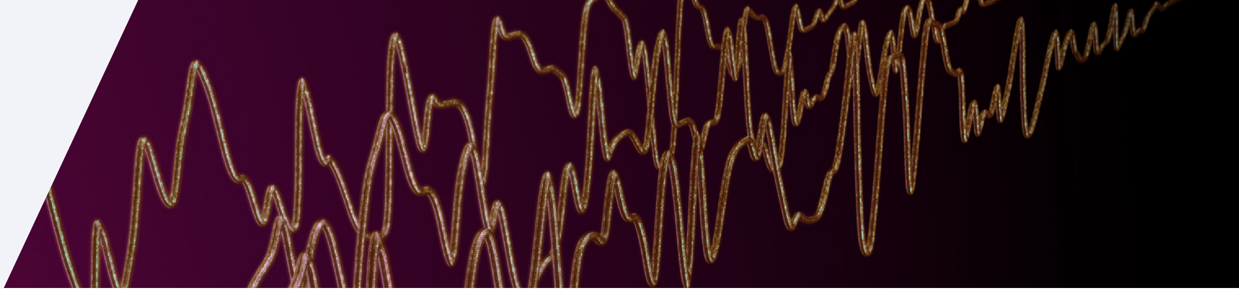
Venafi



SERVICES BRIEF

SSH Risk Assessment

Get an accurate and prioritized view of your enterprise SSH risks with mitigation recommendations

Venafi Services: SSH Risk Assessment

SSH keys are routinely untracked, unmanaged and unmonitored, creating a widespread, unknown risk of unauthorized access. The Venafi SSH Risk Assessment reveals an organization's level of SSH risk exposure and delivers actionable recommendations to mitigate those risks.

Prerequisite

Venafi customers with Venafi Platform version 18.4 or 19.x

Main Standards Leveraged*

- NIST 800-30 Revision 1, Guide for Conducting Risk Assessments
- NIST 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations

*Also includes mapping to other standards and regulations

8 SSH Risk Assessment Steps Completed by Venafi Experts

1. Prepare and Identify Existing SSH Controls
2. Map Risk Controls to Standards
3. Identify Risks Using the Venafi Platform
4. Determine the Severity of Risks
5. Classify Actions to Eliminate Risks
6. Ascertain Monitoring Options
7. Document and Report
8. Make Risk Mitigation Plan

Unseen Enterprise SSH Risk

Today, Secure Shell (SSH) is the de facto standard for remote administration and integration, leveraging public-private keypairs as machine identities for automated authentication and access. Most organizations leave it up to individual power users to get and manage their own SSH keys for system administration or IT automation. This results in ad hoc processes and inconsistent security practices that leave SSH keys open to compromise by adversaries.

Almost all enterprises make common mistakes around SSH key security, policy and auditing practices, which exposes businesses to costly security threat scenarios like unauthorized access, obscured network traffic and time-consuming incident response procedures.

The combination of a lack of SSH machine identity lifecycle management, no expiration of SSH keys and popular widespread usage can generate literally millions of SSH keys and create a broad attack surface for insider threats and cybercriminals. Mitigating this often invisible and widespread threat risk can require excessive effort from already overloaded IT risk and information security teams. Instead, enterprises need visibility into SSH key use and well-defined actions to achieve acceptable SSH usage risk.

Jump-Starting Your SSH Risk Assessment

Most organizations have not taken a proactive, comprehensive approach to managing their SSH risks. By reviewing live SSH vulnerabilities and potential threat scenarios, Venafi SSH Risk Assessment helps organizations by providing an accurate and prioritized view of their enterprise SSH risks, accompanied by detailed, actionable mitigation options.

Risk Metrics Plus Mitigation Guidance

The Venafi SSH Risk Assessment leverages National Institute of Standards and Technology (NIST) 800-30 Revision 1, Guide for Conducting Risk Assessments,[1] to evaluate and quantify SSH risks. Risk metrics include multiple factors such as the number of discovered hosts and keys, severity of the discovered SSH vulnerabilities, likelihood of threat occurrence and combined global risk level.

Using a custom-made risk rating worksheet, Venafi experts identify SSH risk vulnerabilities with corresponding security controls listed in NIST 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations,[2] and provide mitigation options ready for consumption by IT risk and information security teams.

Table 1: Sample SSH Risk Assessment Report

Ref/ ID	Risk	NIST Mappings	#Keys/ Clients	#Keys/ Hosts	Risk Severity	Risk Likelihood	Risk Level	Mitigation/Warning/ Remedies
2	Duplicate Host Key	IA-3	# N/A	65	Moderate	Low	Moderate	Rotation/utilize API to build new machines with unique keys
3	Passphrase Uknown	IA-8, PL-8	1	# N/A	Low	Low	Low	Reset or rotate
4	User Access Orphan		497	# N/A	High	High	Low	Removal or rotation
5	Private Key Orphan		278	# N/A	Low	Low	Low	Removal
6	Known Host Orphan		0	1577	Very Low	Very Low	Very Low	Removal
8	Duplicate Private Key		277	# N/A	Moderate	High	High	Create separate key for each host, provision corresponding known_ hosts keys, then remove old keyset
18	Shared Private Keys		267	65	Very High	Very High	Very High	Remove collocated keys or split them and rotate

8 Steps in SSH Risk Assessment

An SSH Risk Assessment can be conducted in organizations running the Venafi Platform (version 18.4 or 19.x). To start, organizations must first meet the prerequisites listed in the SSH Risk Assessment Requirements and Constraints section below. Once met, Venafi experts will conduct the following steps, which result in the detailed overview of the organizations' existing SSH risk exposures and ensuing mitigation steps.

Step 1: Prepare and Identify Existing SSH Controls

- Scope assessment
- Inventory regulatory controls standards and policies already in place

Step 2: Map Risk Controls to Standards

- NIST 800-53, 800-171, 800-131A, and IR-7966 and related cybersecurity frameworks
- HIPAA, FISMA, ISO, SOX-404, PCI DSS, GDPR, Basel
- Audit SSH Practitioner Guides (ISACA, SANS, etc.)

Step 3: Identify Risks Using the Venafi Platform

- Conduct network scanning and crawling of file systems
- Inventory SSH hosts and keys
- Assess SSH policies
- Run continuous monitoring

Step 4: Determine the Severity of Risks

- Utilize the Venafi Risk Rating tool
- Institute standard and nonstandard operating procedures
- Establish when and how mitigation will happen

Step 5: Classify Actions to Eliminate Risks

- List needed actions
- Define necessary steps for each action

Step 6: Ascertain Monitoring Options

- Select best monitoring options for environment
- Validate continuous monitoring to ensure ongoing use of controls and processes

Step 7: Document and Report

- Document how risk was assessed and rated
- Identify mitigation processes and success factors

Step 8: Make Risk Mitigation Plan

- Distinguish and prioritize next steps
- Assist in creating a mitigation project plan with desired outcomes

Identified SSH Vulnerability Risks

- Duplicate Host Key
- Root and User Access Orphan Keys
- Private Key Orphan
- Known Host Orphan
- Duplicate Private Key
- Vulnerable Protocol
- SSHv1 Enabled
- Password Authentication
- Noncompliant Encryption Algorithm
- Noncompliant Key Format
- Noncompliant Command
- Noncompliant Source Restrictions
- Missing Options
- Key Older Than Allowed
- Key Smaller Than Required
- Key Size <= 768
- Shared Private Keys
- Passphrase Unknown
- Unknown Client
- Key Not Rotated
- Environment Crossing

SSH Risk Assessment Requirements and Constraints

The following must be met by an organization prior to the initiation of a Venafi SSH Risk Assessment.

- Venafi Platform version 18.4 or 19.x required
- Scanning limited to development segments
- Work conducted with Technical Director from Venafi
- Firewall rules enabled to allow Venafi Platform access into development segment
- Configuration management requirements provided such as
  - LDAP joining tool for correct access (sudo, dzdo, suexec, pbrun, etc.)
  - Process execution policies (sshd_config, etc.)
- Management process changed to allow Venafi to enable SSH key changes (policy, inventory, key management, continuous monitoring, etc.)
- Architecture plans provided to define future needs such as
  - Access control options
  - Self-service needs
  - Policy folder structure
- Overview of existing Venafi deployment
  - Accept SSH expansion options
  - Current Venafi Platform services implemented

Understand, Plan and Protect SSH Machine Identities

This bottom-up risk assessment program enables information security decision makers to engage quickly and get a true understanding of SSH risks present in their environment. Prioritized risk findings and candidate mitigation options allow for budgetary and organizational planning, all to improve protection of enterprise SSH machine identities critical to day-by-day IT processes.

To get a Venafi SSH Risk Assessment for your organization, reach out to your Venafi account representative.

References

1. NIST Special Publication 800-300, Revision 1, Guide for Conducting Risk Assessments. September 2012.
2. NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. April 2013.

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**