anchore

CASE STUDY

Mattermost Reduces Alert Fatigue and Accelerates NIST Compliance with Anchore

Mattermost, a secure collaboration platform built for defense, government and critical infrastructure environments, required deep container-level visibility to support NIST-aligned security requirements for highly regulated customers. By integrating Anchore Enterprise into their GitHub Actions pipeline, and adopting distroless images, Mattermost replaced noisy, manual scanning processes with a centralized, policy-driven workflow that reduced false positives and strengthened continuous compliance operations.

Mattermost

Palo Alto, CA
www.mattermost.com

INDUSTRY
Software development

SEGMENT
Secure Collaboration Platform

Challenges

- Fragmented scanning tools prevented centralized, deep visibility into OS container vulnerabilities.
- Manual vulnerability review processes and previous tools generated excessive false-positive noise that wasted valuable engineering time.
- A highly regulated defense and critical infrastructure customer base required centralized vulnerability visibility and alignment with stringent security frameworks including NIST 800-53.

Solutions

Anchore Enterprise secures the software supply chain with:

- Automated container vulnerability scanning integrated directly into GitHub Actions, inspecting exactly what is installed within container images to eliminate false positives across all release candidates.
- Adoption of hardened Chainguard distroless images alongside Anchore's automated policy enforcement helped establish a "Start Safe, Stay Secure" posture.
- A closed-loop remediation workflow integrated with Jira and custom playbooks to prioritize and track fixes.

Results

- Reduced developer alert fatigue and improved vulnerability signal quality by eliminating false-positive noise through Anchore's accurate, on-disk scanning.
- Centralized vulnerability management across all production container images, closing a critical security blind spot.
- Automated continuous validation against NIST-aligned security policies while future-proofing for upcoming defense STIG requirements.

Introduction

Mattermost is a secure, open-source collaboration platform purpose-built for technical and operational teams in high-trust environments. Strict adherence to federal compliance frameworks, particularly NIST 800-53, is foundational for serving their customer base of defense agencies and critical infrastructure operators.

While Mattermost had strong application-level security practices in place, they recognized a necessity to enhance their container strategy. Legacy SCA tools and manual open-source scanners lacked structured visibility into the underlying operating system (OS) vulnerabilities hidden within containers, creating blind spots and generating false-positive noise. They needed a centralized solution to improve visibility, eliminate alert fatigue, and operationalize continuous compliance practices without slowing development velocity.

Challenges

» Legacy SCA tools create an OS security blind spot

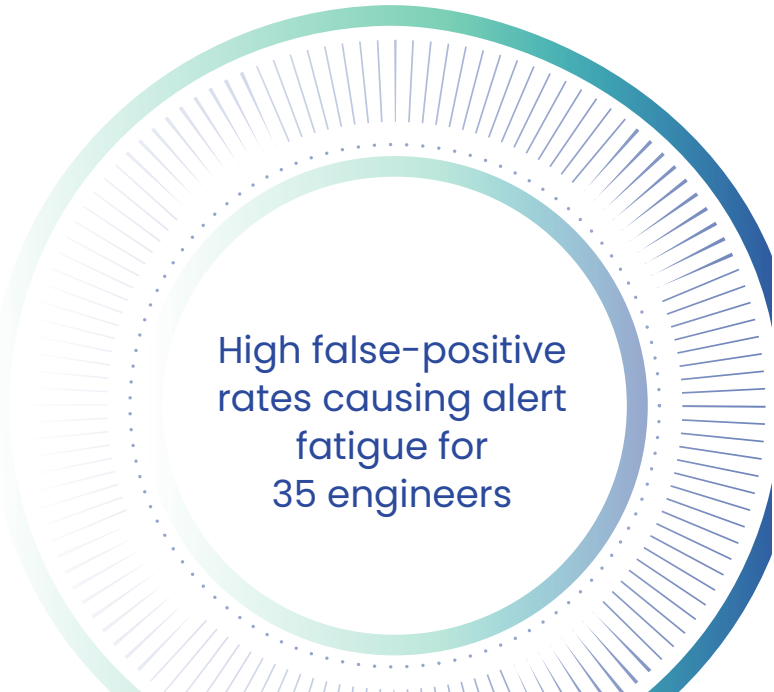
When shipping software in containers, organizations distribute an entire operating system alongside their application. Mattermost's existing dependency tools generated application-level visibility, but they lacked a dedicated, unified solution for OS-level vulnerabilities within container images.

» Manual vulnerability reviews waste engineering time

Previously, the security team relied on a manual, disjointed process to review vulnerabilities. Developers had to pull images locally to their machines and run open source CLI scanners. Not only did this create operational silos, but the heuristic nature of these tools generated excessive alert noise and inconsistent results, forcing the engineering team of ~35 developers to waste valuable time chasing non-existent threats.

» Defense and critical infrastructure customer base demand centralized compliance reporting

Defense agencies operate under strict mandates requiring every software component to meet verified security standards. Frameworks like NIST 800-53 provide the immediate benchmarks for hardening systems and documenting required security controls, while the ability to scale into future DISA STIG requirements remains critical for growth. Mattermost required a centralized system to ensure continued adherence to the stringent demands of government and regulated industry markets.



Solutions

Mattermost selected Anchore Enterprise as their centralized container security platform to solve the compliance and visibility challenges presented by their highly regulated defense and critical infrastructure customer base:

» Native CI/CD integration eliminates false-positive fatigue

Mattermost eliminated dependency on local scanning by integrating Anchore Enterprise directly into their release pipelines using a reusable GitHub Action. Anchore now automatically scans every release candidate (RC) and final release. Anchore's highly accurate approach which looks specifically at what is physically installed on the image rather than making heuristic assumptions, effectively eliminated the false-positive noise that had previously plagued the team.

» Integrated DevSecOps pipelines automate the vulnerability remediation lifecycle

Mattermost established a seamless workflow that connects security findings directly to engineering action. When Anchore identifies a vulnerability during a scan, the system generates a Jira ticket for remediation tracking. This automatically initiates an internal playbook and creates a dedicated Mattermost channel for the security and engineering teams to securely collaborate on the fix. Release candidates automatically trigger Anchore scans through GitHub Actions to evaluate compliance against Mattermost's NIST-aligned policy framework. When violations are identified, Jira tickets and internal remediation workflows are automatically initiated, enabling security and engineering teams to coordinate resolution before software reaches production.

"Anchore Enterprise is basically the glue that binds all of our existing steps and creates a loop. It finds vulnerabilities, automatically creates Jira tickets, coordinates with our engineering teams, and then scans again to validate the fix…and all of this is automated."

—Eva Sarafianou, Senior Engineering Lead, Product Security & Release, Mattermost

» Validating a "Start Safe, Stay Secure and Compliant" foundation

Mattermost adopted a "Start Safe, Stay Secure and Compliant" framework through the strategic technology partnership between Anchore and Chainguard. To drastically reduce their attack surface, they migrated to"distroless" container images—shrinking image sizes by 97% (from ~75MB to ~2MB) and reducing OS level vulnerabilities so developers can focus on their applications.

However, establishing this secure baseline only covers the "Start Safe" phase. To "Stay Secure and Compliant," Anchore Enterprise acts as the continuous validation layer. Anchore deeply monitors the pipeline, ensuring Mattermost developers can safely build upon these optimized images without introducing vulnerabilities into their monthly releases.

» Scalable policy enforcement for defense customers

Serving defense and critical infrastructure customers requires strict adherence to federal security frameworks. Anchore enabled Mattermost to transition from ad-hoc manual reviews to automated policy-as-code. By implementing Anchore's out-of-the-box NIST 800-53 policy pack as their default standard, Mattermost successfully stabilized their container vulnerability management while future-proofing their architecture for upcoming DISA STIG requirements.

Results

By centralizing their container security with Anchore Enterprise, Mattermost reduced developer alert fatigue and strengthened their continuous compliance operations:

» Restored developer time

By eliminating false-positive noise through Anchore Enterprise scanning, the engineering team reclaimed valuable time previously wasted investigating inaccurate vulnerability reports.

"Anchore won on best scanning results, no false positives, and a clean platform UI. It's actually pretty interesting to see [other] tools missing findings. So yeah, definitely by far, the best scanning results, no false positives."

—Eva Sarafianou, Senior Engineering Lead, Product Security & Release, Mattermost

» Centralized OS-level visibility

By complementing their existing application-level SBOMs with Anchore's deep container inspection, Mattermost successfully closed their security blind spots. The security team now has a single pane of glass to view and prioritize OS and application level vulnerabilities across all production container images before they ever reach the customer.

» Audit-ready continuous compliance

With Anchore's policy-as-code engine, Mattermost transformed compliance from a manual checklist into an automated workflow. By enforcing NIST 800-53 out-of-the-box, Mattermost standardizes their vulnerability management today while actively future-proofing their architecture to support the upcoming DISA STIG requirements of their defense and critical infrastructure customers.

"With this process, we're not just scanning better... we're starting from a cleaner foundation using Anchore Enterprise and distroless images."

—Eva Sarafianou, Senior Engineering Lead, Product Security & Release, Mattermost

By leveraging Anchore Enterprise, Mattermost strengthened its container security program with a deeply integrated and automated workflow that supports regulated customer requirements while enabling developers to focus on delivering mission-critical capabilities.

anchore

©2026 Anchore