Stop Unauthorized Abuse of Privileged Access by Protecting Your SSH Keys

Take control of your SSH keys to minimize your risk of intrusion
SSH Keys—Lowest Cost, Highest Risk Tool

All enterprises rely on Secure Shell (SSH) keys to authenticate privileged users and establish trusted access to critical systems, including application servers, routers, firewalls, virtual machines and cloud instances. Yet, despite the sweeping access they grant, most SSH keys are not tightly controlled. While SSH infrastructure and associated keys are generally free, poor SSH key management practices can expose businesses to costly security risks.

SSH Mismanagement

SSH keys are not subject to the same stringent security controls organizations apply to usernames and passwords, including complexity, minimum lengths, frequent reviews and rotations. Yet, SSH keys provide critical protection for machine identities, serving as access credentials, authenticating and enabling administrator-to-machine or machine-to-machine access. Even though SSH keys are the credentials that provide the most privileged access in an organization (including root-level privileges), they are routinely untracked, unmanaged and unmonitored.

A complex web of SSH keys is already being used in every enterprise network for privileged administrative operations by system administrators: they govern secure machine-to-machine automation of critical business functions. Once SSH keys are put in place to enable client authentication, they enable ongoing, automatic connections from one system to another, without requiring a password. This creates a persistent trust relationship—one that cyber criminals and malicious insiders are eager to access and misuse.

Most organizations do not realize the potential impact of an SSH compromise and have allowed users and system administrators to generate and manage SSH keys across hundreds, or thousands, of systems, with access and configuration left up to each administrator’s discretion. These ad hoc processes and inconsistent security controls leave organizations without an accurate inventory or a regular review of their SSH trust relationships.

Because there is no inventory or centralized management, security teams are afraid to remove any SSH keys—they’re not sure which keys are still active, who owns them or what the keys do. This approach can result in thousands, or even millions, of active SSH keys across an organization. More often than not, these keys are not regularly reviewed or rotated, nor are they subject to policy enforcement.
SSH Security Risks

Weak SSH key management practices can create significant cyber security risks because of the privileged access SSH enables and the large number of untracked persistent SSH trust relationships most organizations have within their environments. Because SSH key risks are not addressed by IAM/PAM, they are among the biggest, yet least understood, risks in network environments:

• **Unauthorized account access:** With thousands, or even millions, of untracked SSH keys in enterprises, cyber criminals have a broad attack surface to exploit.
  - Default SSH configurations allow users to manage their own SSH authorized keys. This practice enables backdoor keys to be put in place by malicious users or attackers.
  - Poorly protected private keys can be compromised by attackers to gain authenticated access to sensitive accounts. Weak, old or unrotated keys, which are common in most organizations, make it easier for cyber criminals to compromise private keys.
  - In addition, when SSH keys are left unmonitored, some walk out the door with terminated employees—either maliciously or innocently—allowing former employees access to corporate networks.

• **Pivoting:** Once cyber criminals have breached a network, persistent SSH trust relationships between systems enable them to rapidly jump, or pivot, from system to system. The more SSH keys administrators deploy without strong oversight and review, the more extensive the risk that an attacker can pivot quickly throughout an organization and gain access to mission-critical systems.

• **Circumvent security controls:** An improperly controlled SSH environment, including poor control of authorized keys file or SSH server configuration, can be used to bypass firewalls and other security technologies. If not prevented through proper configuration, users can setup SSH for port forwarding, which can enable other systems to leverage the authorized connections through firewalls.

• **Unauthorized use of SSH Server:** When an SSH Server is activated on a system, it enables remote login to that system. Since SSH implementations like OpenSSH are freely available, users can enable SSH services on systems that haven’t been SSH enabled, opening those systems to remote attack.

One G5000 organization discovered 1.6 million SSH keys on just 8,000 servers on one section of their network. Using an automated solution, they were able to quickly reduce this number by over 65% to just 600K keys, with further reductions planned.
Protect SSH Keys with a 4-step Process

Because SSH is used for privileged access and process automation across a broad number of mission-critical systems (Unix, Linux, routers, firewalls, etc.), it’s important that organizations implement sound security, policy and auditing practices for SSH keys.

1. **Build Inventory:** To identify SSH vulnerabilities and ensure proper controls, organizations need centralized visibility into all SSH servers, private keys and the authorized keys that grant SSH access, as well as SSH configurations that limit access. Because SSH keys are generally stored in user home directories, the most efficient and accurate way to discover keys across all systems and accounts is using an automated solution.

2. **Identify Vulnerabilities:** Once a complete inventory is established, organizations must be able to rapidly use it to identify which SSH keys and servers are not compliant or vulnerable. Weeding through hundreds of thousands, or even millions, of SSH keys manually is infeasible, so organizations must employ tools that proactively identify vulnerabilities and issues. These vulnerabilities include SSH root access, weak keys, backdoor keys, keys that have never been rotated, lack of source restrictions and forced commands, duplicated private keys, port forwarding and insecure configurations. Automation should be built into the ongoing identification process—effective detection and response to anomalous use of SSH keys is only possible with machine-speed automated alerts and notifications.

3. **Remediate:** Organizations must quickly remediate identified SSH issues, including removing unauthorized keys, rotating or replacing weak and old keys, removing SSH root access, removing duplicate private keys and enforcing security controls that are designed to limit the accessibility and use of SSH keys. Automation is required for timely incident response and can include the automatic rotation, installation and configuration of SSH keys. Automating these procedures ensures consistent policy enforcement of SSH key lifecycle management and verifies that all changes are centrally logged and tracked.

4. **Monitor:** SSH key security requires continuous monitoring and tracking. Orchestrating management and security operations enables SSH audits to regularly review SSH entitlements, assess risk, avoid compliance violations and increase accountability for identity and access management.
Secure Trust by Protecting Your SSH Keys

Educate yourself on the risks that SSH poses and stop viewing SSH keys as simply an operational tool that can be self-managed by system administrators. With Venafi, you can continuously apply controls that secure privileged access across your enterprise. The Venafi platform delivers complete, enterprise-wide visibility into SSH key inventories and automates the entire SSH key lifecycle from issuance to decommissioning. With Venafi, you are able to secure and control all SSH keys to minimize your risk of unauthorized access to critical systems.

TRUSTED BY THE TOP

5 OF 5 Top U.S. Health Insurers
5 OF 5 Top U.S. Airlines
4 OF 5 Top U.S. Retailers
4 OF 5 Top U.S. Banks
4 OF 5 Top U.K. Banks
4 OF 5 Top S. African Banks
3 OF 5 Top AU Banks

ABOUT VENAFI

Venafi is the cybersecurity market leader in machine identity protection, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access.

To learn more, visit www.venafi.com