4 Steps to SSH Key Management

with SSH Communications Security

Your enterprise may have more Secure Shell trust relationships than employees. A lot more!

A typical 1,000 server environment server has over 15,000 Secure Shell key based trust relationships, with 10% of these granting a high level of privilege including root.

Follow these four steps to gain visibility and control over your Secure Shell environment.

DISCOVER

Your Secure Shell access management problems didn't happen overnight. They have been growing for years. The first step is finding out who has access to what.

Locate all SSH private & public user keys

Associate SSH user keys with **identities**

Map all trust relationships

Now You Are Able to:

- Lockdown the environment so that only the key manager can remove or deploy keys
- Begin compliance and security remediation efforts
- Develop policies for Secure Shell access in your environment

MONITOR

The next step, gain vital visibility into who is accessing what across your entire Secure Shell environment.

Monitor any changes in the key environment including moves, adds and deletes

Monitor configuration changes including access level (ie root), what commands are permissible, authentication methods and allow/deny sub-channels

Now You Are Able to:

Gain security intelligence into your Secure Shell environment to identify policy violations and malicious activity

REMEDIATE

Step 3, remove obsolete authorizations, rotate old keys and implement security policy for your Secure Shell environment.

Remove rogue, orphaned and unused keys

Rotate existing keys

Enforce policy on SSH version, keys and configurations

Now You Are Able to:

- Ensure that only authorized identities have access to your Secure Shell environment, and with proper permissions
- Bring your organization back into compliance
- Improve your security posture

MANAGE

The final step, compliance and security are not one time events. Stay secure and lower operational costs with centralized Secure Shell management.

Full life-cycle management including configuration, provisioning, removal and rotation

Simplify management using group-based controls

Integrate into your enterprise identity management systems and active directory

Now You Are Able to:

- Centrally manage all of your Secure Shell users keys ensuring both compliance and security
- Prevent users from secretly adding keys
- Lower costs – less manual activity means fewer errors
- Through API's, automate Secure Shell access controls with existing processes and solutions

Ready to take the first step?

Secure Shell HealthCheck™

Secure Shell HealthCheck is a security assessment service that delivers a detailed analysis of how Secure Shell is deployed and used in your network. Contact us to get your check-up and find out if your environment is at risk or out of compliance.

Source: http://www.ssh.com/services/health-check

brought to you by : ssh