Automated Identity for Kubernetes, Microservices & Cloud Workloads

Modern workloads need short-lived, automated, and scalable identities. Manual certificate handling in Kubernetes or cloud environments introduces risk, delays deployments, and breaks Zero-Trust. QCEcuring automates workload identity from issuance to rotation.

Introduction

Cloud-native applications rely on thousands of microservices, containers, APIs, and distributed workloads communicating across dynamic environments. Traditional certificate management cannot keep up with frequent scaling, redeployment, and ephemeral workloads.

QCEcuring Cloud-Native Machine Identity provides automated certificate issuance, rotation, and trust management for Kubernetes, serverless, containers, and multi-cloud workloads. Every identity is short-lived, policy-enforced, and monitored—enabling Zero-Trust communication across clusters and services.

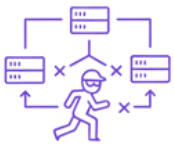
The Problems

Hard-coded long-lived credentials

Manual mTLS certificate injection

No rotation inside Kubernetes

Poor visibility into service identity



Risk of lateral movement attacks

The Solutions

Automated workload identities

Short-lived certs with auto-rotation

Kubernetes-native integration

Service mesh & API support

Policy-driven trust controls

Key Features

Kubernetes-Native Automation

Auto-issue and rotate certificates for pods, services, and workloads.

Short-Lived Certificates

Reduce risk with frequent, automatic identity renewal.

Service Mesh Integration

Works with Istio, Envoy, Linkerd, Consul, and mTLS-based clusters.

Cloud IAM Compatibility

Supports AWS IAM Roles, Azure MSI, GCP Workload Identity.

Unified Policy Management

Define issuance, trust, and rotation rules across clusters.

Identity Telemetry

Real-time visibility of certificate expiry, usage, and workload trust status.

How It Works

Worklolad requests identity

Policy + trust rules validated

Short-lived certificate issued

Deployed to mesh / container / API

Auto-otation maintains Zero-Trust

Business Benefits

Enforces Zero-Trust between workloads

Prevents credential theft & replay attacks

Accelerates microservice deployments

Ensures strong mTLS everywhere & Provides full identity visibility

Use Cases

Kubernetes workload identity

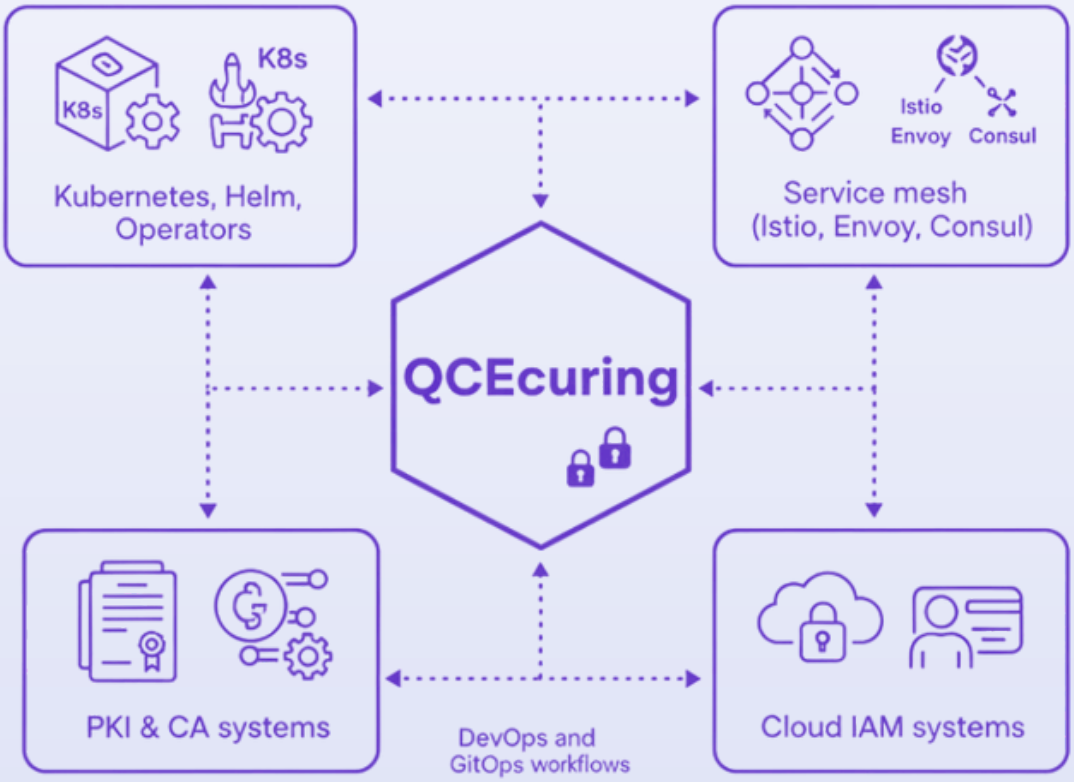
Service-to-service mTLS

API authentication

Multi-cluster identity federation

Serverless identity rotation

Integrations



Deployment Options

On-Prem

Deploy into private Kubernetes clusters with local trust anchors.

Cloud

Ideal for cloud-native clusters needing scalable, automated identity services.
On-Prem

SaaS

A fully managed workload identity platform with instant onboarding.

Hybrid

Link cloud and datacenter workloads with unified identity governance.

The Value We Deliver

- Zero-trust ready architecture
- Strong automation
- Real-time identity insights
- High scalability
- Simple developer experience
- Enterprise-grade automation

Looking to secure Kubernetes and cloud-native workloads with automated identities?
Connect with **info@qcecuring.com** to explore how our platform simplifies workload identity and strengthens Zero-Trust across your infrastructure.