CIO STUDY

CIOs Massively Underestimate SSH Risks

300% growth in SSH malware targets organizations with weak SSH key management

Venafi

Why is SSH key management so critical now?

SSH is a critical security component of digital transformation. And in 2021, nearly every organization is in the process of adopting digital transformation strategies to achieve business-critical initiatives, such as migrating IT infrastructure to the cloud and developing and iterating apps and services using DevOps methodologies. Research and advisory firm Gartner notes in its *2019 Gartner CEO and Senior Business Executive Survey* that 82% of CEOs have a digital transformation or management initiative, up from 62% in 2018. And in its recently published *Hype Cycle for Identity and Access Management Technologies 2020*, Gartner points out: "For many enterprises, the global pandemic has compressed years-long strategic change into months, even weeks. For others, it has forced them to adopt approaches that they'd previously been cautious about."[1]

Trusted machine identities are critical to the success of digital transformation strategies. These strategies also require a massive increase in the number of machines—including devices, virtual machines, APIs, algorithms and containers—on enterprise networks that must be managed and protected. Many machines use SSH to ensure secure communications, but the resulting SSH machine identities are particularly difficult to manage and secure because SSH keys never expire and are rarely removed.

While CIOs are concerned about the security risks SSH machine identities pose, Venafi data indicates they seriously underestimate the scope of these risks. To better understand the scale of this problem, Venafi sponsored a study by market research firm Coleman Parkes that surveyed 550 CIOs from five countries: United States, United Kingdom, France, Germany and Australia. Venafi then compared the survey data with aggregate SSH risk assessments conducted over a two-year time period. These assessments evaluated an average of 4,500 hosts, more than 14 million SSH client keys and more than 3.3 million SSH host keys across multiple global organizations.

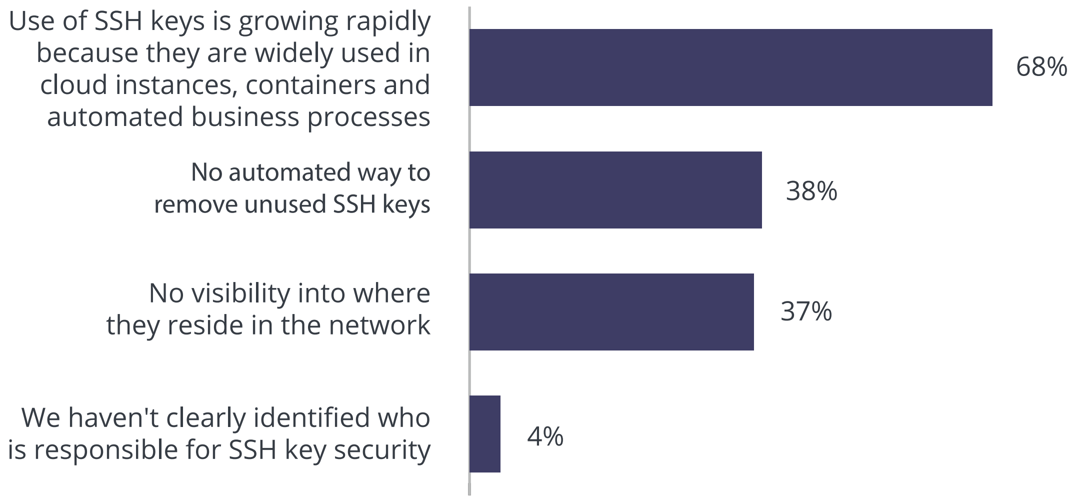
The key findings indicate that CIOs do not understand the scale or potential impact of the security risks connected with their SSH keys:

- 68% of CIOs admit that managing SSH will only become more difficult as digital transformation accelerates.
- 96% of CIOs say their policies require the removal of keys when employees are terminated or transferred, but 40% don't have automated ways to remove unused keys.
- According to Venafi Risk Assessments, enterprises have an average of more than 3,000 SSH shared private keys—a flagrant violation of best practices.
- These Risk Assessments also found that enterprises average more than 10,000 root access orphan keys that can act as permanent back doors for hackers and SSH malware.

86% of CIOs say they are actively managing SSH keys—but are those programs effective?

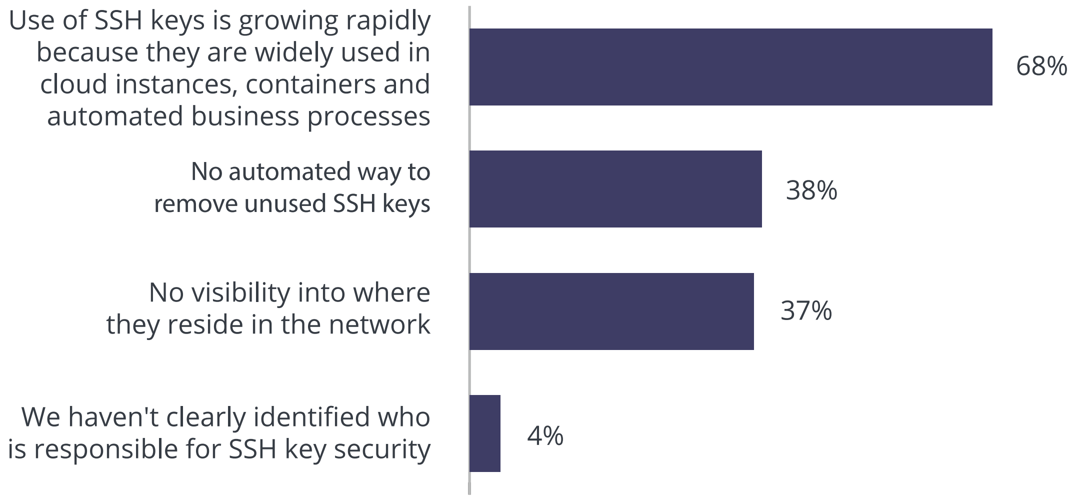
In the Coleman Parkes survey, 86% of CIO respondents say they actively manage SSH machine identities. However, it's debatable whether these management programs are effective. For one thing, the SSH protocol has been baked into application and enterprise frameworks for more than 20 years—and unlike SSL/TLS machine identities, SSH machine identities do not expire.

What makes the management of SSH keys difficult?



Moreover, most organizations lack the formal processes and technologies to remove SSH keys that are no longer needed. In fact, almost 40% of respondent CIOs say they do not have an automated way to remove unused SSH keys. This problem promises to grow more tortuous, something CIOs seem well aware of as SSH key populations continue to balloon.

What makes the management of SSH keys difficult?



Organizations have an average of half a million SSH keys.

The Venafi SSH Risk Assessments cited in this white paper examined a fraction of each organization's network. In each case, the network segment analyzed comprised, on average, 4,500 servers with nearly half a million SSH keys. This number of keys would be impossible to manage without an automated system in place to enforce policy—and the total amount of SSH keys across the entire network would be magnitudes higher in difficulty.

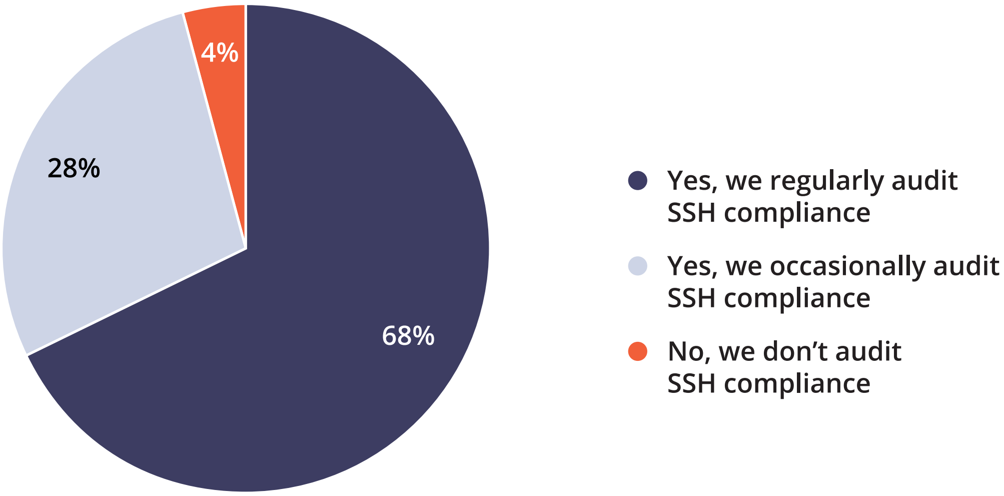
Kevin Jacque, the SSH global architect at Venafi who conducted Risk Assessments, says most organizations don't have any idea how many SSH keys they have—and that the final number often is off by as much as 100% from their original estimate. "Enterprises rarely have a handle on their SSH inventory because very few of them have complete visibility into that inventory," Jacque says.

There are several reasons that key sprawl is a universal condition. Here's a common scenario: When a new admin is added to the team, they may see old SSH keys. But because they have no insight into how those keys are being used, they don't remove them for fear of inadvertently disabling a machine or process that requires those keys. This same admin can easily generate their own keys—none of which ever expire—using the ssh-keygen command. "And if an admin is reassigned or terminated, it's unlikely their keys will be revoked for the same exact reason," explains Jacque. "Multiply this scenario over many years, and you can see why the population of SSH keys spirals out of control in nearly every organization."

68% of CIOs say they regularly audit SSH policies—what are they missing?

According to the Coleman Parkes study, 96% of CIO respondents say they audit against their SSH key management programs.

Does your organization audit against your SSH policy?



However, these audits clearly don't accurately assess the risks connected with improperly managed SSH keys.

Why SSH audits fail to accurately evaluate risk

More than 95% of all CIO respondents say their SSH key management program requires the removal of SSH keys whenever IT administrators change roles or are terminated. However, organizations without visibility and intelligence into the location and ownership of all employee keys can't verify their compliance with this policy.

If organizations can't enforce policies governing employee client key issuance, they will almost certainly find it impossible to secure SSH machine identities. To properly audit against appropriate key removal, organizations need to track ownership of keys and limit employees to one non-shareable SSH private key. This policy, properly enforced, would enable enterprises to easily revoke and remove keys when employees are terminated or reassigned. The organization would also be able to track the ownership of a specific key should an incident occur and limit potential damage.

An epidemic of duplicate and shared private SSH keys

Venafi's Risk Assessments show that enterprises have, on average, more than 10,000 duplicate private keys—slightly more than two per each server analyzed—and more than 3,000 shared private keys—or one per every two servers. According to Jacque, the number of duplicate private keys typically stems from ineffective or nonexistent policy regarding securing the location of the private key and not placing it in multiple locations. This lack of clear and specific policies cause employees to assume that their private keys are disposable, especially since they are so easy to generate.

While Jacque points out that, in many cases, duplicate private keys are benign, the prevalence of duplicate private keys increases the likelihood of any one of these keys being compromised, which in turn compromises all of the connections that can be done with this key.

Shared private keys, while similar to duplicate private keys, are, in fact, much worse. Instead of one user who has many private keys associated with them, a shared private key is a single key that multiple users share. A user may share their private key with a fellow employee so they can access a remote machine without having to use their own key for convenience. But this practice can easily get out of control, as there is no way to prevent additional users from gaining access to the same key. Jacque points out that his team found an individual shared private key spread across as many as 200 different servers—presenting an extremely attractive target for threat actors.

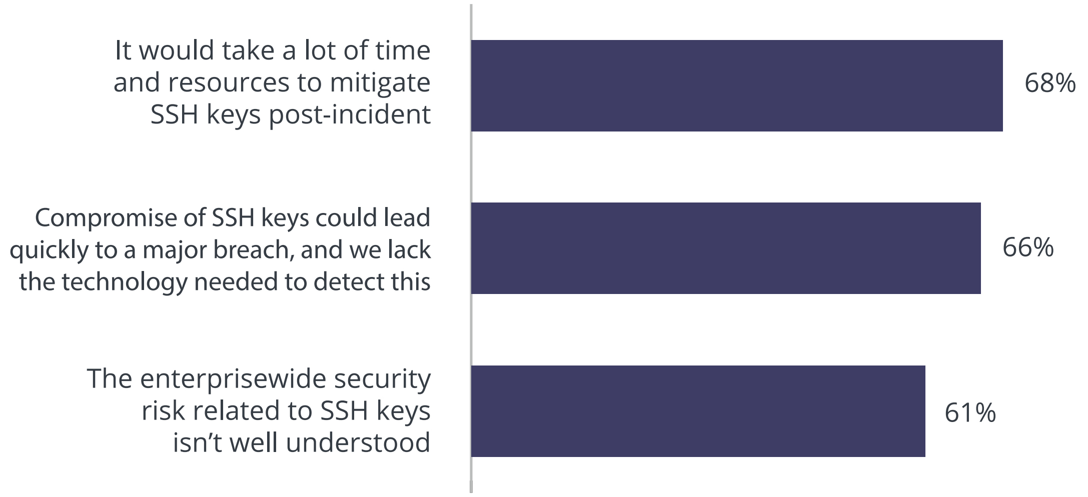
Shared private keys have been shown to be an ideal cover for malicious intent. Edward Snowden, who stole and leaked classified files from the NSA, coaxed 25 NSA employees into sharing the usernames and passwords associated with their SSH keys, telling them he needed them to do his job. Jacque says that Snowden likely leveraged these shared private keys to gain access to systems he otherwise wouldn't have had access to. "Once on these hosts, he would have been able to embed other SSH keys, giving him the ability to potentially elevate his privileges and move laterally throughout the network."

Given the seriousness of the risks connected to these practices, it's not surprising that CIOs are worried.

80% of CIOs are concerned about the security risks connected with SSH keys—justifiably

CIOs know the way they manage and protect SSH machine identities is problematic. The respondents in the Coleman Parkes study say they are concerned about the security of their SSH keys for several reasons:

Which SSH key management issues are you most concerned about?



However, CIOs are critically underestimating the security risks connected with their SSH key populations. Venafi Risk Assessments show that most organizations have severe SSH-based security problems that go beyond those connected with duplicate and shared private keys. Most of them also have a frightening number of root access keys and an even more worrisome number of root access orphan keys. Root access and root access orphan keys pose the greatest security risks for organizations because they can create persistent back doors into networks that can last for months—or even years.

According to Jacque, organizations often misuse root access keys to make access to remote devices easier. "While some applications require root access to function, the majority do not. The practice of using root access keys creates an unnecessary blind spot because activities logged during that session are simply logged as root. Moreover, with root permissions the individual could clear activity logs, making their presence untraceable. This becomes a major liability when an incident arises," Jacque says.

The dangers of unmanaged root access keys

According to Venafi Risk Assessments, enterprises have, on average, 11,000 root access keys—or 2.5 root access keys per server analyzed. Root access keys provide the highest levels of access to machines. If a threat actor gains access to root privileges, they can access anything on, say, a remote server—or multiple servers if it has been cloned, as often happens with virtual machines.

"The recommended best practice would be to disable root access in the `sshd_config`, forcing individuals to use their own keys to access a host and `sudo` to root for privilege escalation. All too often, this isn't the case. Admins trying to track down the root access key when it is widely granted in the environment is a nearly insurmountable task," Jacque says.

The inherent risks of root access orphan keys

Root access orphan keys, which give any user of that key unlimited privileges on a given box, pose one of the most dangerous SSH security risks that organizations face. Too often organizations lack awareness into the existence of this type of key to begin with. Moreover, the problem rarely is limited to a single root access orphan key, which is dangerous in and of itself. Venafi Risk Assessments have shown that enterprises have, on average, more than 7,000 root access orphan keys—or at least one root access orphan per every server analyzed. These 7,000 untraceable keys each can serve as permanent back doors for threat actors to exploit because they never expire.

Because these orphaned keys connect as root without a means to identify the individual behind them, root access orphan keys are perfect shields to hide malicious activity. When these orphans are discovered, InfoSec teams have no way to identify the responsible party that used the key, leaving them to wonder whether this connection is legitimate or malicious.

The scale and scope of security risks posed by weak SSH key governance is serious in its own right and also puts organizations at risk of audit failures. These risks become even greater when evaluated against a rising tide of threats.

Hackers routinely exploit critical vulnerabilities in weak SSH key management

Jacque points out that vulnerabilities caused by unmanaged SSH keys are a primary vector for cybercriminal activity. Because cybercriminals can hide their identities so easily using legitimate SSH keys, they increasingly are taking advantage of them. Ample evidence underscores these threats, with several publicized attacks capitalizing on these SSH-based vulnerabilities.

For example, the recent SaltStack vulnerability allowed cyberattackers to take advantage of SaltStack's open source Salt framework to configure, manage and monitor servers in data centers and cloud environments.[2] The SaltStack vulnerability enabled attackers to take over servers and exfiltrate all sensitive information on them, including vulnerable SSH keys that were not managed or password protected. An array of sites, applications and servers have been affected by the attack. Among them were the CA DigiCert and the technology giant Cisco, which had to shut down their servers until the incident was contained.

Yana Blachman, principal threat intelligence analyst at Venafi, explains that once attackers exploited this vulnerability, they were able to take full remote control over vulnerable servers and move to other connected machines over SSH by compromising the SSH keys on these servers. "Due to the interconnectivity of the servers and the reliance on SSH for remote connection, exfiltrated SSH keys also enabled the attackers to expand their attack and move to other machines—which is why SaltStack called all users to change their keys," says Blachman. "It was the only way to block the attackers' access to the affected servers."

Without an accurate inventory of SSH keys, trying to change the SSH keys vulnerable to an attack like SaltStack would be a problematic and time-consuming task, Jacque adds.

Commoditized SSH malware preys on weak SSH key management

In addition to taking advantage of security risks posed by weak or poorly managed SSH keys, threat actors are increasingly making use of malware that exploits weaknesses in SSH key management. Given that a single vulnerable SSH key can provide multiple opportunities for attackers, the fact that organizations may have half a million or more improperly managed SSH keys leaves them open to a large and poorly understood attack surface.

In fact, SSH-based capabilities that used to be limited to sophisticated criminal organizations and nation-state actors are continually becoming commoditized—compounding existing SSH security risks. And because SSH is the machine identity used in Linux and other Unix flavors—the preferred operating systems in the cloud—threat actors know their chances of exploiting these weaknesses have a high probability of success.[3] According to the Venafi Threat Intelligence team, the use of malware exploiting poorly managed machine identities went up 300% between 2015 and 2019, growing 100% between 2018 and 2019 alone.

This trend continues to accelerate with the rise of commoditized malware over the last two years. More and more malware that can be purchased on the dark web, often under the guise of "malware-as-a-service," offer SSH capabilities that can exploit the many weaknesses in SSH machine identity management. Crimeware and malware-as-a-service in underground markets enhances the reach of prolific and commodity malware and lowers the barriers for those interested in engaging in cybercrime or cyberattacks.

One of the most prevalent malware-as-a-service in 2020 is TrickBot, a universal crimeware solution that targets enterprise environments. TrickBot uses a modular structure that lets its authors rent parts of the malware to others for specific malicious activities. In 2019, TrickBot added SSH key-grabbing capabilities for Microsoft SSH client PuTTY and OpenSSH. In addition to causing damage through its software, TrickBot also supplies cybercriminals with access to ready networks of devices already infected with it.

Other advanced botnets, such as Lemon_Duck and FritzFrog, have evolved in the past year targeting mostly cloud applications and Linux servers. Both rely on SSH for their proliferation and lateral movement across the network, acting like "worms." As organizations accelerate their digital transformation plans in response to the global pandemic, infiltration through weak or improperly managed SSH keys has become more lucrative than ever before.[4]

Why CIOs need better SSH machine identity management

While CIOs clearly understand the importance of securing their SSH machine identities, they seriously underestimate the scope of the risks associated with poorly managed SSH keys. The growing disconnect between policy and practice is evident from the number of duplicate shared keys, as well as the volume of SSH root access and root access orphan keys on their networks.

The clear misalignment between CIOs' views of their SSH key management programs and the state of their SSH key populations illustrate that most organizations lack the capabilities they need to make their SSH machine identity management programs effective. They lack visibility into their complete SSH key inventory, have no means to obtain the continuous intelligence necessary to understand and mitigate risks related to existing SSH key setups, cannot monitor usage for anomalies, or achieve compliance with risk management standards and frameworks. Moreover, they lack the automation needed to streamline and secure SSH key lifecycles and respond quickly to imminent threat events that may impact business-critical assets.

For most organizations, these gaps in SSH key management will continue to grow as organizations move more workloads to the cloud where SSH keys are used for many routine tasks. These issues also routinely crop up in security audits.

What can organizations do to take control of their SSH keys? Here are some best practices, all of which require a comprehensive SSH machine identity management solution that provides full visibility and leverages automation to manage and enforce policies:

- Discover all SSH machine identities in the environment—and make this discovery a continuous process to ensure complete SSH inventory—using automation.
- Determine the ownership and use cases for each SSH key with the help of automation.
- Map all trust relationships to identify and remove any orphaned, shared or duplicate keys, using automation.
- Control SSH identities and authorized keys with the help of automation.
- Control SSH configuration files and known hosts files using automated processes to prevent any tampering.
- Automate the enforcement of clearly defined SSH key management policies and audit against them.

In particular, automating full lifecycle machine identity management is critically important for SSH machine identities, especially given that they don't expire. Venafi Trust Protection Platform currently is the only commercial enterprise solution on the market that provides a full lifecycle machine identity management platform for all machine identity types—even in large, complex networks. It does this by providing visibility into SSH keys and intelligence into vulnerabilities and threat risks around those keys, and by automating the key lifecycles across business-critical systems.

If your enterprise organization needs help gaining control over your SSH key population—or you're otherwise interested in learning how Venafi has helped hundreds of the world's most security-conscious organizations build effective machine identity management programs, contact us at **venafi.com**.

References

1. Ant Allan. Hype Cycle for Identity and Access Management Technologies, 2020. Gartner. July 16, 2020. 1-2
2. Zorz, Zeljka. SaltStack Salt vulnerabilities actively exploited by attackers, patch ASAP! Help Net Security. May 4, 2020.
3. Blachman, Yana. Attacks on Linux Servers in the Cloud—The Rise of SSH-Abusing Malware. Venafi Blog. August 26, 2020.
4. Hernández, Luciano. What Is TrickBot? F-Secure. November 20, 2019.

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**