docker

Enhance government operations with secure development tools

Enhance government operations with secure development tools

Government agencies are a heightened target for cyber criminals, nation states, and hackers. Your agency's infrastructure - and the software behind it - is critical for smooth government operations. As you modernize your tech stacks, it's essential to invest in trusted, reliable, and secure tooling that safeguards your sensitive data and upholds compliance with federal regulations.

Docker provides an ecosystem of container development tools that help government agencies secure their software supply chains against malicious cyber threats. With Docker, you can containerize your software for any impact level and deploy to TS/SCI environments. Consider using the following solutions to maintain public trust with the confidence that your software is relevant and reliable.

Docker Desktop & Hardened Docker Desktop (HDD)

Containers are inherently secure due to their isolated environment, separated from the host using a Linux Virtual Machine (VM) so they can't access host files that are not owned by the user. They offer configurations for network proxies, registries, tool updates, host file sharing, and more. Docker Desktop is no different.

On top of this base layer of security, Docker Desktop provides an extra layer of security with Hardened Docker Desktop. HDD enhances container isolation by further separating containers from each other and from the container runtime. It prevents malicious containers from modifying security settings, interfering with Docker Engine, or breaching the Docker Desktop Linux VM. Admins can use HDD to maintain a high level of control over Docker Desktop settings with the ability to preset and lock them.

Three key HDD features support a simple, powerful, and centralized way to maintain compliance and ensure software integrity:

- Enhanced Container Isolation (ECI) - Run containers fully isolated, keeping users from modifying organizational level configurations.
- Registry Access Management (RAM) - Limit the online registries where developers can pull images, ensuring they use only trusted content.
- Image Access Management (IAM) - Control the types of images that developers can pull from Docker Hub, to restrict content to their team members.

Both Docker Desktop and HDD run in the background without interrupting developer workflows.

Docker Scout

Docker Scout helps developers find and fix vulnerabilities at the earliest stages of software development. It provides a unified, layer-by-layer view of software dependencies, their known vulnerabilities, and recommended remediation paths. Docker Scout includes a software bill of materials (SBOM) that integrates seamlessly with any existing CI/CD pipeline or build process. As a result, developers stay focused on deploying their key deliverables without having to actively manage security. Admins also maintain a verifiable record of their containerized software components.

Image Access Management & Trusted Content

Free and open source software (FOSS) is fundamental in software development, but it carries inherent risks. Docker's Trusted Content provides vetted and reliable container images for your teams to build from a strong foundation. When used in combination with Registry Access Management and Image Access Management, you can ensure that your developers are only using images that fit agency compliance requirements.

Docker's Trusted Content includes:

- Docker Official Images - Container images curated and maintained by Docker, providing a reliable foundation for building containers. These images exemplify container image best practices.
- Docker Verified Publisher - Container images from trusted publishers and their repositories, vetted by Docker.
- Docker-Sponsored Open Source - Community-driven image projects supported by Docker.

Docker Extensions

Let developers continue to use their favorite tools in the environment they use everyday with Docker Extensions. Docker offers a marketplace of reputable tooling so you don't have to worry about vetting and adopting new software. Powerful extension functionalities such as debugging, testing, security, and networking can be added to further augment the Docker Desktop experience.

Developers have the flexibility to extend Docker's functionality further through the Extensions SDK. They can build custom integrations to tailor the platform to their specific needs and compliance requirements seamlessly with their existing workflows.

Use Docker's secure development solutions for your government infrastructure

Learn more about the #1 most used development tool.