MIRANTIS

Docker Enterprise

The fastest way to securely build, share and run modern applications anywhere

Docker Enterprise is the industry-leading and only container platform providing a simple, as-a-service experience and a central point of collaboration across dev and ops to build, share and run modern applications. Based on industry standards, Docker Enterprise is the easiest way to use containers and Kubernetes at scale, delivering the fastest time to production for modern applications across any public, private, multi- or hybrid-cloud environment.

Docker Enterprise brings speed, choice and security throughout different stages of the application lifecycle and across the full Kubernetes stack, enabling the rapid development and progressive delivery of modern applications, leveraging the infrastructure and knowledge organizations have in place today. This means improved developer productivity, increased release frequency, cost savings, and a secure pipeline to Kubernetes environments anywhere.

Docker Enterprise delivers:

Speed: Simple, as-a-service experience and streamlined workflows that deliver faster time-to-production for modern applications

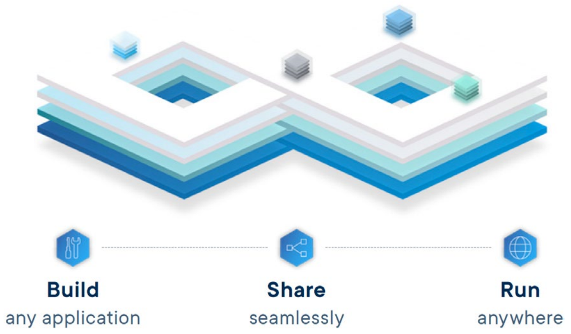
- Accelerate developer onboarding and improve productivity, leveraging existing skill sets
- Simplify and streamline processes across dev and ops with a central point of collaboration
- Rapidly deploy, manage and update production-ready Kubernetes environments, without requiring deep expertise, with the option to have Mirantis remotely manage complete operations of the full Kubernetes stack

Choice: Flexibility to use the clouds and Kubernetes environments of your choice

- Support a diverse set of application stacks and infrastructures using validated and secure container content from Docker Hub
- Run applications in any data center or cloud, on any architecture and any OS
- Deploy a full stack of hardened open source technologies to enable cost savings with no vendor lock-in

Security: Continuously ensure secure governance and compliance throughout different stages of the application lifecycle and across the full Kubernetes stack, without slowing down innovation

- Comply with corporate and architecture standards, without impacting developer productivity
- Trust the provenance of all applications and ensure secure separation of concerns
- Ensure security across distributed and hybrid environments--100% portable security model across any infrastructure
- Leverage support and managed services from leading open cloud experts to enable security compliance and the best possible SLAs for the full cloud native stack



Securely build, share and run modern application anywhere

Common Use Cases:

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

Build

Rapidly build containerized applications and microservices in a secure way while leveraging existing skill sets. Spend your time coding, not agonizing over deployment.

As-a-Service experience – Allow developers to work on code, not operationalizing the infrastructure, by leveraging Mirantis open source experts to remotely manage the full Kubernetes stack

Frictionless App Deployment – Consistently deploy different types of applications to Docker Enterprise through either the UI or CLI, and get an overview of what containers are running where using the Universal Control Plane. Leverage Kubernetes YAML to deploy to Kubernetes, or deploy applications with Docker Compose files to either Swarm or Kubernetes.

Automate workflows with CI/CD integration – Docker Trusted Registry webhooks can pass real-time information to 3rd party tools like CI/CD solutions to speed up application testing and delivery.

Share

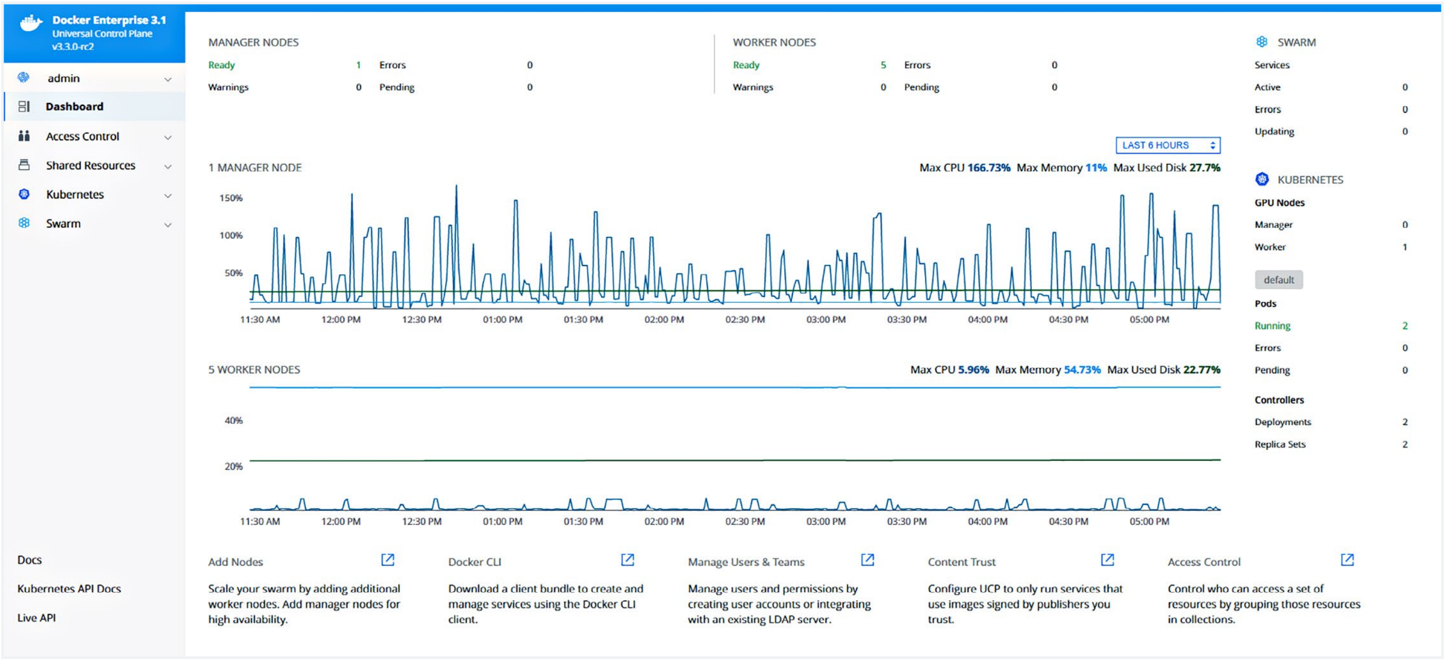
Seamlessly find and securely share certified and approved content leveraging Docker Hub, the world's largest library of container content, and Docker Trusted Registry (DTR), your organization's secure, private registry.

Secure, distributed image management – Docker Trusted Registry delivers secure storage and management of images and granular access control to repositories. Build a globally consistent supply chain for distributed development teams by connecting multiple Docker Enterprise clusters to a centralized registry, mirroring different image repositories across multiple registries, or provide a locally cached repository for reduced latency and improved performance. Leverage validated and secure container content from Docker Hub to support a diverse set of application stacks and infrastructures.

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.

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 – Optional Docker Security Scanning for DTR 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.



MANAGER NODES

Ready	1	Errors	0
Warnings	0	Pending	0

WORKER NODES

Ready	5	Errors	0
Warnings	0	Pending	0

SWARM

Services

Active	0
Errors	0
Updating	0

KUBERNETES

GPU Nodes

Manager	0
Worker	1

Pods

Running	2
Errors	0
Pending	0

Controllers

Deployments	2
Replica Sets	2

1 MANAGER NODE — Max CPU 166.73% Max Memory 11% Max Used Disk 27.7%

5 WORKER NODES — Max CPU 5.96% Max Memory 54.73% Max Used Disk 22.77%

Add Nodes
Scale your swarm by adding additional worker nodes. Add manager nodes for high availability.

Docker CLI
Download a client bundle to create and manage services using the Docker CLI client.

Manage Users & Teams
Manage users and permissions by creating user accounts or integrating with an existing LDAP server.

Content Trust
Configure UCP to only run services that use images signed by publishers you trust.

Access Control
Control who can access a set of resources by grouping those resources in collections.

Docker Enterprise includes Docker Universal Control Plane (UCP), which helps manage your cluster and applications through a single interface

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.

Policy-based image promotion – 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.

Automated image cleanup – Define policies to reduce container image sprawl and optimize disk space by setting up policy-based image tag pruning and using integrated garbage collection.

Run

Deploy, manage and secure modern applications with globally consistent Kubernetes environments that run on any cloud.

Simplified Kubernetes experience – Docker Kubernetes Service (DKS) is a certified Kubernetes distribution that delivers 'sensible secure defaults' out-of-the-box. DKS makes Kubernetes easy to use and more secure for the entire organization without requiring deep expertise. Advanced configuration through Kubernetes CLI is still available for experienced users.

Choice of orchestration – Docker Enterprise includes Docker Kubernetes Service and is the only platform that runs both Swarm and Kubernetes simultaneously on the same cluster, giving organizations the flexibility to choose orchestrators interchangeably for both Linux and Windows nodes. Docker Kubernetes Service Enterprise includes Kubernetes 1.17 and includes support for autoscaling and Container Storage Interface (CSI)., native Kubernetes access controls, and storage protection.

Automated lifecycle management – Cluster management tools enable teams to easily deploy, scale, backup and restore and upgrade a certified Kubernetes environment using a set of simple CLI commands. This delivers an automated way to install and configure Docker Enterprise across public, private, hybrid and multi-cloud deployments, including bare metal, OpenStack, AWS, Azure, or VMware.

Transparent cluster upgrades – Apply blue-green upgrades to your container infrastructure to reduce and eliminate application impact. Control your infra software lifecycle with more control and less risk.

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.

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 architecture.

Universal Control Plane (UCP) – Manage all system components from a unified 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. In addition, export cluster metrics to an external Prometheus server for local management and monitoring.

Enhanced access controls – Integrate Docker Enterprise with corporate LDAP/AD, SSO through SAML 2.0 or PKI certificate-based authentication. 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 – 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.

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.

Choice of operating system – Docker Enterprise is supported on multiple Linux distributions (CentOS, Oracle Linux, RHEL, SLES, or Ubuntu) and on Windows Server 2019.

Choice of 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.

In addition, there are numerous 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 apply to other regulated industries.

Encrypted communications – Automatic mutual TLS authentication ensures that the default mode of communication within the system is encrypted and protected. Swarm and Kubernetes network encryption protects 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.

Group Managed Service Accounts (gMSA) for Swarm – Support for gMSA brings Docker Enterprise to a wider set of Windows Server applications that require Active Directory authentication. Swarm allows the creation of credential specs with Docker Configs to bring ease of use and automation to gMSA.

Enterprise Support and Certified Partner Ecosystem

Mirantis 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 and managed services from the source – Get SLA-backed support from the team that built the platform, who have joined forces with Mirantis open cloud experts to provide support for the complete Kubernetes stack. Multiple support plans are available, including OpsCare managed services, ProdCare (enhanced 24x7), Business Day (9am-6pm, Monday to Friday) , Business Critical (24x7), and others.

Professional Services – Based on proven methodologies learned from working with hundreds of enterprise customers, Mirantis offers a set of Solution Architecture engagements to accelerate your containerization journey 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.

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 distribute their Networking and Volume Plugins as containers for Docker Enterprise. Built with best practices, they must also pass a suite of API compliance testing, and are scanned and reviewed. Cooperative support from Docker and the plugin provider is included.

Certified Infrastructure – Delivering a prescriptive approach to deploying Docker Enterprise on AWS, Azure and vSphere, certified infrastructure complements Docker Enterprise's automated lifecycle management capabilities by providing reference architecture and ecosystem solution briefs.

Get Started with Docker Enterprise

Docker Enterprise is available as an annual subscription inclusive of software and support. To learn more, visit www.mirantis.com/docker-enterprise. Experience Docker Enterprise for free with a 30-day trial. Get started at www.mirantis.com/free-trial.

US
+1-650-963-9828
mirantis.com/contact

EMEA
emea@mirantis.com

Japan
+81-3-6635-6355
info.jp@mirantis.com

China
china@mirantis.com