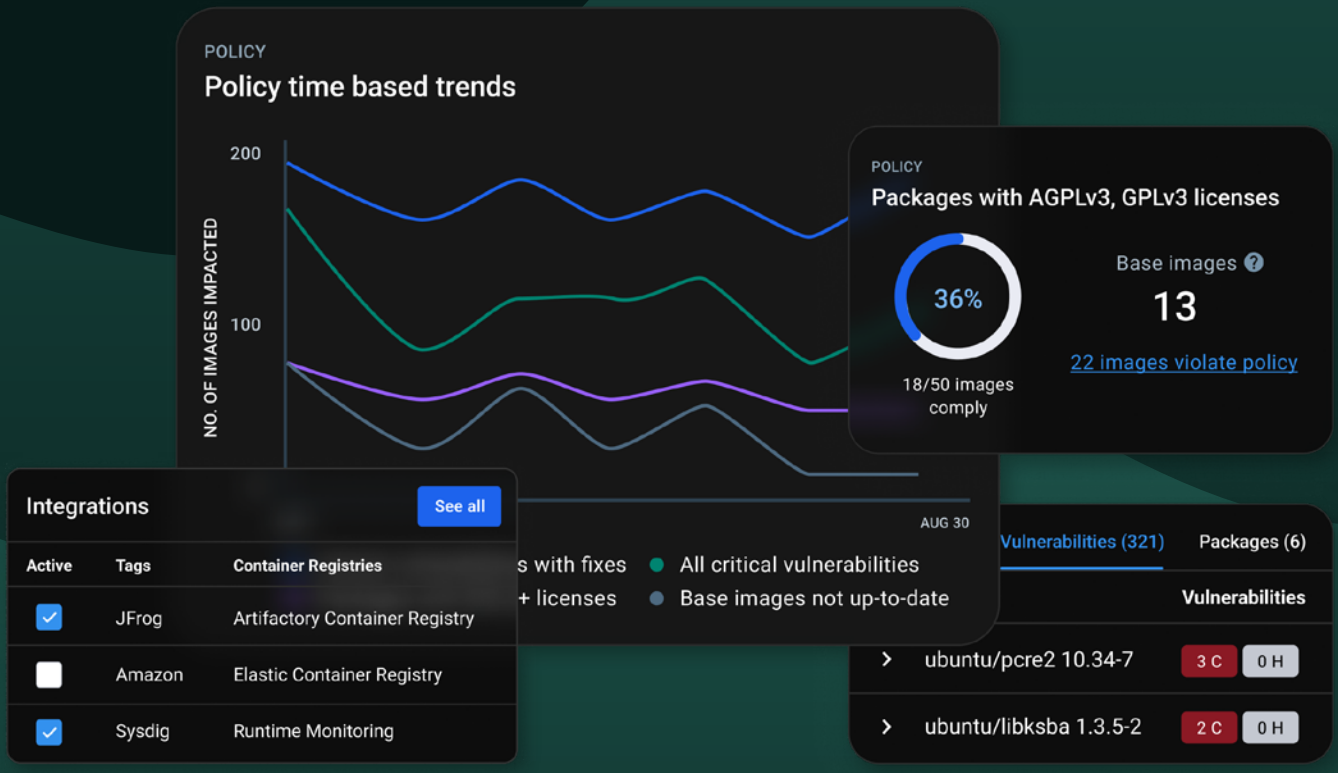
docker scout

Manage and secure the software supply chain

Docker Scout is a software supply chain product that generates focused and actionable insights for container images



Manage and secure the software supply chain

Customer pain points

Two common day-to-day challenges we hear time and time again from developers are:

Developers lose significant time managing a reliable and secure Software Supply Chain while addressing questions such as: Is this artifact coming from a compliant source? Who has altered it and what is its provenance? Is it aligned with internal licensing policy? Docker customers confirm that maintenance can take up to 30% of a developers' time each month in some organizations. Docker Scout Policy Evaluation is designed to solve this time-consuming challenge in a continuous approach that meets developers within the tooling that they use today.

Additionally, security concerns are identified so late in the path to production that they can prevent applications from being deployed entirely or lead to suboptimal application security posture. This results in high productivity costs. Security blockers act as one of several blockers leading to Docker survey respondents indicating a full day per month of lost productivity due to missed releases, process challenges, and other hurdles.

Our solution to the problem

Docker Scout addresses these challenges head on with solutions that embed directly into common developer workflows:

Docker Scout enables developers to make smarter decisions early in the development lifecycle through context-aware recommendations that ensure improvements to both reliability and application security posture efforts.

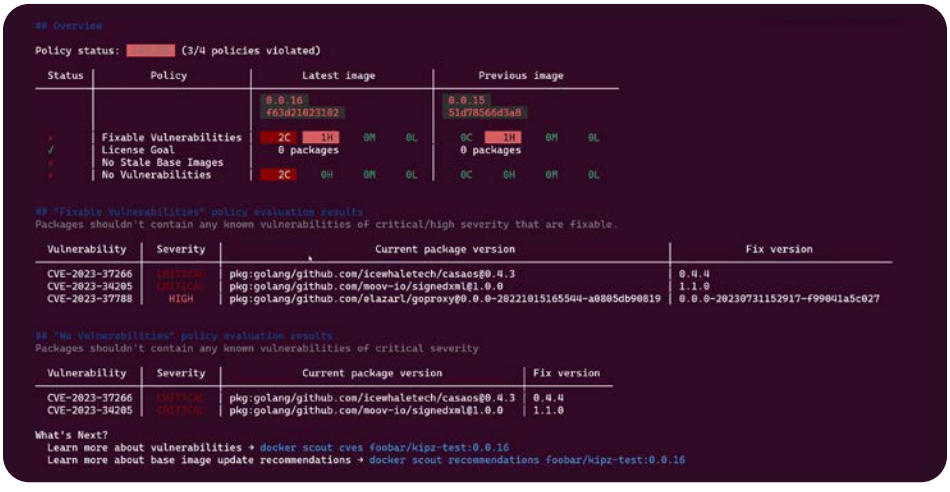


Image 1: Policy in CLI and recommended remediations

scout

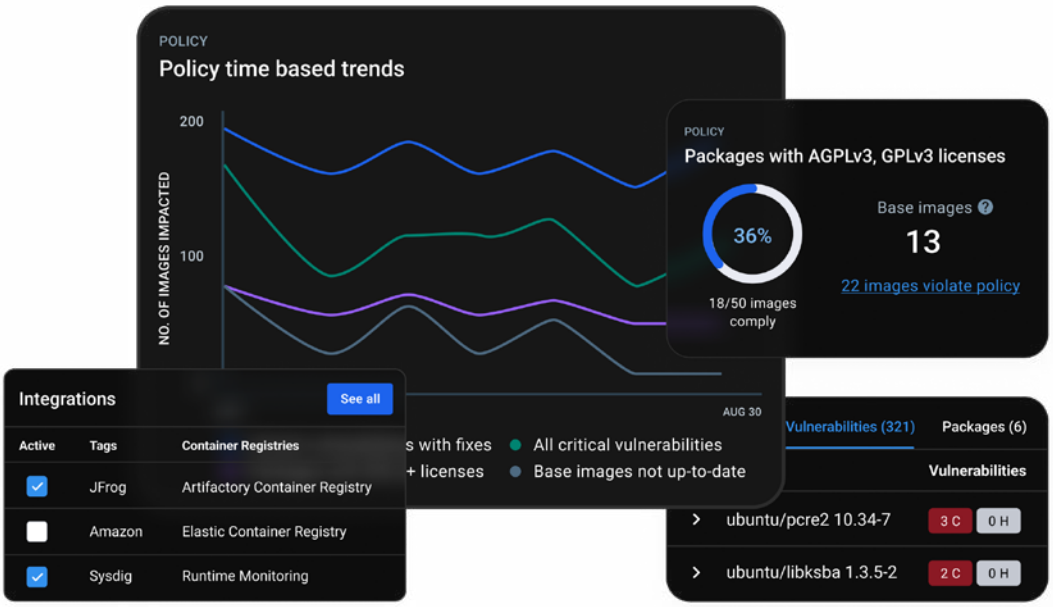


Image 2: Docker Scout UI elements that help simplify software supply chain management, including policy trends, integrations, and monitored vulnerabilities.

Key Benefits

End-To-End Developer and Security Workflows Across the Software Supply Chain

Secure Software Supply Chain

Docker Scout offers developers insights and context into their components, libraries, tools, and processes, resulting in increased transparency of the software supply chain. As Docker is used by 20 million developers, the ubiquity of Docker's portfolio cements Docker Scout's role in building within a more transparent and secure software supply chain.

Application Security Posture

Scout detects, highlights, and suggests corrections based on relevant changes in state of policies. Application security is ensured by providing suggestions to tackle security concerns before they hit production.

Trusted Content

In addition to Trusted Content such as Docker Official Images that form the basis for more secure builds, Docker is compliant at the platform level with SOC 2 Type 1, GDPR, CCPA, CPA, CTDPA, VCDPA, UCPA and The APEC Privacy Framework, and provides RBAC for more fine-grained security and compliance requirements.

Shared Collaborative Workflows For Platform, Development, and Security Teams

Recommended Remediation Paths

Clear, concise recommendations within developer workflows and on scout.docker.com help drive development teams to the best path for resolution of security concerns within their builds. These recommendations are driven by the specific context of the associated components that are most relevant for a given product or service architecture.

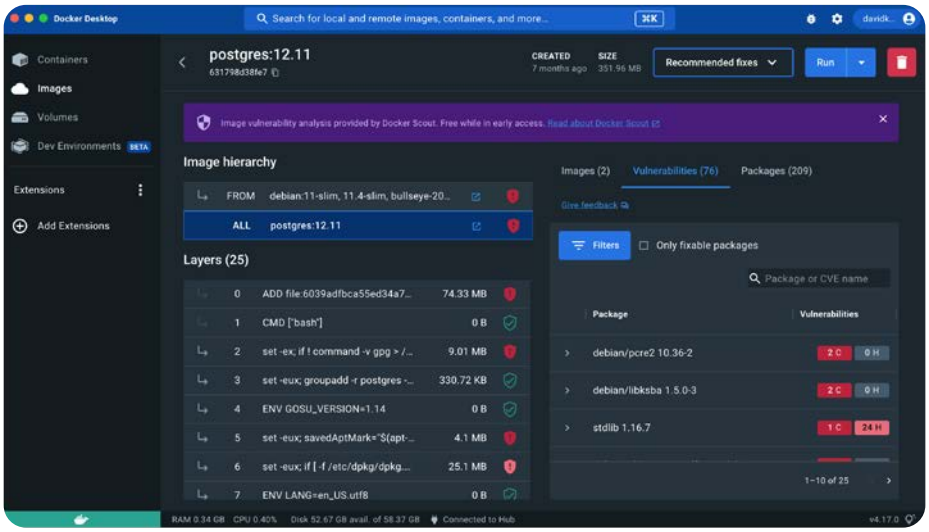


Image 3

Policy Evaluation

Internal security and compliance policies often limit developers' ability to build efficiently, but those policies exist to ensure the reliability and application security posture across an entire product portfolio. Docker Scout helps our customers to continually align with policy requirements rather than manually making those assessments with their own tooling. Docker Scout's Policy Evaluation is nuanced and gradual, meaning that it takes into account the specific context of each image and its associated packages. In contrast, many competing policy evaluation solutions take a less actionable, more binary approach. This means that they simply flag any application that does not meet all of the policy requirements, regardless of the context. This can lead to a lot of non-actionable insights, which can impact developers' overall productivity.

Secure Artifacts

Secure, trusted content is the foundation of secure software applications. A key aspect of this foundation is Docker Hub, the largest and most used source of secure software artifacts. This includes Docker Official Images, Docker Verified Publishers, and Docker-Sponsored Open Source trusted content. Docker Scout policies leverage this metadata to track the life cycle of images, generate unique insights for developers, and help customers automate the enhancement of their Software Supply Chain objectives; from inner loops to production.

Docker Scout: Software Supply Chain, Simplified

Docker Scout is designed to be with you in every step of improving developer workflows — from helping developers understand which actions to take to improve code reliability and bring it back in line with policy, to ensuring optimal code performance. The Docker Scout team is excited to get the latest solutions into our customers' hands, ensuring safety, efficiency, and quality in a rapidly evolving ecosystem within the software supply chain.

To learn more and get started.

Visit the Docker Scout product page today!