Full Control of SSH Access with Zero Operational Risk

Untracked SSH keys create silent security gaps across servers and cloud systems. Shared keys, orphaned keys, and keys that never expire become high-risk access points. Qcecuring makes SSH key governance simple by automating discovery, ownership mapping, rotation, and access control—so your team stays secure without slowing down operations.

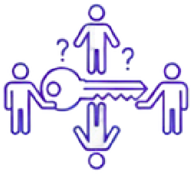
Introduction

SSH keys act as powerful “digital master keys” that control administrative and machine-to-machine access. When unmanaged, they become extremely difficult to monitor and can lead to unauthorized access or compliance failures. Manual SSH key management often results in shared credentials, outdated keys, and limited visibility into who can log into what systems.

QCecuring SSH Key Lifecycle Manager brings order, automation, and Zero-Trust principles to SSH access. It discovers every key across servers and cloud environments, maps each key to its rightful owner, rotates keys automatically, and enforces policy-based access approvals. This ensures only the right people—and only for the right time—can access critical systems, with complete audit visibility.

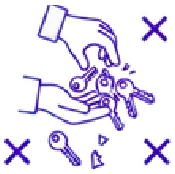
The Problems

Orphaned SSH keys



Shared keys

No rotation



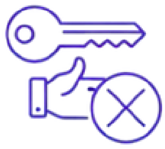
Manual distribution

No audit trail

The Solutions

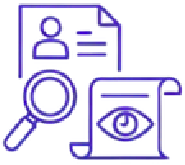
Discovers all keys & Maps each key to its owner

Rotates keys automatically



Removes unauthorized keys instantly

Enforces approval-based access



Provides complete audit trails

Key Features

SSH Key Discovery

Scans Linux servers, cloud VMs, containers, and automation scripts to locate every authorized key.

Owner Mapping & Access Control

Automatically links keys to users and systems, preventing unknown or shared access.

Automated Key Rotation

Rotate keys periodically or instantly based on policy, risk, or employee offboarding.

Just-In-Time SSH Access

Provide temporary, time-bound access with approvals and automatic expiry.

RBAC & Identity Integration

Integrates with Active Directory, LDAP, Okta, Azure AD, SSO.

Full Audit Trails

Track every login, command, and key usage for compliance teams.

How It Works

Discover keys across all systems

Link keys to their rightul owners

Enforce policies & approvals

Rotate keys automatically

Monitor usage in real time

Business Benefits

Eliminates unauthorized access

Prevents insider threats

Reduces audit effort

Strengthens Zero-Trust posture

Use Cases

Cloud VM access governance

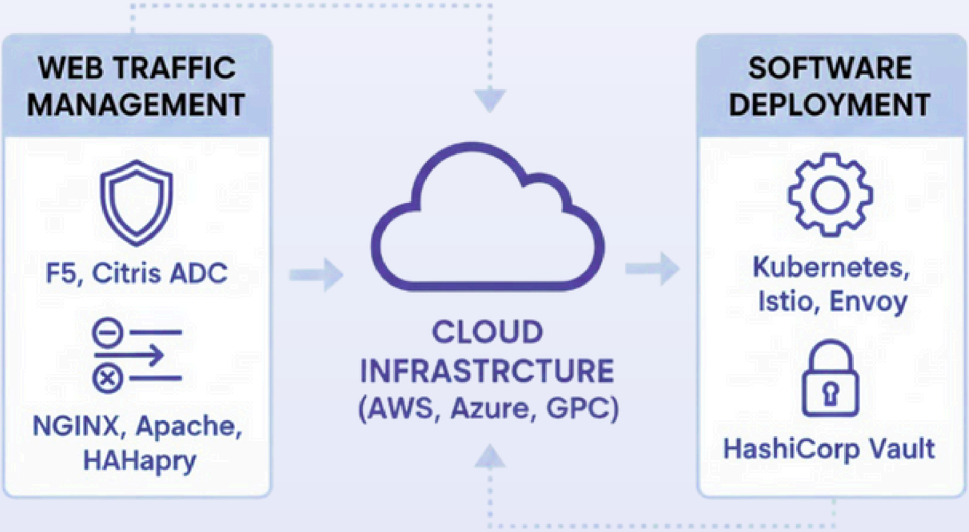
DevOps temporary access

Privileged access enforcement

Offboarding employees securely

Rotating SSH keys across 100s of systems

Integrations



WEB TRAFFIC MANAGEMENT

F5, Citris ADC

NGINX, Apache, HAHapry

CLOUD INFRASTRCTURE (AWS, Azure, GPC)

SOFTWARE DEPLOYMENT

Kubernetes, Istio, Envoy

HashiCorp Vault

AUTOMATION PIPILINES

Gitalb jenkins

Deployment Options

On-Premises

Install the SSH Governance platform within your datacenter for full control over keys, policies, and access. Ideal for organizations with strict security requirements.

Cloud

Deploy in a secure cloud environment with easy scaling and cloud-native integrations across AWS, Azure, and GCP.

SaaS

Use our fully managed service for instant onboarding and zero infrastructure management. All updates and security controls are handled for you.

Hybrid

Combine on-prem and cloud setups — keep sensitive keys local while managing discovery, rotation, and access from a unified cloud console.

The Value We Deliver

- ✓ Easy onboarding
- ✓ Developer-friendly workflows
- ✓ Real-time insights
- ✓ Automated security hygiene
- ✓ Zero-Trust aligned
- ✓ Enterprise-grade automation

Looking to secure SSH access and remove risks from unmanaged keys?
Our SSH Governance platform simplifies key rotation, enforces access policies, and provides complete visibility into who can access your critical systems.
Contact **info@qcecuring.com** our specialists to explore how automated SSH lifecycle management can support your security and compliance needs.