



## Not all system access is equal!

In today's compliance and regulatory driven world, the enterprise must take steps to assure appropriate levels of access control and audit are in place. These controls should be based on the network, system, application and other resources to be accessed. e-DMZ Security's eGuardPost has been designed to meet the access control and audit requirements of your most privileged and sensitive users to your most critical resources.

### This user community may typically include:

- ✓ Remote Vendors, Outsourcing, Consultants
- ✓ Application and System Developers
- ✓ Support and Service
- ✓ Administrators



Regardless of your specific requirement — remote vendor support, the requirement to grant developer access to production resources, the control of administrative sessions, or other any internal or remote requirements, eGuardPost provides the security, access control, session control and compliant auditing you require.

Built around the rule that not all access is equal, eGuardPost is deployed as a session gateway between your sensitive users and critical resources. Combining a unique set of capabilities, including session request/approval controls, session proxy and resource access controls, eGuardPost allows you to securely control who has access, when they have access and to what resources they have access.

eGuardPost includes full session recording — every keystroke, mouse movement and application access is captured, recorded and logged for future audit and/or forensic review or playback. Nothing is done through eGuardPost that is not recorded!

- ✓ Want to know what a vendor was doing when granted access?
- ✓ Review administrative access to your HR system?
- ✓ Review developer changes to production resources?

With eGuardPost, you simply filter recorded logs based on user, system accessed and/or date, highlight the session of interest and hit REPLAY!

Below is an example which shows a filtered list of recorded sessions, and a screen capture of a replay of the highlighted session. The forensic and compliance audit value of the full session recording kept with eGuardPost is unmatched.



### Session Recording Features

- ✓ Searchable recording logs based on user, resource and/or date
- ✓ Auto-archive and retrieval
- ✓ Compressed and encrypted Not AVI files – manageable size
- ✓ Highlight log and REPLAY
- ✓ VCR-like replay controls



### Full Session Recording and Playback

eGuardPost captures all user activity through a proxy. This includes every keystroke, mouse movement, application accessed and more. Everything the user does is recorded with DVD-like playback controls. Recordings are easily searchable and retrieved based on user, system and/or date. eGuardPost's "Replay Session" functionality allows Playback of the entire session and includes DVD style controls including the ability to pause, run at up to x 16 speed or move to a specific time within the recording.

### Recording Logs and Management

Session recordings are not AVI files - they are stored in a compressed format and are fully encrypted. Since eGuardPost only records changes (no activity = no recording) recording sizes are typically minimal and very manageable. Typically, a 30 minute session would result in a recording of approximately 1 - 3 MB. eGuardPost supports auto archiving of logs via scp, sftp or ftp and is configurable based on time and/or remaining disk capacity - archived logs are automatically managed by eGuardPost for replay.

### Session Proxy

eGuardpost will proxy all sessions between the user and the specific resource they are authorised to access. The proxy type is based on the resource being accessed and can include: SSH, RDP, http, ICA, Telnet, x5250 and VNC (contact Preventia for the up-to-date list of supported proxies). The session proxy protects the back-end resource against viruses, worms and other Mal-ware because the user has no direct connectivity to the resource.

recording and playback facilities. Enhanced capabilities of the joint solution include session authorisation, auto-logout of session, full session recording and playback.

### Secure Purpose Built Appliance

The eGuardPost solution is delivered via a secure Appliance which includes an embedded hardware Firewall card for enhanced protection along with full AES 256 Bit disk encryption. As a purpose built appliance, there is NO console or underlying Operating System access. Only authenticated in-bound connections via port 443 and 22 are allowed, all other traffic is blocked.

### Session Authorisation Control

eGuardPost supports configurable authorisation controls based on the user and/or the resource being accessed. Session authorisation can either be auto-approved or require one (or more) approvals before a connection would be established.

### File Transfer Control

eGuardPost can be configured to allow or deny a user the ability to upload files through the session proxy. eGuardPost also provides support for the "Cut and Paste" functions through the session proxy.

### Easily Expandable

eGuardPost can support as many sessions as you might need. The base eGuardPost appliance supports up to 100 concurrent sessions. By adding additional Distributed Processing Appliances (DPA) you can expand the concurrent session support by 100 sessions per additional DPA. eGuardPost will automatically load balance sessions between the primary eGuardPost and the additional DPA(s).

### Password Management

eGuardPost can tightly integrate with e-DMZ's Password Auto Repository (PAR) - allowing configurable account password management that can include "Auto Log-in" of users to ensure NO account credentials are ever exposed.



e-DMZ Security,™ eGuardPost™ and Password Auto Repository™ are trademarks of e-DMZ Security, LLC. ©2008 e-DMZ Security, LLC. All Rights Reserved.