Can Your SSH Key Management Program Pass an Audit?

Ask yourself these questions.

Venafi

Introduction: Is your SSH machine identity management program truly ready for your next audit?

Nobody enjoys audits, but they are the primary way to measure the success of your security programs. The rise of digital transformation, with its many cloud-based initiatives, has led to an explosion of SSH machine identities—and with that rise, an increased potential for risk. InfoSec experts are growing concerned about the many risks that can arise from improperly managed SSH keys.

In particular, malware engineered to exploit weaknesses in SSH key management has grown dramatically over the past several years, and much of that malware has been commoditized so that even cybercriminals with minimal technical skill can use it to attack your network. TrickBot, a universal crimeware solution designed to target enterprise environments, uses a modular structure that enables users to rent SSH key-grabbing capabilities for Microsoft SSH client PuTTY and OpenSSH, as well as supply them with access to read 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.” And in early 2021 a flood of new malware, such as Kobalos, Hildegard and Pro-Ocean are targeting SSH machine identities to infiltrate systems.

Because the security risks connected with SSH continue to rise—and with it, the potential for misuse or compromise of SSH keys—regulated industries, including financial services, healthcare and government, must implement SSH security controls and maintain compliance with regulations. PCI-DSS, HIPAA/HITRUST and FISMA are just a few of the many standards bodies that require companies to perform regular audits of their SSH key management program to prove compliance. And given the unprecedented rise in the attack surface, these bodies are paying attention to audits more than ever before.

While some organizations have SSH policies and key management programs in place, many still don’t. And the ones that do have them in place often discover—through failed security audits—that they aren’t being enforced. If you’re uncertain about the results of a recent security audit or have failed the SSH portion of your audits in the past, this eBook can help you get on the right track. Ask yourself the questions below to strengthen the security of your SSH machine identity management program—and make sure your organization’s SSH security posture is audit-ready.

000GST010100010HGH10101000PK5757VK18101001010001

Question 1:
Do you have an accurate inventory of your entire population of SSH keys across your enterprise?

An accurate inventory of your entire population of SSH keys across your enterprise is a nonnegotiable precursor to having any sort of enforceable policy. Put bluntly, it's useless to have SSH key management policies in place if you can't enforce them—and without complete visibility into your SSH key population, you won't be able to.

If you're overwhelmed with SSH key sprawl, you're not alone. It's a common enterprise problem because SSH keys don't expire and people are reluctant to remove them from networks when they don't know what will stop working if they do. So, when administrators find unknown keys on a network, they usually leave them alone because they don't want to risk inadvertently disabling a remote server that may need those keys to run a business-critical application.

2840.09
2250.35
6169.06
374.97
3643.93
5201.20
4178.29
2472.89
3039.11
8716.78
8784.90
312.40
4864.89
8227.89
6165.08

But not knowing about the number of keys on your network or what users and processes they're associated with, puts your organization at even greater risk. You need a complete and accurate inventory of your entire SSH key population. This inventory should include every key across your enterprise, how they are being used and what they are controlling. So, if you find orphaned keys that can't be mapped to its matching key pair, it needs to be investigated and possibly removed so that you don't leave your organization open to unnecessary risk and compromise.

The problem is that most organizations don't have the necessary technology to find all the SSH keys on their networks, let alone create an accurate inventory of these keys. Having an accurate inventory, however, helps to ensure you pass your audit.

Are you sure you have a complete inventory of your SSH key population?

Question 2:
Are you continuously monitoring your SSH key inventory?

It isn't enough to create a one-time or annual inventory of your SSH keys. You must also continuously monitor your environment for new keys, as well as for keys that are no longer in use or are being used in noncompliant ways. This has become much more important as organizations shift their infrastructures to the cloud because cloud migration, along with other digital transformation initiatives, are driving the explosive growth of SSH keys.

You need this intelligence to respond quickly to changes that create risk by taking the appropriate steps to remove or restrict access. Moreover, this intelligence gives you the ability to prioritize actions based on risk profiles, as well as provide you with a roadmap of next steps. Continuous monitoring gives you the capability to dynamically respond to changes and produce evidence for auditors to support it.

Do you perform real-time, continuous monitoring of your SSH key inventory?

Question 3: Do you have a policy that requires the rotation of SSH keys that are out of compliance?

Unlike SSL/TLS certificates, SSH keys never expire. In the same way that TLS machine identities and human identities are rotated on a schedule, SSH machine identities need to be rotated regularly to minimize the risks that can occur if these keys are left on your network indefinitely. Without regular rotation, your risk of SSH key compromise increases significantly. Administrators and other users may not be as aware of the security risks posed by SSH keys as you are, and putting trust in them to always do the right thing is risky. Rotation removes or replaces keys that are out of compliance, including those that have been shared or copied, as well as those that don't meet the policy set by your organization. It also removes the risk of a terminated employee maintaining access long after they've left the company.

226.34
698.11
698.11

If an SSH key is compromised and regular rotation is not enforced, your organization is at risk for repeated unauthorized access—potentially for years. And if like many organizations, you are dealing with SSH key sprawl, that risk of unauthorized access goes up exponentially. Although your key governance should also limit creation and usage of SSH keys, the sheer number of keys already on your system or being created as a result of digital transformation initiatives, means that rotation is a fundamental policy your organization must have to minimize SSH key security risks. Automated rotation is the easiest and best way to ensure that SSH keys are rotated on a schedule—and no keys are missed.

Do you have a comprehensive and automated SSH key rotation policy that is audit-ready?

Question 4: Does your SSH key governance limit creation and usage of SSH keys using specific controls?

You need specific SSH key governance policies in place to limit who can create SSH keys and restrict the parameters around configuration of these keys. When creating new SSH keys, users should follow a specific workflow to ensure that all created keys adhere to allowable key lengths, formats and algorithms. If a user doesn't follow this workflow and, for example, creates a new key using the ssh-keygen command (an easy way to create new keys), your policy should require that these keys are automatically removed.

Similarly, your policies should include restrictions that limit where 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. In other words, if an administrator works in Dallas, and their key is being used from a Russian IP address, your policies specify that their key can't access your network.

Do your SSH key governance policies have these controls in place? If not, you'll need to establish these controls in order to guide policy implementation.

Question 5: Do you have a policy in place that requires SSH keys associated with an employee are immediately revoked once they are terminated or reassigned?

When an employee is terminated, you immediately cut off their access to email, applications and services. Their passwords stop working, and even the key card enabling them to enter your office building becomes just another piece of plastic.

Organizations should have a policy in place that requires any SSH key associated with a reassigned or terminated employee be immediately revoked. Surprisingly, however, many organizations don't have this policy in place—and if they do, it's hard to enforce without an accurate inventory of their SSH key population. When organizations fail to take the necessary action to remove these keys, they are unnecessarily accepting the risk of a terminated employee accessing their network or worse, one of the keys being compromised.

Does your SSH key governance policies include immediate, automated revocation of the SSH keys of a terminated or reassigned employee? If you don't have such a policy in place, as well as automated enforcement of it, you definitely will not pass your audit.

Question 6: Does your SSH key governance include policy on how SSH keys must be stored?

SSH private keys provide the highest level of privileged access to critical systems. They can access your mission-critical apps and private customer data, among other things. So, like real-world keys, they shouldn't be left on a desktop where they could be stolen, shared via email or absconded with on a thumb drive by the guy who quit the company last week. Proper storage of keys is such a basic security policy that paradoxically, you might have forgotten to have an explicit policy in place spelling out how they must be stored.

But if you want to pass your audit per NIST standards and your industry's regulatory framework, you must have a detailed written policy that states that all SSH keys must be stored in a key vault or centralized repository designated for this purpose—and nowhere else. If you do not have this policy in place, you leave your organization vulnerable to easily preventable risk.

Does your SSH machine identity management program specify and enforce how SSH keys are stored?

Question 7: Do you have automated centralized management of all your SSH keys?

Many organizations still rely on individual IT administrators to oversee how the SSH keys that individuals need are issued and used. But this poses an inherent threat to these organizations, particularly in large organizations with millions of SSH keys. Humans don't always follow policies. Sometimes they take shortcuts or make mistakes, which can undermine privileged access policies you have in place. Because IT admins focus on keeping things running, they aren't always incented to follow SSH key policies—particularly in an emergency when SSH is the fastest way to gain access to an asset, application or service.

Instead, you need centralized management of your SSH keys. Centralized management provides you with clear visibility of all your keys and the ways they're being used, even on fast-changing dynamic networks. In addition, it lets you prioritize and then proactively respond to any policy violations that could cause potential security risks. And the combination of centralized management and continuous monitoring is essential to providing enterprisewide audit evidence of SSH key compliance and remediation.

Are your SSH keys manually managed or in silos—or have you centralized and automated their management?

Conclusion:
Want to reduce your threat attack surface and minimize misuse and compromise? Proactively prepare for the SSH portion of your security audit.

The goal of any security audit that measures your SSH key management policies is to measure the level of protection they provide. If you fail the SSH portion of your audit, chances are that your enterprise is vulnerable to a host of risks, including the types of malware just described.

Because cybercriminals have discovered how relatively easy it is to infiltrate networks via improperly managed SSH keys, the development of malware targeting this fairly common vulnerability has accelerated dramatically. To make matters more alarming, this malware is increasingly being commoditized and easier for enterprising threat actors to deploy than ever before.

As these threats accelerate, your organization becomes more vulnerable to potential SSH misuse and compromise. You need three things to counteract these threats:

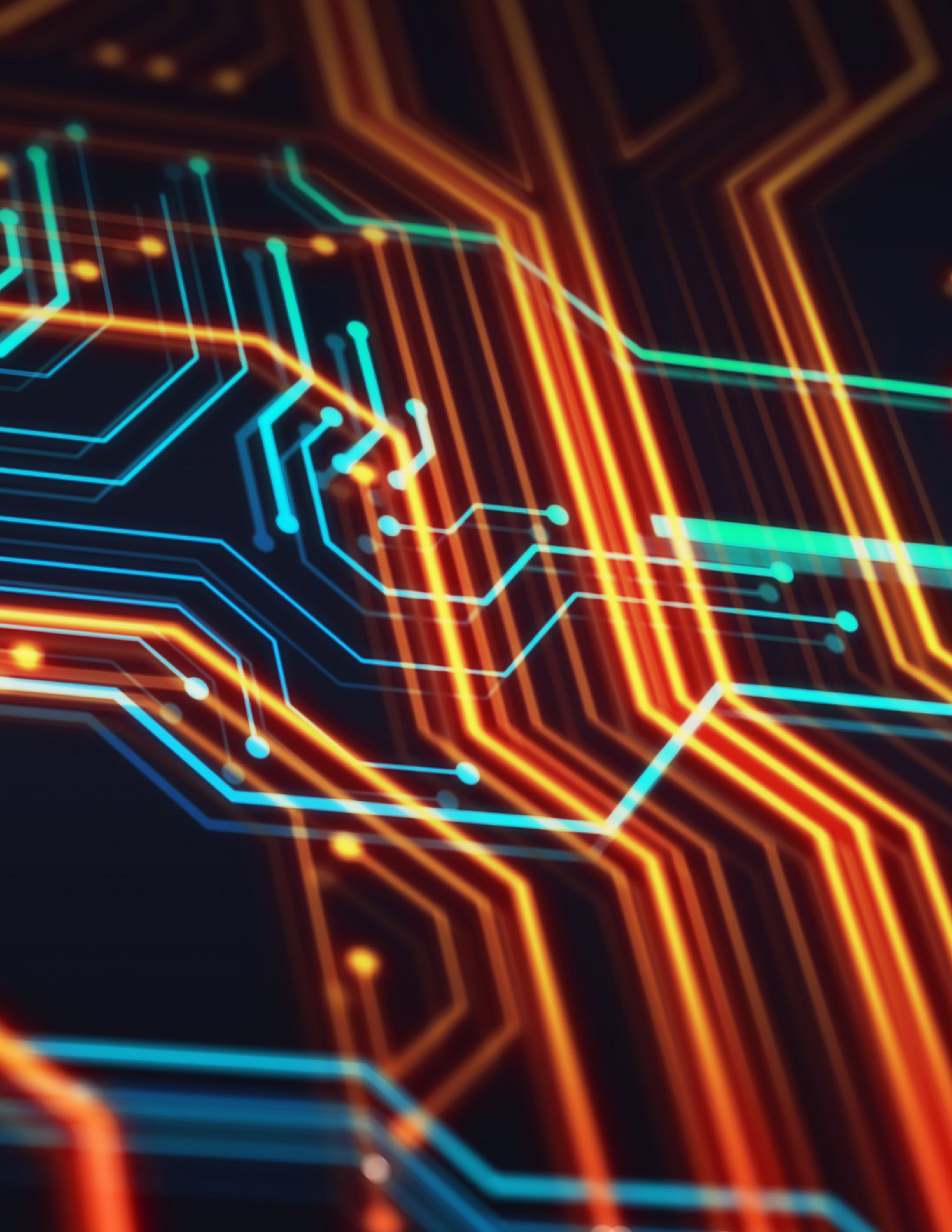
- Visibility into your entire SSH key population in real time
- Actionable intelligence on how your SSH keys are being used so you can spot anomalies and identify risky behaviors
- Enforcement of your SSH key management policies using automation

Only then can you ensure that your organization is safe from SSH malware and other vulnerabilities. And the added bonus of having these three things? You will pass the SSH portion of your audit!

Make sure your SSH keys are secure and in compliance so you're ready for the next audit.

Do you know how many SSH keys are floating around your organization? Do you have actionable intelligence that tells you how these keys are being used and where they are on your network? Many large organizations are shocked to learn they have tens of thousands of orphaned or unknown SSH keys.

Want to get a handle on your SSH population?
Sign up for a free, confidential Venafi SSH Risk Assessment:
venafi.com/ssh/risk-assessment



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**