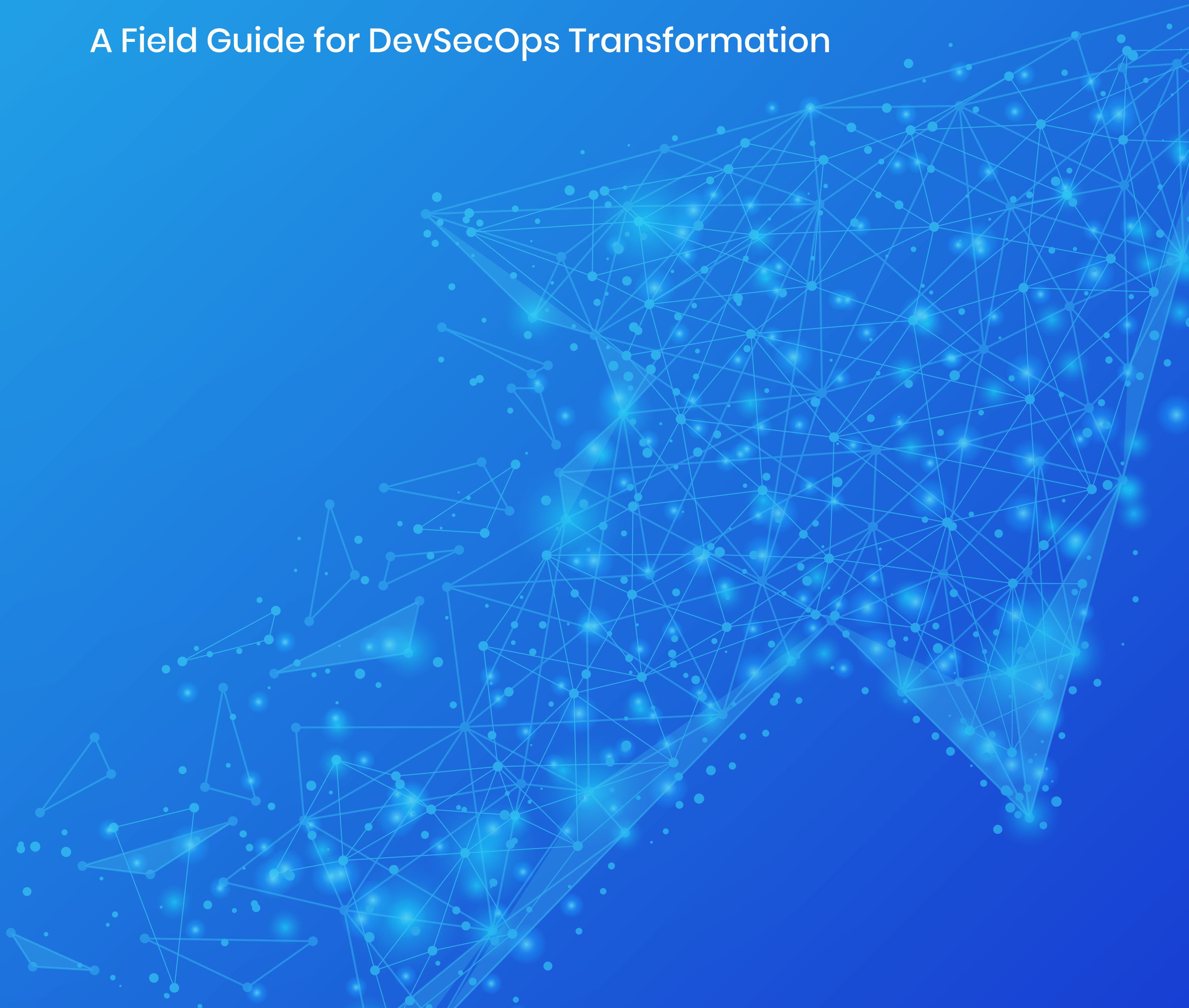
anchore

INSIDE THE ANCHORE TECHNOLOGY SUITE: OPEN SOURCE TO ENTERPRISE

A Field Guide for DevSecOps Transformation



CONTENTS

Executive Summary

Anchore technology enables organizations to achieve their security and compliance automation and 'shift left' objectives by providing a range of open source tools and enterprise products ready for integration into existing and greenfield software delivery life cycle (SDLC) designs. Whether an organization is adding the fundamental modern security functions and content analysis into a container-based toolchain or is ready to centralize, manage and control security and compliance requirements at an organizational level, **Anchore** has the expertise, tools, and products to achieve goals along the journey.

Anchore Toolbox includes open source, lightweight single-purpose tools ideal for individuals, small project teams, and open source projects taking their first steps into container security. While the open source nature of Anchore Toolbox is suitable for integrating into DevSecOps toolchains, the tools are designed to satisfy the basic low-level functions in support of a DevOps to DevSecOps transformation.

Anchore Enterprise targets the container scanning challenges that organizations face during the compliance process, addressing the concerns of Developers, Operations, Security, and Compliance teams by providing a unified analysis and control platform that teams use to communicate and implement security and compliance requirements in practice. This solution includes a graphical policy definition, reporting, security, and other enterprise features to support stringent security and compliance programs.

Introduction

Anchore Toolbox and Anchore Enterprise together provide automated security and compliance controls for DevOps toolchains.

Anchore Toolbox is Anchore's contribution to the open source and DevSecOps communities. The goal for toolbox is to enable wherever you are on your DevSecOps journey. It's Anchore's way to give back and help organizations transform their software delivery through automated compliance using open source tools.

We'd also like to see it to introduce container scanning tools into the DevOps toolchain. Developers and DevOps teams can download Anchore Toolbox and use the single-purpose tools to launch a proof-of-concept security project during their journey from DevOps to DevSecOps.

Anchore Enterprise targets container security challenges at the organization level. It's the container scanning and reporting solution for the Chief Information Security Officer (CISO) and product security team charged with having to shift security left and move their existing DevOps toolchains into the DevSecOps world.

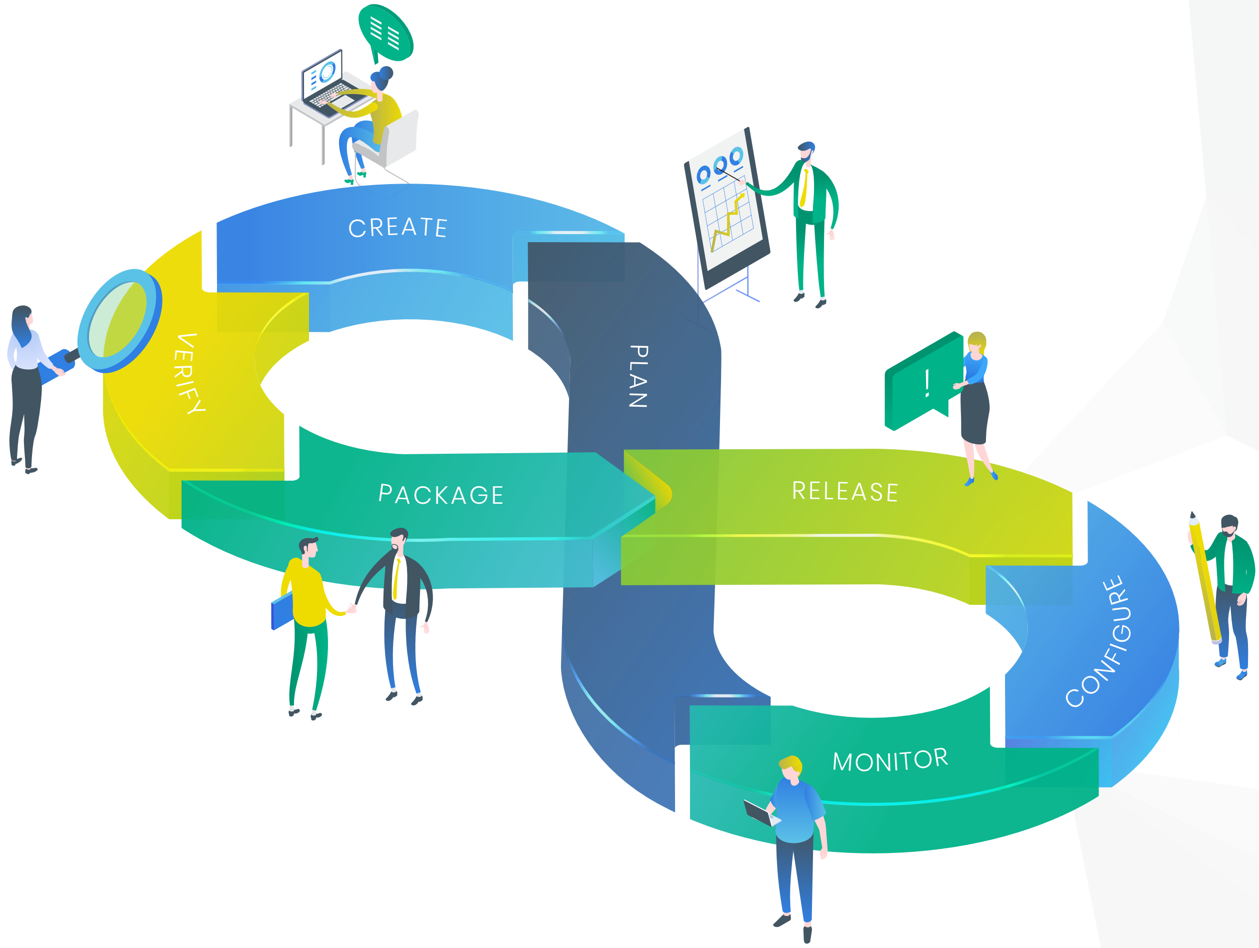
The Role of Containers in DevSecOps Transformation

Containers play a predominant role in DevSecOps transformation, especially with organizations that must adhere to compliance. The **Anchore** technology suite can support customers are every stage of their journey. Toolbox provides the essential functions to add a container vulnerability scanning function into their DevOps toolchain. Anchore Enterprise includes the deep scanning and policy support your enterprise requires ensuring container security and compliance in your continuous integration toolchain.

Container Security and the DevSecOps Tool Chain

Digital transformation in the commercial and public sectors, both before and during the COVID-19 crisis, often drives additional security and compliance requirements. Corporations are moving applications to the cloud to support their now remote workforce and serve their customers better. The United States Department of Defense (DoD) and other government agencies are all pursuing a range of cloud initiatives to support national security, medical research, and other activities that benefit United States citizens.

The DevOps toolchain is continuously evolving and will continue to do so to meet market changes. Still, corporate and federal agency security leaders face the challenge of adapting security tools, policies, and processes to secure their DevOps toolchain and containers in particular without sacrificing delivery velocity.



Anchore Enterprise helps businesses and federal agencies build true DevSecOps toolchains to help them through the challenges of securing containers across the toolchain and keeping them in compliance. You can integrate Anchore Enterprise at each stage of your DevSecOps toolchain, including your development, continuous integration/continuous development (CI/CD) system, image registry, and Kubernetes deployment.

When you shift left with container security, your reporting requirements also multiply. Your systems are collecting more data, which means the volume of your reporting increases. Your security team, management stakeholders, and just as importantly, your auditors will ask for reports that only enterprise reporting features can support. Such features start with a graphical reporting editor to let you create new report formats as necessary. Even better, you want a container security solution that includes prepackaged reports that meet common requests from stakeholders and auditors.

Container Security in the Compliance World

During the container adoption life cycle, security is a common cause of a failed compliance audit and the expensive mitigation that comes after your auditor's findings to return your organization to compliance.

There are compliance standards specific to containers, including the CIS Benchmark for Docker and NIST SP 800-190. Many of the leading federal and commercial compliance standards, such as PCI-DSS, FedRAMP, Security Technical Implementation Guide (STIG), and others, are still moving towards more automation-oriented designs and frameworks.

Supporting container scanning in a compliance environment takes more than a standard DevOps approach.

Open source and proprietary tools provide only partial, uncoordinated solutions that require significant engineering to build an end-to-end container security solution. Service level agreements (SLAs), reporting tools, and access to the latest threat data also vary across these tools.

Policy as Code and the Art of Container Security

Policy as code sometimes called compliance as code, is writing code in a high-level language to automate and manage policy compliance. When your enterprise renders policies in text files, they can apply DevOps tools and processes such as version control, automated testing, and automated deployment to their policies.

Implementing policy as code for containers is best managed outside of your cloud services provider (CSP) dashboard because these tools only work on already deployed containers. Implementing policy as code as part of your DevOps toolchain helps your organization shift policy compliance as part of a DevSecOps transformation.

Anchore Toolbox: Open Source Container Scanning for Individuals and Teams

Anchore has put development resources and time behind the development of Anchore Toolbox to support the open source community. We believe that open source is foundational to the growth and maturation of DevSecOps tools and organizational initiatives.

Toolbox targets DevOps teams who want to introduce container scanning into their infrastructure.

Inside Anchore Toolbox

Anchore Toolbox is an ongoing open source tools project to secure software development toolchains. It means these tools are easy to use, single-use, and built for speed because we designed the tools for integration into CI/CD toolchains. The first two offerings as part of Anchore Toolbox are Syft, a software bill of materials (SBOM) generator, and Grype, a container scanner that checks for known vulnerabilities.

Syft: Create SBOMs

We built Syft as an open source and single-purpose tool to catalog container images and filesystems to discover packages and libraries. Syft supports packages and libraries, including APK, DEB, RPM, Ruby Bundles, Python Wheel/requirements.txt, JavaScript NPM/Yarn, Java JAR/EAR/WAR, Jenkins plugins, JPI/HPI, and Go Modules.

You can use Syft to identify Linux distributions, including Alpine, BusyBox, CentOS/Red Hat, and flavors of Debian and Ubuntu. The tool also supports Docker and OCI image formats.

Grype: Scan Containers

Your developers can use Grype to scan the contents of a container image or file system to find known vulnerabilities. Grype can find vulnerabilities in the following operating systems:

- Alpine
- BusyBox
- CentOS/Red Hat
- Debian
- Ubuntu

Your developers can also use Grype to find vulnerabilities in programming language-specific packages, including:

- Ruby (Bundler)
- Java (JARs)
- JavaScript (NPM/Yarn)
- Python (Egg/Wheel)
- Python pip/requirements.txt/setup.py listings
- Supports Docker and OCI image formats

Future Development for Anchore Toolbox

Anchore Toolbox follows an open source development model that enables testing things in the open and iterating quickly. We plan to continue working with the open source and DevSecOps communities to seek new and interesting concepts for tools to join Anchore Toolbox. Our mission with Anchore Toolbox isn't to build enterprise-level solutions. Instead, it's to provide DevOps teams with reliable open source tools backed by community support that they can integrate into their enterprise environment.

Ideal Use Cases for Anchore Toolbox

The ideal use cases for Anchore Toolbox revolve around individuals and small teams. **Here are some typical use cases:**

- **Open source projects** that want to integrate container scanning into their overall project architecture
- **Open source developers** who want to add container scanning to their development workflows
- **DevOps teams** looking to add basic security checks to their CI/CD pipelines
- **Project teams** in small to medium businesses that are just starting with containers and DevOps
- **Hobbyist and student developers** who want to learn more about container scanning

Anchore Toolbox is a community-supported project with no proper technical support. While **Anchore** strives to provide up-to-date vulnerability data, there are no guarantees around the data's quality or availability. Grype requires always-on internet access, meaning you can't run it in air-gapped environments. Syft doesn't require internet access.

Anchore Enterprise: Security and Compliance Beyond Vulnerability Scanning

Commercial and public sector organizations work in high-stakes security and compliance worlds that require more than just our open source Anchore Toolbox. These organizations require continuous security and compliance plus reporting to satisfy their auditors and maintain compliance.

Inside Anchore Enterprise

Anchore Enterprise is built for enterprise security organizations responsible for security and compliance across business units. Our team built from the ground up as an enterprise-grade container scanning solution that you can integrate into DevSecOps toolchains to help shift container security left.

Here’s an overview of Anchore Enterprise features:

Deep Image Inspection

Anchore Enterprise tackles deep image inspection challenges with Linux-based OCI compliant images and official Microsoft published Windows containers using base image comparison, creating a complete Software Bill of Materials (SBOM). The inspection includes an analysis of every binary or text file in the container filesystem. Indexing all metadata, including name, permissions, hash, and timestamp, also occurs during the inspection. You also have the option to parse optional regex-based file content in a container.

Security Scanning

Anchore Enterprise scans container images to uncover known vulnerabilities in OS and language packages, including NPM, Python, Node, and Java. Your DevSecOps team can run CVE scans, Dockerfile checks for external network calls, insecure syntax usage, lack of best practices, and credential scanning for the leakage for passwords, SSH keys, AWS keys, and other secrets through automation or the Anchore Enterprise dashboard. Anchore Enterprise also includes Operating System vulnerability information for RHEL, CentOS, Debian, Ubuntu, Oracle, Alpine, and Google Distroless.

Compliance & Audit

Compliance takes on a new meaning for corporations and government agencies. Recent events have made them migrate more of their legacy applications to the cloud to support new remote working models for their employees, contractors, and constituents. The Anchore Policy Engine can ensure compliance with defined organizational best practices and regulations.

There’s also out-of-the-box policy support for NIST and Docker CIS. Your developers and compliance team can use Anchore Engine’s graphical policy editor to edit and maintain their security policies in response to new security advisories. The engine also includes policy rules for image metadata, file metadata, file contents, licenses, OS or language vulnerability status (CVSS v2, v3).

The Anchore Enterprise Reporting API (GraphQL) makes it easy for your in-house developers to integrate reporting data into your existing IT operations and cybersecurity reporting tools.

You can also AllowList and DenyList images or files and use per-account policies to govern your container compliance.

The Anchore Policy Engine also lets your security team schedule reports highlighting top security issues.

SDLC Integrations

You can integrate Anchore Enterprise into popular continuous integration/continuous deployment (CI/CD) tools such as Jenkins/CloudBees, CircleCI, Codefresh, CodeReady, GitHub Actions, and Atlassian Bitbucket Pipes. We have customers using Anchore Enterprise in on-premise and cloud implementations.

Anchore Enterprise supports third-party notifications via industry-standard group chat and DevOps tools, including Slack, Microsoft Teams, Atlassian Jira, and GitHub, to notify engineers that their support has run successfully.

Security Integrations

Anchore Enterprise supports role-based access control (RBAC), including global or per-account read only/read write (RO/RW), image submission only, and policy editing rights. There is also support for single sign-on (SSO) and industry-standard enterprise authentication standards such as lightweight directory access protocol (LDAP) and security assertion markup language (SAML). There's a local feed service for internet-disconnected or air-gapped environments plus Prometheus support.

Ideal Use Cases for Anchore Enterprise

Anchore Enterprise targets product security teams with enterprise responsibility for DevOps, DevSecOps, and application security in their organization. It delivers transparency by unpacking a container so your security team can determine what's inside. Our solution can integrate into multiple SDLC stages, including the CI/CD pipeline, the artifact registry, or Kubernetes itself. Your operations team can also use Anchore Enterprise to model internal and external compliance requirements from your security team and auditors. All the while, your security teams gain audit/response tools to enable them to see what's running inside the containers they're scanning in your DevSecOps toolchain.

Here are some ideal use cases for Anchore Enterprise:

- **Adding another level of security** to your DevOps toolchain as you transition from DevOps to full DevSecOps and prevent dangerous image builds from proceeding and compromising your end-customers and mission-critical applications
- **Protecting your container supply chain** from compromised containers
- **Registry scanning to stop the** publication and reuse of nonconforming images before they reach production
- **Preventing images that haven't been** scanned from being deployed into Kubernetes

The Right Tool for DevSecOps Transformation

Choosing Anchore Enterprise versus Anchore Toolbox comes down to the scale at which your security team plays in your enterprise. Large enterprises with a centralized CISO office or product security team with corporate-level responsibilities will want Anchore Enterprise with its policy, persistence, notifications, and compliance.

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