Zero Trust keyless SSH access

From static keys to keyless access with Zero Standing Credentials

Eliminate unmanaged SSH trust of human users and non-human identities (NHIs) and transition to certificate-based, identity-bound access with PrivX™ PAM and Key Manager.



The Zero Trust migration to keyless SSH access starts with bringing SSH keys under control and effective SSH key management. Our holistic approach covers both interactive and automated connections and is executed in five steps: discover, audit, remediate, automate, and migrate.

Benefits

Reduce access risks

Discover SSH keys and trust relationships, eliminate orphaned or excessive access, and enforce ownership. Prevent PAM bypass.

Improve operational efficiency

Manage and automate SSH key lifecycle management from a centralized view. Identify, audit, and remediate policy violations.

Zero Trust keyless access

Follow a structured path from static credentials to just-in-time, certificate-based access without changes to your applications.

1. Discover

Establish a complete inventory of SSH trust relationships across source and destination hosts. PrivX Key Manager is deployed, integrated with directory services, and connected to managed hosts - a trust graph of users, service accounts, hosts, and cross-application access paths is created.

2. Audit

The PrivX Key Manager policy engine is used to evaluate the SSH key estate against defined security rules and compliance criteria, automatically flagging violations, excessive permissions, and risk conditions.

3. Remediate

Remediate your environment and any policy violations by removing or restricting unnecessary access. PrivX Key Manager helps you align server configurations with enforcing certificate-based access.

4. Automate

Establish centralized approval workflows and lifecycle governance. Access requests, key rotations, and onboarding of new systems are executed through controlled, auditable processes rather than host-level manual changes.

5. Migrate

Transition human and service access from static keys to certificate-based, identity-bound access through PrivX - Zero Standing Access.
(in detail on page 2)

* Quantum-safe migration

PrivX Key Manager helps you create a complete inventory of cryptographic assets and track quantum-safe algorithm usage to support your transition strategy to Post-Quantum Cryptography (PQC).

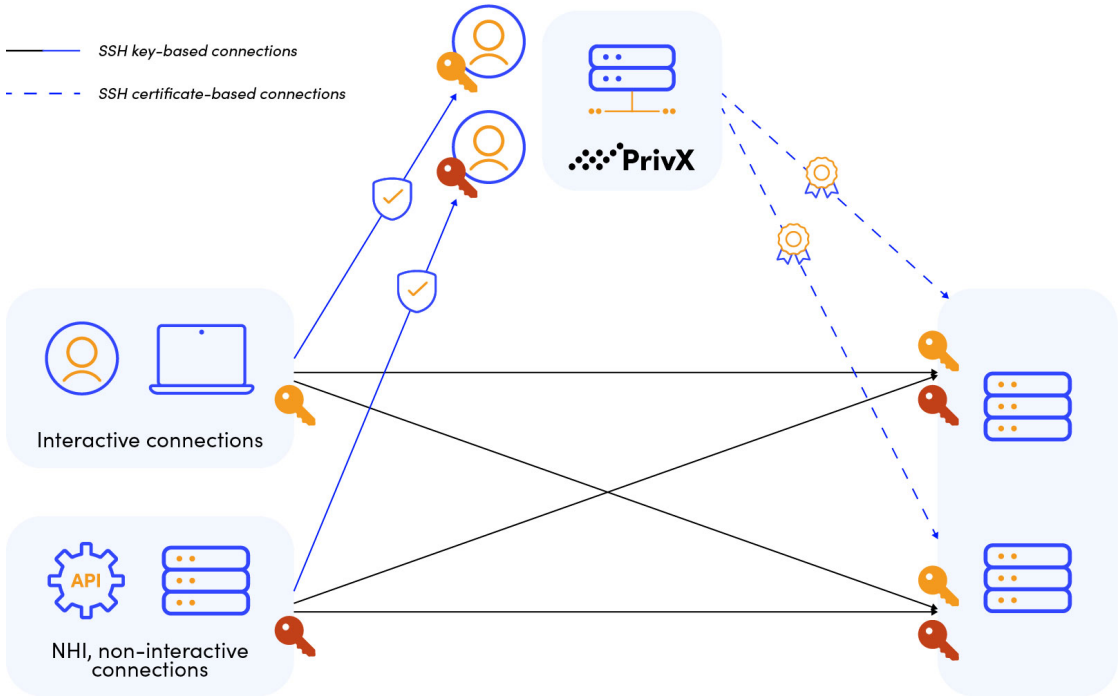
Why migrate to keyless SSH?

After the migration, all SSH trust relationships have been inventoried and governed, access is granted through just-in-time mechanisms, and static authorized keys are removed. Machine trust relationships are assigned to applications with defined owners. SSH servers trust a central certificate authority. Access policies are evaluated centrally and all sessions are auditable.

Throughout the migration process, operational continuity is preserved, while reducing unmanaged trust.

1.5M

Our biggest customer has 1.5M SSH authorized keys to remove and migrate to ephemeral certificates.



How Zero Trust keyless migration works with PrivX Key Manager and PrivX PAM

Host deployment

Defined delegated principals determine which target accounts are allowed for Zero Trust access. Target hosts are deployed to PrivX PAM using the deployment script: *deploy.py*

Evaluation

The evaluation begins in the PrivX Key Manager GUI using the "Migrate to Zero Trust" workflow. It validates host existence in PrivX inventory, target principals in hosts, existing authorizations, and duplicate/conflicting key usage.

Execution

The deployed SSH client configuration forces SSH traffic through PrivX PAM using *ProxyCommand*. Source accounts are marked as Zero Trust-enabled and assigned to roles, which are created/updated in PrivX alongside external authorized key counterparts.

After the migration, SSH clients connect through PrivX PAM, which validates role membership and issues a short-lived certificate. Target hosts validate the certificate against the PrivX CA. Static *authorized_keys* entries are no longer required for migrated access.