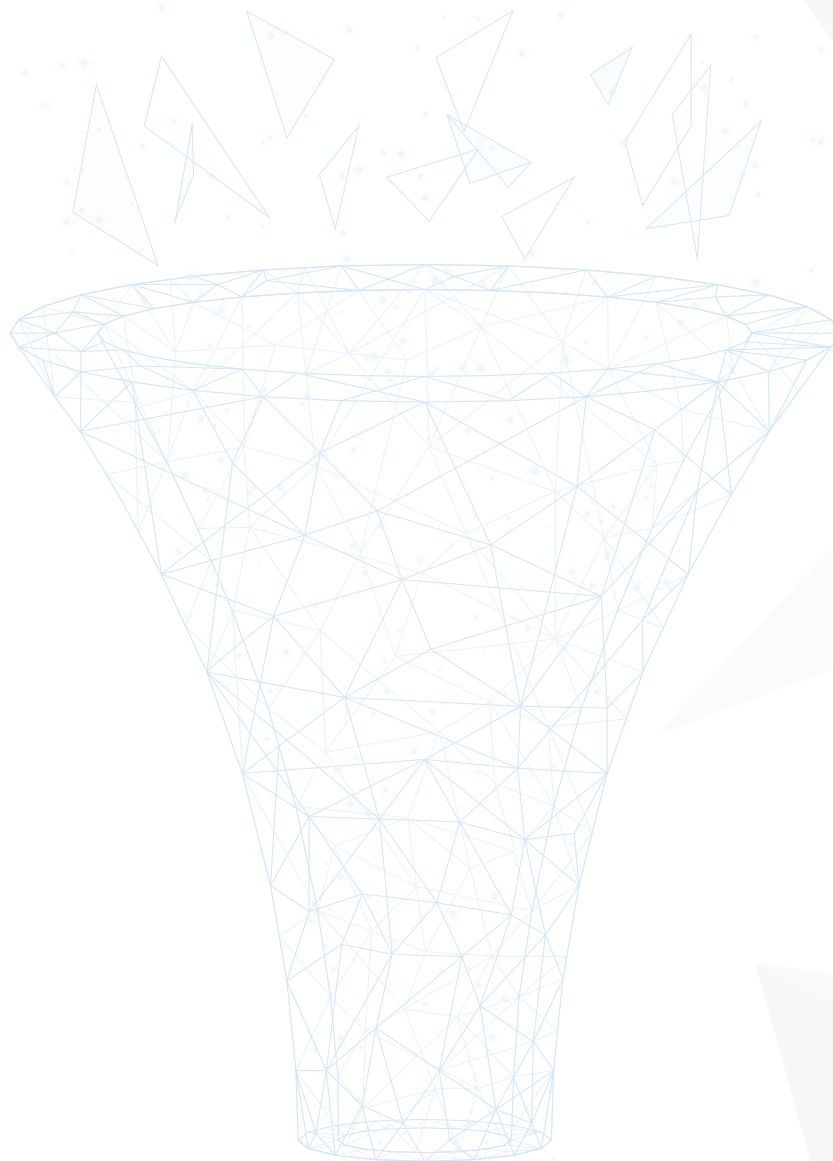
Above: the detail provided by Iron Bank for a particular image

Users can also inspect the scanning artifacts produced as a part of the container hardening process. These are formatted as a collection of CSV files with detailed pass/fail status for specific policy gates. This gives end users the ability to validate compliance in detail before downloading and deploying images.

Current Status

The images are already available for use. By following the steps above, a DoD end user can begin setting up their own DevSecOps pipeline. The scanning artifacts generated by Anchore serve as a critical component for the program achieving and maintaining Continuous ATO. As a result, this allows the program to overcome the 9-12 month timelines it takes to receive authorization to operate as it was in the past. The increased time to production greatly reduces financial burden and ultimately allows the developers to focus on increasing automation and building out new features quicker than before.

The repository already has numerous different products for programs to begin using and building their own pipelines using already approved and hardened containers. Ranging from service mesh products such as Istio, logging tools such as Elasticsearch/FluentD/Kibana (EFK), configuration management tools such as Ansible or Chef, continuous integration and source code management in Gitlab, and container security in Anchore Federal. Vendors will continue to be on-boarded into Repo1 and Iron Bank, providing the best software available for immediate use by DoD programs.



Conclusion

The Iron Bank alleviates a huge burden for developers on DoD systems, allowing them to abandon lengthy software development lifecycles of the past. By taking advantage of the DoD DevSecOps Platform and using hardened images from Iron Bank, users gain the following:

01 Speed: Signing up for the Iron Bank and consuming images is an easy process, and can result in hardened containers running in an end-user cluster within minutes.

02 Security: All images have already been hardened based on guidelines and requirements that establish a baseline of security and prevent bad practices during the build stage.

03 Flexibility: Iron Bank contains software from over 100 vendors, allowing users to avoid being locked-in and reliant on a single vendor in their stack. This allows end users across various DoD programs to choose the best vendor software for their own environment.

04 Compliance: The Iron Bank provides a record of all scans, along with a complete set of scanning artifacts for each image. Additionally, the USAF reviews vulnerability findings for each image in the Iron Bank. For images that fail to meet certain requirements, justifications with specific plan of action in order for software to remain available.



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.

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

anchore

✉ info@anchore.com

🌐 anchore.com

