Case Study

How JWP Balances Dev and Security Priorities with Docker Scout

Industry: Software as a service — video technology

Location: Headquartered in New York City, USA, with offices in London, Eindhoven, and Skopje

About: JWP, a pioneer in video streaming and player technology, empowers publishers and broadcasters with an end-to-end platform for delivering and monetizing exceptional video content across web, OTT applications, and CTV platforms. Serving more than 7,000 clients globally, JWP powers video for more than 1 billion users and generates over 9 billion impressions and 8 billion video plays each month.

Highlights

Fixed vulnerabilities
Fixed thousands of vulnerabilities; improved security and efficiency.

Ignored noise
Ignored tens of thousands of non-critical issues; reduced noise and improved prioritization.

Deployed rapidly
Enabled over 400 repositories in under an hour with seamless integration and quick setup.

Introduction

A year ago, JWP, a global leader in video streaming, shared its initial success story with Docker Scout on their blog. At the time, they had enabled more than 300 repositories for Docker Scout within an hour, showcasing the ease and efficiency of integrating Docker Scout into their development workflow. This move was part of their broader strategy to enhance security without compromising delivery speed or operational efficiency.

Fast-forward to today, and JWP's journey with Docker Scout continues to evolve. With a mission to empower their customers through monetization, engagement, and seamless video delivery, JWP's services have facilitated the streaming of more than 860 billion videos. During the past year, Docker Scout has helped JWP fix thousands of vulnerabilities and ignore tens of thousands of non-critical issues, thereby significantly reducing noise and improving efficiency. A robust technical infrastructure, including thousands of nodes and multiple Kubernetes clusters, supports this remarkable achievement.

JWP's journey with Docker Scout highlights the importance of adaptable security tools in modern software development. By balancing developer autonomy with centralized security oversight, Docker Scout has helped JWP maintain a secure and innovative development environment, paving the way for future advancements and continued success.

> "Docker Scout has been more than just a tool for us; it's been a strategic asset"
>
> **Stewart Powell**
> Engineering Manager

Challenge

Balancing cross-team security collaboration and prioritization

As JWP enabled Docker Scout across more than 400 repositories, the company faced the challenge of developing securely without slowing down their developers. This was further complicated by shifting security responsibilities to development teams, a strategy common among many organizations aiming to empower developers.

However, this approach presented challenges, particularly due to the overwhelming volume of security alerts developers had to manage. Having to cut through this noise made it difficult for developers to prioritize and address vulnerabilities effectively.

JWP needed to balance security responsibilities more evenly between their centralized security teams and development teams. This balance was crucial for optimizing the time and effort of both teams while addressing JWP's specific security needs. This required a strategic approach to prioritize vulnerabilities and ensure compliance while optimizing the development workflow. The main challenge was establishing a collaborative environment where the security team had the necessary visibility without inundating developers with alerts.

Solution

Docker Scout provided a balanced solution. It integrated seamlessly with JWP's CI pipelines, offering real-time feedback and a centralized dashboard. This dashboard allowed the security team to oversee the entire landscape, ensuring compliance and strategic vulnerability management.

JWP now operates a decentralized development model where each team owns its CI pipelines. Docker Scout's centralized dashboard offers a unified view of all vulnerabilities across their container images. "The centralized dashboard has been a game-changer for us. It gives our security team the visibility and control they need without micromanaging each development team's processes," says Stewart Powell, Engineering Manager at JWP.

Following early adjustments, Docker Scout's VEX (Vulnerability Exploitability eXchange) policy statements have proven invaluable in prioritizing and managing vulnerabilities effectively. These features allowed JWP's security team to strategically prioritize vulnerabilities based on real-world risk rather than theoretical scenarios.

This shift was significant in environments where particular vulnerabilities might exist but pose minimal risk due to how JWP's Kubernetes clusters are configured — such as not running privileged containers or running as root. "VEX statements have helped us understand and manage vulnerabilities more practically," Powell explains.

> "With Docker Scout, we were able to go into Docker Hub, check a box, and, with virtually no effort from my team, provide developers with a comprehensive software supply chain and image vulnerability management program."
>
> **Stewart Powell**
> Engineering Manager

> "The centralized dashboard has been a game-changer for us. It gives our security team the necessary visibility and control without micromanaging each development team's processes."
>
> **Stewart Powell**
> Engineering Manager

> "The ability to prioritize vulnerabilities based on our specific requirements has had a significant impact on our business."
>
> **Stewart Powell**
> Engineering Manager

Furthermore, Docker Scout's real-time feedback loop has significantly streamlined JWP's workflows. Developers receive immediate feedback during the build process, ensuring that potential issues are addressed promptly. During the past year, Docker Scout has helped JWP fix thousands of vulnerabilities and ignore tens of thousands of non-critical issues. This process has fostered a culture of proactive security within the development teams, who are now more receptive to feedback from the security team.

The user-centered design of Docker Scout also played a crucial role. It has helped build trust and cooperation between the security and development teams, shifting to a collaborative dynamic. The security team can now make informed decisions about vulnerabilities in context and focus on actionable insights. "Docker Scout has really improved how our teams work together," says Powell. "It's not just about finding vulnerabilities; it's about understanding them in context and prioritizing what matters most."

"Docker Scout has enabled JWP to maintain our rapid development pace while ensuring a robust security framework, ultimately supporting our mission of delivering seamless and secure video streaming experiences to their global audience. Docker Scout has been more than just a tool for us; it's been a strategic asset," Powell says. "It helps us deliver on our mission while keeping our systems secure and our development teams empowered."

> "The real-time feedback from Docker Scout has been invaluable. It helps our developers catch and fix issues early, making the whole process much smoother."
>
> **Stewart Powell**
> Engineering Manager

> "Docker Scout has really improved the way our teams work together. It's not just about finding vulnerabilities; it's about understanding them in context and prioritizing what matters most."
>
> **Stewart Powell**
> Engineering Manager

Key benefits of Docker Scout:

Simple integration

Quick setup within Docker Hub enabled hundreds of repositories in under an hour.
Docker Scout's integration required minimal effort. "With Docker Scout, we were able to go into Docker Hub, check a box, and with virtually no effort from my team whatsoever, provide developers with a comprehensive software supply chain and image vulnerability management program," says Powell.

Unified dashboard

Docker Scout's dashboard provided real-time visibility into vulnerabilities, allowing the security team to prioritize effectively and improve team communication. This centralized approach reduced friction in handling security alerts.

VEX policy statements

Effective prioritization of vulnerabilities based on exploitability and context.
VEX policy statements helped the security team distinguish between critical and less urgent vulnerabilities.

> "What's nice about a tool like Scout is that our security team is really competent, very engaged, and very motivated to get stuff fixed. But they've also got a little bit more context now on what is fixable, what makes sense to prioritize, and what this risk looks like in context."
>
> **Stewart Powell,** Engineering Manager

Real-time developer feedback

Get immediate insights during image builds to address security issues proactively. Docker Scout provides real-time feedback to developers, allowing them to address issues on the fly. The tool contextualizes vulnerabilities, helping the security team focus on pressing issues.

Faster vulnerability resolution

The ability to identify and prioritize vulnerabilities quickly has led to faster remediation times.

Increased developer efficiency

Real-time feedback and contextual risk assessment have reduced the noise for developers, allowing them to focus on critical issues without being overwhelmed by alerts.

Enhanced security compliance

With Docker Scout, JWP has maintained compliance with security standards, such as PCI DSS Level 1, ensuring a robust security framework.

Results and outcomes

One year after integrating Docker Scout, JWP has transitioned from focusing on initial vulnerability detection and fixes to maintaining a strong, ongoing security posture. As showcased in this article, the integration of Docker Scout enabled hundreds of repositories within an hour, illustrating the tool's efficiency and ease of adoption. The sustained impact of Docker Scout on JWP's operations today highlights its effectiveness in ensuring long-term security and development efficiency.

Strengthened security posture

Docker Scout has played a pivotal role in improving JWP's security posture. The tool offers real-time visibility into vulnerabilities across all container images through a centralized dashboard. This has enabled the security team to prioritize and address vulnerabilities more effectively, leading to a more secure environment.

"Our security team is very competent and motivated to fix issues. They now have more context on what is fixable, what should be prioritized, and how risks should be viewed in context," says Powell.

> "Part of our philosophy up to this point has been shifting the responsibility for container security to development teams. And now we're getting back to a place where we are more focused on sharing responsibility between centralized security teams and engineering teams."
>
> **Stewart Powell**
> Engineering Manager

> "Initially, we focused on shifting security left to the developers. But we soon realized there needed to be a balance, and we've learned valuable lessons from that experience."
>
> **Stewart Powell**
> Engineering Manager

> "Our security team is competent and motivated to get stuff fixed. With Docker Scout, they have more context on what is fixable and what makes sense to prioritize."
>
> **Stewart Powell,** Engineering Manager

> "Getting that real-time feedback from Scout as you're building images is great."
>
> **Stewart Powell,** Engineering Manager

Enhanced team collaboration

Adopting Docker Scout has fostered better collaboration between JWP's development and security teams. The centralized dashboard provides a unified view, facilitating clear communication and coordinated efforts to manage vulnerabilities. Development teams receive real-time feedback on container health and security, allowing them to address issues promptly. This collaboration has been vital in maintaining a high-security standard without compromising development speed.

Streamlined vulnerability management

A standout feature of Docker Scout involves the VEX policy statements, which help the security team prioritize vulnerabilities based on their exploitability and context. This information has enabled JWP to focus on critical vulnerabilities that pose real risks while managing less critical issues appropriately. "The concept of a vulnerability that exists but can't be fixed is tricky, but VEX policy statements have gone a long way in helping us manage these effectively," Powell notes.

Conclusion

JWP is poised to continue leveraging Docker Scout to maintain and enhance its security posture. The tool's ability to provide real-time insights and facilitate team collaboration ensures that JWP can remain agile and responsive to emerging security threats.

"Trusting the experts to know best and moving some of that thinking back to the security team in terms of prioritizing vulnerabilities has been crucial," Powell says. As JWP continues to evolve, Docker Scout remains a critical component in the company's strategy to deliver secure, high-quality streaming services.

Learn more

- Subscribe to the Docker Newsletter.
- Get the latest release of Docker Desktop.
- Vote on what's next! Check out our public roadmap.
- Have questions? The Docker community is here to help.
- New to Docker? Get started.

> "Trusting the experts to know best and moving some of that thinking back to the security team in terms of prioritizing vulnerabilities, has been crucial."
>
> **Stewart Powell**
> Engineering Manager

> "Any bit of information that gets us closer to ensuring our systems are patched and secure keeps us closer to our objective."
>
> **Stewart Powell**
> Engineering Manager

> "Docker Scout provides feedback beyond what's kept in code, giving another level of visibility that's accessible to more than just developers."
>
> **Stewart Powell**
> Engineering Manager

> "What's powerful about Scout is with a very high-level overview about the nature of a vulnerability, we can make decisions about security in terms of our specific operating requirements."
>
> **Stewart Powell,** Engineering Manager