anchore

DevSecOps for a DoD Software Factory:

6 Best Practices for Container Images

Introduction

The [DoD Software Modernization Implementation Plan](), released in March 2023, aims to reduce software delivery times from years to minutes by building containerized software through an ecosystem of **DoD software factories** that implement modern DevSecOps practices. The DoD has stated that this approach will depend on commercial tools to help implement DevSecOps software factories.

Anchore Enterprise is a proven tool for container image security. The Federal Edition of Anchore Enterprise, known as Anchore Federal, is used across multiple DoD software factories, including Air Force Platform One, Iron Bank, Navy Black Pearl, and more.

"Anchore is one of the few container security companies that are approved as part of the DoD Enterprise DevSecOps initiative and a key compound for ensuring the security and compliance of software containers within the DoD Iron Bank."

U.S. AIR FORCE

This white paper identifies six best practices for container security outlined by the DoD and related NIST standards and maps Anchore Federal features and capabilities to those standards.

The best practices in this whitepaper are aligned to requirements and recommendations in DoD guidance[1] and the relevant NIST standards.[2]

Securing Container Images in a DoD Software Factory

This whitepaper explores six best practices for securing container images in a DoD software factory. These best practices pull from DoD guidance and NIST controls for container image security.

[1] DoD Software Modernization Implementation Plan, DoD DevSecOps Reference Design, DoD Container Hardening Guide, Container Image Creation and Deployment Guide

[2] NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations), NIST SP 800-37 (Risk Management Framework for Information Systems and Organizations), and NIST SP 800-190 (Application Container Security Guide)

1 Use Trusted Base Images

A base image in a software container is the foundational layer for an image. It typically contains a minimal operating system with the necessary tools to install packages and make updates over time.

Because a base image can be used in many container images, it must come from a trusted source. For a DoD software factory, the DoD Container Hardening Guide states that a base image must be downloaded from an approved source, known as a DOD Base Container Image Approved Source (DBCIAS). These approved sources come in two types: trusted and untrusted repositories.

The following sources are currently approved and should be used in order of priority:

1. **Iron Bank/DCAR (approved DOD-wide; trusted).**
2. **Product vendor proprietary repository (untrusted).**
3. **Docker Hub (untrusted).**
4. **Red Hat Container Repository (untrusted)**

Creating Trusted Base Images with Anchore Federal

The Iron Bank team uses Anchore to identify vulnerabilities and perform policy checks on container images to ensure they meet the Iron Bank requirements. Anchore Federal is also used in other software factories across the DoD, including Platform One, Black Pearl, and more. It is ready to deploy in classified and air-gapped environments, including IL4 and IL6.

Companies providing container images to DoD programs or the Iron Bank can easily integrate Anchore Federal into their DevSecOps toolchain to perform vulnerability scans and security checks as software is developed. Finding and fixing any vulnerabilities and security findings early helps to streamline authorization to operate (ATO or cATO) or acceptance into the Iron Bank.

2 Harden Container Images

To ensure the DoD's container images are secure, cybersecurity engineers and DevSecOps engineers must perform vulnerability and compliance scans and then remediate or otherwise address the findings of those scans. Hardening requirements specified in the **DoD Container Hardening Guide** and **Container Image Creation and Deployment Guide** include removing unnecessary tools and services, using a signed base image, remediating vulnerabilities, and restricting privileges.

In addition to these general requirements for all containers, DISA **publishes product-specific STIGs** (Security Technical Implementation Guides) for individual technology services. STIGs prescribe specific security settings and configurations for common technologies such as RHEL, Apache, MySQL, Oracle Database, Kubernetes, Postgres, SUSE, Ubuntu, and many more. When a STIG is not available, a DISA Security Requirements Guide (SRG) for the generic category of technology (application server, database, operating system, container platform) should be used instead.

Lastly, the DoD recommends building containers without a connection to the internet to ensure dependencies and other packages are loaded and built from trusted sources. The hardening process is fully automated for containers submitted to the Iron Bank (an approved and trusted DoD-wide container repository), and the build process is conducted in an air-gapped environment.

Automating Container Hardening with Anchore Federal

When building a DoD software factory, Anchore Federal enables you to automate the container hardening process in the development pipeline and check that all of the DoD requirements have been met. By automating necessary checks during development, you can identify any issues early and ease the authorization process.

Anchore Federal performs vulnerability scans on container images and makes remediation recommendations. It also alerts you to vulnerabilities on the CISA list of Knonwn Exploited Vulnerabilities.

In addition to vulnerability scanning, Anchore Federal leverages out-of-the-box policy packs for NIST, DoD, DISA, and FedRAMP to perform various other checks, such as identifying malware, secrets, loose privileges, or insecure configurations. Anchore Federal also provides a Static STIG Checker that integrates into the CI/CD pipeline to shift-left STIG checks for container images and identify issues well before production.

3 Continuous Vulnerability Scanning and Remediation

A key goal of the DoD Software Modernization Strategy is to shift security left in the development lifecycle. Detecting and fixing vulnerabilities and security issues earlier reduces the time and cost. Automated continuous vulnerability scanning of container images from build to CI/CD pipeline to registry to production ensures that container images remain secure throughout development and that no vulnerabilities can slip into production.

The DoD advocates using commercial vulnerability scanning tools to scan images in software factories. The **NIST SP 800-190 Application Container Security Guide** highlights that traditional vulnerability management tools are often misaligned with the unique issues of container images and recommends that you "adopt container-specific vulnerability management tools and processes for images to prevent compromises."

Vulnerability Scanning for Container Images with Anchore Federal

Anchore Federal is a continuous container vulnerability scanning solution that also provides remediation recommendations. Anchore Federal provides visibility into all image layers, not just the base image. It can "crack open" multiple levels of files (such as .jar, .war, .ear files) to find dependencies and vulnerabilities hidden inside. Anchore Federal also recommends remediation actions to address the vulnerability.

Anchore Federal also includes the Anchore Vulnerability Feed, which aggregates multiple public vulnerability feeds and curates them to reduce false positives. The Anchore Vulnerability Feed uses data from Anchore's user community, customer environments, and research by the Anchore Security Team to suppress false positives and correct inaccurate metadata in public vulnerability feeds. Anchore Federal supports using an on-premise vulnerability feed service that can be periodically updated for air-gapped environments.

4 Consistent, Automated Policy Enforcement

The DoD recommends implementing automated policy enforcement for container images in the **DoD Enterprise DevSecOps Reference Design**. Policies can optionally be used as a control gate to prevent container images from progressing through the software factory (into the registry or production) if they don't meet the requirements. Even once containers are in production, you should set up tools to ensure that there are no newly reported vulnerabilities in your deployed images.

In addition, the DoD highlights that continuously updated, centralized reporting and monitoring of the compliance state of all of your container images is critical to identifying weaknesses and risks at the organizational level.

Preconfigured and Customized Policy Enforcement with Anchore Federal

Anchore Federal is built around a policy enforcement engine that supports a variety of security checks, including vulnerabilities, secrets, malware, insecure configurations, and more. A consistent set of policies can be applied to images at all stages, from build to registries to production environments.

Anchore Federal includes several out-of-the-box policy packs that map to controls for NIST, DoD, DISA, and FedRAMP to streamline policy enforcement. Users can customize policies and even create new policy packs that combine all the controls relevant to their organization.

Anchore Federal also provides centralized reporting to show the current and historical vulnerability results and compliance state of all container images. Users can access pre-built reports, create custom reports, schedule reports, and get notified when reports are available. Anchore Federal also provides a GraphQL API to query the aggregated data and metrics.

5 Manage Provenance with SBOMs

Understanding the software supply chain is crucial in managing risk. The DoD has emphasized the importance of tracking the provenance of software components and dependencies within a software application. The NIST 800-53 control catalog includes several controls related to provenance.

More recently, the federal government has explicitly specified that SBOMs are the preferred mechanism for tracking and sharing the provenance of software.

The 2021 Executive Order on Improving the Nation's Cybersecurity, requires software providers to give an SBOM to federal purchasers. The NIST 800-218 Secure Software Development Framework requires software suppliers to the US federal government to "collect, safeguard, maintain, and share provenance data for all components of each software release (e.g., in a software bill of materials [SBOM])." Soon, software suppliers will be required to attest to these practices and could face significant liability if they fail to follow them.

What is an SBOM?

Executive Order 14028 defines a "Software Bill of Materials" or "SBOM" as a "formal record containing the details and supply chain relationships of various components used in building software. The SBOM enumerates these components in a product. It is analogous to a list of ingredients on food packaging." Learn more.

Automated SBOM Management with Anchore Federal

"Adversaries attempt to compromise our national defense daily, and the software supply chain is a growing attack vector. At Platform One, security is not an afterthought, it is the first thought. Anchore's industry-standard software bill of materials (SBOM) formats help Iron Bank publish SBOMs for broad consumption and track for unexpected drift to mitigate supply chain risk for the Department of the Air Force."

Colonel Timothy Helfrich, Senior Materiel Leader, Cyber Systems Group, USAF

U.S. AIR FORCE

Anchore Federal generates detailed SBOMs at each step in the development process, providing a complete inventory of the software components, including the direct and transitive dependencies you use. These SBOMs can then be combined to create an application-level SBOM with a comprehensive list of the application's ingredients.

Anchore Federal stores all SBOMs in an SBOM repository to track the provenance of your software components for each release and enable ongoing monitoring of your software for new or zero-day vulnerabilities that can arise even post-deployment.

Anchore Federal uses SBOMs to identify vulnerabilities and risks for remediation, provide rich metadata for policy rules, and meet compliance requirements. It also detects SBOM drift in the build process, issuing an alert for changes in SBOMs so they can be assessed for risk, malware, compromised software, and malicious activity.

6 Continuous Monitoring (ConMon) of Container Images

The DoD requires continuous monitoring of container images even after they are deployed into production. Several types of checks must be performed. First, it's essential to validate that all container images running in production have passed the required security checks. In addition, the images in the container registry and production should be continually checked to identify any new vulnerabilities that may arise after an image is deployed.

ConMon and SBOM Monitoring with Anchore Federal

Anchore Federal uses an SBOM-powered approach to continuously monitor deployed container images. Anchore Federal monitors your container registry for new container images and scans new images to generate an SBOM and identify new vulnerabilities or policy violations. Anchore Federal also inventories your container images running in Kubernetes or ECS environments and provides a summary of your compliance state and vulnerabilities. You can instantly search the SBOM repository for new zero-day vulnerabilities to find container images that use the affected component and identify where the images are deployed in production.

Next Steps

Automate your DevSecOps Practices with Anchore Federal

The DoD is embracing software factories to enable secure and rapid software delivery to warfighters. DoD software factories combine DevSecOps practices and the agility provided by software containers. As DoD programs implement software factories to speed up software development, they must also automate security processes at each stage of the DevSecOps pipeline. Meeting the DoD's security and compliance requirements requires new tools explicitly designed to identify vulnerabilities and security issues in containerized software.

Anchore Federal automates security processes for containerized software to ensure DoD software factories operate smoothly while producing secure software. It is designed to meet the specific needs and requirements of the DoD and is proven across multiple DoD software factories, including Air Force Platform One, Iron Bank, and Navy Black Pearl.

SCHEDULE A DEMO

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. To learn more about Anchore's solutions, visit **Anchore.com.**

anchore

sales@anchore.com

anchore.com