Venafi

How Safe Are Your SSH Keys?

Is your organization exposed to an attack that misuses SSH keys?

Are you vulnerable to an SSH compromise?

You know that your organization is using SSH to safeguard privileged access. But you may not realize that your SSH keys could be vulnerable to insider and cyber threats. The majority of those we surveyed didn't. Results from a 2017 study show that most organizations don't have the SSH visibility or security policies they need to secure their privileged access.

2

Is your SSH security better or worse than your peers?

3

Are you taking shortcuts with your privileged access?

Have you thought about what would happen if an attacker got access to one or more of your SSH keys? Despite the sweeping access they grant, most SSH keys are not as tightly controlled as their level of privilege requires. In most organizations, SSH keys are routinely untracked, unmanaged and unmonitored. An independent survey of over 400 IT and security professionals in the U.S, U.K and Germany, revealed that most organizations don't provide adequate protection for their SSH keys.

Does that make you wonder how well your organization is prepared to defend your SSH privileged access? Find out where your SSH security may fall short.

4

SSH grants sweeping access.
A compromise could be disastrous.

5

How big is your SSH attack surface?

Stop and think about all the systems in your organization that rely on SSH keys for privileged administrative access and secure machine-to-machine automation. You'll need to start by adding up application servers, routers, firewalls, virtual machines, cloud instances, and other devices and systems that leverage SSH. Like most large organizations, you're probably using SSH with 1,000 systems or more.

But that's not even the full scope of your SSH environment. Most of those systems can be accessed with multiple SSH keys. And those SSH keys do not expire, so if you don't enforce review and rotation policies, they accumulate over time. In very large enterprises, it's not uncommon to have a million SSH keys. If not properly protected, these keys could represent a million points of potential security breach.

6


Most organizations have more SSH keys than they realize.

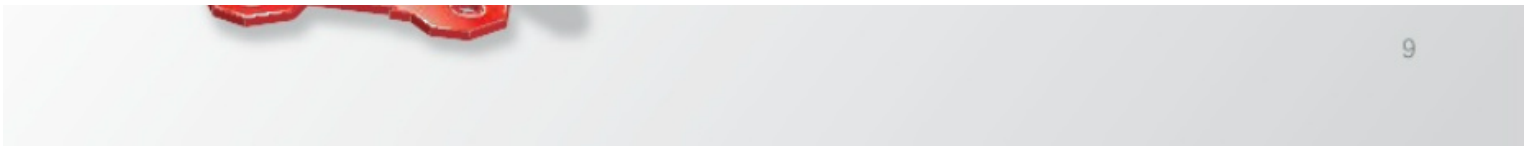
Are your SSH keys already compromised?

Do you know how many SSH keys your organization has, how many systems they can access, who uses them, and when they were last changed? If you're like most, you've allowed your system administrators to generate and manage their own SSH keys so you don't have insight into the SSH trust relationships that provide critical privileged access. That's probably why only 10% of those we surveyed said they have a complete and accurate SSH key inventory.

Given the lack of a proper inventory, security teams are hesitant to remove any SSH keys that enable access, even when administrators with access have been reassigned or are terminated. Security teams simply don't know which keys are being used by automated processes that will break if they are removed. The result? Your organization ends up with thousands of SSH keys that provide access to mission critical systems—all without reviews, rotations or policy enforcement. Do you know where your SSH keys are, how much access they provide, and who can use them?

8


Only 10% have a complete and
accurate SSH key inventory.


9

Are your SSH keys configured for security?

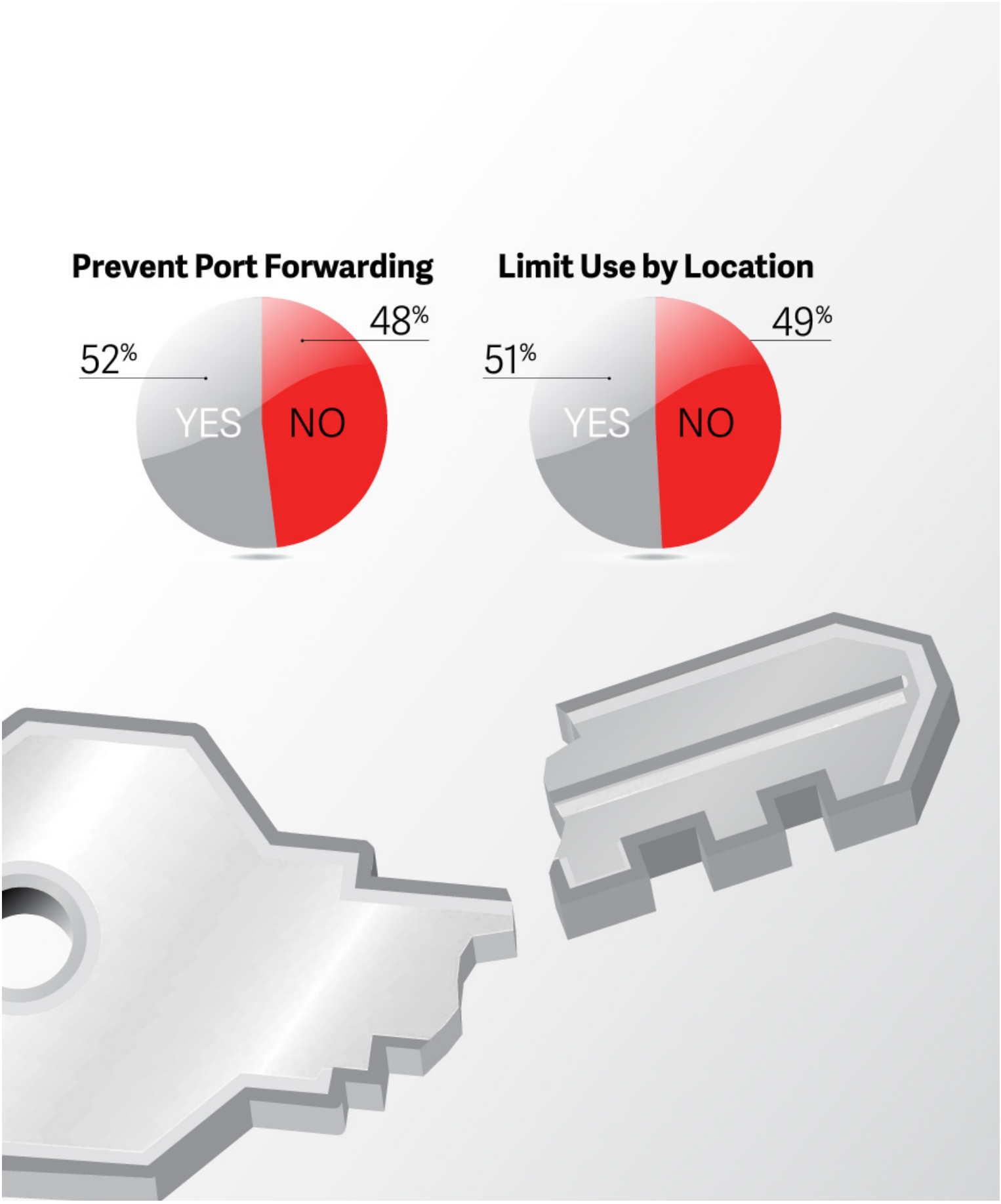
If you are not using secure configurations for your SSH environment, cyber criminals can exploit SSH to gain unauthorized access and pivot between systems. Let's say one of your administrators decides to enable port forwarding on an SSH connection that is approved to traverse through one of your firewalls. This administrative loophole can allow attackers to bypass firewalls. Yet close to half (48%) do not prevent port forwarding through proper SSH configuration.

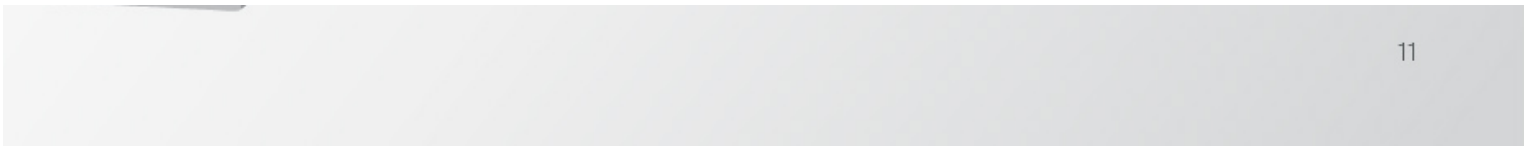
Organizations also fail to limit SSH key use by location. SSH configurations can restrict the locations from which each authorized SSH key can be used. When access is limited to the known locations of administrators and machine-to-machine access, it prevents malicious access from other locations. But again, close to half (49%) don't do this.

How secure are the SSH configurations in your organization?

Only about half limit port forwarding or SSH use by location.

10


Prevent Port Forwarding
48%
52%
YES
NO
Limit Use by Location
49%
51%
YES
NO


11

How often do you rotate SSH keys?

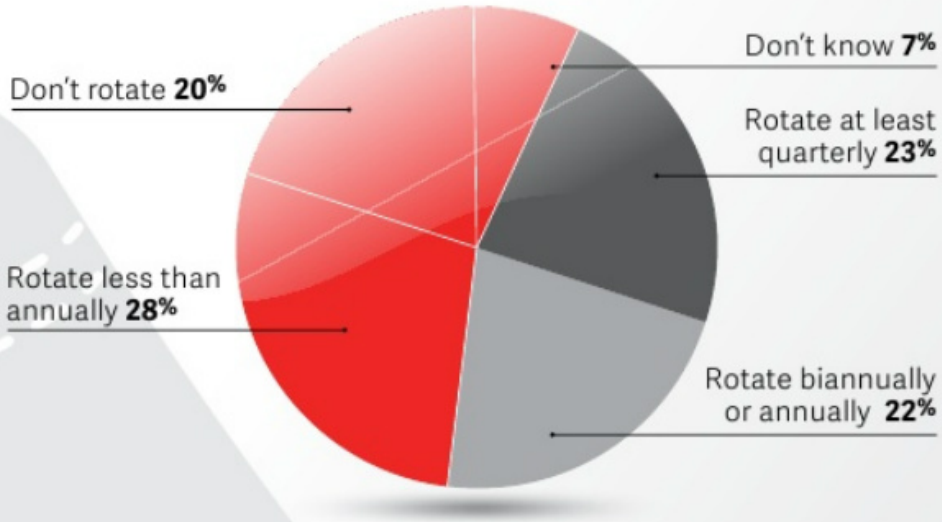
Would your organization allow users to keep the same password for a year or more? No chance, right? But many organizations do just that with SSH keys. Over 28% say they don't rotate their SSH keys every year and over 20% never rotate them at all.

Without proper rotation, your risk of SSH key compromise increases significantly because you're basically leaving users and administrators to their own devices with SSH. They can copy and share SSH keys to simplify administration across systems. And often keys are not removed after employees are terminated or reassigned.

The result is an unmanaged tangle of SSH trust relationships that leaves you vulnerable. If an SSH key is compromised and regular rotation is not enforced, your organization is at risk for repeated unauthorized access — indefinitely.

12

Frequency of SSH Key Rotation



Nearly 50% don't rotate SSH keys annually—or ever.


13

Do you know who is managing your SSH keys?

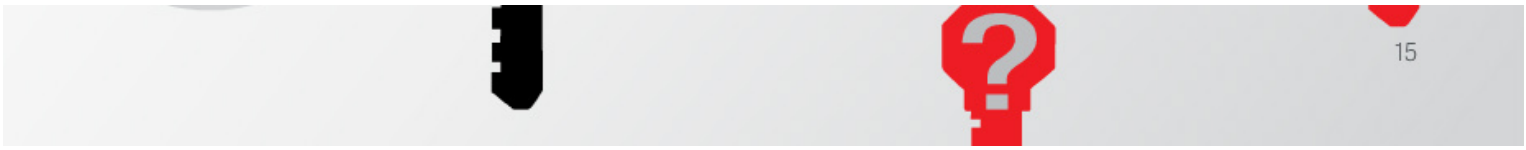
You've got to place a certain amount of trust in system administrators who manage systems. But the majority of organizations give system administrators carte blanche to manage SSH access with no oversight. Even though system administrators come and go on a regular basis, 59% allow most, if not all, of their administrators to manage the SSH keys for the systems they control.

Does your organization view SSH keys as simply an operational issue that can be self-managed by system administrators? If so, administrators who are self-policing their SSH keys are likely to leave them unprotected. After all, system administrators are not always security experts, and they are regularly reassigned or leave your organization.

If you don't have centralized management for your entire SSH environment, you have no way of determining the success of SSH policy enforcement. Can you detect when SSH keys are being used inappropriately?

14


59% let most administrators manage SSH keys for systems they control.


15

Who is allowed to configure SSH access?

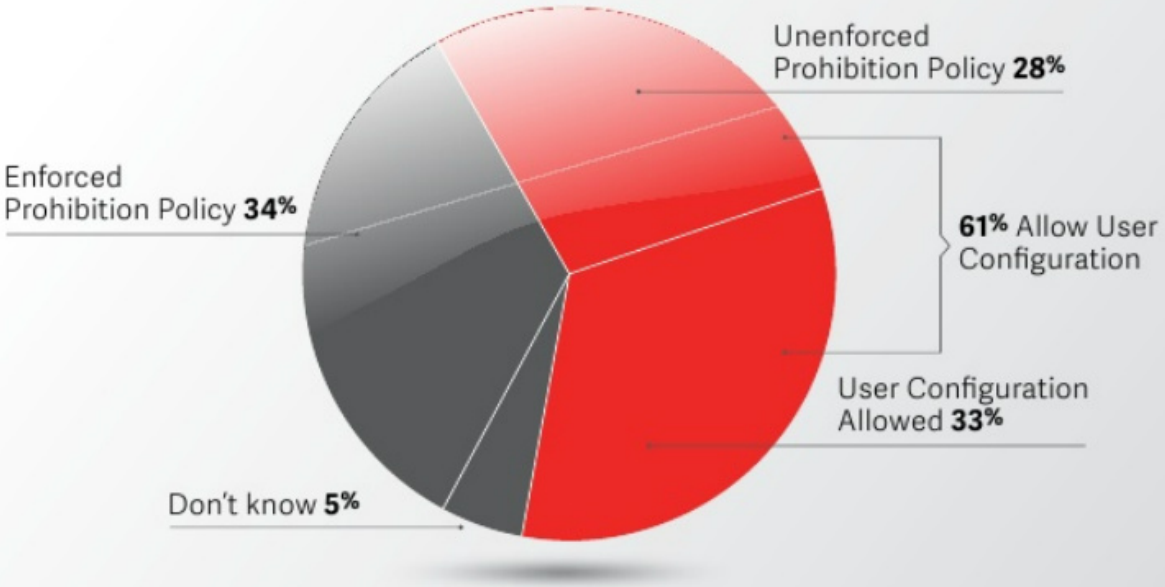
Organizations generally don't allow users to configure their own accounts. That being said, 61% of those surveyed allow SSH users to configure their own authorized keys—even though they grant privileged access. Often, this doesn't end well because, unlike their security counterparts, security is generally not a system user's first priority. When you trust high levels of privileged access to folks who may have to prioritize speed and efficiency over security, you end up with inconsistent security controls, or worse, a compromise of privileged systems or data.

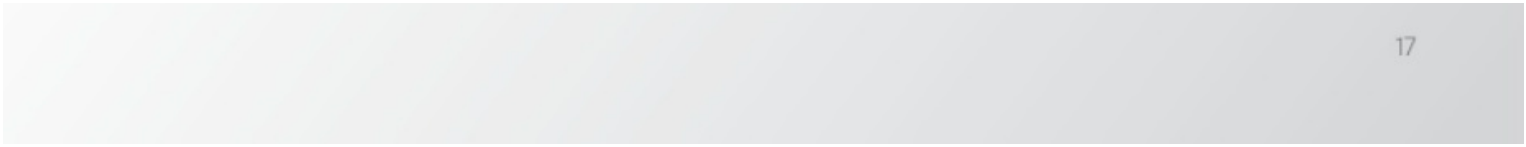
If your organization is like more than half of those we surveyed, your SSH environment would be more secure in the hands of your IT security team and a limited number of carefully monitored administrators.

61% let users configure their own authorized SSH keys.

16

User Configuration of Their Own Authorized SSH Keys




17

Is SSH becoming a security liability instead of an asset?

SSH is one of your most important security tools for securing privileged access. Plus, they are used widely by your system administrators. But don't forget that SSH keys are also used to secure automated machine-to-machine communications for sensitive business operations.

As administrators deploy SSH keys to enable automated processes, the number of trusted connections between systems continues to grow. In SSH environments that manage 5,000 or more systems, the use of SSH in automated applications and scripts increases threefold. Because this automated SSH usage often goes unmonitored, it inflates the SSH attack surface as well as the chances that an attacker who compromises one system can pivot to other systems by leveraging those trusted SSH connections.

How much does your organization rely on SSH in automated processes? If you're not sure, it's time to take a serious look at your SSH environment.

18


Enterprises with large SSH environments are 3X more likely to use SSH in automated processes.

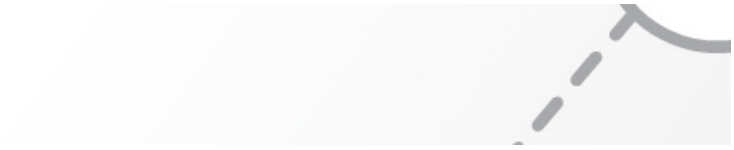
19

PAM won't fix your SSH problems.

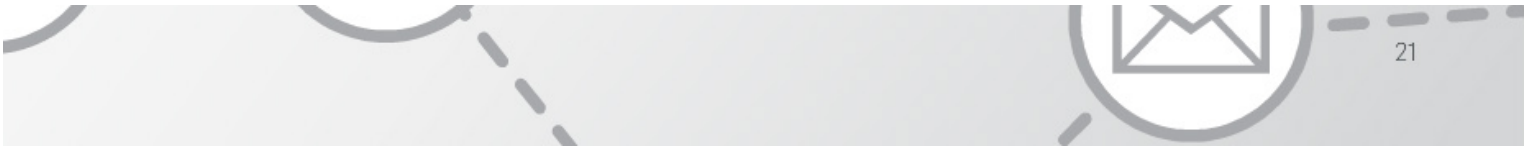
You may think that your privileged access management (PAM) systems will ensure proper oversight of SSH. In theory, that's true. However, PAM solutions don't help secure SSH keys used to automate machine-to-machine authentication for critical business functions.

Most security and audit programs overlook this important risk. In most cases, reviews of SSH entitlements are much less frequent than username and password reviews—47% only require system and application owners to review SSH entitlements annually, at most.

20




USER NAME
PASSWORD
47% require, at most, annual entitlement reviews.


21

Are your auditors asking the right questions about SSH?

An internal or external audit of SSH management practices can show you how vulnerable you are to SSH key theft and misuse—but only if audits are regular and comprehensive. Many executives rely on auditors to review security controls for their mission critical processes, but most auditors fail to review SSH. Only half of organizations reported their auditors conduct regular reviews of SSH entitlements and over a quarter said they don't audit any of the best practices surveyed.

The security and integrity of your SSH infrastructure is critical to protecting your organization's systems and data. However, if you're like most organizations, you may not have auditor oversight for this critical security infrastructure. And, even if you do, what would happen if your audit findings required remediation or other action? Are you prepared to act quickly?

Over a quarter do not apply any of the auditor best practices surveyed .

22


Auditing Practices
Review of entitlements
51%
Control of keys files
46%
Port forwarding policy
43%
Rotation and retirement
33%
None of these
27%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%


RULES
PRACTICES
NO AUDIT
ENTITLEMENTS
ACCESS
POLICY

What can you do to improve your SSH security right now?

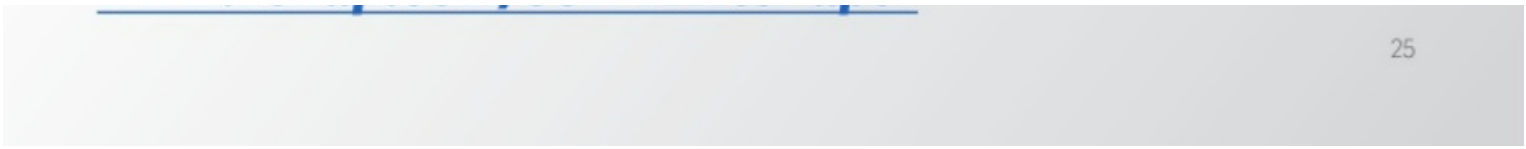
You never want vulnerable SSH keys to enable the compromise of your organization's most critical systems and data, or to enable attackers to rapidly jump between systems. But you're up against cyber criminals who will invest considerable resources to gain the trusted status established by SSH. You need to make sure they don't get yours.

As your business grows, so does your SSH environment. It's time to prioritize SSH management and security using a centralized, automated approach—you don't want a large number of untracked persistent SSH trust relationships that leave you at risk.

Make sure that SSH remains a security asset, not a liability.

24


Learn the top four actions you can take to improve your SSH security. Download our SSH security white paper.
www.venafi.com/SSH-WhitePaper


25

About the Study

Source: 2017 survey conducted by Dimensional Research

Respondents: 411 IT and security professionals with in-depth knowledge of SSH

Geography: Survey respondents from the United States, United Kingdom and Germany

Goal: Evaluate current SSH management and security practices

TRUSTED BY THE TOP

4 OF 5 Top U.S. Banks

4 OF 5 Top AU Banks

4 OF 5 Top U.K. Banks

4 OF 5 Top S. African Banks

5 OF 5 Top U.S. Health Insurers

5 OF 5 Top U.S. Airlines

4 OF 5 Top U.S. Retailers

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

Venafi

26