

# Venafi Encryption Director™ SSH Key Manager™

DISCOVERY | MONITORING | REPORTING



## WHAT IT DOES

Venafi Encryption Director SSH Key Manager enables organizations to rapidly inventory and monitor SSH keys across their enterprise environments through:

- Continuous Discovery
- Monitoring & Alerts
- Extensive Reporting



## WHY IT'S VALUABLE

Simplify the management of SSH keys across the enterprise environment and reduce the unquantified and unmanaged risks that result in data breaches, failed security audits and unplanned system downtime.

## ELIMINATE UNQUANTIFIED AND UNMANAGED RISKS

SSH (Secure Shell) plays a critical role in securing mission-critical systems and infrastructure in organizations, including for firewalls, routers, switches, and Unix and Linux systems. SSH relies on encryption keys to be deployed on these systems and on other systems that access them to encrypt communications and to authenticate systems and users. Poor key management practices are resulting in significant unmanaged and unquantified risk within organizations, including unauthorized access, failed security audits and unplanned system downtime.

## SSH KEY MANAGEMENT: BUSINESS AND TECHNICAL CHALLENGES

SSH is used to secure Telnet communications—much like SSL secures web-based HTTP communications. Encryption keys are used in SSH to secure communications, reduce vulnerabilities, and authenticate systems and users. Because of the historically distributed nature of SSH deployments, SSH keys are not typically tracked, rotated or managed. When combined with the large volumes of SSH keys in use, organizations face a myriad of risks and challenges. These may include the following:

### Weak Encryption

2048-bit encryption keys are now recommended by the US National Institute of Standards (NIST), and organizations should no longer be using smaller or weaker key sizes. Yet most organizations are still using hundreds or thousands of 1024-bit (and even 512-bit) SSH keys to protect their most critical systems.

### Compromised Keys

Organizations rarely or never change their SSH keys, and some have been deployed for five years or more. During this time, administrators have come and gone, each having had the ability to make copies of these keys and later access critical systems and accounts, many with root privileges.

### System Outages

When organizations attempt to update and replace old SSH keys, they must account for every location where a key is used. Otherwise they can experience unexpected system downtime and outages if a system that was not correctly updated attempts to perform operations relying on the old key.

### Compliance Violations

SSH is used for privileged administrative and application access accounts, which are governed by regulations such as Sarbanes Oxley, PCI, and Basel II. Typical management practices make it impossible to provide an up-to-date inventory of where SSH and its associated keys are used, or whether the keys are being managed consistent with industry best practices and regulations, creating significant compliance risk.

### Viruses Going Viral

Once a worm infiltrates a system it will typically leverage access the system has to other systems (via SSH) to infect those systems. If SSH keys have been deployed unchecked and not removed when access is no longer appropriate, an organizations' infrastructure and systems can become fertile ground for a rapidly-spreading virus infiltration.

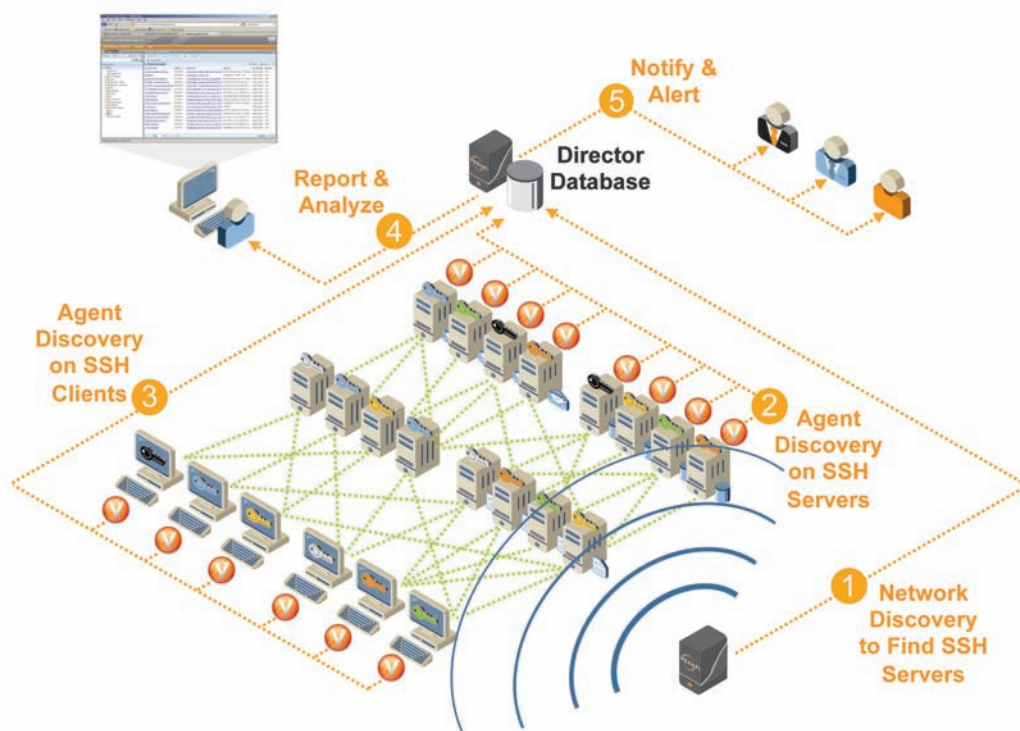


## VENAFI ENCRYPTION DIRECTOR SSH KEY MANAGER

Venafi Encryption Director™ SSH Key Manager™ enables organizations to quickly develop an inventory of their SSH environment and take effective action to remedy risks and challenges. SSH Key Manager is built on the Venafi Encryption Director platform, which for nearly a decade has enabled many of the world's largest organizations to manage their encryption environments effectively.

In order to establish a comprehensive inventory of SSH keys, Director SSH Key Manager provides both network and agent-based discovery. The network discovery identifies where SSH servers are deployed and whether those servers are configured in compliance with corporate policies, including key lengths, protocol versions (SSH v1 is considered unsecure), supported authentication methods and other information.

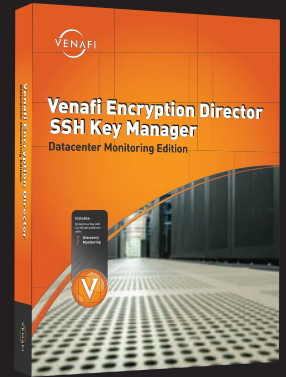
The following diagram illustrates how Director SSH Key Manager enables organizations to establish an SSH inventory and map trust relationships between systems:



Once SSH servers are identified by Director, agent-based discovery can be run on the servers to identify trust relationships with other systems acting as SSH clients. The agent can then be further deployed to those client systems to close the loop on understanding full key dependencies and locations. All discovery results are correlated at the Director server and the result is a comprehensive inventory of SSH systems, configuration information, keys and trust relationships.

Venafi Encryption Director SSH Key Manager helps you:

- Develop an inventory of SSH keys, servers & configuration information
- Get in compliance with key length and algorithm standards
- Eliminate risk by identifying lost, orphaned and unused keys
- Ensure critical system availability through key dependency mapping



**Director SSH Key Manager provides network and agent-based discovery on the following operating systems:**

- Windows® 2003 Server (32 and 64 bit)
- Windows 2008 Server (32 and 64 bit)
- Windows XP
- Windows 7
- Red Hat® Enterprise Linux
- Linux 2.6 Kernel
- IBM® AIX 5.3 and 6.1
- Solaris® 9 and 10
- HP-UX® 11 on PA-RISC and Itanium



Contact **Venafi** at:

Worldwide: +1 801 676 6900  
EMEA: +31 641 789 667  
info@venafi.com

[www.venafi.com](http://www.venafi.com)

Copyright © 2011 Venafi, Inc. All rights reserved. Venafi and the Venafi logo are trademarks of Venafi, Inc. in the United States and other countries. All other company and product names may be trademarks of their respective companies. This datasheet is for informational purposes only. Venafi makes no warranties, express or implied, in this summary. Covered by United States Patents #7,418,597, #7,568,095, #7,650,496, #7,6,50,497, #7,698,549 and other patents pending.

Part number: 4-0005-0211