

ACCESS CONTROL

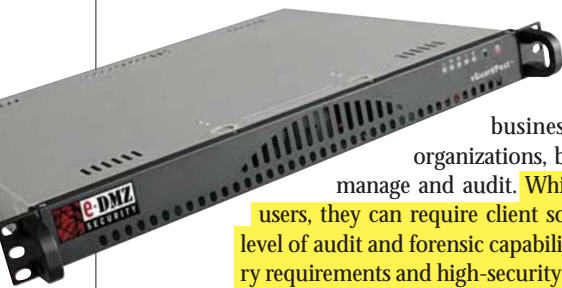
eGuardPost

REVIEWED BY STEVEN WEIL

e-DMZ Security

www.e-dmzsecurity.com

Price: **Starts at \$10,000 for five concurrent sessions**



Secure remote vendor and system administrator access to information systems is a critical business requirement for many organizations, but it can be a challenge to manage and audit. While VPNs are fine for most users, they can require client software and don't offer the level of audit and forensic capabilities demanded by regulatory requirements and high-security environments. eGuardPost is a hardened appliance that can be used to secure, manage and audit these sensitive connections.

Policy Control

eGuardPost allows security managers to apply granular access controls to remote connections. The appliance comes bundled with Security's Password Auto Repository (PAR), e-DMZ's flagship product, which securely stores and manages administrative passwords.

We were able to successfully create multiple users and enforce a variety of access controls on them.

Once users log in via HTTPS and are authenticated via RSA Security's SecurID, Secure Computing's Safe-Word or LDAP (or against user accounts created and stored on eGuardPost), eGuardPost determines what type of remote access they are allowed and which systems they can connect to. Security managers can assign specific roles (e.g., requester, approver, auditor and administrator) to remote users.

eGuardPost can be configured to automatically log in specific users; it retrieves the necessary password from the local or a remote PAR. The password is never shown to, or known by, the remote user.

Testing methodology: Our test network included a Windows XP laptop, an unmanaged switch and three Windows 2003 Web, FTP and domain controller servers.

Security managers can also require that certain remote connection requests be approved by one or more designated persons. Connection requests and approvals can be sent to a ticketing system.

Configuration/Management

Configuration is straightforward and easy thanks to excellent documentation. The appliance is managed via HTTPS. The management interface is well designed and mostly easy to navigate.

Systems to be managed are defined, users are created, and the security manager determines which users have what type of remote access to which systems. You can even limit access to specified time periods, which will be very useful for vendors and contractors, as well as admins assigned to particular tasks. Systems and users can be placed into and managed as groups.

Users do not need to install any software; eGuardPost proxies all remote connections. It can establish connections to systems via Telnet, Windows Terminal Server, SSH, VNC and X5250.

Reporting

eGuardPost's forensics capabilities are unique, offering VCR-like recording and playback of every mouse, keyboard and screen action during a remote session. We conducted multiple remote sessions via eGuardPost then watched their recordings; each was flawlessly presented. eGuardPost can automatically move recorded sessions to designated archives.

eGuardPost can produce detailed reports of user rights and activities, security alerts, firewall events, database events and Web server events. Reports can only be exported to Excel and some of them are a bit cryptic. The appliance supports SNMP and syslog.

Effectiveness

We found eGuardPost to be a very effective product, correctly and efficiently managing and auditing all of the many remote connections we sent through it. eGuardPost is carefully hardened, with an embedded firewall and hard drive encrypted with 256-bit AES. Our security scans of the appliance found no vulnerabilities.

Verdict

eGuardPost is a well-designed and highly capable product that meets an important need. It has strong security and great forensics capabilities. •

Reprinted with permission from Information Security Magazine, March 2007.

© 2007 TechTarget. All Rights Reserved. FosteReprints: 1-866-879-9144