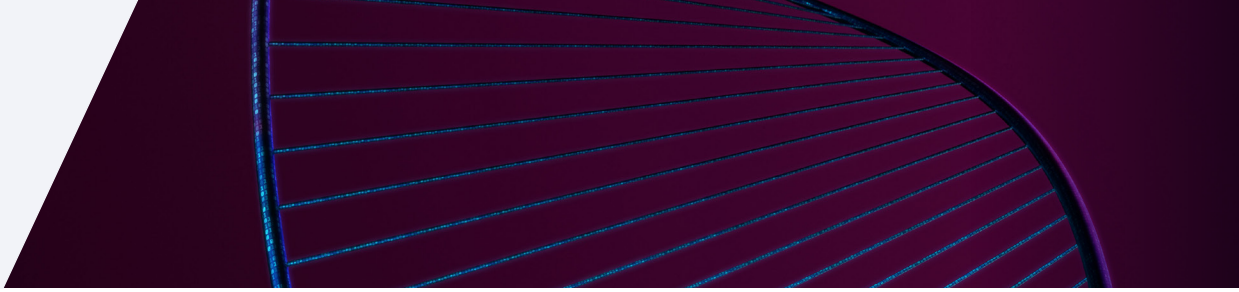
Venafi



SOLUTION BRIEF

Protect Privileged Access—Manage and Secure SSH Keys

Don't let unprotected SSH keys leave your most sensitive systems and data vulnerable

All organizations rely on SSH as an encrypted protocol to authenticate privileged users, establish trusted access and connect administrators and machines. However, most organizations are unaware of how widely SSH keys are used and that they provide the highest level of rights and privileges to critical systems and data.

SSH is used for secure administrative access, but what happens if it's not secure? Despite the sweeping access SSH keys grant, including root access, most are not as tightly controlled as their level of privilege requires. If your organization doesn't know which administrators or SSH keys have access to which servers, your IT environment may already be at risk.

SSH Mismanagement

Think about the stringent security controls your organization applies to usernames and passwords, and then compare this with how SSH keys are managed in your organization. Big difference? There is in most organizations.

Just as usernames and passwords authenticate and control user access, SSH keys provide a similar function for machines. SSH keys secure and automate administrator-to-machine and machine-to-machine access to critical business functions. Even though SSH keys provide the highest levels of privileged access, they are routinely untracked, unmanaged and unmonitored.

SSH Security Risks

SSH keys enable ongoing automatic connections from one system to another, without requiring a password. The systems typically secured by SSH include application servers, routers, firewalls, virtual machines and cloud instances, as well as many other devices and systems. Each key creates persistent trust relationships between these systems. Cyber criminals want this trusted status and invest considerable resources into acquiring SSH keys so they can use them in their attacks.

The following risks are created when SSH keys are not properly managed:

- **Can't control unauthorized account access.** With thousands or even millions of untracked SSH keys in enterprises, cyber criminals have a broad attack surface to exploit.
- **Can't revoke past employee privileges.** When left unmonitored, SSH keys can be used by current or terminated employees who either maliciously or innocently walk out the door with them. This gives them ongoing privileged access to the network.
- **Can't detect pivoting.** Once cyber criminals have access to a compromised SSH key, the persistent SSH trust relationships between systems enable them to rapidly jump, or pivot, from system to system. The more SSH keys that organizations have without oversight and review, the more extensive the risk.

- **Can't rely on the effectiveness of security controls.** Lax SSH controls, including poor control of authorized keys file or SSH server configurations, can be used to bypass firewalls and other security mechanisms.
- **Can't prevent unauthorized creation of SSH Servers.** Since SSH implementations like OpenSSH are freely available, users can enable SSH services on systems that haven't previously been SSH enabled, opening those systems to remote attack.

4 Steps to SSH Security

Sound security, policy and auditing practices for SSH keys are required to secure SSH environments. The following four steps will help secure your organization's SSH usage:

1. **Build a comprehensive inventory.** For SSH visibility and control across the network, organizations need centralized visibility into all SSH servers, private keys (the authorized keys that grant SSH access) and any SSH configurations that limit access.
2. **Identify vulnerabilities.** To reduce the risk of breach and compromise, organizations must be able to analyze their SSH key inventory to identify which SSH keys and servers are vulnerable. Effective detection of and response to anomalous use of SSH keys is only possible with automated alerts and notifications.
3. **Remediate.** Once vulnerabilities are identified, they must be fixed quickly to prevent ongoing exposure to a potential breach. To reduce risk, organizations need automated responses to SSH issues, including removal of unauthorized keys, rotation/replacement of weak and old keys, removal of SSH root access, removal of duplicate private keys and enforcement of security controls that limit the accessibility and use of SSH keys.
4. **Monitor.** To meet ongoing security and compliance requirements, SSH keys must have continuous, automated monitoring and tracking. SSH audits should regularly review SSH entitlements, assess risk, avoid compliance violations and increase accountability for identity and access management.

Secure Trust by Protecting Your SSH Keys

SSH key risk is one of the biggest yet least understood risks in enterprise environments. Venafi delivers complete, enterprise-wide visibility into SSH key inventories and automates the entire SSH key life cycle. This ensures consistent policy enforcement, timely incident response and centralized tracking of SSH changes. With Venafi, you can secure and control all SSH keys to minimize the risk of unauthorized access to your critical systems.

Trusted by

5 OF THE 5 Top U.S. Health Insurers
5 OF THE 5 Top U.S. Airlines
3 OF THE 5 Top U.S. Retailers
3 OF THE 5 Top Accounting/Consulting Firms
4 OF THE 5 Top Payment Card Issuers
4 OF THE 5 Top U.S. Banks
4 OF THE 5 Top U.K. Banks
4 OF THE 5 Top S. African Banks
4 OF THE 5 Top AU Banks

Venafi is the cybersecurity market leader in machine identity management, 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 venafi.com**