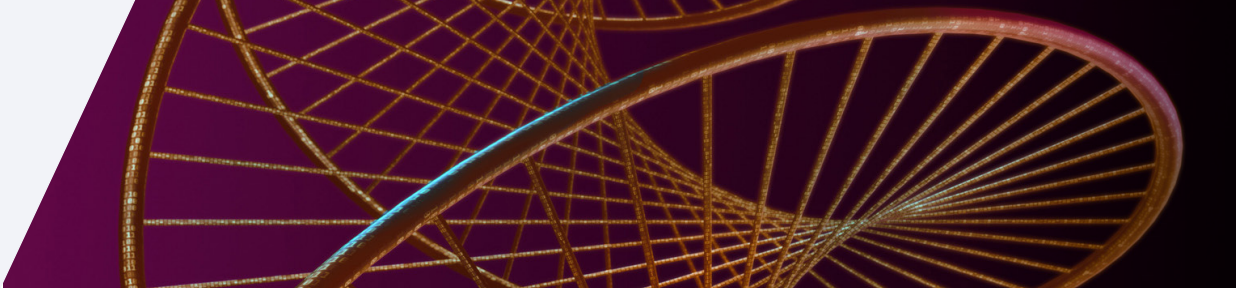
Venafi



DATA SHEET

Venafi SSH Protect

SSH Machine Identity Management

Key Features

Visibility

- Discover SSH keys to create an accurate inventory and begin active monitoring.
- Use agent-based and agentless scanning tools.
- Organize keys and metadata into folders.
- Integrate with Active Directory.

Intelligence

- Identify policy violations and vulnerabilities and get recommended actions from a single-pane dashboard.
- Report on servers, users and access privileges.
- Map SSH key policy violations to NIST 800-53.
- Identify insecure configurations and port forwarding.

Automation

- Specify, monitor and enforce SSH key policies, including rotation.
- Automate custom remediation of policy violations.
- Log when a key was used and who used it.
- Integrate with SIEM, CyberArk and others.
- Automate provisioning on any device via a self-service UI.

Additional Benefits for CyberArk Customers

Venafi's integration with CyberArk further secures the SSH key lifecycle by automatically placing private keys discovered by SSH Protect into CyberArk's Enterprise Password Vault (EPV) and continuously monitoring those SSH sessions.

All organizations rely on SSH machine identities as an encrypted protocol to authenticate privileged users, establish trusted access and connect administrators and machines. However, most organizations are unaware of how widely these keys are used, let alone what levels of rights and privileges they provide to access critical systems and data. With the rapid growth of digital transformation, the number of machines requiring SSH machine identities continues to grow, forcing organizations to rely more heavily on them than ever before—with no signs of this slowing down.

Most organizations manage their SSH keys manually, which can lead to unknown sets of SSH keys, uncontrolled SSH key setup, inability to enforce SSH policies and increased risk of unauthorized access. When SSH keys are manually managed, organizations lack the visibility and intelligence necessary to prevent security breaches. As a result, SSH keys become a security liability, leaving organizations vulnerable to failed audits and exposed to adversaries who could exploit weak security practices to gain unauthorized access to mission-critical systems.

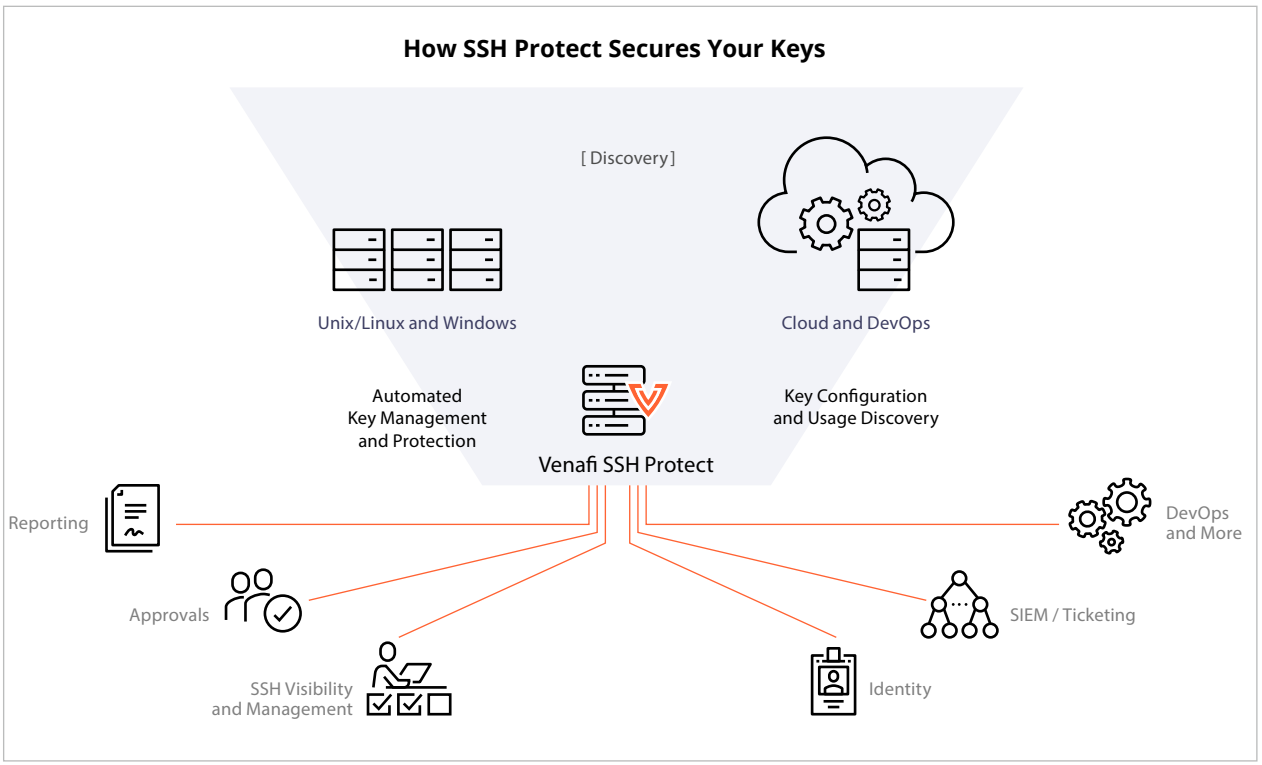
Why Use Venafi SSH Protect?

Discover SSH issues to plan remediation

SSH Protect, part of the Venafi Control Plane for machine identities, discovers SSH host and authorized keys throughout your infrastructure and adds them to a continually updated inventory. In this database, the type of key, location of all copies, public and private components, algorithm and key sizes are routinely assessed and tracked.

Mitigate high-priority threat risk exposures

Because many large organizations have key pairs running into the millions, SSH Protect helps you focus on your most essential systems first. These can be tagged by business units, by system administrators, by machine or application type or by compliance needs.

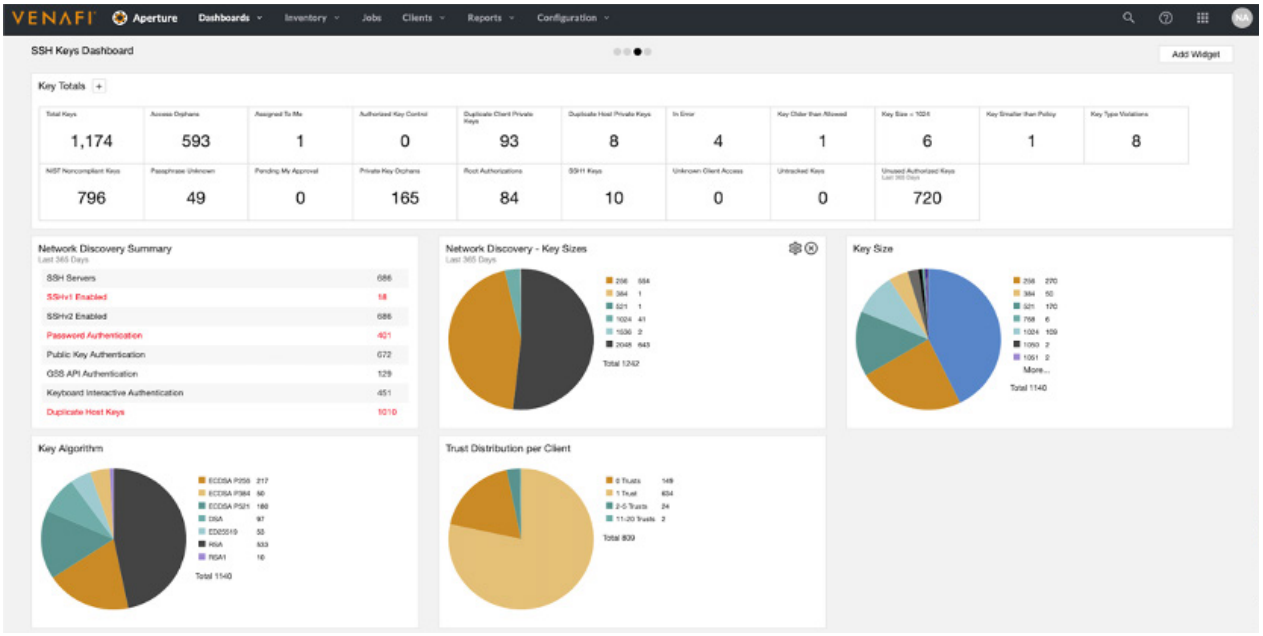


Monitor key usage and work toward full automation

Keys that have privileged access and for which key usage patterns are well understood can be flagged and managed first. And once this baseline is known, new keys deployed by SSH Protect can be automated for rotation or updated on a regular schedule—ending hours of manual labor.

Crypto-Agility: Prepare for a fast response

SSH Protect helps prepare you for the next crypto event, whether it involves a migration to new standards or replacement of newly found risks. SSH Protect can rapidly and securely update thousands or millions of keys in bulk, saving you substantially on speed and cost while keeping you in compliance for audits.



SSH Protect Single Pane Dashboard. Gain a comprehensive view of the SSH inventory; obtain rapid identification of vulnerabilities, including SSH access via root, potential backdoor keys, weak key lengths, old keys, duplicated private keys and much more.

SSH Certificates

Organizations can now use Venafi SSH Protect to issue SSH certificates for client and host authentication. SSH certificates greatly improve security and policy enforcement because unlike SSH keys, SSH certificates have metadata built-in, including an expiration date, making them harder to exploit. They also simplify SSH management, as well as support ephemeral credentials.

InfoSec teams

- Get improved visibility and insights into who is requesting certificates for SSH
- Sign SSH certificates using the built-in certificate authority or create multiple certificate authorities and define specific issuance restrictions
- Validate that all certificate requests are compliant with restrictions configured by them
- Protect the keys that sign SSH certificates by storing them in an HSM, increasing security and helping prevent misuse

Developers

Quickly and easily adopt SSH certificates through integrations with multiple configuration solutions:

- Native integration for Ansible and Terraform to request SSH certificates
- VCert command line utility to request SSH certificates for Windows, Linux and macOS
- Software development kit (SDK) for Go, Python and Java to request SSH certificates

Venafi Free SSH Risk Assessment

Venafi's SSH Risk Assessment helps jumpstart your overall risk evaluation. Once you have an accurate and prioritized view of your enterprise SSH risks with mitigation recommendations, you'll soon be able to pass even the most stringent audits!

The Venafi Control Plane

The Venafi Control Plane for machine identities accelerates digital transformation and eliminates security incidents and revenue stream disruptions caused by machine identity management failures. With comprehensive support for all machine identities in data centers, clouds, hybrid environments and at the edge Control Plane gives enterprises the observability, consistency, reliability and freedom of choice needed to stop outages, automate for efficiency, prevent misuse and compromise and modernize with speed and agility.

For more information about this product, its features, and how other customers use it, scan this QR code or go to:

venafi.com/platform/ssh-protect

Venafi is the cybersecurity market leader in identity management for machines. From the ground to the cloud, Venafi solutions automate the lifecycle of identities for all types of machines—from physical devices to software applications, APIs and containers. With more than 30 patents, Venafi delivers innovative solutions for the most demanding, security-conscious organizations in the world. **To learn more, visit venafi.com.**