HOW TO GET YOUR LINUX ENVIRONMENT PCI COMPLIANT WITH KEYTOS

KEYTOS

TABLE OF CONTENTS

/ INTRODUCTION

Most companies that manage credit card transactions are familiar with PCI compliance. PCI compliance ensures that companies meet the industry standards for protecting customer data when processing payments. With the growth of the cloud, these payment systems are rapidly evolving including the move from Windows only systems to the inclusion of Linux. In this paper we will talk about the PCI requirements to consider when introducing Linux to your payment processing environment and how EZSSH can help you mitigate those issues.

KEYTOS

/ The Windows Identity Advantage

When using Windows systems, many PCI requirements are met by simply leveraging existing Active Directory accounts and group policies that are centrally managed by your IT Security team. Some of these requirements are:

2.1.1
Are default passwords/passphrases on access points changed at installation?

7
Restrict access to card data on need-to-know basis.

7.1.3
Is access assigned based on individual personnel's job classification and function?

8.1.1
Are all users assigned a unique ID before allowing them to access system components or cardholder data?

8.1.3
Automatically deprovision users when their role changes, or they leave the organization. to access system components or cardholder data?

8.1.4
Inactive Accounts are removed after 90 days of inactivity.

8.2.3

Are user password parameters configured to require passwords/passphrases meet the following?

- A minimum password length of at least seven characters
- Contain both numeric and alphabetic characters
- Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.

8.2.4

Are user passwords/passphrases changed at least once every 90 days?

8.2.5

Must an individual submit a new password/passphrase that is different from any of the last four passwords/ passphrases he or she has used?

8.2.6

Are passwords/passphrases set to a unique value for each user for first-time use and upon reset, and must each user change their password immediately after the first use?

8.3

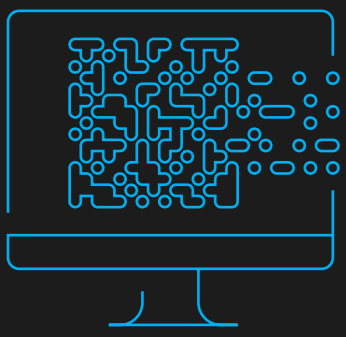
All Individual access requires Multi-Factor Authentication.

10.1

Is access to system components linked to individual users?

/ Linux Challenges

Due to Linux's open-source design, centralizing identity to a single dependency was not part of the design. Instead, Linux designers opted for local accounts that can be protected with strong authentication such as SSH keys. This is a great solution for small deployments such as a home NAS or a small company's single server. However, as Facebook noted on this white paper, this does not scale to the requirements of our new connected reality.



This fundamental difference makes is very hard to integrate Linux services into existing Windows environments since many of the Windows's advantages are lost due to the lack of native support for Active Directory. Below we will talk about how EZSSH can help you get your Linux systems ready to meet and exceed PCI requirements.

/ Linux Solution

At Keytos we looked at this problem and architected a solution that not only helps you meet these requirements but also prepares your organization for the zero-trust password-less future. While improving user experience and reducing IT costs. To understand the solution, let's break down this complex problem into two smaller problems: Access Management and Credential Management.

/ Access Management

Access Management PCI Controls

- ✓ **7** Restrict access to card data on need-to-know basis.
- ✓ **7.1.3** Is access assigned based on individual personnel's job classification and function?
- ✓ **8.1.1** Are all users assigned a unique ID before allowing them to access system components or cardholder data?
- ✓ **8.1.3** Automatically deprovision users when their role changes, or they leave the organization.
- ✓ **8.1.4** Inactive Accounts are removed after 90 days of inactivity.
- ✓ **10.1** Is access to system components linked to individual users?

How EZSSH Improves Access Management

Restrict Access on a Need-to-know basis

EZSSH advanced Access Management portal enables you to leverage your existing Azure Active Directory accounts and security groups and assign those groups to specific access policies, giving you granular control on who has access to each server farm.

EZSSH raises the bar of granular access management by adding dual key approval for critical environments. Our manual approval policies, enable you to set dual key approval for critical environments requiring the users to get approval from another previously appointed user before accessing critical data.

Identity Lifecycle

Since Linux uses local accounts, account deprovisioning is not automated or synced with the deprovisioning of the corporate account.

EZSSH mitigates this by creating short term credentials into your environment, requiring the user a valid and compliant AAD credential, each time a user authenticates to the environment. Removing the need to deprovision users when they do not longer require access.

/ Credential Management

Credential Management PCI Controls

2.1.1 Are default passwords/passphrases on access points changed at installation?

8.2.3 Are user password parameters configured to require passwords/passphrases meet the following?

- A minimum password length of at least seven characters
- Contain both numeric and alphabetic characters
- Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.

8.2.4 Are user passwords/passphrases changed at least once every 90 days?

8.2.5 Must an individual submit a new password/passphrase that is different from any of the last four passwords/passphrases he or she has used?

8.2.6 Are passwords/passphrases set to a unique value for each user for first-time use and upon reset, and must each user change their password immediately after the first use?

8.3 All Individual access requires Multi-Factor Authentication.

How EZSSH Improves Credential Management

EZSSH uses SSH certificate with a trusted certificate authority that issues short term (1 hour to 1 week) credentials The use of short-term credentials, removes the need for users and administrators to manage credentials. To authenticate the user, EZSSH removes the need for the user to manually manage SSH credentials by leveraging your existing AAD credentials, this enables you to use your existing corporate security such as multi-factor authentication, conditional access while the user uses a known workflow to access your Linux environment.

/ The Keytos Advantage

EZSSH does not only enable you to meet the minimum requirements, it helps you exceed them. Since we leverage native SSH Certificates, we are the only Linux access management solution that enables advanced access management without the need to install a 3rd party agent in your endpoints.

While this white paper focused on how EZSSH helps you manage your Linux access, other Keytos solutions can also work together to EZSSH to automate your organization's security.

EZCA

A critical part of any PCI compliant infrastructure is the Public Key Infrastructure (PKI) that enables secure TLS encryption as required in PCI requirements 2.3 and 4.1. EZCA removes the complexities of running and managing your own PKI by offering secure and compliant cloud-based certificate authorities, as well as an extension to your existing Windows Certificate Authorities that remove the need for your team to manually track and lifecycle certificates.

/ Cloud Watcher

To expand the PCI requirement: “11.5 Is a change-detection mechanism (for example, file-integrity monitoring tools) deployed to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files?” to your cloud environment, we also have Cloud Watcher, a free to use, open source tool that we created for internal use that monitors and alerts you on any change to your cloud infrastructure.

/ Conclusion

Existing security solutions have evolved as an afterthought for the changing digital world. With the move to the cloud, we have a unique opportunity to centralize our security management, removing the security tasks from everyday engineers and transferring it to secure systems designed for this specific task. This move will not only improve the security posture of the organization, and avoid costly security incidents, but it will also improve productivity.

At Keytos we are committed to helping companies across the world become more secure by fully removing the need for passwords. We do this by creating easy to use secure and compliant identity tools that make it easier for organizations to manage access the secure way than the insecure way.

Learn how organizations around the world are using Keytos tools to improve their Identity management process

Talk to an Identity Expert