SSH.COM

WHITE PAPER

Why Unmanaged SSH Keys Will Make You Fail Your Audit

The 14 Critical Areas Where Auditors Will Assess Your IT Security Compliance with SSH.

Contents

In a hurry? Just browse the above list & skip to Page 20

Introduction

Yes, you can fail an audit because of unmanaged SSH keys & yes, you almost certainly have them

Fact: enterprise usage of SSH keys is extremely common.

If you are a modern enterprise, you are almost certainly using SSH – even if you don't know it. The Secure Shell (or SSH) is essentially the de facto choice for granting secure access to and from servers, and between servers (i.e. M2M connections). It is also used in nearly every network environment for secure remote administration and file transfers.

If you're in the cloud at all, you're most likely using SSH keys

According to an IBM study, 85% of enterprises already operate multi-cloud networks since 2018, while 98% of enterprises are expected to use multiple hybrid clouds by 2021. Keep in mind that cloud services would include IaaS, PaaS, and many (if not all) SaaS solutions.

Further indicators of unmanaged SSH keys in your enterprise:

1. Do you use Linux, Unix, or Unix-like OS's in your tech landscape?
2. Have you been operating for more than 10 years?
3. Do you utilize or operate a data center?
4. Are you using machine-to-machine (M2M) connections?
5. Do you use secure file transfer (SFTP) or remote access?
6. Do your vendors or contractors use any of the above?

Since you're almost certainy using SSH, you must have SSH keys.

Therein lies the problem, especially if you're not 100% certain about your organizational SSH usage. The SSH protocol is so easy, convenient, and highly secure when used properly – it really should be no surprise that we consistently find enterprises (or more specifically IT departments) creating and distributing SSH keys like candy.

Then once we find those SSH keys, we usually discover that around 90% of those keys are unused, orphaned, and/or unmanaged. The number of SSH keys we discover typically ranges from the hundreds-of-thousands, to multiple millions
– all capable of granting instant access to your (otherwise) secured servers.

Even worse, many enterprises have been accumulating SSH keys for 10+ years, without any controls or management policies.

All of which is exactly why auditors know tocheck specifically for this issue.

> **If you're not 100% sure of your SSH key status - ask the experts to help you find out.**
>
> SSH Auditing and Risk Assessment services are considerably more economical options compared to regulatory censures & fines.

"So why should I *really* care about SSH key management?"

From an audit standpoint, the risk is obvious.

You will fail – and then you'll have to fix it anyway. Likely at greater expense and hassle, certainly with a lot more scrutiny.

This special report will examine the more important reasons why, including which specific areas that auditors will fail you.

Relevant Regulatory Requirements

SSH Key Management is in the scope of the following standards:

- Basel II and III
- EU Cybersecurity Act*
- FISMA
- GDPR
- HIPAA
- NERC-CIP
- PCI-DSS
- Sarbanes-Oxley (SOX)

*currently voluntary, may eventually become mandatory

Good to Know

Universal SSH Key Manager® (UKM) can generate readily configured policies based on SOX, HIPAA, NIST, SANS CIS and PCI-DSS standards. Once configured, UKM can automatically determine which SSH keys are in violation, so admins can take

Recommendation

Following any of the IT security frameworks listed here – should help you meet all your audit and compliance requirements. Universal SSH Key Manager® (UKM), would also help facilitate this process.

IT Security Frameworks that cover SSH Key Compliance:

- FEDRAMP
- Fips 140 / 199 / 200
- ISACA SSH Guide
- ISO/IEC 27001
- NIST 7966 / 800-53
- NIST Cybersecurity Framework
- SANS CIS
- SSAE-16

The 14 Specific Areas Where IT Auditors Will Fail You

The following section will cover:

- The common areas (or categories) of compliance affected by organizational use of unmanaged SSH keys.
- Why auditors will penalize you for incompliance in this area.
- What can be done to address the issue, or at least an idea of where to look for solutions.

Important:

Each specific regulatory framework uses their own specific terms, definitions, and criteria for compliance. However, they will generally all cover the same topics and issues. This means you can be penalized for a compliance issue described in this report, even though the specific regulation calls it (or argues incompliance) by a different name.

Disclaimer:

We have included most of the common regulatory standards that enterprises have to worry about. The purpose is to point you in the right direction for compliance issues regarding SSH keys only. It is outside the purview of this report, to provide all the needed in-depth advice and specifics to help you pass your audit. This report is provided as a general guideline only and should be treated as a starting point for further action.

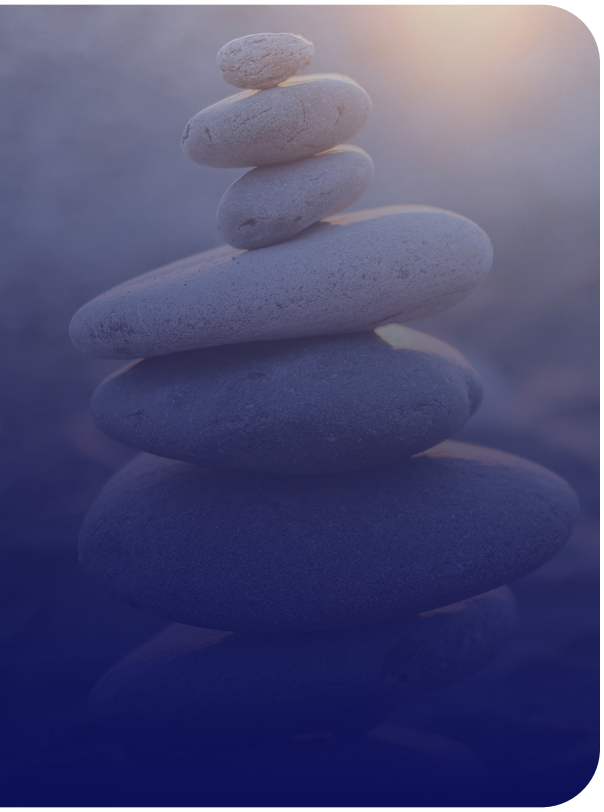
We highly recommend seeking expert help and advice, in order to ensure compliance with any regulatory requirements audit(s) affecting your enterprise.

1 Inadequate or Non-Existent IT Security Policy for Usage of SSH Keys

A security policy for use of SSH within your organization is expected, and should be part of your overall Corporate Security Policy. It is a point that auditors will look for, because SSH belongs to a class of encryption software that includes cryptographic key management.

For example – this class includes VPNs, encrypted email, secure messaging, IPsec, HTTPS, as well as SSH and SSH derived standards, such as SCP and SFTP (which you're probably using, right?). Since you almost certainly using some form of encryption in your enterprise (and if you're not, you may have bigger audit problems coming up) so SSH needs to be included among this list.

Now if SSH is being used in your organization, your policy needs to reflect its usage. It's mandatory. If you are aiming to get an exception to this point, then the usage exceptions still need to be documented, especially if they are not in-line with your overall policy (and this question will be asked). There is no real easy way around it, and you cannot ignore it without serious risk.



Recommendation:

Address SSH specifically within your IT security guidance, procedures, and/or technical standards. You first need to assess how SSH is used within your organization, and then determine whether it's in-line with your existing policy – and document accordingly.

How SSH Key Management helps you:

Solutions like Universal SSH Key Manager® (UKM) are designed to help enterprises understand the true use of SSH within their technical environment. UKM then also provides you with tools to define and set policies for managing SSH keys to required standard.

2 Inadequate Identity and Access Management Controls

SSH is considered a secured or privileged access method, which means it is a part of (or should be) any IAM control policy used by your organization. For example, it is used for practically all administrative connections to servers, routers, firewalls, and other networked devices.

SSH keys are also considered login and authentication credentials. So all the processes and protections required by standards such as FISMA or PCI-DSS for such credentials, are applicable to SSH user keys. It's required, and really for good reason.

If someone were to compromise just one SSH key (among the millions found in a typical enterprise), this can be used relatively easily to penetrate your network. Furthermore, it is then possible to move freely across said network without detection, under the guise of an encrypted connection. In the worst case, an attacker can use this key to create hard-to-notice backdoors into your systems, that bypass your privileged access control solutions.

For these reasons, it is paramount to secure your SSH keys and bring them into your control

Recommendation:

An SSH audit and/or vulnerability assessment, using a lightweight scanning and reporting tool – should provide you with all the actionable information you need. At least, it would provide you with a broad-scope indication of your true SSH usage.

How SSH Key Management helps you:

Any deployment of an SSH Key management solution (such as UKM) should provide a risk assessment, usage analysis, and key discovery phase. After these initial phases, it then becomes possible to take control of your SSH keys.

3 Inadequate Auditability and Traceability Capabilities

If you have no visibility or control over your unmanaged SSH keys, then how can you possibly audit them for appropriate use, or trace their usage across your network? The short answer: you can't. Auditors will of course know this, which is exactly why they'll ask you this question.

Anyone in possession of a private SSH user key, will have access to accounts / systems / processes with the corresponding public key. Tracking and controlling distribution of these keys is thus a basic and critical security requirement.

Since SSH keys also never expire, a key created years ago, by an admin who has long since left the company is still an open security risk waiting to be exploited.

Case: Equifax 2017

One of the 'big 3' consumer credit reporting agencies, was breached by hackers using compromised SSH keys. Over 140 million accounts were affected, resulting in hundreds of lawsuits and a $575 million settlement with the FTC.

The breach went undetected for months, and it took many more months for Equifax to figure out the scope of the breach and what data was compromised.

Recommendation:

Consider using an SSH key management solution that enables tracking and tracing of SSH keys as they are created and distributed by users. Any solution should be able to provide this basic functionality, on top of discovering older or currently active keys.

How SSH Key Management helps you:

UKM goes further than many comparable solutions, by providing admins with syslog data for any SSH keys being used on the network. Additionally, you can gain the ability to identify and match user accounts to any keys they generate.

4 Inadequate Inventory of Authorized, Secured, or Privileged Assets

Since SSH keys are by design a privileged access credential, they fall under the purview of many regulatory standards. There is really no way around this. At minimum, an inventory of all relevant SSH keys will be required by auditors as proof of compliance.

Recommendation:

Consider performing an SSH key audit or using an SSH key discovery tool, to find any keys floating around your technology landscape (whether active or inactive).

How SSH Key Management helps you:

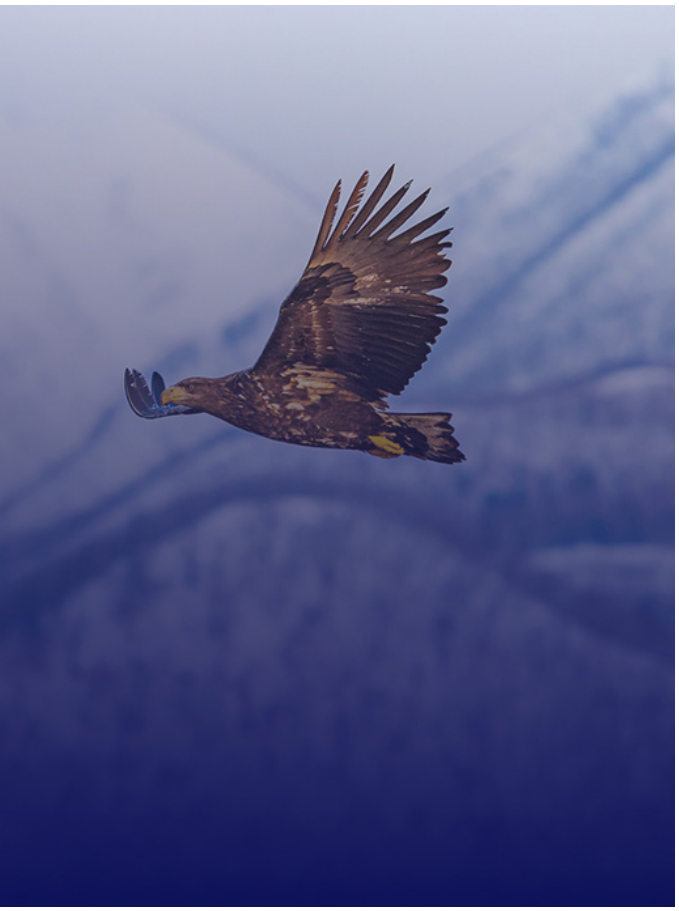
Solutions like Universal SSH Key Manager® (UKM), by design, must create an inventory of SSH keys in order to perform the 'management' part of their capabilities.

5 Inadequate or Non-Existent Assignment of Ownership and Accountability

One of the most common issues enterprises face with SSH keys, is that 'no one' has any idea who is responsible for them. Partially this is because SSH is so useful and convenient, that admins and users would simply create and distribute SSH keys as needed. The other part is that many organizations simply did not think of creating this assignment.

Put simply, who is responsible for keeping track of SSH key inventory and usage? Who makes sure that the usage is appropriate and in-line with IT security policy? Once that person is named, are they aware of their roles, duties, and responsibilities?

These are basic questions that your auditor will ask you.



Recommendation:

Consider performing an SSH key audit or using an SSH key discovery tool, to find any keys floating around your technology landscape (whether active or inactive).

How SSH Key Management helps you:

Solutions like UKM, by design, must create an inventory of SSH keys in order to perform the 'management' part of their capabilities.

6 Inability to Track and/or Revoke Access

SSH keys (which can grant privileged access, remember?) can be generated and distributed in an instant. SSH keys also never expire, which often means they are quickly forgotten, and therefore never revoked. See the problem? Your auditors do as well.

This is also one of the fundamental reasons for SSH key management as an organization security process. If your keys are unmanaged, you simply cannot know where they are, or what they're doing, or who's doing it. Furthermore, it is impossible to revoke that privileged access, if you don't know whether the key even exists in the first place.

Recommendation:

Consider using an SSH key management solution, as this is a core feature. First to discover where all your keys are located, and secondly to map out all the trust relationships for those keys. It is then possible to determine what subset of these keys can be safely revoked WITHOUT causing an unplanned service disruption / outage.

How SSH Key Management helps you:

Solutions like UKM go a step further, by utilizing an 'intelligent directory discovery' process, which automatically identifies where active (and forgotten but potentially active) keys reside in your system. Meaning you don't have to know that directory from the start. You also shouldn't be fooled by raw numbers, as SSH keys can only work (i.e. be a threat), if they reside in a folder that is actually being used by your SSH client / server.

7 Lack of Proper Segregation of Duties and Change Transparency

Put plainly, if you don't have an SSH key management solution, or any sort of SSH key management policy – and you're just now thinking of assigning responsibility for SSH-related processes. Then you certainly won't meet the requirement for segregation of duties. Let alone the requirements for change transparency.

The major concern in this area, is the ability for one person to 'abuse their powers'. Since SSH keys can provide encrypted access to most (if not all) your critical systems, it makes sense to have some internal oversight or auditing function i.e. to make sure inappropriate usage can be identified and reported.

Similarly, any changes to your SSH processes should be recorded, and some form of authorization function, should be described in the SSH section of your overall IT Security policy.

Case: Citibank 2013

A disgruntled Citibank employee, after a poor performance review, managed to take down 90% of Citibank's networks across North America. All by transmitting one command, using an SSH key, to 10 core Global Control Center routers. The attack took under 2 minutes to execute.

Recommendation:

Consider defining an authorization function, and integrating this into your overall SSH management policy. The SSH management function should also be divided into multiple roles, for example administration and oversight, as best suited to your requirements.

How SSH Key Management helps you:

A good SSH Key Management solution, should include some form of syslog reporting – which can then be configured according to your IT security policy. A proper configuration should provide timely reports and alerts, which can then be easily made available to appropriate oversight and management roles.

8 Lack of Assured Protection for Private, Sensitive, and/or Personal Data

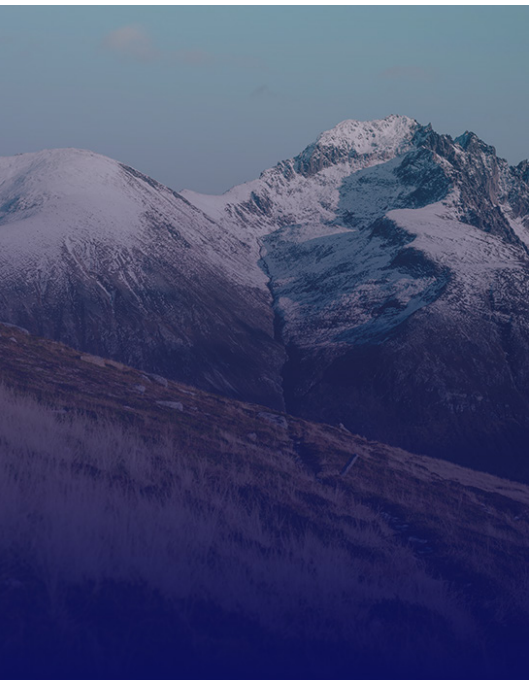
Regulatory standards like HIPAA and GDPR etc. focus heavily on data privacy issues, so they pay special attention to the protection of private data. Other standards like PCI-DSS care a great deal that sensitive data (like credit card information) is suitably protected. All standards in some shape or form, care about data protection.

In other words, the auditor needs to be assured that all appropriate actions are taken to secure such data. Since SSH is considered a vulnerable access point (if left unmanaged) – the auditor is likely to be very interested in your SSH management policies, as part of your larger Data Protection Policy i.e. it doesn't matter how strong (or secure) the tunnel is, if you leave the entrance wide open.

Case: Anthem Inc. 2015

The Anthem medical data breach of 2015 involved 80 million company records, 'and almost 40 million customers who may now have identity theft problems for the rest of their lives.

The case was settled in 2017 for $115 million, while their lawyers got $31 million. All because of poor SSH policy.



Recommendation:

Consider explicitly defining and incorporating SSH into your data protection procedures, in the same section that discusses password and privileged access policies. Also consider using an SSH key management tool to complete your inventory of your access credentials. You should also define policies for key rotation and revocation, as you would your password policy

How SSH Key Management helps you:

Solutions like Universal SSH Key Manager® (UKM) enable you to discover and inventory SSH keys throughout your technology landscape. You can also define data protection policies at the top-level, and bring your SSH key usage in-line with this policy. Policy enforcement can then be automated, and inappropriate usage can be reported and/or blocked as appropriate.

9 Lack of Governance Procedures, Frameworks, and Policies for SSH Usage

As we'd hope is abundantly clear by now, SSH key management needs to be included within your overall Corporate Security Policy (e.g. Basel and SOX are especially stringent). In many cases, being 'aware' of the issue is not enough – you also must have a plan of action for addressing it, and this means having a procedure or framework for it.

The first point of contention will of course be whether any policy exists at all. If it doesn't, then you'll need to have one ASAP. Having procedures and frameworks in place to deal with SSH can be argued, for example, whether they are complete or robust enough to meet the specific requirements.

Case: JP Morgan Chase 2014

Attackers exploited the lack of good SSH key practices at JP Morgan Chase Bank, in order to break into their systems and steal data affecting 2 out of 3 US households.

The attackers attempted to target 9 other financial institutions, but only JP Morgan Chase was breached.

Recommendation:

Consider using an existing framework for SSH usage, or a best practices guideline published by a reputable body. Your choices include the ISACA SSH Practitioner Guide or NIST 7966/SP 800-53r4 specification. Frameworks like ISO/IEC 27001, COBIT, and SANS CIS also contain more generally applicable guidelines which include SSH-relevant recommendations.

How SSH Key Management helps you:

If/when you are being audited – having a solution like Universal SSH Key Manager® (UKM), either in place or 'soon to be implemented', goes a long way to assuring the auditor that any incompliant SSH issues are being suitably addressed. At the minimum, it should buy you some time and/or breathing room to comply, without risking a failed audit or audit censure.

10 Failure to Properly Manage Secured Access for Third-Party Services

A point sometimes forgotten (except by auditors) is that compliant security policies also need to include third parties like consultants, contractors, and vendors. What more often happens when an organization discovers SSH-based vulnerabilities within their organization, is that the third-parties are forgotten in the uproar or rush to bring SSH in-line with an otherwise compliant policy.

Does your cloud service provider introduce SSH vulnerabilities outside your notice? What about your SaaS-service providers? What about the temp worker who is only coming in for three weeks to fix something? What about that third-party IT support service? All of them can, and often do, use SSH-based access and authentication to do their jobs and/ or provide their service. It's normal.

Case: Apache 2017

The main site of the Apache Software Foundation was compromised using an SSH key from a 3rd party hosting provider.

Most ASF services were taken offline as a result, and the incident led to concerns about the integrity of the Apache Web Server.

Recommendation:

Just remember that after you (and your team) puts in all the effort of developing a compliant SSH policy, that the usage policy for third-parties is not forgotten in the mix.

How SSH Key Management helps you:

Third-party coverage is (or should be) included in a dedicated solution. Our product, UKM, certainly does. It can identify when external SSH keys attempt to access your internal resources, and the same already defined policies (once configured) are readily applied to any access requests – whether they come from an internal or external source.

Case: NordVPN 2018

NordVPN was unknowingly breached due to an errant 3rd party SSH key, and this situation was undiscovered for over a year.

The company only found out about it when 'someone' dumped a full SSH session (including configuration files, private keys, session details etc.) from one of their servers onto 8chan.

11 Lack of Assured Protection for Private, Sensitive, and/or Personal Data

The key word for this compliance requirement is 'periodically' i.e. that all security policies and procedures are regularly reviewed and updated, to account for new developments. It's a basic and well-known audit requirement, and pretty much all standards like FISMA, PCI-DSS, and NERC-CIP etc. are tough on this requirement.

Your auditor may argue, that by not having an SSH policy, when it is a known (and critical) security risk – means that you're not periodically reviewing new security threats. This is more likely to be an additional check mark against you. But it could be the very thing that pushes you over the warning line, all the way to the failure line. So why risk it?

Case: Marriott Hotels 2018

After acquiring another hotel chain, their 'old and unreviewed' reservation system was compromised with the aid of SSH keys. These keys stored on the same server as the encrypted database, and over 500 million guest records were stolen, including credit card information and passport numbers. Ultimately Marriot had to pay the price for this breach.

Recommendation:

Consider making SSH key policy a part of your regular IT security policy review process. As long as it is 'part of the list', then this should be enough for most cases – though you'd make a much stronger case by incorporating other SSH related topics mentioned here.

How SSH Key Management helps you:

Using a solution like Universal SSH Key Manager® (UKM), would certainly help show the auditor that you take SSH key security seriously. However, you still need to include SSH as part of yout periodical review of IT security policies to prove compliance.

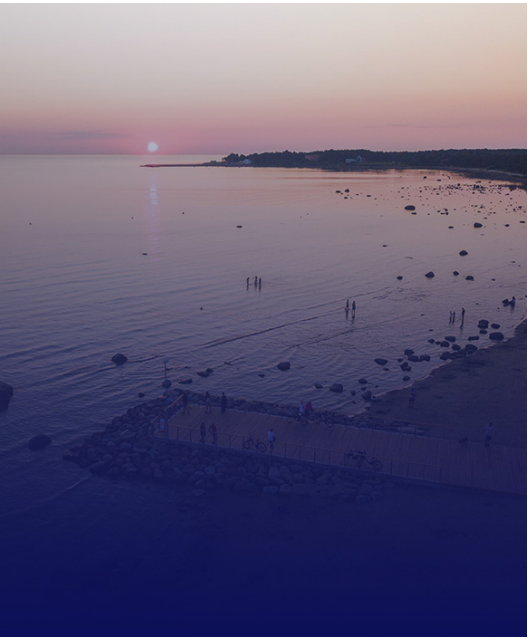
12 Failure to Properly Manage (or Harden) Configurations

Hardening is essentially reducing the vulnerable 'attack surface' of your network. One of the main methods of accomplishing this, is by appropriately configuring your software to remove easy vulnerabilities. For example, using encryption when possible, requiring strong passwords, and changing default settings etc. Naturally your corporate policy should document these processes.

SSH is considered a serious attack vector by auditors, because anyone who finds the 'right' SSH key, will be able to access your systems as a privileged user. Since SSH keys never expire, the issue is compounded by older keys that were 'used once and then forgotten'. Hence the need to bring SSH configurations in-line with your corporate IT policy on software configurations.

Case: Sony Pictures 2014

A hacker group obtained dozens of SSH private keys, and used them to steal private data and install malware. This included a listening implant, backdoor, proxy tool, data wiping tool, and target cleaning tool. They did this for months undetected. The hack provoked a response from the US government, including 'proportional military response' to the alleged state actor.



Recommendation:

Review your documentation to ensure your configuration standards are reflective of your security goals for SSH usage. Also consider using automated tools to report upon inappropriate configurations e.g. unmanaged and legacy SSH

How SSH Key Management helps you:

Solutions like Universal SSH Key Manager® (UKM) can be configured to determine, report-on, and enforce your security policies upon SSH keys in your tech environment – both current and historical. Once these configurations are defined and set according to policy, much of the process can be automated.

13 Failure to Assure Continuous Compliance

Auditors are not only interested in assurance that you comply today, but also that you have taken reasonable steps to comply in the future.

This is where having a dedicated SSH key management solution really shines, as there is no better way of assuring this key point.

Recommendation:

Consider making SSH key management a standard part of your security practices, and make sure to continually review your compliance position while maintaining secure systems. Alternately, you could consider utilizing a dedicated SSH key management solution, to gain the right tools right away and simplify the whole process.

How SSH Key Management helps you:

Solutions like UKM should make it easier to comply on a long-term basis. SSH Communications in particular, participates in defining the standards and best practices of SSH usage in enterprises and regulated industries. Accordingly, we make sure that our UKM product is always on point with any changes to compliance standards. Or at least, provide the flexibility in configuration so that changes can be created and deployed reasonably easily.

Case: Heartland 2008

Lack of SSH Compliance had a key role to play in one of the most expensive data breaches in history. Their payment systems customers lost close to $200 million, while costs to Heartland were estimated at $140 million.

The breach went undetected for almost a year.

Case: Yahoo 2014

Lack of SSH key management had a critical role to play in the “largest data breach ever”, as suffered by Yahoo in 2013-2014, yet it was only discovered by the company in 2016. All of their 3+ billion user accounts were affected.

Yahoo ended up settling the class action lawsuit for $117.5 million in 2019.

14 Failure to Sufficiently Protect Critical Systems

This is probably the most critical point where an auditor fault you, especially if you have no SSH management policy at all. Standards like NERC-CIP and PCI-DSS are especially strict on this. Since SSH is so ubiquitous in cloud and data center environments, it is very likely that many (if not all) your most critical systems depend on SSH connections to function. This is especially true for machine-to-machine (M2M) connections.

Therefore, if someone were to compromise just one SSH key to a critical system, this means they can establish a privileged (trusted) AND encrypted (obfuscated) connection to that critical server. Then it would be a trivial matter to break that connection (service disruption) and/ or steal data (data breach) – and in the worst cases, the attacker could establish permanent hidden backdoors (security compromise) or takedown your whole network (complete service disruption).

Recommendation:

Strongly consider running an SSH audit and/or SSH risk assessment of your technology landscape, to make absolutely sure you have sufficient visibility and understanding of how (and where) SSH is being used in your company. Only then can you really make an informed decision about the best way to proceed with this knowledge.

How SSH Key Management helps you:

Products like UKM give you visibility into your true SSH key landscape, while providing you with all the tools needed to effectively manage SSH keys. Our company helps define the best practices and evaluation criteria used by regulatory bodies, and we have built our product according to these exact concepts. For example, UKM can readily generate configured policies based on SOX, HIPAA, NIST, SANS CIS and PCI-DSS standards.

Conclusion

Out of sight, is NOT out of mind

We hope that it is clear from looking at the complete list of audit areas, that unmanaged SSH keys are a real security concern, and that auditors have valid reasons for considering them as such.

Therefore, your organizational ability to manage SSH keys, does in fact, have a tremendous impact on wether you pass or fail your next audit.

Please keep in mind, we're not saying this as a scare tactic or hyperbole – but to demonstrate how auditors might think about your IT security compliance, by leaving your SSH keys unmanaged.

Since the risk exists, and is well-known in cybersecurity circles, it must therefore be addressed and mitigated. It's as simple as that. Out of sight does NOT equal out of mind – not in the eyes of your auditor at least.

Luckily, many of these points can be addressed with relatively few fixes

The most important takeaway

While security breaches involving unmanaged SSH keys may be relatively rare, they do happen, and when they do – they are often record-breakingly bad.

Recommendations

Depending on your situation and/or starting point with SSH key management – the corresponding step is recommended as shown below.

SITUATION	SOLUTION
You don't really know if you're using SSH keys somewhere in your organization.	Ask us for help.
You're unconvinced whether an SSH key issue really exists in your organization, but you want your IT team to stop bothering you about it.	Get an SSH Risk Assessment.
You're sure you have unmanaged SSH keys, but not sure of the scale, complexity, or risk.	Get an SSH Risk Assessment.
You're now convinced that you'll fail your audit due to lack of SSH Key Management.	Get a proper SSH Key Manager like UKM.
You don't want to risk failing an audit, because that's a bigger pain than dealing with getting your SSH keys under control.	Get a proper SSH Key Manager like UKM.
You just want to solve this ASAP.	Get Universal SSH Key Manager® (UKM).

Now a few 'famous last words' to consider:

"We'll just take care of it all ourselves. Surely it can't be that hard!"
Sure buddy. We'll see you in two years then!

"Well we found someone to do it cheaper. It's part of a package!"
Sure buddy. We'll see you in three to five years then!

Our Solutions

Products & professional services

SSH Risk Assessment

SSH Risk Assessment will help you determine where you are incompliant in your chosen regulatory standard, as well as identifying IT security vulnerabilities.

The Risk Assessment Report will include (but not limited to) information such as:

- All information supplied in the Audit, plus...
- SSH Key Usage Analysis (using data from syslog import).
- SSH Login Analysis e.g. login methods & successful/failed access attempts.
- SSH Key Compliance Analysis e.g. against NIST, SOX, etc. as desired.
- SSH Server Config. Compliance Analysis e.g. against NIST recommendations.

This process will help you better understand your IT security status (especially in compliance) as well as making better informed decisions for further action.

Universal SSH Key Manager® (UKM)

UKM is the premier dedicated SSH Key Manager solution on the market.

Enterprises trust our SSH key solution, because of our extensive experience going all the way back to 1995, when our founder Tatu Ylönen first invented them. UKM projects will generally include an SSH Key Audit and Risk Assessment as part of our due diligence process. The first step to solving the unmanaged SSH key issue is to fully understand the real situation.

Be sure to mention whether you are interested in solving your unmanaged SSH key problem as quickly as possible, and therefore wish to acquire the full UKM solution. We can then bundle these projects to save time and offer you a better price.

Finland

SSH Communication Security Oyj
Karvaamokuja 2 B 00380 Helsinki
www.ssh.com
+358 20 500 7000
info.fi@ssh.com

USA

SSH Communication Security, INC.
434 W 33rd Street, Suite 842
New York, NY, 10001, USA
www.ssh.com
+1 781 247 2100
info.fi@ssh.com

Hong Kong

SSH Communication Security LTD.
35/F Central Plaza, 18 Harbour Road
Wan Chai
Hong Kong
www.ssh.com
+852 2593 1182
info.fi@ssh.com