PCI and PA DSS

Compliance Assurance with the Wallix Bastion

WALLIX
TRACE, AUDIT & TRUST

PCI and PA DSS Compliance Assurance **with the Wallix Bastion**

Introduction

Wallix provides support for PCI compliance out-of-the-box with the Wallix Bastion - Wallix Bastion. The Authorisations are created according to Network Security, Cardholder Data, Vulnerability Management, Access Control, and Information Security Policy.

The Wallix Bastion helps fulfil PCI audit requirements by recording all sessions created through the Wallix Bastion and providing a full audit trail. Enterprise IT environments consist of heterogeneous devices, systems, and applications that require secure access.

To ensure compliance with PCI requirements, information systems are monitored and recorded in real time. Investigators are able to see the session as if it were live and as such can see if mistakes were made or if there was a malicious act committed.

Notifications can be sent when a critical device is connected to allowing for a Security Administrator to monitor the session as if they were seeing the users screen. This allows for immediate reaction and remediation.

Groups can be created to offer the same protection to out of scope devices and applications as to those in scope

Requirements

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. The PCI DSS standards apply to all organizations that store, process, or transmit cardholder data and all affected organisations must be PCI compliant.

The PCI DSS standards are enforced by the founding members of the PCI Security Standards Council consisting of American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.

The first PCI DSS standard was released on December 15, 2004 and its latest revision was released November 2013.

WALLIX
TRACE, AUDIT & TRUST

REQUIREMENTS	WHAT WALLIX ADMINBASTION PROVIDES
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	The Wallix Bastion works as a Proxy normally placed within the DMZ, allowing only authorised access to the privileged devices from both internal and external networks
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorised publicly accessible services, protocols, and ports.	WAB Access Manager provides a secure connection from the DMZ to the Wallix Bastion Connections to the WAB Access Manager are via Https and connection to the Wallix AdminBastion are via REST API
1.3.7 Do not disclose private IP addresses and routing information to unauthorised parties.	Connecting via the Wallix Access Manager provides links to Authenticated users to authorised resources without showing the IP address.
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	When adding resources to the Wallix Bastion a password must be added, at this point password policies are taken into account and can include the auto-change of passwords on in scope devices
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	The Wallix Bastion provides the ability to control access to only specific applications and systems
2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	**CLI Connections** Connections through the Wallix Bastion can use SSH with each user account being able to provide their own SSH keys **RDP Connections** By default, Remote Desktop connections are encrypted at the highest level of security available (128-bit).
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	Via the use of Groups the Wallix Bastion helps with keeping an up-to-date inventory of privileged devices within Scope for PCI DSS
6.4 Follow change control processes and procedures for all changes to system components.	With workflow the Wallix Bastion helps to show that change control procedures are in place by providing ticket number and description of change being carried out along with a copy of the session recording being added to the change request file once the change has been completed
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.	The Wallix Bastion provides an extra layer of protection via group authorisation A User group can only access a resource group if authorisation is in place
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	The Wallix Bastion ensures that only Authorised sessions are connected from authorised users to authorised resources

REQUIREMENTS	WHAT WALLIX ADMINBASTION PROVIDES
7.1.1 Define access needs for each role, including: **• System components and data resources that each role needs to access for their job function** **• Level of privilege required (for example, user, administrator, etc.) for accessing resources**	The Wallix Bastion provides the ability to place users and resources into groups ensuring that only authorised users are able to access authorised resources
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	The Wallix Bastion works on least privilege access controls, with the ability to give limited access to elevated roles when needed
7.1.3 Assign access based on individual personnel's job classification and function.	Users are placed into groups relating to their job classification and function
7.1.4 Require documented approval by authorized parties specifying required privileges.	Wallix Bastion Workflow provides an auditable documented approval for elevated privileged access
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	Wallix Bastion only allows authenticated users to connect to authorised resources based on their need to know and does not allow or show resources that the user is not authorised to connect to
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	The Wallix Bastion uses Unique User Names / ID providing a full audit trail
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts	The out of the box configuration for password control on the Wallix Bastion is set to lock the account after 5 failed attempts
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to reactivate the terminal or session.	As standard the timeout for the Wallix Bastion is set to 15mins after which time the user will have to re-authenticate
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components.	The Wallix Bastion uses the following Username / Password & 2FA authentications KERBEROS, RADIUS, LDAP, LDAP-AD LDAPS & LDAPS-AD
8.2.6 Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	If user the account is created with a password stored locally on the Wallix Bastion then a simple tick box option ensures that the password is changed on the first logon

REQUIREMENTS	WHAT WALLIX ADMINBASTION PROVIDES
8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use.	If using local username and password the option to change password at fist login should be chosen
8.5.8 Do not use group, shared, or generic accounts and passwords.	All users, admins and auditors have their own specific login credentials which can if needed be tied to AD/LDAP etc.
8.5.9 Change user passwords at least every 90 days	Password Manage enables the password to be changed at check in along with hourly, daily, weekly or monthly
8.5.10 Require a minimum password length of at least seven characters	Password manager allows the use of complex passwords of any length
8.5.11 Use passwords containing both numeric and alphabetic characters.	Password manager allows the use of complex passwords of any length with special characters and numbers
8.5.12 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	As standard the configuration for password control on the Wallix Bastion is set to not allow the previous 4 used passwords this can be extended to a higher number. The use of configurable prohibited password list further secures the Wallix Bastion
10.1 Implement audit trails to link all access to system components to each individual user.	The Wallix Bastion not only provides a full audit trail showing User name, IP address, remote account, protocol used, start end time duration but also a full video recording of the session

WALLIX

TRACE, AUDIT & TRUST

WALLIX Group is a cybersecurity software vendor dedicated to defending and fostering organizations' success and renown against the cyberthreats they are facing. For over a decade, WALLIX has strived to protect companies, public organizations, as well as service providers' most critical IT and strategic assets against data breaches, making it the European expert in Privileged Access Management.

As digitalization impacts companies' IT security and data integrity worldwide, it poses an even greater challenge if the data involved is highly sensitive. The recent regulatory changes in Europe (NIS/GDPR) and in the United States (NERC CIP/Cyber Security Directorate) urge companies belonging to sensitive sectors to place cybersecurity at the heart of their activity.

In response to these challenges, WALLIX created a bastion designed to secure organizations' core assets while adapting to their daily operational duties: WALLIX Bastion. The WALLIX bastion accompanies more than 100 operators in sensitive sectors to conform with regulations and over 400 organizations in the protection of their critical assets, securing the access to more than 100,000 resources throughout Europe and the MEA region. It was also the first government-certified solution in the market.

WALLIX partners with a trained and certified network of over 90 resellers and distributors that help guarantee effective deployment and user adoption.

WALLIX is the first European cybersecurity software editor to be publicly traded and can be found on EuroNext under the code ALLIX. As one of the leaders of the PAM market, major players trust WALLIX to secure access to their data: Danagas, Dassault Aviation, Gulf Air, Maroc Telecom, McDonald's, and Michelin are among them.

WALLIX is the founding member of Hexatrust. The WALLIX bastion was elected "Best Buy" by SC Magazine and awarded at the 2016 Computing Security Awards, BPI Excellence, and Pôle Systematic.

Twitter: @wallixcom
More information on: www.wallix.com

OFFICES & LOCAL REPRESENTATIONS

WALLIX FRANCE (HQ)
http://www.wallix.com/fr
Email : sales@wallix.com
250 bis, rue du Faubourg Saint-Honoré
75017 Paris - FRANCE
Tél. : +33 (0)1 53 42 12 90
Fax : +33 (0)1 43 87 68 38

WALLIX UK
http://www.wallix.co.uk
Email: ukinfo@wallix.com
1 Farnham Rd, Guildford, Surrey,
GU2 4RG,UK
Office: +44 (0)1483 549 944

WALLIX DEUTSCHLAND
http://www.wallix.de
Email: deinfo@wallix.com
Landsberger Str. 398
81241 München
Phone: +49 89 716771910

WALLIX USA (HQ)
http://www.wallix.com
Email: usinfo@wallix.com
World Financial District, 60 Broad Street
Suite 3502, New York, NY 10004 - USA
Phone: +1 781-569-6634

WALLIX RUSSIA & CIS
http://www.wallix.com/ru
Email: wallix@it-bastion.com
ООО «ИТ БАСТИОН»
107023, Россия, Москва,
ул. Большая Семеновская, 45
Тел.: +7 (495) 225-48-10

WALLIX ASIA PACIFIC
(Bizsecure Asia Pacific Pte Ltd)
Email: contact@bizsecure-apac.com
8 Ubi Road 2, Zervex 07-10
Singapore 408538
Tel: +65-6333 9077 - Fax: +65-6339 8836

WALLIX AFRICA
SYSCAS (Systems Cabling & Security)
Email: sales@wallix.com
Angré 7ème Tranche Cocody
06 BP 2517 Abidjan 06
CÔTE D'IVOIRE
Tél. : (+225) 22 50 81 90

www.wallix.com