VIAVI Solutions Reports Software Supply Chain Security ROI with the JFrog Platform



Headquarters
Chandler, AZ

Industry
Manufacturing

Employees
3000+

JFrog Products
JFrog Artifactory · Xray · Advanced Security

1000+
Hours saved (Developer time recovered)

20%
Efficiency gains in developer output

$1.2M
Cost savings over 3 years

THE CHALLENGE

Behind VIAVI Solutions' impressive global footprint lies a complex history of integration. VIAVI Solutions is a global organization that has grown significantly through acquisition and the absorption of smaller companies with their own tools, workflows, and storage systems. What once reflected each team's independence had become difficult to manage cohesively at scale, resulting in duplicated efforts, inconsistent onboarding, and diminishing clarity regarding product delivery.

Security was particularly hard to scale. SBOMs were always a requirement, but fulfilling them meant manually compiling information from multiple sources, a time-consuming and error-prone task. Vulnerability alerts were piling up with little context to help teams prioritize what actually mattered, and developers were leaning on familiar container images simply because they were known quantities.

The question wasn't the team's capability, but whether their tools provided what they needed to work with confidence.

Catalyst:

"We got JFrog and leveraged JFrog Xray scanning; we identified gaps in our vulnerability exposure, and learned how much work we had to go through to remediate it. We began to really consider the source and what version we were using."

Bill Goodrich, Principal DevSecOps & Automation Engineer, VIAVI Solutions

THE SOLUTION

VIAVI used the JFrog Software Supply Chain Platform to establish discipline and consistency across its entire organization. This foundation helped the team standardize processes, enforce policies, and gain confidence in their software releases.

Solution Area	Before JFrog	After JFrog
Artifact Management	Fragmented storage systems and inconsistent tools across acquired teams. Zero Confidence in trusted inputs; developers relied on outdated, unverified container images out of convenience.	Establishes Artifactory as the single source of truth across teams. Supports documented onboarding standards and helps deliver predictable, repeatable builds.
Vulnerability Scanning	Massive blind spots regarding inherited legacy containers and open-source packages. Developers manually searched Google to figure out if packages were safe or bad.	Automated continuous scanning directly in pipelines helps surface actual vulnerability profiles. Visualizes detailed package analyses in one place, driving the use of hardened images.
Alert Management	Severe alert fatigue from endless lists of unprioritized CVEs. Testing and retesting working containers was highly labor-intensive and cost-prohibitive.	Contextual analysis filters out alert noise by assessing whether a vulnerability is applicable in their specific environment. Developers can focus remediation on applicable vulnerabilities, helping accelerate product delivery.
SBOM Generation	Fulfilling VIAVI's Software Bill of Materials (SBOM) requirements was an error-prone, manual effort. Key personnel were pulled away from core development to compile reports across disparate sources.	SBOM data is captured as artifacts are scanned, so SBOMs can be exported as a byproduct of the development process. Reports reflect current scan data and can include known vulnerability information.

"Things are now easier to visualize and see in one place – now we don't have to Google to see if a package was good or bad; we have a detailed analysis. With JFrog Advanced Security, we have contextual analysis to see if it's applicable to us or not."

Bill Goodrich, Principal DevSecOps & Automation Engineer, VIAVI Solutions

RESULTS

Consistency, Confidence, and Measurable ROI

Over 1,000 developer hours recovered.

Time previously spent on manual tasks – SBOM compilation, chasing irrelevant vulnerability alerts, and managing inconsistent artifact storage – has been redirected toward meaningful development work. Developers are spending less time gatekeeping packages and more time building.

20% improvement in developer output.

Standardizing on a single platform with consistent, verified builds reduced the variability and rework that had been quietly eroding team productivity across the organization.

$1.2M in cost savings over three years.

Consolidating from 20+ fragmented tooling approaches down to one platform reduced redundant spend and the ongoing overhead of maintaining disparate systems across acquired teams.

Vulnerability exposure was addressed earlier and more accurately.

JFrog Advanced Security's contextual analysis helped the team cut through alert noise and focus remediation efforts on vulnerabilities that were actually applicable to their environment, rather than chasing every flag that came through.

Confident, predictable builds.

With Artifactory as a single source of truth, teams pull from the same verified images, containers, and packages. Variability in what ships is significantly reduced, and acquired teams are onboarded into a documented, enforced standard from day one.

SBOM generation went from a manual burden to a largely automated output.

What had previously required pulling from multiple sources and compiling by hand is now captured as a natural byproduct of the development process, reflecting current scan data and known vulnerability information.

"Because we're now able to operate more efficiently, our developers have more time to focus on meaningful work. We're able to standardize across processes, ensure security, and, as a result, have much more confidence across the software supply chain."

Bill Goodrich, Principal DevSecOps & Automation Engineer, VIAVI Solutions



WHAT'S NEXT

For VIAVI, the work of securing the software supply chain is an evolving discipline, and the team is already thinking well ahead of where they are today.

- **AI security is the most immediate frontier.** VIAVI's AI/ML teams are building their own models and working with open-source LLMs from sources like Hugging Face, which flow through Artifactory and are scanned via JFrog. As AI-generated code and AI dependencies become a larger part of how the organization works, the same rigor applied to traditional packages will need to extend to this new and rapidly expanding attack surface.

- **Shift left earlier, and more consistently.** The team is focused on getting developers running Frogbot and JFrog CLI scans as early as possible in the development cycle, directly from the repository, so known issues in artifacts are caught long before they reach the pipeline. The goal is to catch and remediate issues at the point of creation, not the point of deployment.

- **Expanding the "developer as designer" model.** With management actively pushing the adoption of coding assistants like Claude Code, VIAVI is thinking carefully about how AI-assisted development fits into a secure supply chain posture. The same principles apply: everything that enters the pipeline, regardless of how it was generated, needs to be scanned, verified, and trusted before it ships.

This customer story is provided for general informational purposes only. It is not legal, compliance, or security advice and does not guarantee any security or product outcome. It reflects information available as of the publication date shown on this page and may not be updated. Results depend on your environment, situation, and configuration. Product capabilities vary by edition and deployment model and are governed by your agreement with JFrog. JFrog is a registered trademark of JFrog Ltd. in the United States. All other trademarks referenced in this document are the property of their respective owners.

Talk to a Manufacturing DevSecOps Specialist to get started with the JFrog Platform.

Learn More | Start Trial

ABOUT JFROG

JFrog empowers thousands of DevOps organizations globally to build, secure, distribute, and connect any software artifact to any environment using the universal, hybrid, multi-cloud JFrog Platform.

LEGAL STATEMENT

Copyright © 2026 JFrog LTD. JFrog, the JFrog logo, and JFrog Artifactory are trademarks or registered trademarks of JFrog LTD or its subsidiaries in the United States and other countries. All other marks and names mentioned herein may be trademarks of their respective companies.

www.jfrog.com
www.x.com/jfrog
www.facebook.com/artifrog/
www.linkedin.com/company/jfrog-ltd