Achieving PCI Compliance for:

Privileged Password Management & Remote Vendor Access

[WHITE PAPER]

Written by
e-DMZ Security, LLC
April 2007

Achieving PCI Compliance

A White Paper by e-DMZ Security, LLC

OVERVIEW:

Though PCI compliance is not a government driven requirement such as Sarbanes Oxley and HIPAA, non-compliance under PCI can have a devastating impact on any enterprise that relies on credit card transactions. Your contract with credit card companies requires that as an organization you comply with PCI. Non-compliance with PCI can result in specific contractual penalties and/or revocation of your rights as an enterprise to process credit card transactions.

Like all compliance and regulatory requirements, there is no single product or policy/procedure that will assure your compliance. THERE IS NO SILVER BULLET for PCI COMPLIANCE. PCI compliance requires that your enterprise deploy many security technologies, and have specific policies and procedures in place. This white paper focuses on the unique issues and solutions associated with both privileged password management and remote vendor access in meeting PCI compliance requirements. Many of the requirements highlighted cannot be resolved or adequately addressed by existing enterprise security technologies such as firewalls, VPN and IDS solutions. Existing legacy policies and procedures are also unable to meet many of the requirements standards presented under PCI.

Management, control and audit of both shared/privileged account passwords and critical remote third party and administrative level connections is mandatory in meeting PCI requirements and other growing regulatory, compliance and best practice security needs. The chart below (*see Appendix A, pg.4*) is based on a review of the "Payment Card Industry Security Audit Procedures-Version 1.1 September 2006." The chart illustrates the particular PCI issues that are mitigated through the deployment of our eGuardPost or Password Auto Repository (PAR) solutions.

COMPLIANCE-DRIVEN PASSWORD MANAGEMENT

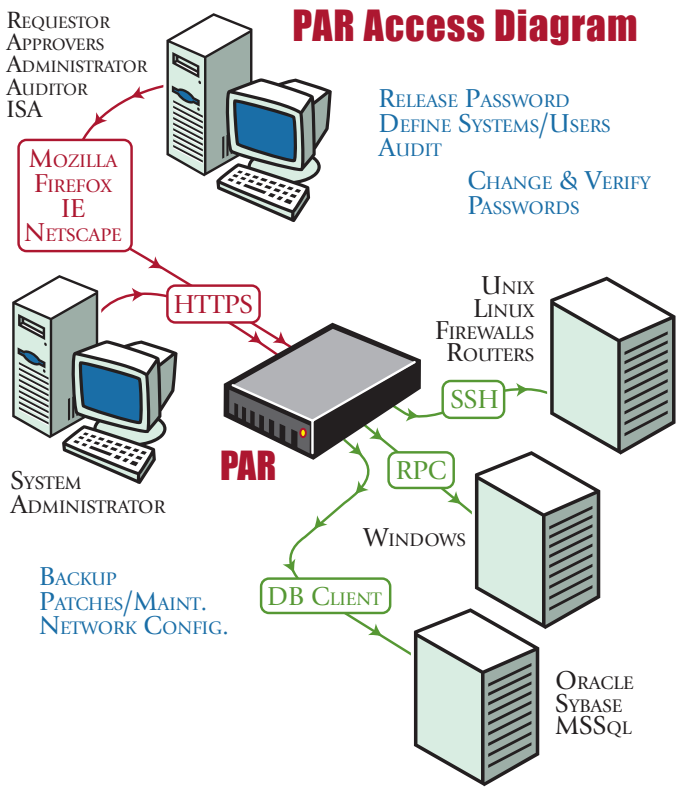
The Password Auto Repository (PAR) was uniquely designed to solve enterprise security and compliance issues associated with the management and control of shared privileged passwords such as *root* and *administrator*. The issue of privileged password management and the unique features of PAR contribute directly and/or indirectly to many specific PCI requirements as outlined in attachment A. Fundamentally, the compliance audit concerns in the area of shared privileged password management center on ACCOUNTABILITY and AUDIT. Given the level of access and shared nature of accounts like root and administrator, internal and external PCI audits are taking a close look at existing enterprise controls. In most cases, the existing manual based policy/procedure solutions (e.g. Safe – envelope) or internally developed technical solutions are not standing up to PCI compliance audits. Under audit scrutiny existing in-house solutions are failing to deliver assured accountability and adequate audit.

PAR, winner of SC Magazine's 2006 Readers Trust Award for Password Management, provides a purpose-built appliance with no client or host based software requirements to resolve your security and compliance concerns for shared/privileged account, service account and hard-coded password management.

The unique capabilities of PAR can help your organization obtain and maintain PCI compliance for many PCI security requirements as reflected in Attachment A. At a high level, the core features, functions and capabilities provided under PAR that help drive PCI compliance include:

- Privileged User Accountability
- Privileged Account Access Control
- Dual Release Controls (Requestor/Approver(s))
- Automated Password Change (time based and last use based)
- Strong Password Generation
- Secure Password Storage

As is shown in the PAR Access Diagram below, administrators connect to PAR via a standard web browser via https. PAR supports role-based access and connections for requestors, approvers and various admin and auditor functions. From a requestor/approver standpoint, PAR securely stores, releases and changes privileged account passwords for a heterogeneous enterprise system environment including Unix, Windows, Databases and other network devices (firewalls, CISCO), AS400 and mainframes. Provided proper authorization (i.e. approval if under dual control) PAR will delivery the current privileged account password to the administrator. Once authorized release window expires or client expires release window, PAR will automatically change the privileged account password. Connections to back-end systems are also clientless using native system protocols. More information on PAR and a live demonstration can be found on our website at: *www.e-dmzsecurity.com.*



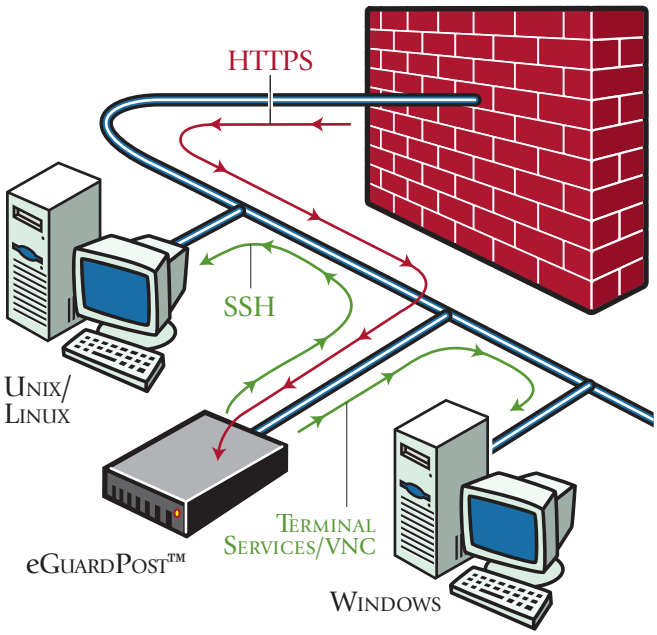
COMPLIANCE-DRIVEN THIRD PARTY ACCESS

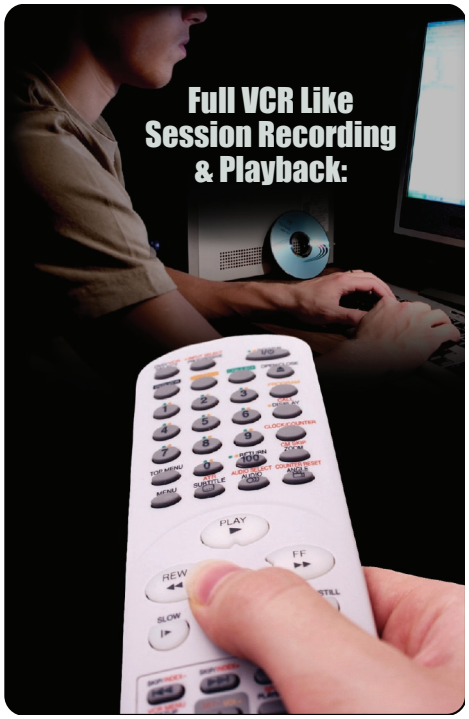
eGuardPost was designed to specifically address the enterprise security and compliance concerns associated with allowing remote third party (vendors, suppliers, consultants, etc.) and administrative access into enterprise networks and resources. Unlike remote employee connections, the enterprise does not have the same level of physical or technical controls

over remote third party connections – yet under PCI the enterprise has the same liability exposure should such access (authorized or not) result in the release or exposure of consumer credit card information. For these reasons, both internal and external PCI audits are focusing on how the enterprise secures, controls and audits third party, administrative and other sensitive remote connections.

eGuardPost working independently or in conjunction with PAR (eGuardPost includes PAR functionality or can integrate with independent PAR appliance) can help the enterprise meet the intention of may PCI Security Standards as is shown in Appendix A. At a high level, the areas of audit under PCI directly addressed with eGuardPost include:

- Vendor accounts monitored
- Logging all action to root and administrator
- Monitor, control and limit access





Technically many of these issues are easily addressed for employees through the deployment of an enterprise VPN, firewall, virus software and IDS. These issues become more challenging when working with remote third party vendors given the lack of ownership and control of the end client system, network and environment.

eGuardPost delivers a compliance-driven solution to the critical audit issues associated with remote third party connections including:

- Remote Session RECORDING: Including keystrokes, mouse movements and all screen changes
- Session Proxy: No direct connection to back-end servers, accounts or applications
- Clientless secure encrypted communication via https

The unique session recording capabilities and VCR-like playback of eGuardPost allow you to easily answer the question "what did the remote vendor do when connected." Like having a camera recording a parking garage, it is not something you would review every day, but when needed it is a great security and compliance value to be able to "go to the tape." eGuardPost was selected for Information Security Magazine's Tomorrow's Technology Today award in the area of forensic and security audit.

APPENDIX A

Requirement	Product	How
2.1 Default passwords	PAR	By requiring that all default accounts are managed by PAR, you can ensure that the passwords are changed based on time and usage.
2.3 Encrypt all non-console administrative access.	eGuardPost	eGuardPost creates a secure proxied SSL connection for non-console based administrative access.
3.5 Protect encryption keys	PAR	PAR provides secure file storage with granular access control.
3.6.6 dual control for keys	PAR	The PAR file storage capability allows for dual (or more) control on the release process.
7.1 Limit access to computing resources and cardholder information	eGuardPost	eGuardPost provides granular control to dictate which systems can be accessed and proxies the access.
8.4 Encrypt all passwords during transmission and storage	PAR	PAR securely stores all managed passwords using AES 256 encryption. Passwords are transmitted via secure SSL.
8.5.4 Immediately revoke access for any terminated users	PAR	PAR can disable any terminated user removing access to PAR and any managed passwords. With PAR automated change controls, no user has any password knowledge unless in an active/authorized release window so terminated users have no account password knowledge.
8.5.6 Vendor accounts are monitored	PAR/ eGuardPost	With PAR, you can require vendor password requests for dual authorization, so passwords will only be provided when approved. Approvals could only be given during allowable access hours. With eGuardPost (add-on to PAR or stand alone) you can have a full session capture of all traffic. Whether connecting to Windows, Unix, routers, etc, all traffic is captured for review with VCR like playback.
8.5.8 Shared admin account	PAR	PAR was specifically designed to address this issue. PAR provides individual accountability to determine who accessed a shared account.
8.5.10, 8.5.11 Password rules	PAR	PAR supports per system and per account based password rules including defining require length, numeric & alpha-numeric characters and more.
8.5.13 Limit Repeated Access	PAR	User's logging into PAR can be disabled after configurable number of attempts. Being disabled will not allow access to any of the stored passwords on PAR the user is authorized to request/obtain.
8.5.14 Set Lockout duration	PAR	Disabled users are locked out until enabled by PAR administrator.
10.1 Individual accountability	PAR/ eGuardPost	PAR will provide accountability of who used a particular account, while eGuardPost can provide a full session capture of the activity.
10.2.2 Logging all action to root or admin	PAR/ eGuardPost	eGuardPost captures the entire RDP or SSH session, providing full replay capability of the activities.
12.5.5 monitor and control access to data	PAR/ eGuardPost	By forcing all access though eGuardPost, you have a full audit trail of any access to data.