Venafi

SOLUTION BRIEF

Successfully Pass Your SSH Key Audits

Protect keys and certificates to ensure privileged access remains secure

The Facts

75% Have No SSH Security
Providing attackers with privileged, root access[1]

60% Cannot Detect New SSH Keys
When introduced into their networks[1]

46% Never Rotate SSH Keys
In spite of the fact that SSH keys never expire[1]

76% Have No SSH Cloud Security
For SSH key usage in the cloud[1]

51% Already Compromised
By an SSH key-related issue within the last 2 years[1]

SSH Audit Challenges

With a dramatic increase in Secure Shell (SSH) key-related compromises, IT security is looking to externally conducted SSH audits to assess risk, avoid compliance violations, and increase accountability for identity and access management. SSH keys provide the highest privileges for accessing servers, applications, and cloud instances. Yet most enterprises lack the basic security and policy to properly protect them from misuse.

Survey results show most organizations have an over-reliance on system administrators, not IT security, to self-police SSH keys.[1] As a result, organizations are unable to identify how many SSH keys they have, who uses them, and what they access.

SSH audit status indicates how vulnerable an organization is to SSH key theft and misuse. Without continuous SSH monitoring and policy enforcement, organizations leave a gaping hole in their security that enables APT operators and malicious insiders to access systems and networks with root-level access and go undetected—often for years.

Impacts on SSH Audits

Without visibility, policy enforcement, and rogue key detection, organizations are unprepared for SSH audits.

Lack of visibility: In a Ponemon Institute survey, 53% of organizations admitted they lack centralized control over their SSH key usage and access policies, and 60% are unable to detect the introduction of new SSH keys into their network.[1] This lack of visibility hinders detection of SSH key security issues.

Inadequate policy enforcement: SSH keys do not expire, creating a perpetual vulnerability if not rotated. But a surprising 82% change their SSH keys at best every 12 months—much longer than the 60-90 day policy for passwords which have less privileged access.[1]

Inability to detect rogue SSH keys: Over half of organizations surveyed responded to a security incident related to SSH key misuse within the last 2 years. Of those that use homegrown scripted solutions to manage SSH keys, 54% were still compromised by rogue SSH keys on their networks—a clear indication that these solutions cannot detect anomalies in SSH key usage.[1]

Without continuous SSH key management and security you will fail to answer an SSH auditor's questions or apply effective audit remediation. Worse yet, these SSH audit failures reflect underlying security issues that leave your organization open to compromise.

SSH Audit Remediation

Attacks perpetrated with stolen SSH keys lend a sense of urgency to SSH audit failures. To ensure fast and complete SSH audit remediation, organizations need complete SSH key visibility and trust maps showing access privileges between administrators, keys, and systems. There should be an audit trail tracking which source user (and client) uses which keys to connect to which destination systems. After this foundation, organizations need continuous monitoring, automated, policy-enforced issuance and rotation, detection of anomalous access, remediation, and escalation.

Just like the human immune system, SSH key security must be able to identify what is "self" and trusted and what is not and therefore dangerous, recognizing the misuse of SSH keys and protecting the organization's most privileged access. Venafi is the Immune System for the Internet, identifying what keys and certificates are trusted, protecting those that are trusted, and fixing or blocking those that are not.

Venafi Trust Protection Platform

The Venafi Trust Protection Platform™ includes Venafi TrustAuthority™, Venafi TrustForce™, and Venafi TrustNet™, providing the following for SSH audit remediation and ongoing SSH key management and security.

Venafi TrustAuthority

Ensures Visibility

- Creates a complete SSH key inventory across networks, applications, and cloud instances
- Provides continuous detection and monitoring of all client and server SSH keys and key pairs to validate compliance
- Maps trust relationships between administrators, keys, and systems, and establishes a baseline of SSH key usage
- Identifies changes to authorized key lists, key additions and deletions, and other configuration policy violations with real-time monitoring
- Validates audit compliance with automated reports and notifications

Venafi TrustForce

Automates Policies and Workflows

- Performs automatic, policy-enforced key generation and rotation
- Controls SSH key attributes such as key length and hash algorithms
- Enables policy enforcement at the host group level and for device access controls

Responds and Remediates

- Remediates unauthorized SSH key configurations automatically
- Detects anomalous SSH key behavior
- Removes rogue or orphaned SSH keys and reverts to approved settings
- Enables SSH key whitelisting and blacklisting for fast remediation, and marks blacklisted keys for deletion

Ensure Trust in Privileged Access via Secure SSH

All enterprises rely on SSH keys to authenticate privileged users and establish trusted and secure access to critical systems, including applications, virtual machines, and cloud instances. But SSH audits often identify significant gaps in SSH security controls. Cybercriminals target these gaps to gain full access to sensitive, regulated, and valuable systems and data.

You can secure the trust established by SSH and remediate audit failures with Venafi, achieving automated SSH key discovery, issuance, and rotation that improves security and speeds incident response and remediation.