EXECUTIVE SUMMARY

# Pass Your IT audits: Address the Risk of Unmanaged SSH Keys.

**A summary of the practical executive recommendations from NIST IR 7966**

## SSH is everywhere in IT

Controlling access to information systems is critical for information security. SSH is the primary access and administration mechanism for enterprise network and security appliances. It is also embedded into various technologies for file transfer, systems management, identity and privileged access management, and machine integrations and automations.

## Unmanaged Access Is Risky & Audit Failure Point

The NIST IR 7966 report, coauthored by Tatu Ylönen, inventor of the SSH protocol, helps organizations understand the basics of SSH with specific emphasis on SSH access management. The document highlights that there is too little planning and oversight of automated access, too much ad hoc management, and a lack of access key life-cycle management, leading to security vulnerabilities and increasingly unacceptable risk.

## Importance of SSH key management

It is important to ensure basic understanding of how SSH works and how key management is handled throughout the organization. The risks involved affect the whole chain of accountability, all the way to the CEO.

## Key Recommendations

### 1 Set Clear Policies and Procedures

Control starts with all stakeholders understanding individual roles and responsibilities. Policies and procedures that ensure accountability are critical to secure diverse systems and rapidly evolving cloud environments.

### 2 Secure SSH Implementation

Note the areas where policies and procedures need to be defined to mitigate vulnerabilities.

### 3 Make Sure Keys Are Set and Used Correctly

How the keys are defined, managed and rotated is critical to security. Often overlooked, special attention should be paid to managing authorized keys for automated processes on a continual basis.

### 4 Build A Clear Process for Provisioning, Lifecycle and Termination

The NIST IR 7966 report defines the process that make sure your SSH keys will be secure now and in the future. It establishes clear specifications on how to define each stage of the lifecycle of individual keys.

### 5 Establish Continuous Monitoring and Audit Processes

By following the recommendations of the report, you will ensure constant visibility and control over the use of the protocol. You will also help define auditing processes and practices for the purposes of compliance and risk analysis.

### 6 Inventory and Remediation of the Current Environment

The report outlines what you need to do to evaluate the current state of your network and how to get it in working order. Most organizations have thousands of untracked identity keys, authorized keys, and corresponding trust relationships granting access across a large number of mission critical systems. Existing legacy keys pose a substantial security risk and make risk analysis difficult if they are not understood. The report instructs how to create inventories of keys and trust relationships and evaluate them against defined policies.

### 7 Automate the Whole System

To cap the process the report outlines how you can gain maximum benefit and security by automating the management of your SSH keys. The recommendations significantly improve the security, efficiency and availability of your system.

### Stay compliant. Get the full report.

The full report is required reading for those responsible for access management. It includes detail on vulnerabilities, best practice, access management deployment and how to evaluate tools. **Download the full NIST IR 7966 report here**.

Universal SSH Key manager is the most comprehensive SSH key management solution for large enterprises. Start your journey towards compliance and risk mitigation with **our free Risk Assessment** or **contact us for a demo here.**