

# Build Modern and Secure Apps at Scale with Docker Business



# Contents

|  |   |
|--|---|
| Introduction .....                                 | 3 |
| Docker Business Enables Security and Scaling ..... | 4 |
| Centralized Management and Visibility .....        | 4 |
| Advanced Access Management .....                   | 4 |
| Audit Logs .....                                   | 4 |
| Role-Based Access Control .....                    | 5 |
| Registry Access Management .....                   | 5 |
| Image Access Management .....                      | 6 |
| Security .....                                     | 7 |
| Vulnerability Scanning .....                       | 7 |
| Single Sign-On (SSO) .....                         | 7 |
| Conclusion .....                                   | 8 |



# 55%

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

## Introduction

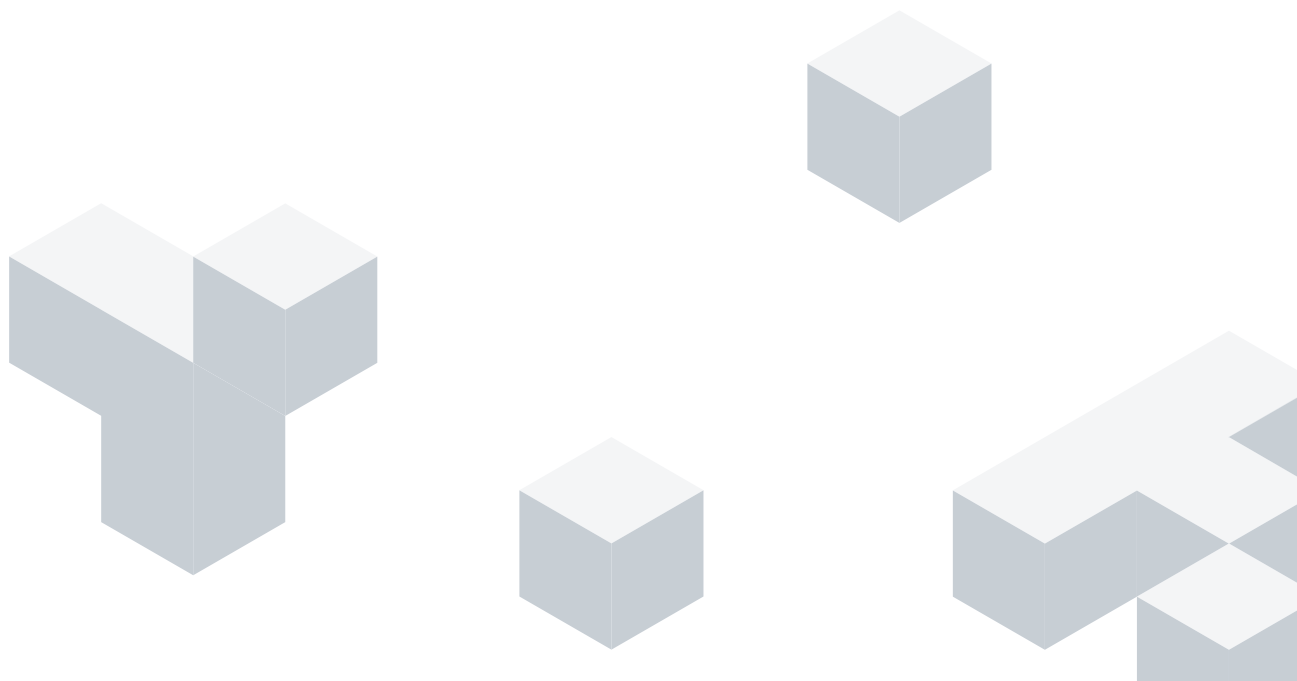
Confidence in cloud deployments is continuing to grow, with more companies shifting workloads off-premises. Between 2020 and 2021, [the use of off-premises services grew from 15 to 37 percent](#) globally, as organizations moved business-critical applications to the cloud.

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 Security and Scaling

Docker Business extends the Docker experience with enterprise-grade management and visibility tools. These tools enable managers 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 marketplace of components and integrations — 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. And, 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 was introduced to help address two key challenges organizations face today:



It includes centralized management and security tools designed to give IT administrators and managers (i.e., Docker admins) greater visibility and control over their Docker workflows without compromising on developer productivity and innovation. The following are some of the tools Docker admins can access with their Docker Business subscription.

### Advanced Access Management

Docker admins can set organization-wide policies via access settings in Docker Hub. These controls provide greater management and visibility over all the registries and images their development teams use, and in a centralized view.

### Audit Logs

Docker admins can pull audit logs with three months of history via a reporting dashboard in Docker Hub. Such logs capture all activities involving creating, deleting, and editing teams and repositories.

**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 admins can implement role-based access controls (RBAC) with a familiar hierarchical structure. Organization subscriptions, teams, and members are centrally managed 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 single sign-on (SSO). When a new organization gets created, Docker admins (or the organization “owner”) can create new teams within that organization. Admins can then add developers to those teams without having to manually add each developer to the organization.

Docker admins can also configure team access permissions for each repository 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.

Role-based access offers significant benefits to organizations operating at scale while minimizing security risks. 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.

## Registry Access Management

Developers accessing public registries with limited to no visibility by the organization, may pose additional security risks. In addition, new registries can be spun up quickly, providing a way for developers to potentially pull malicious software or push sensitive data and intellectual property. Registry Access Management was introduced to minimize such risks for Docker Business customers. It allows organizations to have greater control over the registries their developers use.

When Registry Access Management is enabled, [Docker admins can set registry access policies in Docker Hub](#). When enabled, admins can limit developer access to only trusted registries such as a private registry on Artifactory. Developers who try to access the affected registry on Docker Desktop will receive clear notifications that the registry is blocked by their organization.

## Image Access Management

Developers pulling random Docker 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.

**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.



**Official Image**



**Verified Publisher**

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 can become unmanageable within large development teams, and can potentially expose organizations to vulnerabilities.

[Image Access Management](#) gives organizations greater control over what developers can access inside 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.

Each image has a status indicating “active” or “inactive.” “Active” indicates that the image has been pulled or pushed within the last 30 days. Users can filter images by status, date, and tags. This insight can help organizations identify and delete stale images to streamline storage.

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 single sign-on (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

### Single Sign-On (SSO)

SSO for Docker enables users to authenticate using their organization's standard SAML 2.0 or Azure Active Directory identity provider (IdP). Organizations will also be able to better manage their Docker instances in a more traceable and secure way. When enabled, Docker users can authenticate using their organization-provided email/username and password. Users must then sign in to Docker Hub or Docker Desktop to initiate the SSO authentication process.

## Conclusion

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

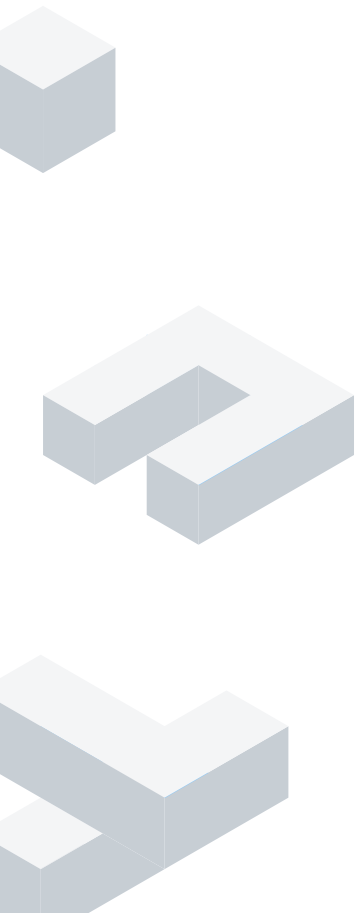
Shipping fast can be risky when it comes to maintaining a secure software supply chain. When organizations focus only on reducing the risk of malicious content in their applications, developer productivity may suffer. However, when developers focus solely on their code and overlook security concerns,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

[Contact sales today](#) to learn how [Docker Business](#) can help enterprise organizations working at scale support their developer teams while prioritizing container security.







## Get started today

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

