anchore | Case Study

NVIDIA

The NVIDIA Product Security organization transitioned from Anchore open source to Anchore Enterprise for continuous container security, driving increased scalability and productivity, policy-based compliance, and role-based reporting for business units and security teams.

NVIDIA at a Glance

Santa Clara, CA | www.nvidia.com

Industry: GPU Manufacturing

Revenue: $27B | Fortune 50

Challenges

- Significant container use with thousands of containerized apps, and hundreds of thousands of containers
- Provide a scalable security process to support growing container adoption with diverse requirements across business units, including large containers of up to 25 GB+
- Address the critical security requirements of NVIDIA GPU Cloud (NGC), a curated catalog of GPU-optimized software containers for NVIDIA customers
- Current security scanning tools for traditional software didn't work for containers. They were complicated to use, time consuming to run, and generated too many false positives
- Automate security checks across multiple CI/CD toolchains, registries, and Kubernetes platforms used by different business units

Solutions

Anchore Enterprise	Anchore Syft

Results

- Improved developer and security team productivity with a centrally-hosted version of Anchore Enterprise
- Ability to ramp up scanning and speed CI/ CD pipelines due to scalable architecture of Anchore
- Robust, fully-documented APIs for Anchore made it quick and easy to integrate with multiple CI/CD tools and registries as well as existing product security processes
- Improved inline scanning for CI/CD pipelines to enable vulnerabilities to be identified early in the cycle, avoiding delays
- Reduced number of false positives due to Anchore's optimized use of vendor-specific vulnerability feeds
- Utilized Anchore's flexible policy engine to allow each business unit to create and run their own compliance checks
- Centralized metrics for the security team on container scans and results

Introduction

NVIDIA is an organization known for its GPUs utilized in computing tasks as diverse as computer graphics rendering and cryptocurrency mining. The most important new use case that GPUs have been utilized to solve is artificial intelligence (AI) and machine learning (ML) tasks. NVIDIA has invested in this segment from both a hardware and software perspective. In 2017 they launched NVIDIA GPU Cloud (NGC) a cloud platform that is specifically designed to power AI/ML workloads. NGC brings together NVIDIA managed GPU infrastructure as well as the AI/ML software components that are industry standard to create a platform that makes it simple to train generative large language models, object detection models, text-to-speech models, and more.

"Our goal was to integrate DevSecOps principles into our SDLC and build an "easy button" for developers to get their code scanned and secured."

The NGC platform is a curated container catalog that hosts a broad range of software including generative AI models, deep learning frameworks, high performance computing (HPC) and visualization applications that maximize the utilization of NVIDIA's GPU environments. Given that NGC is publicly available for NVIDIA users and customers, software hosted on NGC must undergo scans by Anchore against an aggregated set of common vulnerabilities and exposures (CVEs), as well as secrets and private keys.

"We were able to actually scale our container security program while saving money."

The results of security scans from Anchore Enterprise are housed in nSpect, an enterprise-wide reporting platform where the product security team collects data from each software development team about known vulnerabilities and dependencies in their applications. Anchore Enterprise will be used across development teams to enable inline scanning of containers during the CI/CD process, providing vulnerability reports to nSpect via API. The nSPect data is used to deliver security reports to the VPs of each business unit showing their risk profile.

The NVIDIA Product Security organization — an arm of the Software GPU division that reports directly to NVIDIA's CEO — transitioned from Anchore open source to Anchore Enterprise to provide scalable inline container scanning in their CI/CD pipeline, centralized container security reporting, and an API-friendly solution that would integrate into the myriad of different DevOps tools used across their business units.

Previously, NVIDIA was using Anchore open source. However, NVIDIA had not set up a centrally-hosted version of Anchore, creating overhead for each development team. By deploying a centrally-hosted version of Anchore Enterprise, the NVIDIA product security team created a scalable solution, a better experience for development teams, with a goal for providing each business unit VP visibility into their risk profile.

Challenge

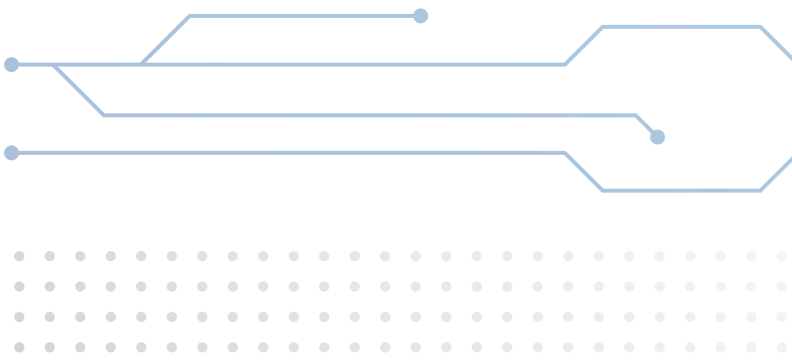
As container adoption accelerated, NVIDIA needed a way to implement security scans for containerized apps throughout the development process. NVIDIA uses containers at a large scale with thousands of containerized apps, and hundreds of thousands of containers. One of their larger teams pushes tens of thousands of containers a day through the development pipeline. NVIDIA also faced a unique challenge because of the large container image sizes they must scan in their pipelines. It was critical that they choose a container security solution that they could easily embed in their development process and scale effectively to avoid creating any bottlenecks.

"Anchore gives us a centralized point with logging and metrics for a complete picture of our container security. We know exactly how many teams are scanning and what sort of images are failing."

Each application team at NVIDIA selects their own tools. This constraint focused the product security team on sourcing a container scanning tool that could easily integrate via APIs with a broad range of CI/CD pipelines including TeamCity, GitLab, Jenkins, Azure, Google Cloud and homegrown solutions. The tool also had to integrate with registries including Docker Hub, Quay, GitLab, and NGC.

"We are API-driven so our end users do not use the UI. The Anchore API is completely documented and provides nice REST response codes that are much more obvious to the developers."

While NVIDIA already had security scanning tools for traditional software, these tools didn't work for containers. They were complicated to use, time consuming to run, and generated too many false positives. Reducing false positives was an important requirement for the NVIDIA product security team and the developers they support. While almost every scanning solution can identify a Python package and provide a list of vulnerabilities, NVIDIA needed the ability to identify vendor-specific variants (such as Ubuntu with OpenSSL patches) and then to include only vulnerabilities that had not been patched in the version that was being used. Without granular identification, developers receive too many false positives, leading them to ignore the security team.



Solution

The NVIDIA team got Anchore Enterprise up and running within an hour using the Helm charts and documentation provided by Anchore. With a scalable architecture, Anchore Enterprise can scan high volumes of containers without causing large delays in development pipelines

"Almost anyone can identify a pipeline package, but if you can't tie it back to a vendor's versions, you get a huge list of false positives. Anchore is way ahead of the game, leveraging vendor-specific vulnerability feeds which results in fewer false positives."

NVIDIA is API-driven and developers use the Anchore Enterprise API to integrate directly into their CI/CD pipelines. NVIDIA was able to leverage Anchore's robust, fully-documented APIs and REST response codes that are meaningful to developers.

NVIDIA wanted to decentralize security policies, allowing each business unit to set their own policies. Teams can define policy documents tied to the SHA of individual files, and if teams choose to bypass a vulnerability, they can adjust their policy and document the exception.

Anchore Enterprise provides NVIDIA with a centralized point where the security team can get logs and metrics that show how many people are conducting scans, what images are failing, and related information.

NVIDIA uses the Anchore's command line tool, AnchoreCTL (based on the open source project Syft), to generate SBOMs from the pipeline and then post them in Anchore Enterprise.

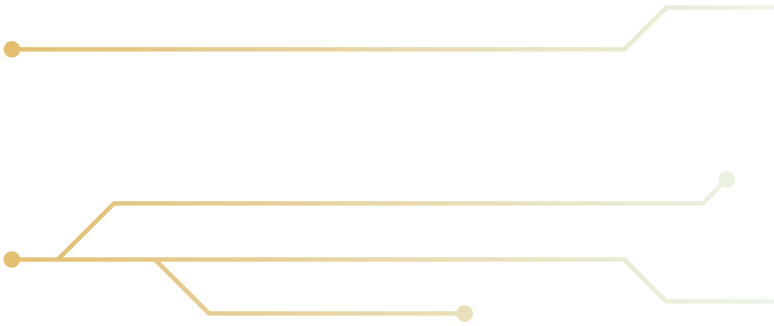
"Anchore's architecture has worker threads that can scale up and scan quickly, keeping the development pipeline moving as the number of containers increases."

Results

By implementing Anchore Enterprise, NVIDIA teams can scan containers during the development process before they ship to internal and external customers. This ensures a high level of security and empowers development teams with the responsibility of resolving security issues prior to release time.

Moving to a hosted solution and Anchore Enterprise enables the NVIDIA product security team to provide a scalable solution that addresses the scanning challenges that the large containers in the NGC pose without a loss in developer or security team productivity. The move also lets them get their false positive challenges under control, saving developers and the security team time.

> ***"I was able to get up and running in an hour with Anchore Enterprise using just the documentation and the Helm charts provided by Anchore. When I found areas for improvement in the docs, I was able to submit merge requests and they were quickly approved."***



About Anchore

Anchore, Inc., based in Santa Barbara, CA, was founded in 2016 by Saïd Ziouani and Daniel Nurmi to help organizations combat the growing complexity of software supply chain security. They recognized how the proliferation of cloud native workflows and the explosion of the open source ecosystem would create significant complexity to traditional software supply chain security. Anchore Enterprise was designed to combat this emerging trend and allow developers to reap the benefits of increased velocity without compromising the security of the software that is delivered. With Anchore, DevSecOps teams can establish a flexible, policy-based approach to their risk management program. Anchore is trusted by Fortune 100 companies and the most stringent federal agencies across the globe.

Contact Us

Anchore, Inc. • 800 Presidio Ave. Ste. B • Santa Barbara, CA, 93101-2210 • United States

(805) 456-8981 • sales@anchore.com

anchore