

Build Modern and Secure Applications at Scale with Docker Business



Contents

Introduction	3
Docker Business Enables Scalability and Security.....	4
Centralized Management and Visibility	4
Advanced Image Management.....	4
Audit Log.....	4
Role-Based Access Control.....	5
Image Access Management.....	5
Security.....	6
Vulnerability Scanning.....	6
SAML SSO.....	7
Conclusion	7



55%

of professional developers — already trust Docker as the standard to build, share, and run modern applications at scale.

Introduction

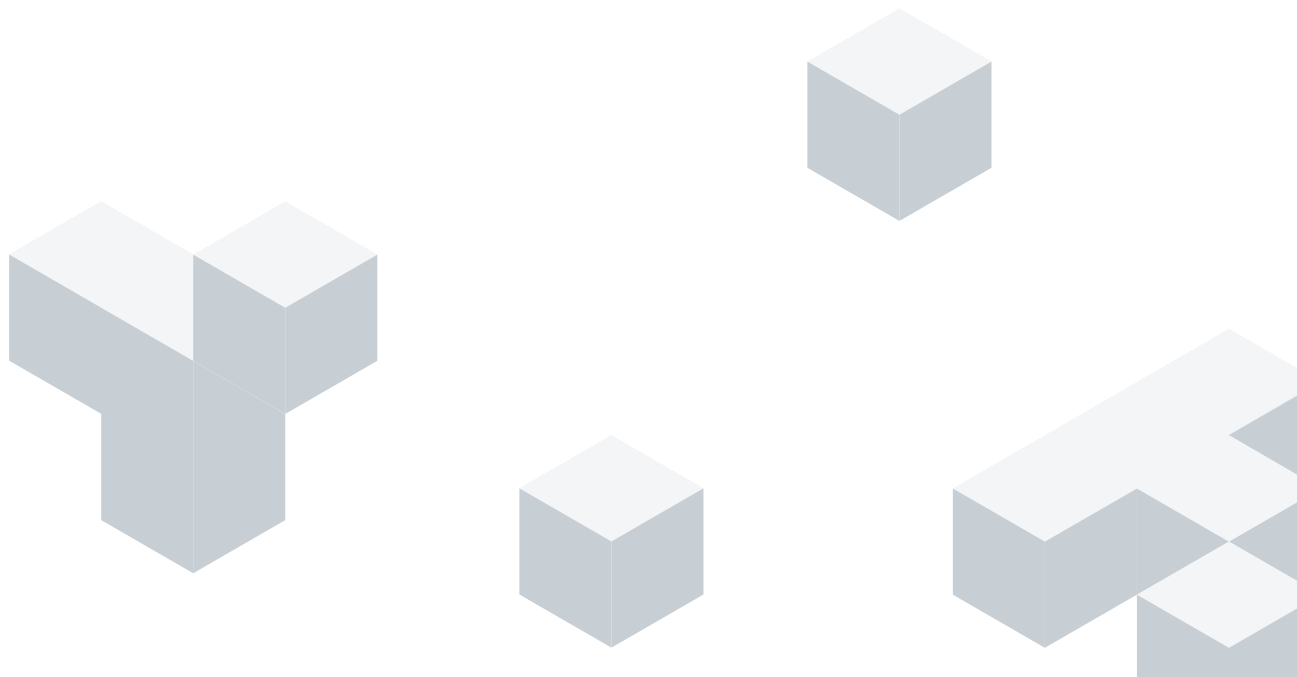
Confidence in cloud deployments is continuing to grow, with more companies shifting workloads off-premises. Between 2020 and 2021, [the use of off-premises services grew from 15 to 37 percent](#) globally, as organizations moved business-critical applications to the cloud.

As more organizations transition from hosting all their IT infrastructure on-premises to cloud-native and hybrid solutions, the complexity of cloud-hosted applications also increases. A [2020 report](#) by the CNCF (Cloud Native Computing Foundation) highlighted a “steady growth in the number of containers that organizations run.” In 2020, 23 percent of surveyed organizations reported running (or planning to run) more than 5,000 containers — a 109 percent increase since 2016. The same year, 61 percent of organizations reported using over 250 containers.

Many solutions are part of larger and complex distributed architectures. These architectures comprise many containerized microservices and hundreds — or even thousands — of developers collaborating on projects.

With the number of software supply-chain attacks increasing by a staggering [650 percent](#) in 2021, coordinating all these developers introduces serious security, management, and visibility challenges.

Millions of developers worldwide — in fact, [55 percent](#) of professional developers — already trust Docker as the standard to build, share, and run modern applications at scale. When organizations adopt Docker Business, they embrace the productivity tool developers already know and love without compromising on security and compliance. Let’s explore how Docker Business helps organizations address the security, management, and visibility challenges they face when scaling their application development.



Docker Business Enables Scalability and Security

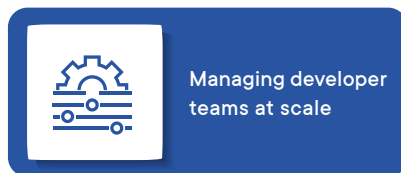
Docker Business extends the Docker experience with enterprise-grade management and visibility tools. These tools enable organizations to track detailed user activity within teams and organizations, control which images users access, and observe changes they make.

Available in a centralized management console within Docker Hub — Docker’s online library and community for container images — these features enable a secure software supply chain and limitless scale without creating friction in the developer workflow.

Centralized Management and Visibility

With the shift toward more remote work since 2020, developer teams are more distributed than ever before. Developers typically need to work with elevated IT privileges. While developers focus on building new features and applications, other critical roles within the organization (such as Operations, IT Security, and InfoSec) focus on minimizing the risks posed by this. The prevalence of distributed teams has made this already challenging task even more difficult. This has led to an unprecedented increase in software supply chain attacks.

Docker Business addresses these two key challenges enterprises and other organizations face:



Advanced Image Management

All Docker Business customers have access to the Image Access Management dashboard in Docker Hub. This dashboard gives organizations visibility over all the images their developers have pushed to the repository.

Each image has a status stating “active” or “inactive.” “Active” indicates that someone pulled or pushed an image in the last 30 days. Users can filter images by status, date, and tags. This insight into the repository’s image activity helps organizations identify and delete stale images to streamline storage.

Audit Log

Docker Business includes an audit log with three months of history. This log captures all activities involving creating, deleting, and editing teams and repositories. This information is available through a reporting dashboard in Docker Hub.

These benefits include improved operational efficiency by enabling quick addition or role changes, increased visibility of granted access, and finer-grained control over access permissions.

Role-Based Access Control

Docker Business allows for role-based access control (RBAC) implementation with a familiar hierarchical structure. Admins (or “owners”) can centrally manage their organization’s subscriptions and teams in Docker Hub.

Developers create and manage their own Docker Hub accounts. However, organizations can automate the process of adding new users to their Docker Business instance via Security Assertion Markup Language single sign-on (SAML SSO). When a new organization gets created, the owner can create new teams within that organization. Owners can then add developers to those teams without having to manually add each developer to the organization.

Owners can also fully configure each repository’s team access permission in Docker Hub as “read,” “write,” or “admin.” As a precautionary measure, Docker Hub limits a user’s ability to read until their email is verified, regardless of their team’s set access level.

This ownership-delegated access function offers significant benefits to organizations operating at scale. These benefits include improved operational efficiency by enabling quick addition or role changes, increased visibility of granted access, and finer-grained control over access permissions. This all adds up to a significant reduction in security risk.

Image Access Management

Developers pulling random images can put their organizations at risk. Managing this risk within small teams is relatively trivial, but scaling out to thousands of developers across time zones and geographic locations creates a much larger, and more serious, challenge.

Docker is continuously working to reduce the risk of pulling malicious images. The following two initiatives provide developers with validation that images come from trusted sources:

Docker Official Images: Curated by Docker, these are the essential base operating systems, programming languages, middleware, and databases that serve as a project’s foundations. These components exemplify best practices and are updated, scanned, and patched frequently for security. No image is older than 30 days.



Official Image



Verified Publisher

Docker Verified Publisher Program: Docker partners with third-party organizations to ensure developers can trust the content and security of commonly-used applications in actively maintained images.

Even with these added image labels, developers are still able to pull community images into their environments if they choose. There is some excellent work shared from personal projects across the container community, but it is not practical to expect the same maintenance and security guarantees as official and verified sources. This reliance on community images becomes unmanageable in a large group of developers and exposes organizations to supply chain compromise.

Image Access Management gives organizations full control over what developers can access in Docker Hub itself. These controls are divided into four categories:

- **Organization Images:** Allows access to images that members within the organization created.
- **Docker Official Images:** Enables toggling between Allowed and Restricted Docker Official Images.
- **Docker Verified Publisher Images:** Enables toggling between Allowed and Restricted Verified Publisher Images.
- **Community Images:** Restricts access to community-created images.

The additional guardrails that Image Access Management provides frees developers to focus on delivering business value while reducing the risks Operations and IT Security teams are concerned about. This feature is an essential step toward securing the software supply chain.

Security

Developers appreciate guardrails guiding them to do their work the right way so that they can focus on solving problems. The central management and visibility of teams, repositories, and image access discussed earlier in this article play a big part in implementing these necessary guardrails that enterprises and other large organizations come to expect.





Docker Business also includes vulnerability scanning and Security Assertion Markup Language single sign-on (SAML SSO).

Vulnerability Scanning

Docker Business customers benefit from unlimited scanning for Docker Hub's Common Vulnerabilities and Exposures (CVE). Regular scanning helps identify the many different risks present in the software supply chain.

When vulnerability scanning is enabled for a repository, Docker automatically scans pushed images and generates reports detailing the problem's source and recommendations for a fix.

There are several advantages to running these static application security testing (SAST) scans in Docker Hub on every new push:

-  Less reliance on developers remembering to run scans locally
-  Increased visibility of potential threats and reassurance that the fixes are applied
-  Shifting left to detect vulnerabilities earlier rather than trying to fix them later
-  Scanning guidance reports, ensuring secure coding while educating developers

Having a single credential reduces the possibility of failing to remove access... a real risk when working with developer teams at scale.

SAML SSO

Docker Business supports SAML SSO, which significantly improves the developer experience. When enabled, developers do not need to sign in again when they use Docker Hub or interact with a repository using the command line.

SAML SSO also greatly simplifies the onboarding and offboarding processes. Onboarding without SSO is typically a pain point for all those involved in the process — particularly new developers, who may sit idle waiting for sufficient access across an organization's systems, and TechOps, who have all that additional work to do setting up and managing multiple credentials. Additionally, offboarding is a significant concern when it comes to managing security. Having a single credential reduces the possibility of failing to remove access when a developer leaves the team or organization, a real risk when working with developer teams at scale.

An additional benefit of SAML SSO is that an organization can take full control of developer credentials in its identity provider, rather than the developer "owning" their own Docker Hub account.

Conclusion

Docker attracts developers and developer teams because of its speed and simplicity. With Docker, developers can ship more and ship faster.

Shipping fast can be risky when it comes to maintaining a secure software supply chain. When organizations focus only on reducing the risk of malicious content in their applications, developer productivity may suffer. However, when developers focus solely on their code and overlook security concerns, organizations need complete visibility to proactively identify threats.

With Docker Business, organizations can leverage Docker's full suite of tools and services to scale their application development, and pull images with confidence. Developer teams can access the hundreds of images that are Docker Verified, Docker Official, or directly from their organization. Organizations can control image access and minimize the risk that their developers pull images that are non-compliant with their security policies. By building secure applications using only trusted content, organizations can minimize downtime to meet their service-level agreements (SLAs) and satisfy regulatory requirements for security and customer data protection.

Organizations can also easily onboard and offboard Docker users using credentials from a single identity provider that they are already using. In addition, role-based access controls help organizations manage what their developer teams can and cannot access.

Docker Business empowers large developer teams to be more productive. It enables teams to build more secure enterprise-grade applications, minimizing risk and maximizing control.



Get started today

Learn how [Docker Business](#) can help organizations working at scale support developer productivity without compromising on security and compliance.

