A Custom Technology Adoption Profile
Commissioned By Venafi

July 2014

# Gaps In SSH Security Create An Open Door For Attackers

## Introduction

Every enterprise is reliant on SSH to authenticate and establish trust with elevated privileges between administrators, applications, and virtual machines in the data center and out to the cloud. However, most lack the visibility or control over how SSH is used or secured.

Most organizations leave themselves open to attack with insignificant policies for SSH, compared to standard user credentials that are rotated frequently. The lack of control or visibility into SSH keys shows a clear gap in enterprise security strategy. This results in SSH being a key target for bad actors to take advantage of.

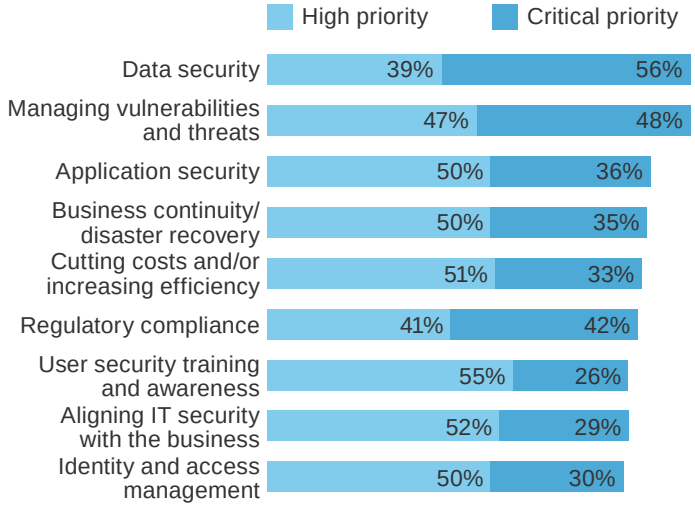
Research shows that organizations have had to deal with a significant amount of attacks based on SSH. However, they are ill-equipped to both detect and respond to attacks based on SSH.

This Venafi-commissioned profile of IT security decision-makers evaluates the level of knowledge and understanding of SSH policies and practices in the US, UK, and Australia, based on Forrester's own market data, and a custom study of the same audience.

**FIGURE 1**

**IT Security Professionals Consider Data Security A Critical Priority**

**"Which of the following initiatives are likely to be your firm's/organization's top IT security priorities over the next 12 months?"**



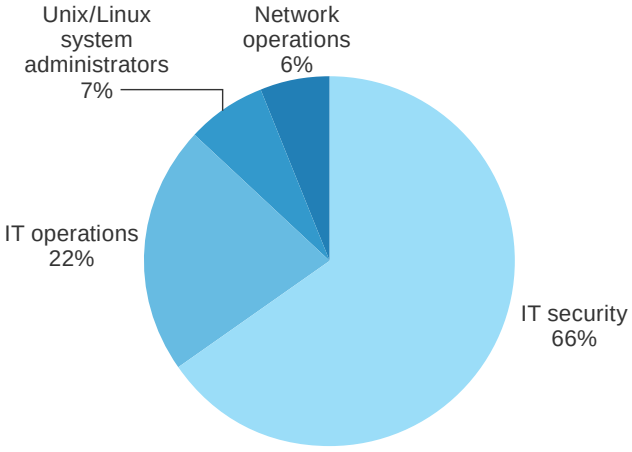

Base: 463 IT security decision-makers

Source: Forrester's Forrsights Security Survey, Q2 2013

**FIGURE 2**

**IT Security Acknowledges Responsibility For SSH Keys**

**"What team or group in your company is primarily responsible for securing SSH (Secure Shell) keys?"**




Base: 106 IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Venafi, May 2014

## The Important Role Of SSH In IT Security

IT security professionals must balance a myriad of threats and security concerns affecting their organization. Data security, however, is of particular concern — 95% of IT security professionals in a recent Forrsights Security Survey named data security to be either a high or critical IT security priority for their organization (see Figure 1).

As every enterprise is reliant on SSH to authenticate and establish trust with elevated privileges between administrators, applications, and virtual machines in the data center and out to the cloud, it is important for IT security to take ownership of SSH. Indeed, two-thirds of IT security professionals acknowledge that they own responsibility for the security of SSH keys (see Figure 2). That said, security professionals lack complete awareness and the knowledge necessary to enforce policy and detect potential malicious activity.

## Lax Policy Enforcement Risks Unauthorized Access

Despite relying on SSH keys to secure data in the enterprise, IT security professionals fail to provide the necessary level of policy enforcement necessary to adequately secure against risks of unauthorized access. For example, nearly three-quarters of IT security professionals fail to rotate SSH keys more often than once a year (see Figure 3) — leaving any key stolen or compromised during this period vulnerable to unauthorized access.

It would stand to reason that lack of necessary policy enforcement would necessitate IT security professionals to actively seek out the use of unauthorized SSH keys to guard against potentially malicious activity. Unfortunately, our survey results show that IT security professionals are not undertaking the necessary due diligence necessary to protect their organization's data — 30% said that they do not scan for unauthorized keys more often than one week, and an additional 36% do not regularly scan for

unauthorized keys at all (see Figure 3). With the consequences of unauthorized access being very concrete for many organizations, two-thirds of IT security professionals not performing the necessary checks for unauthorized SSH keys should be a wake-up call.

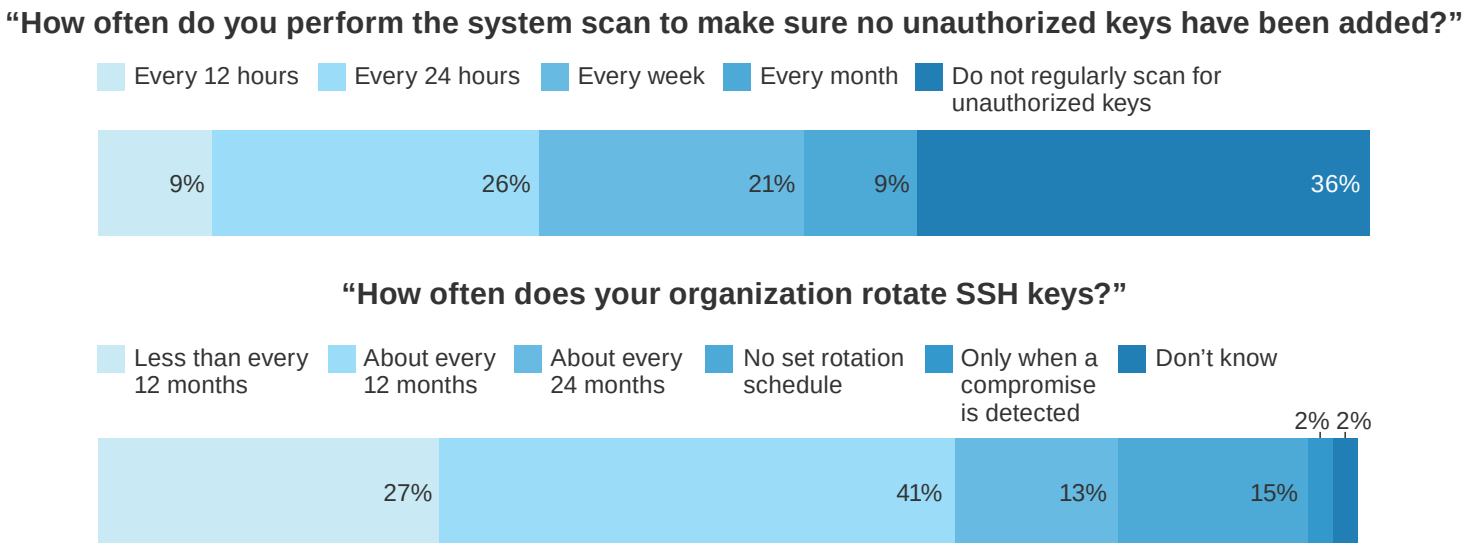
## Vulnerability To Attack

The consequence of lax policy enforcement and infrequent scanning for unauthorized access around SSH keys is a major vulnerability. IT security professionals are indeed aware of these consequences — they associate a variety of vulnerabilities with SSH and SSH management. In our survey, the top five concerns range from weak passwords on Internet-facing servers and sharing of SSH host keys to lack of visibility into what SSH keys are being used for (see Figure 4). Ultimately, IT security professionals do not feel they have complete control.

These concerns are certainly exacerbated by the fact that IT security professionals tend to rely on busy system administrators more than any other method of detection to identify rogue SSH keys that may be inserted into their network (see Figure 5). Although they do utilize other methods of detection, these methods can be less effective given that SSH keys provide an encrypted tunnel into the network and infer a trusted status to potentially malicious sources.

The end result of these vulnerabilities is that 47% of IT security professionals reported in our survey that they had to deal with a security incident due to compromised or misused SSH keys in the last 24 months. As they could only answer to incidents they were aware of, the sad reality is that this percentage is likely much higher.

**FIGURE 3**
**Two-Thirds Of IT Security Professionals Rotate SSH Keys Once Per Year Or Less Often**

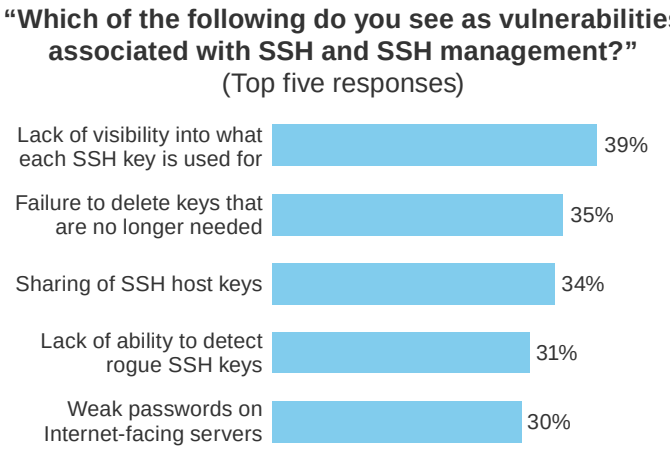



Base: 106 IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Venafi, May 2014

**FIGURE 4**

**Top Five Vulnerabilities Associated With SSH And SSH Management**

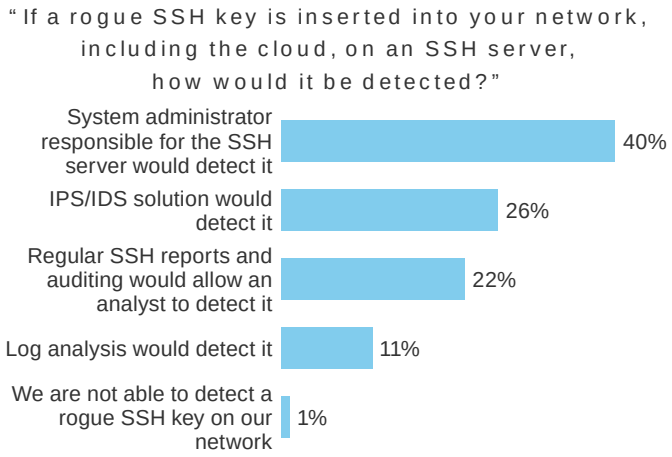



Base: 106 IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Venafi, May 2014

**FIGURE 5**

**Over-Reliance On System Administrators Is Most Common Method To Rogue SSH Key Detection**




Base: 106 IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Venafi, May 2014

## Closing The Gap

As most organizations are reliant on SSH keys to conduct business, vulnerabilities that can result in data loss or catastrophic disruptions must be addressed immediately. We see how IT security professional lack the necessary visibility and policy enforcement to properly identify unauthorized SSH key use, and the elevated privileges that SSH keys provide, prove that their protection by IT security is of paramount importance.

Organizations can close the unacceptable gaps in SSH security by:

- **Centralizing control and visibility** for all SSH hosts in the data center and out to the cloud in order to effectively enforce policy for all enterprise SSH keys. Policies should be applied to specify even the use of SSH keys in the environment limiting any potential opportunity for stolen SSH keys to be used for expansion on the network or insiders.
- **Establishing a baseline** of normal key usage. This is achieved by first gaining an understanding of where keys are deployed and used, who has access to them, and what trust relationships have been established within the network.
- **Rotating keys regularly.** No organization will accept domain credentials only being rotated once per year or more, yet domain credentials do not provide the same privileged level of access to critical systems that SSH keys do. Regular rotation of SSH keys should be applied and is essential in providing effective security.
- **Continuously monitoring** SSH key usage on the network to identify any rogue SSH keys. Reliance on system administrators to self-govern and identify any rogue SSH keys is not scalable, nor is it a good security strategy — akin to asking each employee to validate that their computer is not infected with malware manually.
- **Remediating vulnerabilities** by ensuring that server and SSH key configurations adhere to common best practices, such as implementing the NIST recommendation of using 2048-bit key lengths or higher.[1]

In most cases, system administrators are responsible for the deployment and protection of their own SSH keys on systems they are responsible for. This creates a silo effect where the organization has no visibility, no ability to enforce policy, and no ability to respond to incidents. Taking these important steps will bring the same effective controls used elsewhere in the enterprise to a core IT systems left unsecured today.

## Methodology

This Technology Adoption Profile was commissioned by Venafi. To create this profile, Forrester leveraged its Forrsights Security Survey, Q2 2013. Forrester Consulting supplemented this data with custom survey questions asked of US, UK, and Australian IT security decision-makers who are aware of their company's SSH (Secure Shell) policies and practices. The auxiliary custom survey was conducted in May 2014. For more information on Forrester's data panel and Tech Industry Consulting services, visit www.forrester.com.

## Endnotes

[1] Source: Elaine Barker and Quynh Dang, "Recommendation For Key Management: Part 3: Application-Specific Key Management Guidance," Draft NIST Special Publication 800-57 Part 3 Revision 1, National Institute of Standards and Technology, May 2014 (http://csrc.nist.gov/publications/drafts/800-57pt3_r1/sp800_57_pt3_r1_draft.pdf).

**ABOUT FORRESTER CONSULTING**

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.