anchore

CASE STUDY

Sabel Systems Leverages Anchore SBOM and SECURE to Scale Compliance While Reducing Vulnerability Review Time by 75%

Sabel Systems, a managed DevSecOps pipeline platform provider for the defense industry, reduced vulnerability review from 2 weeks to 3 days using Anchore Enterprise while maintaining zero critical vulnerabilities in multiple IL5 environments. The Code Foundry platform enables DoD missions to achieve both platform and vehicle ATO through automated security scanning and compliance workflows that provide real-time transparency to government auditors.

SABEL SYSTEMS

Beavercreek, OH
www.sabelsystems.com

INDUSTRY
Information Technology

SEGMENT
Secure Development Pipeline-as-a-Service

Problems

- Manual vulnerability review cannot scale with application growth
- DoD customers required cloud-agnostic, IL5-compliant DevSecOps solutions for accelerated ATO
- Complex environment demanded seamless integration across multiple CI/CD tools and cloud providers

Solutions

Anchore Enterprise delivered:

- Automated vulnerability scanning and SBOM generation integrated into CI/CD pipelines
- On-premise IL5-ready deployment with DoD policy packs for automated compliance
- API-first architecture enabling flexible integration across GitLab, Jenkins, and Kubernetes

Results

- 75% reduction in vulnerability review time (from 1-2 weeks to 3 days)
- Scaled zero critical vulnerabilities policy across 100+ applications
- Real-time audit transparency through compliance evidence dashboards

Introduction

Sabel Systems provides a managed DevSecOps pipeline-as-a-service for Department of Defense (DoD) missions and defense contractors developing mission-critical vehicle systems. The company's Code Foundry platform fills a crucial gap in the marketplace by offering a comprehensive software development platform specifically designed for applications that must run on air-gapped, field systems rather than traditional, cloud-dependent, web deployments.

Code Foundry operates as a platform-agnostic solution that is designed to operate across different infrastructure environments (e.g., AWS GovCloud, private DoD-approved cloud, and on-premise infrastructure). With a lean team of 10 supporting 100+ active developers, the platform manages hundreds of applications for next-generation military vehicles.

Problems

Sabel Systems faced three critical challenges in delivering a DevSecOps platform that could meet the demanding requirements of DoD vehicle development programs:

» Manual vulnerability review cannot scale with growth

As Sabel Systems supported Army, Air Force, and Navy Digital Engineering initiatives, a common challenge emerged within their software acquisition pathway. The DoD security teams were unable to adequately support the 100+ developers they served. The manual review process—time-consuming, labor-intensive, and prone to error—became a bottleneck that threatened the platform's ability to fulfill its mandate of producing secure applications. This inefficiency underscored the urgent need for a scalable solution. What had worked in the early days was now buckling under the pressure of scaling a successful business.

To address this, Sabel Systems designed its Code Foundry architecture to eliminate the need for the DoD's standard manual vulnerability review process and ensure the software acquisition pathway could scale to support enterprise-level functionality.

» DOD customer demanded exacting compliance and deployment cababilities

Code Foundry customers operate in one of the most demanding technical environments in software development: DoD vehicle systems that must achieve Authority to Operate (ATO) before field deployment. The DoD software acquisition pathway mandates modern DevSecOps practices but within fully air-gapped environments; a challenge for many traditional cloud-based security tools.

Beyond technical requirements, Code Foundry needed to support the complex organizational structure within the DoD. Different military branches have distinct preferences for cloud environments and security protocols, requiring a truly agnostic solution that can be deployed anywhere while maintaining consistent security standards.

» Technical aritecture required seamless multi-tool integration in controlled environments

Code Foundry's technical architecture presented unique integration challenges. Operating in IL5 (controlled unclassified) environments on NIPR networks means that the security software must run without external connectivity. Additional requirements are seamless integration with diverse CI/CD toolchains such as GitLab, Jenkins, Bitbucket, GitHub, and various Kubernetes distributions without requiring extensive per-environment configuration.

Solutions

Sabel Systems selected Anchore Enterprise to scale their vulnerability management across hundreds of applications with limited resources, streamline compliance workflows, and leverage a platform purpose-built for DoD environments.

» Automated vulnerability scanning enables scale without additional headcount

Sabel Systems' lean security was able to remove manual review bottlenecks with Anchore Enterprise and is now able to support their growing customer base and applications without adding personnel. Anchore Enterprise's automated approach allows the same 10-person security team to effectively support 100s of applications across multiple DoD contractors. Anchore Enterprise integrates directly into Code Foundry's CI/CD pipelines, automatically scanning every container image as soon as it's built and providing immediate feedback on security posture. Rather than security reviews becoming a constraint on business growth, they now happen seamlessly in the background.

» On-premises deployment meets DoD security and compliance requirements

Anchore Enterprise's DoD-tailored on-premise and IL5-compliant deployment capabilities deliver comprehensive security entirely within government-approved infrastructure.

Anchore Enterprise includes pre-built policy packs specifically designed for DoD requirements, including FedRAMP, NIST, and STIG compliance frameworks. Through automated compliance enforcement, Code Foundry customers receive real-time notifications of compliance issues, enabling them to address problems early in development rather than discovering them during costly ATO audits. This proactive approach helps customers build their ATO packages with confidence while avoiding the time-consuming remediation cycles that typically delay program timelines.

Anchore Enterprise's native compliance dashboards and reporting offer the DoD auditors real-time transparency into the compliance state of all parties. Instead of waiting weeks for static compliance reports, auditors access live security data directly, creating dynamic review meetings and building trust through transparency.

» API-first architecture enables flexible integration across diverse environments

Anchore Enterprise's API-first architecture deploys via Helm charts into Kubernetes clusters and integrates seamlessly with GitLab CI, Jenkins, and other CI/CD tools that different military branches prefer.

Anchore CTL, the vulnerability scanner for Anchore Enterprise, executes scans directly within the Kubernetes cluster, a critical security advantage for modern infrastructure teams. By baking AnchoreCTL directly into Code Foundry, Sabel Systems created a secure approach that eliminates the need to open network connections to external systems. This addresses a common security concern where external security tools create potential attack vectors.

"We include AnchoreCTL in an image and use that image to run the scanning and analysis steps. We do that so we can keep all the connections inside of the cluster without having to SSH into an already running pod."

—Robert McKay, Digital Solutions Architect, Code Foundry, Sabel Systems

Results

The implementation of Anchore Enterprise transformed Sabel Systems' operational efficiency and positioned Code Foundry as the premier DoD DevSecOps platform:

» Zero critical vulnerabilities maintained across 100+ applications

Anchore Enterprise enables Code Foundry to maintain their strict security policy of **zero critical or high vulnerabilities at scale**. This level of security assurance is essential for applications that will eventually deploy to mission-critical vehicle systems.

» 75% reduction in vulnerability review time

Code Foundry's now automated vulnerability review process was **cut from 1-2 weeks to 3-days** leading to faster platform updates and more responsive customer support.

"Before Anchore, it would take us a week to two weeks to go through everything that an image could have—we'd have to first build the actual software on the image and then go through all the different connection points and dependencies. Using Anchore has brought that down to a 3-day review time."

—Robert McKay, Digital Solutions Architect, Code Foundry, Sabel Systems

» Real-time audit transparency replaces static deliverables

Code Foundry now provides government reviewers with live access to security dashboards and compliance data. This transparency accelerates the review process and builds trust between contractors and government oversight teams.

"The idea is that you can replace your static contract deliverables with dynamic ones – doing review meetings based on Anchore's live data instead of 'here's my written report that took me a week to write up on what we found last week,' and by the time the government gets it, it's now 2-3 weeks old."

—Joe Bem, Senior Manager, Code Foundry, Sabel Systems

By leveraging Anchore Enterprise, Sabel Systems has established Code Foundry as the trusted platform for DoD contractors requiring the highest levels of security, compliance, and operational efficiency in their software development workflows.

Request a demo

anchore

sales@anchore.com
anchore.com