



Privileged Access Control Solutions

**Cost Effective,
Compliant
Remote Administration
for the
Retail Market**

[APPLICATION NOTE]

Written by

Martin Ryan, Vice-President, e-DMZ Security, LLC

Introduction

For multi-store outlets, including retail, banking, grocery, gas, hospitality, convenience stores and others, reducing (or avoiding) the cost of in-store system support and maintenance while maintaining compliance with PCI, SOX and other requirements has become a strategic challenge. At the same time, deployment of new retail applications, supply chain automation and POS integration continue to improve internal operations, while increasing the potential need for costly in-store support services and/or extending remote support requirements beyond what existing solutions are capable to securely manage.

A growing number of retail companies are finding eDMZ Security's eGuardPost the perfect solution to deliver the cost savings associated with centralized remote administration of in-store systems and applications while at the same time enhancing security, PCI and other regulatory compliance.

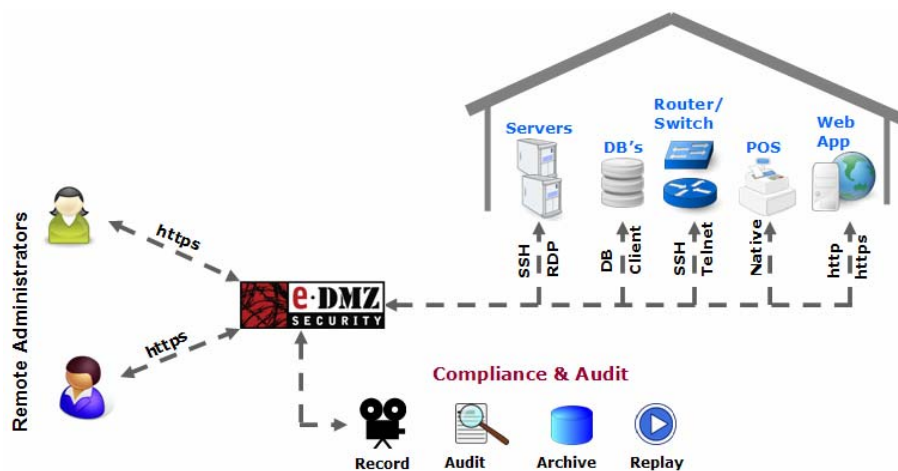
eDMZ Security Solution Overview

Delivering cost savings and compliance admittedly sounds a bit like marketing hype or at the very least an oxymoron. This would be true if eGuardPost approached the problem with traditional technologies such as VPNs, terminal services, etc. However as you will see, eGuardPost goes outside the "traditional technology box" to combine a unique set of capabilities into a single secure and expandable appliance in order to deliver secure, trusted and compliant remote administration of all your in-store systems, devices and/or applications. eGuardPost features include:

- ▶ Hardened secure appliance: Built-in firewall, full disk encryption and more
- ▶ Secure clientless deployment – no administrator client software or back-end target system agent software required to deploy
- ▶ Extensive proxy connectors to support direct proxy communication or communication through existing "jump box", terminal server, etc. Proxy connectors include
 - RDP
 - SSH
 - http/https
 - ICA

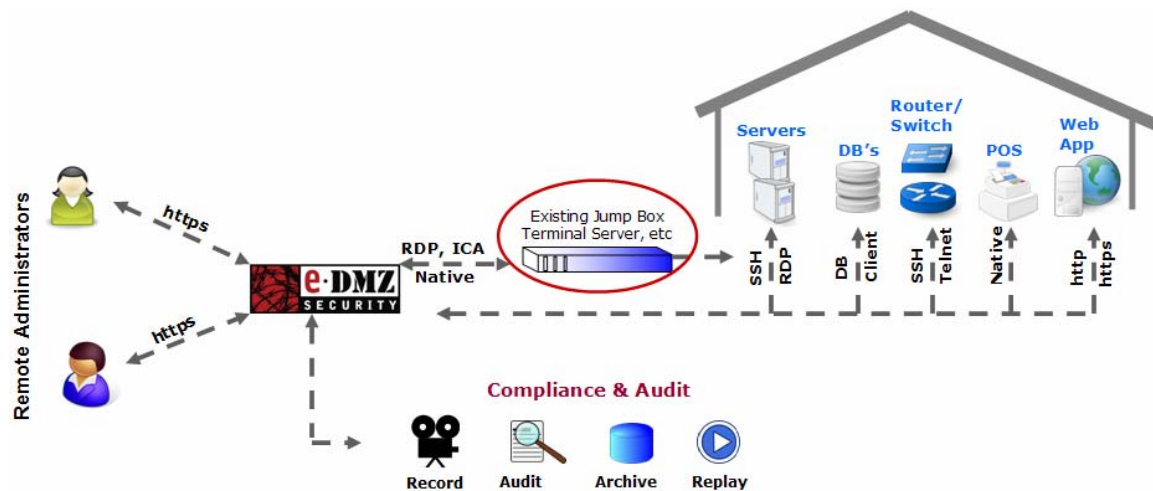
- Telnet
 - X5250
 - VNC
-
- ▶ Auto-login of remote administrator sessions – no password exposure
 - ▶ Fine-grain access controls to control specifically what/where administrators can connect
 - ▶ Time-based access controls
 - ▶ File transfer and cut/paste controls
 - ▶ Configurable dual (or more) connection authorization controls
 - ▶ Full session recording with auto archiving. All activity, keystrokes, mouse clicks, applications – everything the administrator does through eGuardPost will be recorded
 - ▶ DVR-like session replay and controls
 - ▶ Optional full password management including automated password change and password synchronization with the addition of our Password Auto Repository (PAR)

eGuardPost is deployed as the “gateway” from which all remote administrators must pass in order to connect/service in-store systems, devices and/or applications.



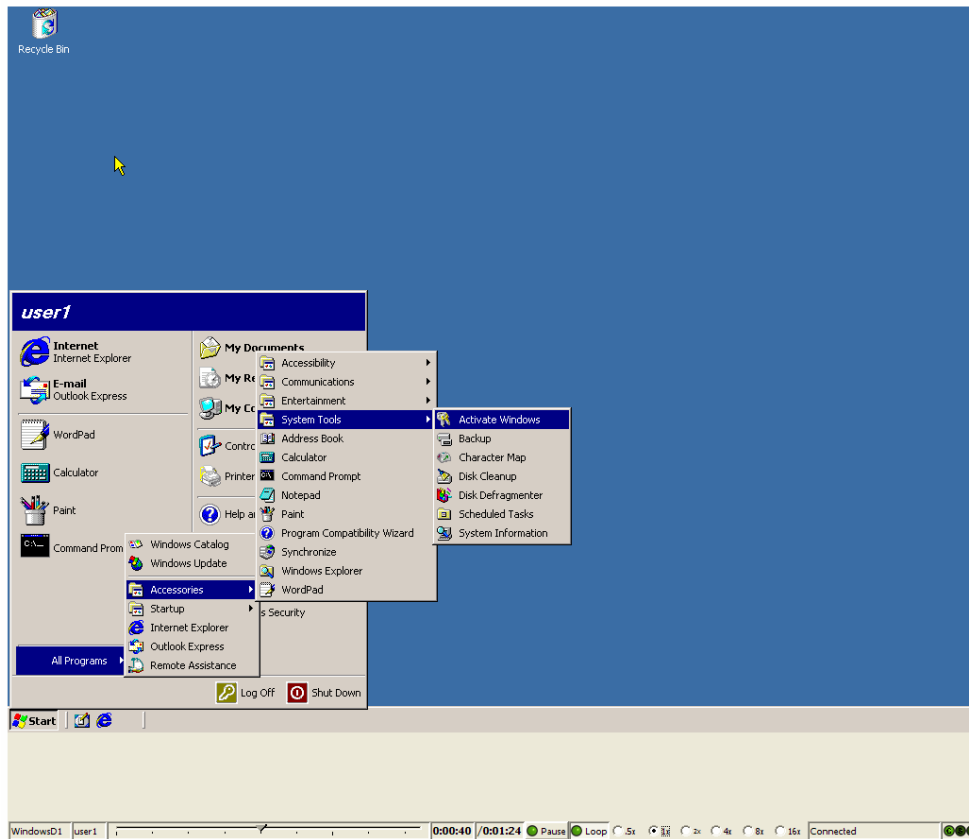
As reflected in the diagram above, remote administrators authenticate/connect to eGuardPost – based on user specific policy, they are able to request connections to back-end devices. If connection is approved (either auto approved or via approval process), eGuardPost will create the appropriate proxy connection to the back-end device (note: POS proxy type may vary based on vendor).

eGuardPost fully supports Virtual Network Computing (VNC) proxy providing full remote desktop support/interaction in a cross-platform environment. eGuardPost also supports Remote Desktop (RDP) proxy, ICA proxy and can easily extend/integrate with existing “jump box”, terminal server or other existing infrastructure as shown in the diagram below:



In the above view, eGuardPost could be configured so all administrative connections are directed through the existing “jump box(s)” or only certain connections. The existing box would function in the same manner with the additional security, full session recording and replay offered by eGuardPost.

One of the truly unique aspects of eGuardPost is the ability to record, archive and replay all administrative activity. Regardless if direct to device or via existing “jump box” or terminal server, anything the remote administrator does will be recorded – keystrokes, mouse clicks, applications access, etc. A replay of an eGuardPost recorded session is as if you were sitting with the remote administrator as they accessed in-store resources. The screen shown below represents a snap shot of a recording replay of an access to back-end windows server.



The replay provides time-stamp information, can be paused, run at up to x16 speed or brought to a specific time frame via the controls at the bottom of the replay window. The level of full session recording provided with eGuardPost not only exceeds any compliance audit requirements, it saves significant time and money when trying to “recreate” events and/or understand actions taken on an in-store server or device.

Delivering PCI Compliance

eGuardPost as a standalone solution or with the addition of PAR helps resolve many PCI requirements with regards to user/session management and password management. The table below provides specific PCI areas that eGuardPost/PAR are able to meet.

PCI Requirement	eGuardPost/ PAR Solution
2.1 Default passwords	By requiring that all default accounts are managed by PAR (eGuardPost add-on), you can ensure that the passwords are changed based on time and usage.
2.3 Encrypt all non-console administrative access.	eGuardPost creates a secure proxied SSL connection for non-console based administrator access.
3.5 Protect encryption keys	eGuardPost w/PAR add-on provides secure file storage with granular access control.
3.6.6 dual control for keys	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 provides granular control to dictate which systems can be accessed and proxies the access.
8.4 Encrypt all passwords during transmission and storage	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	eGuardPost can disable any terminated user removing access to eGuardPost and by default any systems they have access. In addition 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	eGuardPost provides full session recording, so all vendor activity can be monitored when connected through eGuardPost. Also, with the add password management features of PAR – vendor accounts can be automatically managed with time and last use based change controls.
8.5.8 Shared admin account	eGuardPost w/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	eGuardPost w/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	User's logging into eGuardPost can be disabled after configurable number of attempts.
8.5.14 Set Lockout duration	Disabled users are locked out for a configurable duration.
10.1 Individual accountability	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	eGuardPost captures the entire RDP or SSH session, providing full replay capability of the activities.
12.5.5 monitor and control access to data	By forcing all access through eGuardPost, you have a full audit trail of any access to data.

Cost Savings/ROI

The ROI cost saving in deploying eGuardPost can vary based on the number and location of outlets, number of in-store devices/applications and location of support personnel. However, the areas in which a multi-outlet retail enterprise will realize cost savings with eGuardPost are common and will typically include:

- ▶ Reduction or elimination of on-site support visits
- ▶ eGuardPost auto-login and/or password management (w/PAR) eliminate the need to manually change in-store passwords in the event support/admin personnel leave or change roles
- ▶ Full session recording will significantly reduce debug and/or forensic time in the event changes impact system or application function/performance.
- ▶ Flexibility to support centralized or decentralized support personnel

Contact Preventia Ltd

If eGuardPost is of interest, please give us a call or send us an email. We can easily support a more detailed webex and/or support on-site proof-of-concept as needed.

Phone: (01273) 883300

Email: info@preventia.co.uk

Web: www.preventia.co.uk

