anchore

CASE STUDY

75% time savings through automated vulnerability management & transparent security

DreamFactory, an API generation platform serving highly regulated organizations required an air-gapped vulnerability scanning and management solution that didn't slow down their productivity. Avoiding security breaches and compliance failures are non-negotiables for the team to maintain customer satisfaction.

DreamFactory

Las Vegas, Nevada
www.dreamfactory.com

INDUSTRY
Software development

SEGMENT
API management

Challenges

- Secure deployments without cloud connectivity
- Air-gapped vulnerability scans for highly regulated industries
- Highly regulated industries require high trust partnerships

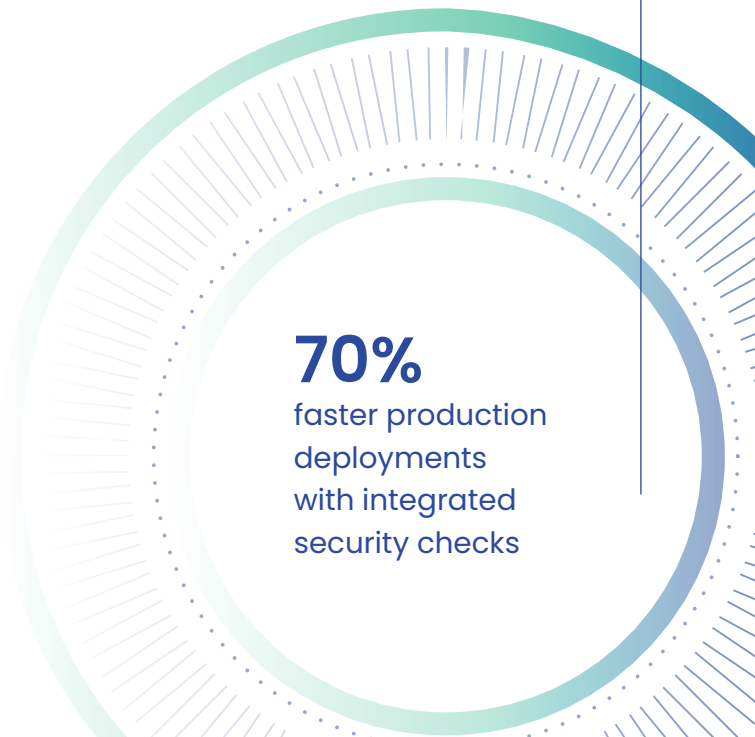
Solutions

Anchore Enterprise secures the software supply chain with:

- Support for on-premises and air-gapped deployments
- Comprehensive vulnerability scanning integrated into CI/CD pipeline
- Automated SBOM generation to build trust fast

Results

- 75% reduction in time spent on vulnerability management and compliance requirements
- 70% faster production deployments with integrated security checks
- Rapid trust development through transparency



Introduction

DreamFactory is an API generation platform that puts a REST API endpoint in front of every table, view, or stored procedure in a database. It then wraps every endpoint in enterprise-grade security, including role-based access control (RBAC), key management, authentication, and rate limiting. With industry estimates reporting that 70% of APIs are internal or private, DreamFactory's solution is critical for organizations looking to streamline their API development process securely.

Built on a Laravel (PHP) web application with Redis and MySQL, DreamFactory releases a new major version quarterly while running daily security scans. The DreamFactory product is designed for on-premises deployment. Anchore Enterprise is deployed in AWS and GitHub actions make callbacks to Anchore for security checks.

Challenge

DreamFactory faced several critical challenges in meeting the needs of its customers, particularly those in the defense community and other highly regulated industries:

» Secure deployments without cloud connectivity

With the ascent of the cloud deployment pattern, always-on internet connectivity became a foundational assumption for customer deployments. Modern software supply chain security took this to heart by adopting continuous scanning strategies that required direct access to production services.

DreamFactory works with the DoD and other highly regulated organizations, such as Oil and Gas. The data that is processed by these organizations have the highest national security implications. The assumption of always-on connectivity no longer holds. On-premises deployments are mandatory, and air-gapping is almost always required. This broke the assumptions of modern software supply chain security strategies and required new solutions to deliver bulletproof security without cloud connectivity.

» Air-gapped vulnerability scans for highly regulated industries

Typically, if software is run on-prem and air-gapped the need for vulnerability scanning is not required. If vulnerabilities do exist they are not considered a priority due to the fact that they have no external connectivity that gives an adversary remote access to the service.

While this is common practice in the enterprise world, this is not the case in highly regulated environments. Both air-gapping and vulnerability reporting are mandatory to protect the data that these organizations process.

» Highly regulated industries demand high trust partnerships

In highly regulated industries, particularly those involved with national security or critical infrastructure trust is a necessity rather than a nice-to-have. Organizations like the DoD and critical infrastructure providers operate in high-stakes environments where security breaches or compliance failures can have catastrophic consequences. The potential to compromise national security, endangering lives, or cause severe financial damage is ever present.

These entities face constant, sophisticated threats from state-sponsored actors, cybercriminals, and other malicious entities. In this context, every software component, partnership, and integration point represents a potential vulnerability that adversaries could exploit, making rapid establishment of trust crucial.

Solution

DreamFactory implemented Anchore Enterprise to address these challenges:

» Support for On-Premise and Air-Gapped Deployments

The same as Dreamfactory, Anchore Enterprise was designed from the ground up to be deployed on-prem and continue to operate in air-gapped environments. External network connectivity is not a requirement for running any of Anchore Enterprise's security features or services.

This alignment made Anchore the obvious choice for Dreamfactory as they sought out partners to help them meet the requirements of their customer base.

» Comprehensive Vulnerability Scanning

In order to generate vulnerability reports without having access to the air-gapped deployments, Dreamfactory integrated Anchore Enterprise into its own build pipeline and ran daily vulnerability scans on all deployment versions. Dreamfactory then notifies their customer's of urgent vulnerability updates, fulfilling their commitment to continuous vulnerability scanning and compliance.

By catching the vulnerabilities in our build pipeline, we can then inform our customers and prevent any of the APIs created by a Dreamfactory install from being leveraged to exploit our customer's network. Anchore has helped us achieve this massive value-add for our customers.

—Terence Bennet, CEO, Dreamfactory

» Automatic SBOM Generation

Anchore's automated SBOM generation is directly integrated into Dreamfactory's build pipeline so that every build is cataloged and stored for reference. An SBOM serves as a trust accelerator in a high-threat environment. It provides immediate transparency into the software's ingredients which enables fast risk assessment and compliance verification.

Since the publication of Executive Order 14028, "Improving the Nation's Cybersecurity" in 2021 all branches of the federal government have taken the "suggestion" that SBOMs are a necessary element of software supply chain security seriously.

We're seeing a lot of traction with data warehousing use-cases. Security is absolutely critical for these environments. Being able to bring an SBOM to the conversation at the very beginning completely changes the conversation and allows CISOs to say, 'let's give this a go'.

—Terence Bennet, CEO, Dreamfactory

Results

» The implementation of Anchore Enterprise transformed Dreamfactory's security posture and business operations:

» 75% reduction in time spent on vulnerability management and compliance requirements: Automated vulnerability scanning and reporting, even for air-gapped deployments frees up engineering cycles for mission critical work.

» 70% faster production deployments: With vulnerability scans integrated into the CI/CD pipeline, Dreamfactory can deploy updates more rapidly without compromising security.

» Rapid trust development through transparency: An automated and complete SBOM record accelerates trust development in an environment where the stakes are unparalleled.

"Anchore has not only helped us meet the stringent requirements of organizations like the DoD," concludes Bennet, "but it has also given us a competitive edge in the market. We're now able to provide a level of transparency and security that our customers in highly regulated industries demand, all while maintaining the efficiency of our development and deployment processes."

By leveraging Anchore Enterprise, Dreamfactory has positioned itself as a trusted partner for organizations requiring the highest levels of security and compliance in their API management solutions.

Request a demo

Watch Now

anchore

sales@anchore.com

anchore.com