Anchore Capabilities Statement

At-A-Glance

- Founded in 2016 in Santa Barbara, California
- U.S. government-accredited small business
- Enterprise and open source expertise
- Named as a required scanning tool in the DoD Container Hardening Guide and Container Image Creation and Deployment Guide
- Used across DoD and Civilian agencies since 2018

SAM.GOV PROFILE

Anchore, Inc.
SAM.gov ID: RDJDDMKSQKT5
DUNS: 080887744
CAGE Code: 8E6S8
Status: Active
SIC Code 73, 737 NAICS 541715 (Primary) & 541990
Renewal Date: 08/13/2022

PURPOSE OF REGISTRATION

All awards

CONTACT INFO

Anchore HQ
800 Presidio Ave. Ste. B
Santa Barbara, CA, 93101-2210
United States
(805) 456-8981
federal@anchore.com

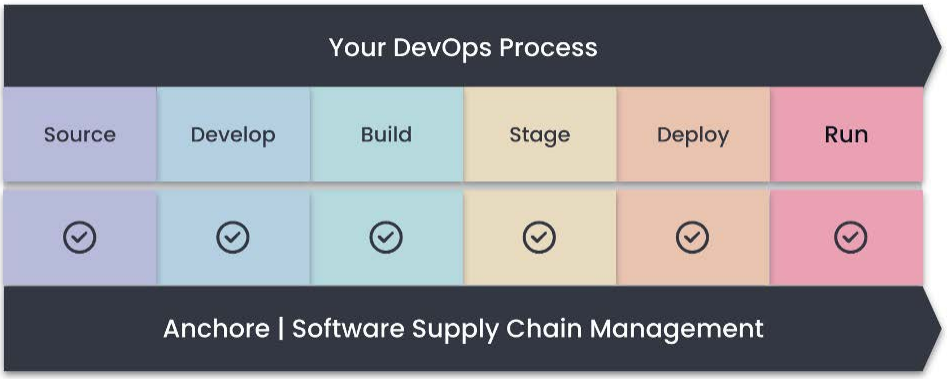
CONTRACTS (VIA CARAHSOFT)

SEWP, ITES, GSA, & 2GIT

About Anchore

Anchore is the first SBOM-powered software supply chain management platform to help government agencies reduce risk and increase transparency in software supply chains. A software bill of materials (SBOM) is foundational to identifying and remediating security risks faster and providing continuous monitoring for new or zero-day vulnerabilities. By using Anchore to generate and analyze SBOMs for applications at every step of the software development lifecycle, government agencies can achieve end-to-end software supply chain security.

Anchore automates security checks at each step in the DevOps process for a frictionless developer experience that optimizes velocity.



Anchore Key Capabilities & Benefits

✓ Flexible Policies for Compliance

Enforce compliance with internal standards and with U.S. government standards, including DoD, DISA STIG, FedRAMP, NIST, CIS Benchmarks, and more using pre-built policy packs or custom policy rules.

✓ Air-Gapped Deployments

Deploy Anchore on-premises with no internet connection in order to run in DoD IL-6 environments.

✓ Vulnerability Scanning and False Positive Management

Scan images for malicious code and secrets in source code repositories, development environments, CI/CD pipelines, container registries, and runtime environments while reducing false positives and false negatives.

✓ End-to-End SBOM Management

Automatically generate comprehensive SBOMs at each step in the development lifecycle and store them in a repository for use in checking for existing vulnerabilities and then continuously monitoring for new vulnerabilities and risks — even post-deployment.

✓ Open Source Dependency Tracking

Use SBOMs to scan throughout the development cycle for both direct and transitive dependencies to pinpoint relevant open source vulnerabilities and to enforce policy rules.

✓ Application-Level View of Risk

Tag and group all artifacts associated with an application, release, or service so you can report on vulnerabilities at the application level and monitor each application release for new risks — including zero-day vulnerabilities.

✓ Drift Detection

Detect drift in the software build process by setting policy rules that alert when components are added, changed, or removed to quickly identify new vulnerabilities, developer errors, and malicious efforts to infiltrate builds.

✓ Notifications and Alerts

Use email, Slack, Jira, webhooks, or GitHub to notify developers and security teams of policy violations, secrets, malware, and more so they can take corrective action.

✓ Remediation Recommendations

Reduce developer time spent fixing vulnerabilities with remediation recommendations and automated workflows to quickly resolve issues.

✓ Continuous Visibility and Monitoring

Identify and manage security/compliance issues with images running in your Kubernetes clusters to identify containers that are unscanned, have new vulnerabilities, malware, or other compliance issues.

✓ Security Reports and Audits

See the big picture with flexible reporting and easy-to-use dashboards for security teams or consume data through an API.

✓ Integrations

Leverage fully supported integrations (powered by 100% API coverage) with the tools you already use such as all major developer tools, CI/CD tools, container registries, and container platforms.

✓ Enhanced Vulnerability Data

Access enhanced vulnerability data with a custom feed that curates data from multiple sources, which optimizes matching and minimizes false positives.

✓ Streamlined DISA STIG Checks

Automate STIG checks against container environments to ease compliance efforts.

The Anchore Mission

The Anchore team of developers, cybersecurity experts, and IT operations veterans help government agencies secure their containerized applications and automate compliance. We believe that a software bill of materials, or SBOM, is foundational to true end-to-end security because you must first know what is in your software before you can secure it. Even prior to its mandated use by Executive Order, the SBOM was the cornerstone of Anchore solutions designed to support federal DevSecOps initiatives.

Contact Us

federal@anchore.com

+1 (805) 456-8981