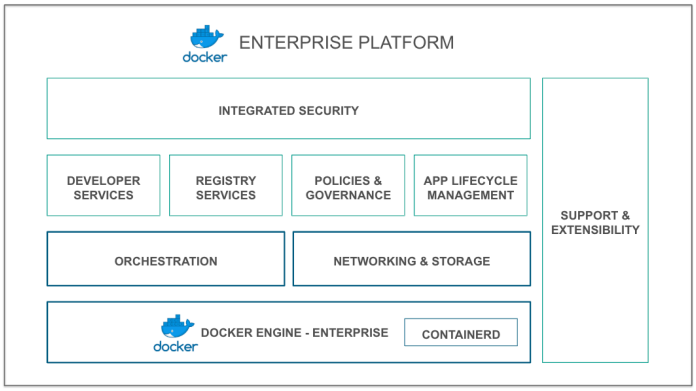
Datasheet

Docker Enterprise

The Enterprise-Ready Container Platform



Docker Enterprise is the only enterprise-ready container platform that enables IT leaders to choose how to cost-effectively build and manage their entire application portfolio at their own pace, without fear of architecture and infrastructure lock-in. Docker's container platform enables organizations to accelerate digital and multi-cloud initiatives by automating the delivery of legacy and modern applications using an agile operating model with integrated security. Because Docker Enterprise includes services, support and training, organizations have a complete containerization strategy for supporting an ever-changing business environment.

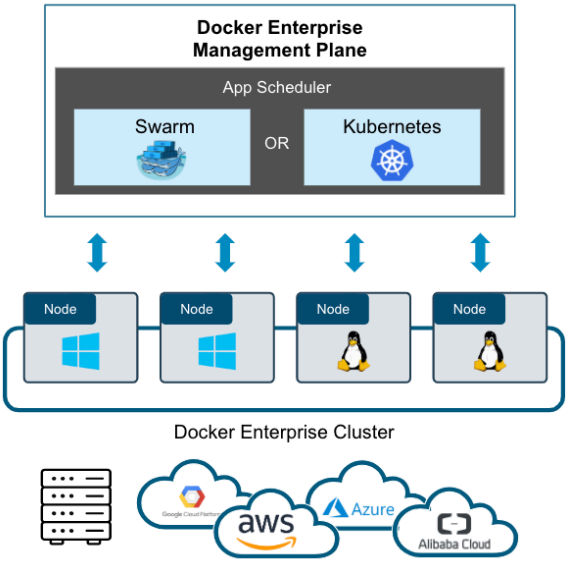
Docker Enterprise Benefits

- **Freedom of Choice**: Docker Enterprise is designed to give enterprises ultimate freedom to implement their multi-cloud strategy with no lock-in. With Docker you're free to innovate across any infrastructure, partner with any Linux vendor or Windows Server, and work with any application type or development language you choose.
- **Agile Operations**: Docker Enterprise enables you to reduce costs and increase operational efficiency by standardizing the way to build, manage, and secure applications across diverse infrastructures including multiple clouds. Our platform unifies processes across any architecture, while aligning with your existing IT operations so you can get applications to market faster, reduce total costs and ease the adoption of new technology as business needs evolve over time.
- **Integrated Security:** Docker Enterprise incorporates additional security at every step of the application delivery lifecycle without getting in your way or adding extra cost. Applications receive greater protection while maintaining performance, improving governance while enabling a seamless workflow for centrally-managed content and policy-driven automation.

Common Use Cases for Docker Enterprise

- Modernizing Traditional Applications
- Microservices & Cloud-Native Applications
- Implementing CI/CD or DevOps Practices
- Data Science
- Edge Computing
- Cloud Migration
- Digital Transformation

Freedom of Choice



Docker Enterprise allows enterprises to freely move applications between multiple infrastructure platforms in a consistent manner. Some key features that support this include:

- **Choice of orchestration** – Docker Enterprise is the only platform that runs both Swarm and Kubernetes simultaneously on the same cluster, giving organizations the flexibility to choose orchestrators interchangeably. Docker Enterprise 2.1 includes Kubernetes 1.11 and includes support for autoscaling, native Kubernetes access controls, and storage protection.

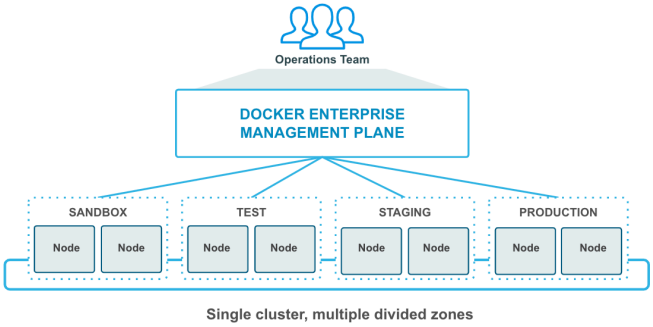
- **Choice of operating system** – Docker Enterprise is supported on multiple Linux distributions (CentOS, Oracle Linux, RHEL, SLES, or Ubuntu) and on Windows Server 2016, 1709, 1803, and Windows Server 2019[1].

- **Certified Infrastructure** – Docker Enterprise is optimized and tested to install easily and operate smoothly on virtual machines, bare metal, and leading cloud providers like Amazon Web Services and Microsoft Azure.

- **Full stack portability** – Developers can define networking, storage, secrets and more at the application level. A separation of concerns allows developers to define app configurations and IT to deploy them with either Swarm or Kubernetes and manage them on different infrastructures without recoding. Eliminate the "works of my machine" problem, once and for all.

- **Extensibility** – Docker Enterprise provides open interfaces, drivers, webhooks and plugins to easily integrate to a variety of enterprise systems and processes. Certified Plugins and Containers provide an extra level of quality and assurance for production environments.

Agile Operations



Docker Enterprise is focused on making the management of a container environment very intuitive and easy for Infrastructure and Operations teams. This focus on the operational experience carries over to managing Kubernetes. Some key features include:

- **Unified management** – Manage all system components from an integrated web console including; users, containers, services, namespaces, controllers, load balancers, networks, volumes, secrets and nodes across both Swarm and Kubernetes.

- **Out-of-the-box dashboards** – Enhanced health status dashboards provide greater insight into node and container metrics and allow for faster troubleshooting of issues. View cluster-level, pod-level or container-specific metrics and track history to identify emerging issues.

- **Extending metrics to Prometheus** – Export cluster metrics to an external Prometheus server for local management and monitoring.

- **Task activity streams –** Get clear visibility into tasks and background activities that are running in the cluster and registry.

- **Simple cluster management** – A single command can create and join nodes to a cluster. Easily add, remove nodes or change roles to adjust to application requirements while getting a highly available cluster for both Swarm and Kubernetes.

[1] Pending Microsoft's release of Windows Server 2019

- **Simplified Kubernetes operations** – Intuitive design and guided workflows in the UI allow organizations to operationalize Kubernetes without requiring deep expertise. Advanced configuration through Kubernetes CLI is still available for experienced users.

- **Frictionless deployment** – Consistently deploy different types of applications to Docker Enterprise through either the UI or CLI. Deploy applications with Docker Compose files to either Swarm or Kubernetes, or leverage Kubernetes YAML to deploy to Kubernetes.

- **Enhanced access controls –** Integrate Docker Enterprise with corporate LDAP/AD and manage roles and responsibilities to all system components including apps, nodes, secrets, networks and volumes. Leverage either pre-configured roles or design custom roles that align to existing organization processes.

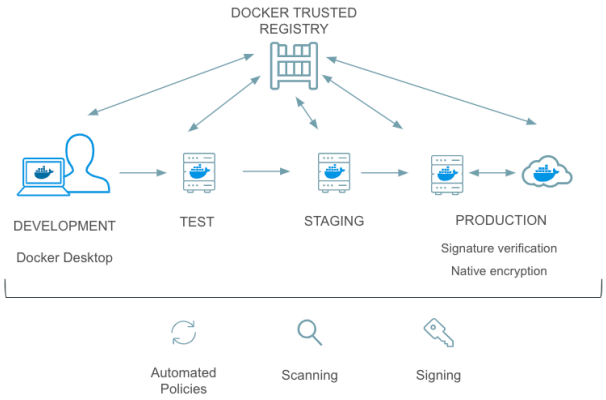
- **RBAC for nodes** (advanced only) – Provide an additional layer of physical isolation by granting certain users or teams access to specific nodes. Applies to both Swarm resource collections and Kubernetes namespaces, enabling a "Bring Your Own Node" service model for IT services organizations.

- **Rolling updates** – Gain confidence in deploying new features and updates with rolling updates. Available performance metrics allow teams to monitor progress and quickly rollback when necessary.

- **Application health checks** – Improve reliability and resiliency with health checks for services. Configure the frequency of checks in the UI or in the image Dockerfile to ensure timely checks and reconciliation, if needed.

- **Integrated networking and routing** – Applications deployed with Swarm and Kubernetes both have access to "batteries included, but swappable" networking and routing solutions. Docker Enterprise comes pre-installed with Project Calico as a highly scalable networking and routing solution, but users may swap this for their preferred Kubernetes CNI plug-in solution. For Swarm-deployed applications, Docker Enterprise includes enhanced application layer routing and load balancing based on the Interlock 2.0 architecture.

Integrated Security



Docker Enterprise delivers a secure software supply chain with an integrated and advanced private image registry solution:

- **Secure image management** – Operate a private registry for secure storage and management of images and granular access control to repositories. Manage images versions, metadata, and optimize storage resources with garbage collection. Repositories can be marked as immutable to prevent inadvertent changes.

- **Image signing, verification and policy –** Docker Content Trust protects images from man-in-the-middle attacks while moving across the network. Users can cryptographically sign an image at build time, creating a record of who created or modified the image, and enforce policies before an application can be deployed to production.

- **Image scanning and vulnerability monitoring** (advanced only) **–** Docker Security Scanning ensures only high integrity applications are running in production. Docker Security Scanning indexes the components in both Windows and Linux images and compares them against a known CVE database. When new vulnerabilities are reported, Docker Security Scanning matches the components in new CVE reports to the indexed components in your images, and quickly generates an updated report. Administrators can also control specific vulnerability scanning results and get visibility into vulnerabilities at runtime.

- **Connect multiple clusters to a single registry** – Build a globally consistent supply chain for distributed development teams by connecting multiple Docker Enterprise clusters to a centralized

registry. This ensures that organizations with a "follow the sun" development approach will seamlessly and securely share their software within a given team.

- **Image content cache** – Reduce latency and improve performance for remote development teams with remote (or satellite) caches to enable faster downloads of Docker images for distributed development teams.

- **Image mirroring** (advanced only) – "Push" or "pull" images from a repository in one registry to a repository in another registry for greater availability and consistency of application content across multiple sites.

- **Policy-based image promotion** (advanced only) – Define policies to automatically promote images from one repository to another repository within Docker Trusted Registry. Criteria can include tags, package names, vulnerabilities, or license review.

- **Policy-based image tag pruning** (advanced only) – Define policies to reduce container image sprawl by automatically removing tags.

- **Garbage collection –** Optimize disk space by removing unused image layers in the repository.

- **Automate workflows with webhooks** – Registry webhooks pass real-time information to 3rd party tools like CI/CD solutions. You can use Webhooks to cause an action in another application in response to an event in the registry.

In addition, there are several features that ensure a secure container platform:

- **FIPS 140-2 validated Docker Engine:** The cryptographic modules in Docker Engine - Enterprise have been validated against FIPS 140-2 standards which also impacts other regulated industries.

- **SAML 2.0 authentication** – Integrate Docker Enterprise to preferred Identity Provider solutions and offload authentication to enable single sign-on or multi-factor authentication.

- **Secure communications** – Automatic mutual TLS authentication ensures that the default mode of communication within the system is encrypted and protected.

- **Swarm and Kubernetes network encryption** – Protect all host-to-host communications with IPSec tunnels.

- **Cryptographic node identity** – Prevent malicious nodes from joining a cluster through built-in root Certificate Authority (CA) with automatic certificate rotation that ensures systems remain secure and online. Support for external CAs and ability to configure rotation frequency provides teams with additional flexibility.

- **Integrated secrets management –** Securely store secrets (API key credentials, etc) encrypted at rest and in transit to only the exact app service that requires them to operate. Docker Enterprise allows teams to easily create, manage and deploy secrets for app services on both Windows and Linux-based containers.

- **Detailed audit logs –** Docker Enterprise includes detailed event logs across both the cluster and registry to capture users, actions, and timestamps for a full audit trail. These are required for forensic analysis after a security incident and to meet certain compliance regulations.

Enterprise Support and Partner Ecosystem

Besides platform capabilities, Docker is committed to delivering an enterprise-grade experience. That includes:

- **Predictable releases and maintenance** – Proactively plan deployments and upgrades with a regular release cadence with 24 months of extended software maintenance per release. Software maintenance includes security patches and hotfixes back-ported to every version under support.

- **Support from the source –** Get SLA-backed support from the team that built the platform. Business Day (9am-6pm) and Business Critical (24x7x365) support plans are available.

- **Professional Services** - Based on proven methodologies from working with our enterprise customers, Docker offers a set of Solution Architecture engagements to accelerate your containerization journey that goes beyond technology implementation. It is a complete approach that considers the people and processes

involved, with services, training and support to guide you through your adoption journey.

- **Trusted Enterprise Partners** - Docker Enterprise is available with Level 1 and 2 support through leading enterprise technology companies including HPE and Microsoft.

- **Certified Containers –** Independent Software Vendors (ISV) package and distribute their software as containers for Docker Enterprise. These containers are built with best practices, tested, scanned, and reviewed. Cooperative support from Docker and the ISV.

- **Certified Plugins –** Technology partners package and distributes their Networking and Volume Plugins as containers for Docker Enterprise. Built with best practices and must pass a suite of API compliance testing, are scanned, and reviewed. Cooperative support from Docker and the plugin provider.

Get Started with Docker Enterprise

Docker Enterprise is available as a monthly or annual subscription inclusive of software and support. To learn more, visit https://www.docker.com/enterprise or send a request to https://dockr.ly/contactdocker.

Experience Docker Enterprise without installing any software through the Docker Hosted Trial. Get started at https://trial.docker.com.