CLOUD NETWORK SECURITY POLICY

Version Number:	3.1
Version Date:	10/09/2025
Owned by:	Security, GRC
Approved by:	Nate Fitch, Sr. V.P., Chief of Staff
Confidentiality Level:	Internal

Table of Contents

1. Purpose

This policy establishes minimum security controls for Docker's cloud network infrastructure across AWS, Azure, and Google Cloud Platform. Built on zero trust principles and defense-in-depth strategies, it ensures that all cloud environments are protected from unauthorized access, misconfiguration, lateral movement, and other threats.

The policy defines requirements for:

- Network segmentation with isolated VPCs/VNets for production, staging, and development environments
- Infrastructure as Code (IaC) using secure configuration baselines validated by policy-as-code engines
- Strict ingress/egress controls with comprehensive logging and monitoring
- Native intrusion detection services (AWS GuardDuty, Azure Defender, GCP Security Command Center) integrated with security operations
- Remote access secured through MFA and role-based controls

This framework ensures cloud networks are securely designed, auditable, and resilient to evolving threats while supporting Docker's compliance with ISO 27001, SOC 2, and customer trust agreements in a dynamic multi-cloud architecture.

2. Scope

This policy applies across all areas of Docker’s global cloud infrastructure, spanning all environments, personnel, and tools involved in the operation, configuration, or management of network-connected resources. The policy governs cloud-based systems operating in production, staging, development, and sandbox environments, whether deployed within Docker’s primary infrastructure or provisioned through integrated third-party services.

It applies to all network components within Docker’s cloud estate, including virtual networks, subnets, firewall rules, DNS, load balancers, cloud-native firewalls, and Kubernetes clusters. Systems covered include Docker-managed compute resources, cloud storage, container orchestration environments, and supporting services that process or transmit Docker business or customer data.

The policy is binding on all Docker employees, contractors, and third-party providers who have access to cloud network infrastructure, including DevOps, security, engineering, and IT personnel. It also governs integrations with third-party platforms that connect to Docker environments via APIs, service meshes, or VPNs. Any system or user with the ability to influence network exposure or routing within Docker’s cloud environments falls under the authority of this policy.

3. Roles and Responsibilities

Role	Responsibilities
Security Team	Establishes and maintains cloud network security policies and standards. Monitors threat intelligence feeds and IDS alerts. Investigates security events and leads incident response for cloud-related exposures. Reviews firewall configurations and validates segmentation compliance.
Cloud Infrastructure Team	Builds and maintains secure network configurations using IaC. Manages deployments via CI/CD pipelines and ensures that configuration drift is detected and remediated. Integrates alerting and backup mechanisms.
Engineering Teams	Assigns accurate metadata and tags to cloud assets. Requests approval for network-affecting changes. Ensures compliance with network policy requirements in application architecture.
Cloud Infrastructure Owners	Oversees the security and compliance posture of designated cloud environments. Performs regular access reviews and ensures proper tagging, monitoring, and control implementation within their environments.
IT / Identity and Access Management Teams	Configures IAM roles and policies for cloud services. Enforces multifactor authentication and session controls for administrative access to cloud consoles and APIs. Validates least privilege access.
Compliance Team	Conducts audits of network logging, segmentation, and monitoring configurations. Prepares evidence for regulatory reviews and third-party security assessments. Maintains documentation for control mappings.

4. Definitions

Zero Trust - A security model that assumes no user, device, or network segment should be automatically trusted, requiring continuous verification of every transaction and connection regardless of location or previous authentication.

Defense-in-Depth - A security strategy employing multiple layers of security controls throughout the cloud infrastructure, ensuring that if one control fails, others remain in place to protect against threats.

Trust Zones - Logically separated network segments with defined security boundaries and access controls, typically organized by environment type (production, staging, development) and data sensitivity levels.

Infrastructure as Code (IaC) - The practice of managing and provisioning cloud infrastructure through machine-readable configuration files rather than manual processes, enabling version control, automated validation, and consistent deployments.

DMZ (Demilitarized Zone) - An isolated network segment that sits between the public internet and internal networks, housing public-facing services while preventing direct access to sensitive internal resources.

5. Cloud Network Design Principles

5.1 Defense in Depth

Multiple layers of defense are applied across all components of Docker's cloud networks. This includes the use of security groups, access control lists, host-level hardening, and identity-based firewall rules. Each layer is configured to enforce least privilege and deny-by-default principles.

5.2 Network Segmentation

Docker's environments are separated into distinct trust zones, such as production, development, staging, and testing. Cross-environment traffic is prohibited unless explicitly authorized and logged. Default VPCs and shared environments are not allowed unless Docker-specific segmentation standards are enforced.

CIDR ranges are predefined per environment. Private subnets, NAT gateways, and firewall rules restrict outbound and inbound access. Public IP exposure is minimized and monitored through automation.

5.3 Secure Configuration Standards

All network configurations must conform to Docker's security baselines, based on CIS Benchmarks or internally reviewed equivalents. Secure configurations must be embedded in IaC templates and validated using automated policy frameworks (e.g., OPA, Sentinel, AWS Config). Changes to configuration baselines require approval via Docker's change management process.

6. Network Security Controls

6.1 Firewall Rules and Security Groups

Administrative ports such as SSH, RDP, and Kubernetes API must never be exposed to the open internet (0.0.0.0/0 or ::/0). Security groups must be reviewed quarterly for production systems and annually for non-production systems. Public-facing workloads must reside in DMZ zones and be isolated from internal resources.

6.2 Intrusion Detection and Monitoring

Docker enables native detection services in each cloud provider environment, including:

- AWS GuardDuty
- GCP Security Command Center

- Azure Defender and Sentinel

Alerting systems must be configured to detect anomalies such as lateral movement, unexpected privilege escalation, and unauthorized firewall rule modifications.

8. Configuration Enforcement and Monitoring

Control	Enforcement Mechanism
Public IP usage	Blocked or flagged through CI/CD pipelines
Time synchronization drift	Monitored using cloud-native tools
IDS alerts	Routed to the on-call Security response team via appropriate channels and logged for triage

9. File Integrity and Time Synchronization Controls

File Integrity Monitoring (FIM) must be enabled on cloud-hosted virtual machines. Time synchronization must be maintained across all environments using Docker-approved internal time authorities. External NTP sources may only be used by approved relay systems.

10. Enforcement and Exceptions

All Docker personnel are expected to comply with this policy in full. Failure to adhere may result in disciplinary action, up to and including termination of employment or contract. In cases involving willful misconduct, malicious activity, or violations of law, Docker may initiate legal proceedings. The organization reserves the right to monitor, audit, and inspect user activity on its systems to ensure compliance.

Any exceptions to this policy must be formally requested, documented, and approved by Docker's GRC or Legal team. Exception requests must clearly outline the business justification and associated risks, and should be submitted to Docker's Risk Submission Portal.

11. Change History

Date	Version	Responsible Party	Description of Change
10/09/2025	3.1	Nate Fitch, Sr. V.P., Chief of Staff	Revised policy approved
09/29/2025	3.0	Chad Fryer, Sr. Security Engineer, GRC	Policy annual review and update

07/23/2024	2.2	Tim Baur, Vice President, Engineering, Platform	Revisions Approval
05/20/2024	2.1	Karen Hajioannou, Senior Security & Compliance Engineer Rachel Taylor, Director, Security, Risk & Trust	Policy annual review and update
02/28/2023	1.2	Brett Inman, Senior Manager, Engineering, Platform	Draft document approved
02/27/2023	1.1	Rachel Taylor, Senior Manager, Security, Risk & Trust	Draft Submitted for review
02/3/2023	1.0	Rachel Taylor, Senior Manager, Security, Risk & Trust	Basic document outline