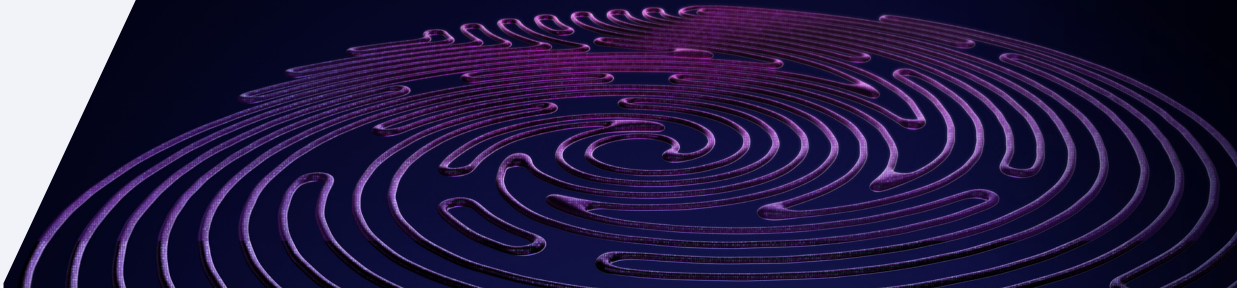

SOLUTION BRIEF

Preventing Audit Failures Due to SSH Risks

Common causes of audit failures and how to eliminate them

Who should read this:
System administrators and InfoSec teams responsible for preparing systems for audit

Secure Shell (SSH) is a cryptographic network protocol that gives users, particularly system administrators, a secure way to access machines over an unsecured network. SSH provides strong authentication and encrypted data communications between two machines connecting over an open network such as the internet.

Because of its prevalence and adaptability to multiple environments, system administrators and InfoSec teams increasingly are using SSH to safeguard administrative access and automated processes for their organizations. They rely on SSH as an encrypted protocol to authenticate privileged users, establish trusted access and connect administrators and machines. However, even though SSH keys can grant root access and privileges to critical systems and data, most organizations do not know how widely SSH keys are used. Many organizations learn too late that they have hundreds of thousands of SSH private keys they were previously unaware of, and most of these keys are not as tightly controlled as their level of privilege requires.

If your organization doesn't have visibility and controls established to manage SSH keys, your IT environment may already be at risk—and an audit failure could be in your future.

Potential Risks of a Failed SSH Audit

As regulations and standards evolve to include SSH key risks, many security teams have been caught by surprise when they fail the SSH portion of regular audits. Typical consequences of a failed audit include:

- **Monetary Penalties and Fines:** Governing bodies like the Office for Civil Rights (OCR) can enforce privacy and security regulations by fining an individual business for failing an audit. Additionally, industry consortiums, such as the PCI Security Standards Council, provide agreed upon standards that members must follow to remain in compliance. Those that fail to adhere to these standards risk monetary fines that can vary anywhere from $5,000 to $100,000 per month.
- **Organizational and Brand Reputation:** When an audit failure hits the news, it can tarnish an organization's reputation—shaking customer confidence and opening doors for competition.
- **Cost to Recover:** Once an audit has failed, it may take a lot of time and effort to clean up the key sprawl and put auditable controls in place. And because many organizations often find that they have 5 to 10 times more keys than anticipated, they may need to spend months and a dozen full-time equivalents (FTE) to build a reasonable SSH key governance program.

Because of the security threats and operational risks connected with poorly managed SSH keys, auditors are becoming increasingly focused on those risks and the visibility and management of SSH keys.

Common Causes of SSH Audit Failures

To avoid SSH audit failures, organizations first need to understand what causes them. SSH audit failures typically stem from four different problems or a combination of these causes:

Lack of Global SSH Visibility: Organizations need centralized visibility into all SSH servers, private keys and any SSH configurations that limit access. Without this visibility, cybercriminals have a broad attack surface to exploit thousands or even millions of untracked SSH keys in enterprises.

Lack of Insight into Global SSH Keys: Lack of insight and intelligence into ownership of keys, as well as orphaned, shared, weak or root keys, can lead to unauthorized access—and should be reported immediately for review and corrective action. Enterprises must also be able to identify out-of-policy SSH practices like cross-environment key usage, improper key lengths or aged keys. Monitoring these SSH risk practices, as well as the enterprise-specific policies and actionable alerts for policy failures, are essential to effective SSH key oversight.

Lack of SSH Policies: Although most organizations enforce stringent security controls to protect usernames and passwords, they typically have few, if any, policies in place to protect their SSH machine identities.

Manual Processes: Most organizations rely on manual processes to manage SSH keys. To reduce risk, organizations need automation to resolve 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.

6 Steps to Check If Your Organization Is Ready for Your Next SSH Audit

Rather than wait for an auditor to check on the health of your organization's SSH practices, you can be proactive about securing your SSH keys.

The checklist below will help gauge the likely outcome of your next SSH audit. If you're lacking one or more of these controls to secure your SSH keys, the chance of passing your next SSH audit may be small.

1. **Put a comprehensive SSH governance program in place:** Enterprise security for SSH keys starts with solid policies and procedures documented by risk managers and executed by InfoSec teams. Before implementing these controls, risk and InfoSec leaders should first check on the status of any existing SSH policies. For instance, does your organization have standards for SSH key length, access control levels, key passphrases or authorized key usage? If so, have these standards been fully documented and communicated to all of your IT and development teams?
2. **Establish effective SSH key authorization and management:** Once appropriate policies, procedures and SSH risk mitigation are in place, organizations need to begin the process of organizing and getting insights on how well various teams have adopted and implemented them. An essential component of this process is a comprehensive baseline inventory that documents all approved authorized keys and how they are used including the details of the trust relationships and the rationale for each key. Auditors may request this information when they validate SSH key management. Auditors typically ask questions like: Who requested this key? Who approved the key? Why is this key needed? How is this key used? Are any usage restrictions in place?
3. **Evaluate vulnerable SSH protocols and weak SSH configuration settings:** The SSH protocol is multifaceted and encompasses many functions, including Secure Copy Protocol (SCP) and Secure File Transfer Protocol (SFTP), which have been adopted by a wide variety of automation tools. Over time, SSH also expanded its encryption algorithms with cyphers like 3DES or AES. Support for public key certificates was added in SSHv2. As vulnerabilities start to spike, especially for older unsupported versions like SSHv1, and support is no longer guaranteed, InfoSec teams now have to deal with many configuration variants and ensure exploitable deployments are rooted out. As a result, risk and InfoSec leaders need to make sure that this is happening and be able to provide evidence for auditors in the form of appropriate configurations and corrective actions taken by InfoSec teams.
4. **Automate SSH key generation, rotation and removal:** Key management often happens via standard command line interface (CLI) with Linux commands; however, that makes it prone to human error. A common mistake across IT admin communities is that keys are not deleted. Although removing keys only requires a simple "rm" command, skipping or deleting the wrong keys can have major impacts. Standards bodies such as ISACA or National Institute of Standards and Technology (NIST) recommend using automated processes and tools to assist users with generating, deploying and managing SSH keys. Not only will the deployment of automated tools make SSH key management less error-prone, SSH audit programs from ISACA, published September 2017, check for this capability.
5. **Establish ongoing monitoring SSH key usage:** Preventing rogue users or malware from installing unauthorized SSH keys, especially those with privileged access, can be difficult. One way to find unauthorized keys is by monitoring all SSH connections using logging procedures and comparing real-life artifacts against known authorized connections. This process, combined with periodic review of all SSH key-based trust relationships and audit of privileged accounts, will help keep IT and InfoSec teams informed and auditors satisfied that the security risks connected with rogue keys and hard-to-manage risks are being addressed.

6. **Build an SSH control assurance program:** Risk and InfoSec leaders may need an ongoing start-to-finish program that includes external guidance on their existing SSH risks and specifies prioritized actions. This is often referred to as an "SSH control assurance program" and involves steps like regular SSH risk assessments, implementation guidance and baseline report construction. External auditors look for these assurance programs.

Venafi Helps You Secure SSH Machine Identities—and Prepare for a Successful Audit

Venafi machine identity management experts recommend the following solutions to help address any of the common causes of SSH audit failures and reduce the security risks connected with weak SSH key management.

SSH Risk Assessment: Venafi's SSH Risk Assessment (performed remotely or on premises) provides organizations with an accurate and prioritized view of enterprise SSH risks, accompanied by detailed, actionable mitigation options ready for consumption by system administrators and InfoSec teams. The risk assessment leverages *NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments*. The assessment evaluation includes multiple risk factors such as the number of discovered hosts and keys, severity of the discovered SSH vulnerabilities, likelihood of threat occurrence, impact and combined global risk level.

Venafi SSH Protect—Visibility, Intelligence and Automation: The Venafi Trust Protection Platform with SSH Protect assists InfoSec and risk management teams in safeguarding mission-critical SSH keys and the automated connections they enable. By combining best practices, outlined in NIST 800-53r4 standards, with our platform-based, enterprise-grade Venafi SSH Protect solution, InfoSec teams have a comprehensive, automated solution that can discover, remediate, govern and audit all SSH machine identities.

SSH Protect, as part of the Venafi Platform, provides visibility, intelligence and automation to reduce risks from poorly managed SSH keys and help safeguard the trusted connections SSH keys enable.

Key features include:

- Agent-based or agentless methods to discover SSH hosts, clients and keys enterprisewide
- Central key inventory, mapping connectivity and risk analysis
- Prioritization and automatic rotation of out-of-compliance SSH keys
- Automation of SSH machine identity lifecycle through self-service onboarding
- Automated notifications to InfoSec and risk teams about policy violations

SSH Mandates and Standards Continue to Grow

Audits evolve over time, generally becoming more dynamic and stringent. In recent years the number of security frameworks and standards that require close inspection of SSH key risks have grown to include:

- National Institute of Standards and Technology: NIST IR 7966; NIST SP 800-53, in AC-2, AC-3 and PS-4 requirements
- Payment Card Industry Data Security Standards: PCI DSS 3.2, sections 7 and 8
- Health Insurance Portability and Accountability Act: HIPAA, through 14CFR 164.308
- Sarbanes-Oxley: SOX-404
- International Standards Organization: ISO/IEC 27001
- Federal Financial Institutions Examination: FFIEC Examination Handbook II.C.19
- Center for Internet Security (CIS): Critical Security Controls 13, 14, 15
- North American Electric Reliability Corporation (NERC): CIP 5, 7

The Time to Prepare Is Now

Don't wait until your auditor calls before taking action. Schedule a risk assessment now to learn more about how Venafi SSH Protect can help you pass your SSH audits.

Please contact your Venafi Sales Executive for more info or go to **venafi.com**.

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