



Subnet

Strengthen Cloud Network Security – with Smart, Automated Subnet Segmentation

Segment workloads, control east-west traffic, and enforce isolation at scale – with JioCloud Subnet built for security, compliance, and control.

The Challenge

Managing cloud networks at scale is becoming harder.

- Misconfigured subnets and access rules open doors to data breaches.
- East-west traffic goes unmonitored, making it difficult to detect internal threats.
- Manual segmentation slows deployments and weakens policy consistency.
- Meeting compliance needs for isolation, control, and audits is an ongoing struggle.



The JioCloud Solution

JioCloud Subnet helps you securely segment cloud workloads by function, environment, or business need. Each subnet defines a clear boundary for communication, reducing lateral risk and improving access control.

With easy provisioning, policy enforcement, and real-time monitoring, you get scalable network hygiene without the manual effort.

Key Features

■ Intelligent network segmentation

Divide your virtual network into subnets for secure workload isolation, application tiering, and zone-based control.

■ Custom IP range allocation

Assign distinct IP ranges to each subnet to prevent overlaps and simplify resource grouping.

■ Workload satellite creation

Create isolated subnet clusters with tailored access for high-performance, high-security use cases.

What You Gain

- **Limit lateral threat movement:** Keep dev, test, and production workloads isolated to reduce risks from internal threats.
- **Enforce access at the subnet level:** Apply precise controls across applications and environments — supporting zero trust principles.
- **Simplify network management:** Monitor and manage subnet traffic, configurations, and segmentation policies with ease.
- **Accelerate deployment:** Use templates and automation to create secure subnet environments faster and with fewer errors.
- **Stay audit-ready:** Maintain strong network hygiene with logging, visibility, and traceability across all subnets.



Use Cases in Action

National Bank - Securing Digital Channels through Subnet Isolation

To protect its internet banking, UPI APIs, and mobile apps, a national bank uses JioCloud Subnet to segment workloads by environment and function.

With JioCloud Subnet, the bank keeps its development, staging, and production environments fully isolated.

Each environment sits in its own subnet, protected by custom access policies. Monitoring tools track all east-west traffic, while automation ensures every team follows consistent security rules.

This setup strengthens defenses, speeds up delivery, and simplifies compliance.

Who It's For

- Cloud Security Architects
- Network and Infrastructure Engineers
- DevOps and Platform Teams
- Security Operations Centers (SOC)
- Compliance and Risk Managers
- Application Owners

Why JioCloud

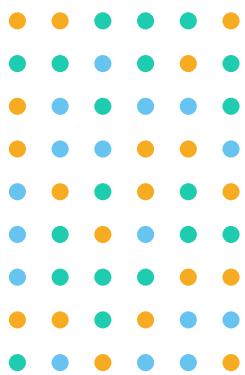
Automated subnet provisioning
Speed up segmentation with pre-approved templates and secure defaults.

Granular isolation policies
Reduce risk by enforcing workload-specific access across zones.

Compliance-ready network architecture
Built-in support for audit logging, access traceability, and data residency.

Localized performance
Regional deployments aligned to India's regulatory and latency needs.

Seamless cloud integration
Works with your existing cloud stack, monitoring tools, and security policies.



Strengthen Your Cloud Network with JioCloud

Email us at jpl.cloudsales@ril.com or visit [\(website\)](#) to see how JioCloud Subnet helps you build secure, audit-ready network environments at scale.

