



e-DMZ Security eGuardPost

Remote access is rapidly becoming a critical business requirement to many organisations, and yet it can be so difficult to manage and audit. Whether it encompasses extending remote access to support personnel, outsourcing vendors, or a mobile workforce, the tools need to be in place to enforce strong security, but also to be able to know and show exactly what each user did while they were connected to the main network.

The eGuardPost appliance aims to deliver stiff access controls, along with transparent password management, and extensive session auditing and reporting facilities. At its foundation is e-DMZ's tried and trusted PAR (password auto repository), and this provides password management that's good enough for regulatory compliance. It can look after typical administrative passwords for Windows and Unix systems, and handle all changes and notifications. As a standalone solution, it can provide a dual control system of password notification and provide end-to-end encryption, which includes AES256 disk encryption, on the appliances hard drive.

The eGuardPost takes PAR and builds on it by providing authenticated and encrypted access for users running Windows RDP (remote desktop protocol) and Unix/Linux SSH (secure shell) sessions. It's a simple concept; as remote users log onto the appliance, this

will determine what levels of access they are allowed, and which host systems they can connect to. These systems can be controlled individually or placed into groups, called collections, whilst users can also be added to groups for easier management.

You can define managed accounts which PAR will look after, so your remote users never need to know what the actual password on the internal system is, as they only log onto the appliance, which then in turn handles the local passwords.

Four main user levels are supported, with the requestor at the bottom of the heap. This user can only access managed systems if allowed by an approver. When they log onto the appliance it automatically sends an email to the associated approver, advising them that they need to check and confirm that the user can access a system. You can also have users with dual requestor/approver roles, whilst the ISA (information security administrator) sits at the top of the tree and is in overall command.

We found eGuardPost remarkably simple to set up and use on our test Windows network. Management is isolated to one of the appliances embedded Gigabit Ethernet ports, while a CyberGuard SG630 firewall/VPN PCI controller card looks after the front door. You need to configure PAR first, but this only takes a few minutes, after which you

can move over to the well-designed eGuardPost web browser interface. All managed systems are declared to the appliance first and then you can select user accounts and groups, and associate them with different systems. Each user has a local account linked to their eGuardPost account, making it easy to determine what they can actually do when they access a system.

The slickest part of eGuardPost is that when a user gains access to internal resources, the appliance records their entire RDP or SSH session. These are stored on the same hard disk as PAR, so are subject to strong encryption, but designated auditors can select a session and see exactly what the user was doing. At present you can only pause and restart the recording, but e-DMZ plan to introduce some more VCR-style controls, such as fast-forward and rewind.

The eGuardPost appliance is a smart security solution for controlling remote access that's made all the more elegant by its simplicity. It delivers very strict controls, and its session auditing capabilities are way beyond anything offered by most competing remote access products. **NC**

e-DMZ Security, LLC
501 Silverside Road Suite 143
Wilmington, DE 19809
1.866.203.9823
eGP-info@e-dmzsecurity.com