



# Seven Things To Consider When Evaluating **Privileged Account Security Solutions**



# Contents

<b>Introduction</b> .....	<b>1</b>
<b>Seven questions to ask every privileged account security provider</b> .....	<b>4</b>
1. Is the solution really secure? .....	5
2. Can it find and protect all of my accounts? .....	6
3. Can it protect all credentials? .....	7
4. Will it work in my environment? .....	9
5. What protections are provided? .....	10
6. How can I minimize the cost of managing it? .....	11
7. How reliable is the vendor? .....	12
<b>Conclusion</b> .....	<b>13</b>

# PRIVILEGED ACCOUNTS: THE ATTACKER'S ALL ACCESS PASS

## This Pass May Be Used For:



Privileged access to every IT system, application and end-user device



Fast and easy movement from system-to-system with low risk of detection



Establishing multiple clandestine beachheads, making it difficult to dislodge attackers from networks



Deleting log data and other evidence of illicit activity

ADMIN

\*\*\*\*\* |

ROOT

\*\*\*\*\*

ADMIN

\*\*\*\*\*

ROOT

\*\*\*\*\*

ADMIN

\*\*\*\*\* |

ROOT

\*\*\*\*\*

# THE PRIVILEGED ACCOUNT DISCONNECT

## Today's Reality



Most organizations don't know how many privileged accounts they have or where they reside – making tracking and monitoring increasingly difficult

## The Real Threat



80%  
TO  
100%

of serious security incidents involve privileged accounts, experts estimate



The average organization has at least  
**3x to 4x**  
as many privileged accounts as employees



Exploits of privileged accounts are  
**widening and getting more sophisticated**

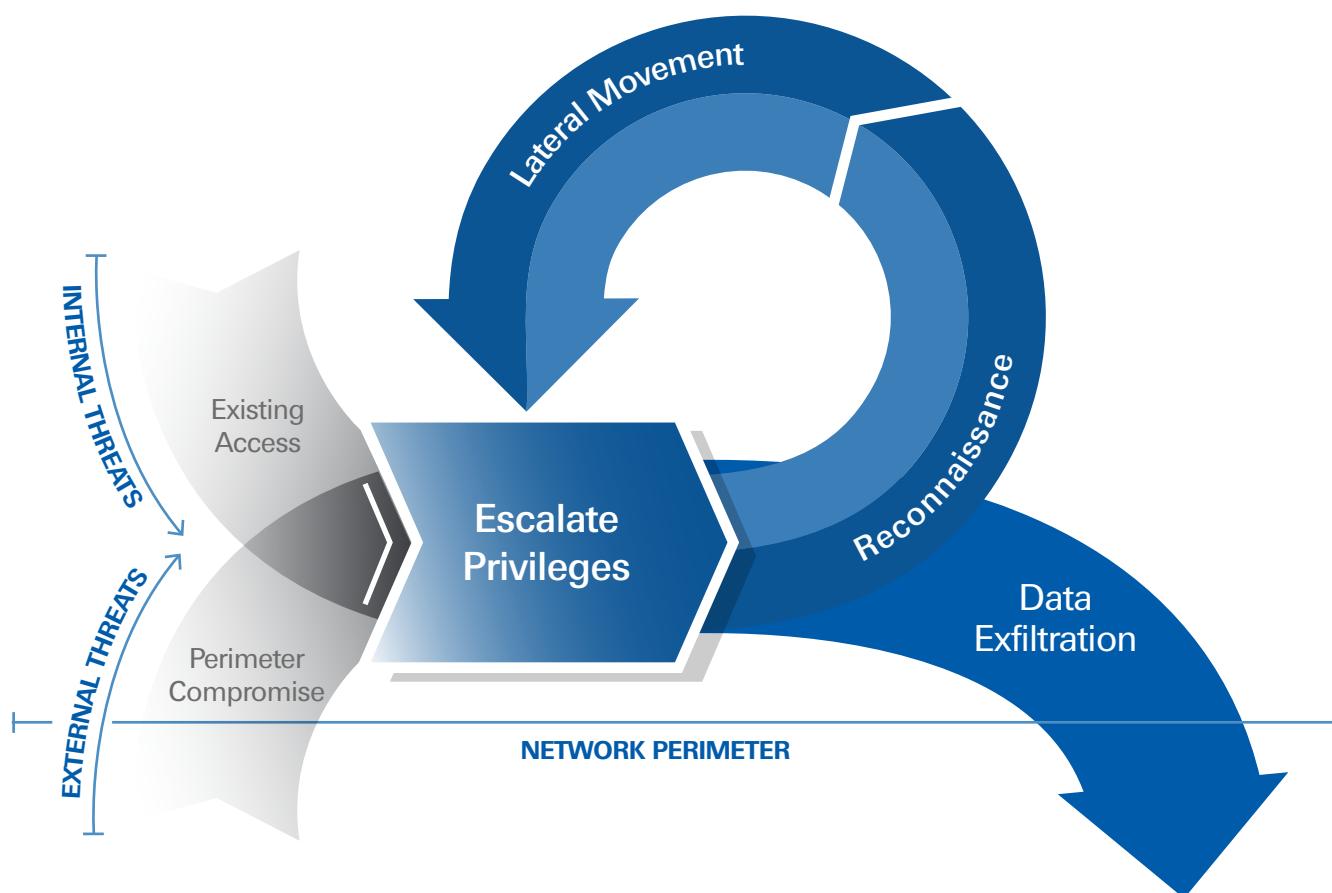
# Privileged account exploits shift the front lines of cyber security

90% of organizations have admitted to being breached at least once, and 59% have claimed two or more breaches within a year's time. It's clear that traditional perimeter defenses are no longer adequate. So what can be done to protect sensitive data and gain a fighting chance against motivated attackers?

Recent high-profile attacks show us that no matter where an attack originates, skilled attackers will end up on the inside. And once they're in, they all follow a similar path: they target sensitive, valuable data. To do this, they first look for access to an internal account, preferably with some administrative privileges. They then leverage the compromised privileged account to continue escalating privileges to see more of the network, access

more on the network, and move around more freely. With the necessary privileges, attackers next do reconnaissance on the network to determine how to best reach the target. With an attack plan in place, attackers move laterally to get into a better position and further escalate their privileges until they successfully reach the target system – or systems – and begin exfiltrating sensitive data.

It's time to adapt to this new threat landscape and take a more proactive stance to security by taking the battle inside the network. The most effective way to win – and keep sensitive data out of the hands of attackers – is to secure privileged accounts, which are required for any malicious actor to carry out a successful attack.



# Seven questions to ask every privileged account security provider

---

You're convinced that protecting privileged accounts is paramount in your security strategy. But how do you go about selecting the right solutions from the right provider? You need a guide to know what to expect, and what to look for as you evaluate potential privileged account security solutions. To help you make informed decisions, the following are seven questions to ask every potential vendor as part of your assessment.



# 1. Is the solution really secure?

Privileged account security solutions store some of your organization's most sensitive assets – the credentials needed to access IT infrastructure, business critical systems, intellectual property, financial information, audit data and more. Before trusting a vendor to protect this information, it's important to verify that the solution itself is secure and capable of protecting these sensitive assets. Not only must the infrastructure be able to stand up against attacks, but the solution should also support flexible credential and access control policies to meet your organization's specific security requirements.

When assessing the security strength of various privileged account security solutions, here are several important questions to ask each potential provider about their offering:

## Security Checklist

- Does it employ multiple built-in layers of security to protect privileged credentials?
- Does it provide tamper-proof audit logs and session recordings for audit integrity?
- Does it support role-based access controls and segregation of duties to ensure that only authorized users may see and access their needed accounts?
- Does it support automated workflows for credential access approval including dual controls and integration with helpdesk ticketing systems?
- Does it include automated, flexible credential management policies, spanning aging, complexity, versioning and archiving?
- Does the vendor offer out-of-the-box support for multi-factor authentication systems?
- Does it provide the flexibility to easily enforce granular policies for specific compliance or business unit requirements?

## Seven Critical Layers of Protection

Highly effective privileged account security solutions should employ multiple, built-in layers of security, including:

### Hierarchical Encryption

Secure data at rest by uniquely encrypting each piece of data as well as each tier of data

### Session Encryption

Secure data in transit by using a built-in VPN

### Authentication

Support a variety of authentication methods to assure the identity of users

### Built-in Firewall

Reduce the attack surface by only permitting certain traffic into a vault

### Segregation of Duties

Ensure users are only able to see and access data unique to their specific roles

### Tamper-Proof Auditability

Store all audit data in a secure, access-controlled location, available to only authorized security admins and auditors

### Comprehensive Monitoring

Monitor all system and security event data associated with the privileged account security solution

## 2. Can it find and protect all of my accounts?

A typical enterprise organization has at least 3 to 4 times as many privileged accounts as employees. These privileged accounts exist in every piece of hardware and software throughout the network, and are accessed by privileged users, applications, scripts and automated business processes. Gaining full situational awareness of all of these privileged accounts presents a significant challenge to IT departments. Compounding the problem is a specific class of privileged accounts: application accounts. These are highly sought after and often exploited by cyber attackers when left unprotected. However, properly securing application account credentials is often difficult, time-consuming and cost-prohibitive.

An effective privileged account security solution must be able to protect access – by securing, managing and routinely rotating credentials – to all privileged user and application accounts on-premises or in the cloud, and across operating systems, databases, applications, hypervisors, network devices and more.

However, before you can start protecting privileged user and application accounts, you must first be able to find them, which can be incredibly difficult. So how do you find them first, in order to effectively protect them?

A good solution should help you discover and inventory privileged accounts throughout your IT environment. The most effective way to gain a comprehensive inventory of privileged accounts is to use a tool specifically designed to scan your environment to find privileged user and application accounts and associated credentials. This way, you'll have access to a comprehensive report outlining privileged accounts, credentials and account statuses with regards to company security policy. With this report, you have a view of privileged accounts accessed by internal and external users, such as third-party vendors or contractors, and can start developing a plan to secure, manage and track the use of all these privileged accounts.



**Companies typically have at least 3x to 4x as many privileged accounts as employees.**

### 3. Can it protect all credentials?

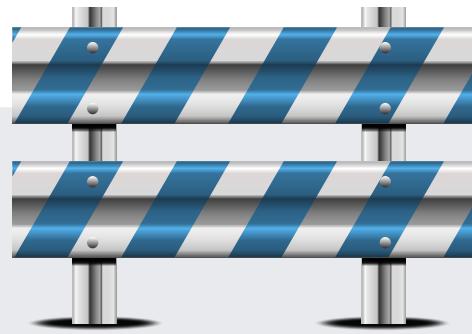
When security teams think about privileged credentials, they usually think about privileged passwords, which present a multitude of issues for security teams. Passwords are often written down or saved by end-users, shared between end-users, or hard-coded or locally stored in plain text by applications, leaving them unprotected and vulnerable. Using compromised privileged passwords, attackers can roam the network freely, accessing sensitive information and evading sophisticated intrusion detection systems.

***The most effective password management solutions will take users out of the equation completely by taking a two-pronged approach:***



#### **Compartmentalized Storage:**

Imagine a series of bank vaults. Each vault contains a collection of user-defined 'safes' where access is limited to a user or group. This architecture allows each user or group to manage their own passwords without giving unwanted access to other parties within the organization.



#### **Limited Exposure:**

Rotating passwords after each use ensures that passwords won't work beyond their initial use, thus making stolen credentials useless to a potential attacker. In addition, organizations can opt to connect the credential management system directly with devices and applications so that the user never sees, copies or enters a password, and the end user's device never knows or caches the credential.

## Can it protect all credentials? (continued)

Yet passwords are only part of the equation. The traditional view of privileged credentials overlooks SSH keys, which commonly provide users and applications with privileged access to Unix accounts.

An end-to-end privileged account security strategy must treat SSH keys as the privileged credentials they truly are. A comprehensive strategy should include key discovery, to understand which users and applications have access to which systems; secure key storage, to remove private keys from endpoints and enforce access controls; and proactive key rotation, so that no private key may be

used as a permanent backdoor. However, it doesn't stop there. Due to the privileged access provided by SSH keys, a comprehensive solution must also include session monitoring to ensure that SSH keys are not misused or abused and threat analytics to rapidly detect and alert on the anomalous use of authorized SSH keys, which could potentially signal an attack in progress.

A comprehensive privileged account security solution will enable your organization to securely store all types of privileged credentials and conceal them from end users to reduce the risk of losing them to the wrong hands.

### The average large enterprise can have ONE MILLION SSH keys in their environment.

*That's one million opportunities to steal your sensitive data*

 64%

have not established security policies for SSH keys

 51%

have suffered SSH key-related compromises

 53%

have no centralized control over SSH keys

46%

never change or rotate SSH keys – and they **never expire**

60%

have no way to detect new keys introduced in the organization

74%

allow administrators to **independently control** and manage SSH keys

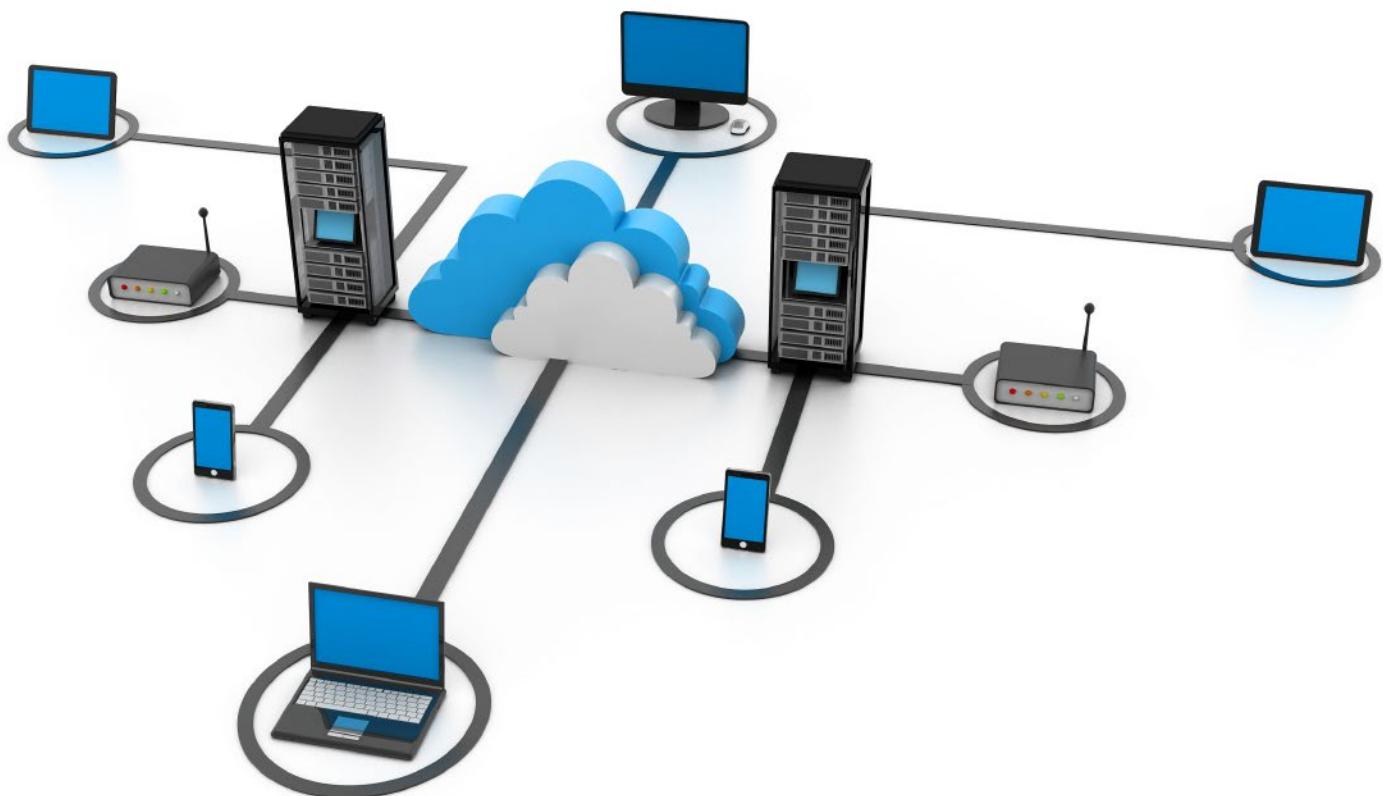
10%

of all SSH keys provide **root access**

## 4. Will it work in my environment?

Your IT environment is unique, tailored to your organization's specific requirements. Be sure that any solution you consider can protect accounts throughout most – if not all – of your IT environment. Any privileged account security solution that can only protect accounts on a limited number of platforms will ultimately leave parts of your environment vulnerable to attacks and require additional investments to cover these gaps. Select solutions that can protect access to a wide variety of accounts across multiple platforms, including but not limited to Windows systems, Unix/Linux systems, mainframes, virtual environments, databases, security appliances, network devices and applications.

Also be sure to seek out solutions that are architected for minimal impact and enable you to extract more value from your existing investments and infrastructure. An optimal privileged account security solution should be able to easily integrate with complementary technologies including Security Incident and Event Management, Identity and Access Management, IT Ticketing Systems and Strong Authentication. Out-of-the-box integrations with such complementary solutions can help you maximize the value of your IT investments, streamline the deployment process and ensure consistent privileged access policies across the entire organization.



# 5. What protections are provided?

To strengthen security and comply with regulatory requirements, it's important to establish an end-to-end lifecycle approach to privileged account management that can be augmented over time and adapt to your organization's changing needs and priorities.

## An end-to-end solution should include the ability to:



**Discover privileged accounts** and credentials, including passwords and SSH keys, to map trust relationships between users and systems and create a plan for securing privileged accounts.



**Monitor and record user activity** during privileged sessions to deter authorized users from misusing privileges and help security teams detect suspicious session activity that could indicate an attack is in progress.



**Proactively protect privileged account credentials** by storing them in a secure, centralized repository that supports strong access controls.



**Isolate privileged sessions** to prevent the spread of malware from user endpoints to critical systems, as well as prevent both users and their devices from ever being exposed to privileged account credentials.



**Enforce access controls** to ensure that only the right users are able to access – or request access to – authorized credentials for true business purposes.



**Enforce least-privileges** to ensure that users have the privileges necessary to do their jobs, but no more.



**Automatically rotate passwords and SSH keys** to strengthen security without over burdening the IT team.



**Remove plain-text application credentials**, such as embedded passwords and locally stored SSH keys, and instead store them in a highly secure, highly available vault.



**Monitor access to privileged accounts** and require users to “check-out” shared account credentials to establish individual accountability over shared accounts and gain a more comprehensive audit trail.



**Leverage behavioral analytics** to detect suspicious user and account activity that could indicate a compromised privileged account.

## 6. How can I minimize the cost of managing it?

A complete end-to-end privileged account security solution requires multiple products to secure, manage, control and monitor privileged accounts, as well as detect active threats. As a result, organizations can be faced with the challenge of integrating and managing multiple solutions in order to achieve maximum protection. A good solution should help you avoid:



**Costly Integrations.** Integrating multiple products from one vendor or many vendors can be expensive due to professional services and custom engineering costs.



**Inefficient Management.** The task of managing separate products through individual interfaces is time-consuming and resource intensive for IT and security teams.



**Inconsistent Reporting.** Compiling reports from several different products leads to inaccuracies and incomplete data. Cumbersome reporting leads to time-consuming and expensive audit processes.



**Inconsistent Policies.** Managing policies in separate systems can lead to potential inconsistencies and conflicts.

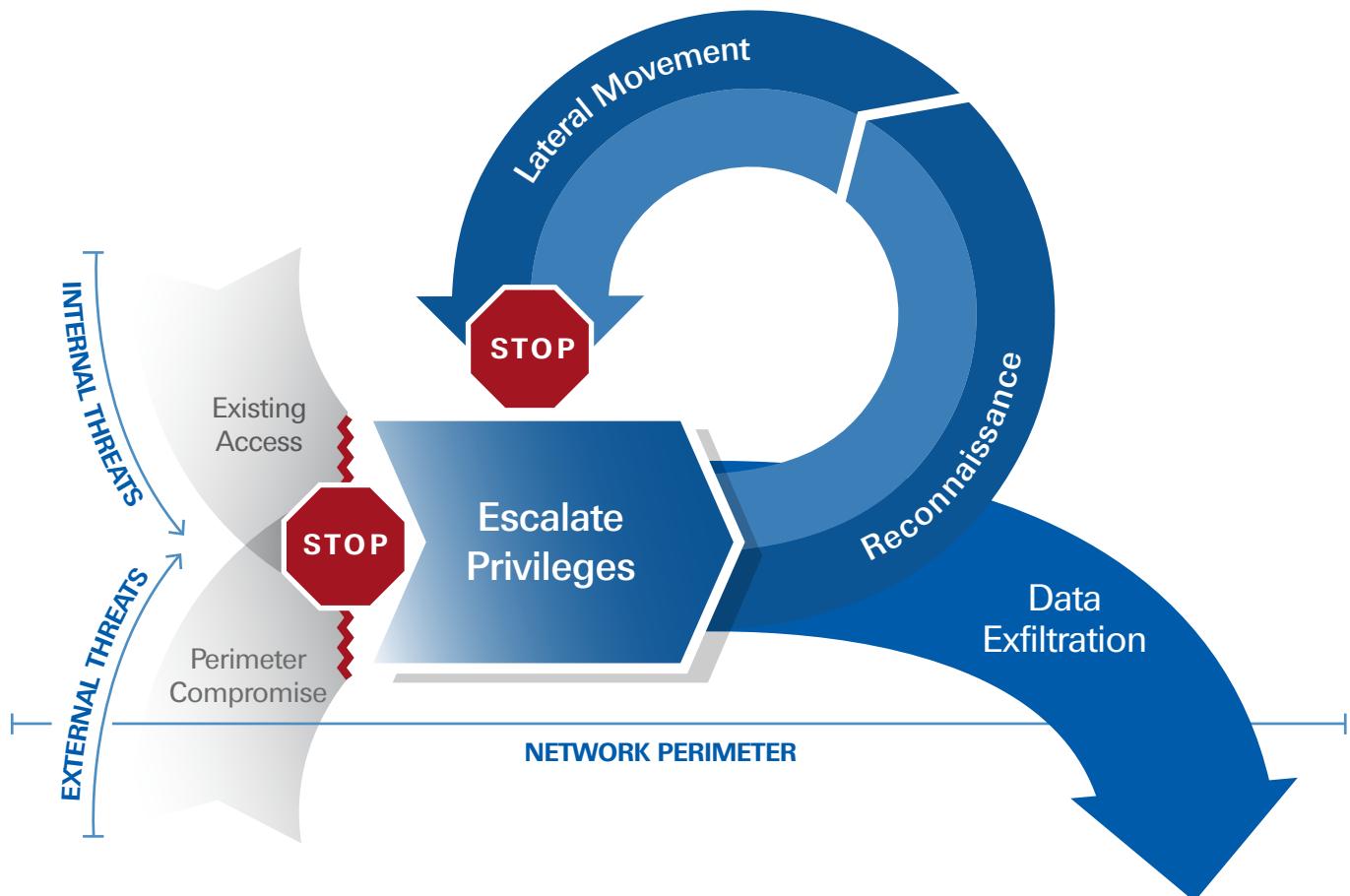
To help streamline deployment and management and lower the total cost of ownership, look for solutions that are built on a single platform, managed from a unified interface, and enable you to utilize multiple products for a comprehensive solution. Also ensure that the platform integrates with all IT environments – on-premises, cloud or OT/SCADA – and can scale out over time based on your needs.

**Single platform = streamlined deployment + management = lower TCO**

## 7. How reliable is the vendor?

The only way to effectively break the attack chain is to proactively prevent attackers from gaining the elevated administrative privileges needed to reach – and steal – sensitive data inside your organization. That's why it's critical to ensure that any potential vendor treats privileged account security as its primary, strategic focus.

The provider's commitment to on-going innovation on this front is equally important. Consider each vendor's focus on building new, complementary threat detection and network monitoring tools to help you find and respond to attacks against your organization's privileged accounts.



# Conclusion

---

Privileged accounts are everywhere. Attack targets and potential security breaches are everywhere. You could piece together a series of privileged account solutions in an attempt to construct an effective defense, then work to connect them, crossing platforms, adjusting settings, and managing them simultaneously. All in the hope that something doesn't slip through the cracks and end up costing you more than you could have imagined.

Or, you could protect all of your privileged accounts, everywhere, with one integrated, privileged account security solution, from one, proven provider who maintains laser-focus on securing enterprises against cyber attacks that take cover behind insider privileges and target critical enterprise assets.

How are **you** protecting what matters most?





To learn more about how CyberArk can help you address your privileged account security challenges, visit [CyberArk.com](http://CyberArk.com).



Sources:

- [www.aberdeen.com/research/9166/RR-SSH.aspx/content.aspx](http://www.aberdeen.com/research/9166/RR-SSH.aspx/content.aspx)
- [www.computerworld.com/article/2488012/malware-vulnerabilities/poorly-managed-ssh-keys-pose-serious-risks-for-most-companies.html](http://www.computerworld.com/article/2488012/malware-vulnerabilities/poorly-managed-ssh-keys-pose-serious-risks-for-most-companies.html)
- [www.cyberark.com/threat-report/](http://www.cyberark.com/threat-report/)
- [www.datacenterjournal.com/it/data-centers-secure-primer-secure-shell-key-mismanagement-risks/](http://www.datacenterjournal.com/it/data-centers-secure-primer-secure-shell-key-mismanagement-risks/)
- [www.isaca.org/Education/Conferences/Documents/NAISRM-2013-Presentations/244.pdf](http://www.isaca.org/Education/Conferences/Documents/NAISRM-2013-Presentations/244.pdf)
- [www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf](http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf)

