



WHITE PAPER

Controlling Access to Critical Enterprise Resources

Abstract:

Remote Vendor Access, Developer Access to Production, Fire-Call Access and more are all examples of “critical” access requirements that bring a unique set of compliance and security requirements. This white paper discusses the issues and offers a unique solution for controlling access to critical enterprise resources.

February 2008

The Issue:

Driven by the regulatory and compliance demands of Sarbanes Oxley section 404, PCI, BS 7799 and others, today's enterprise place a strong emphasis on separation of duties (SoD) and internal access control to help assure no individual has the access, control and/or power to intentionally or inadvertently damage production resources. While many enterprises have developed SoD through policy and procedure, many still struggle with balancing SoD and the real-time requirements of granting temporary access to critical resources such as:

- Developer Access to Production Resources
- Fire-call Access
- Support Access
- Vendor Access

Critical outages or application problems in a production environment can have an immediate and devastating impact. For example, you're a large financial or POS driven enterprise and the production credit card "validation system" is unavailable for several minutes – how many thousands of customers are forced to use a competing company's credit card for a store transaction in those minutes? Do they try your card again? Do they walk out from completing the purchase? You're a business with a strong on-line presence, what is the cost of production web issues or back-end production application problems? Resolving production issues quickly can save the enterprise millions of dollars – as a result, even companies with strong SoD controls may "bypass" controls in an effort to quickly resolve production problems.

The balancing act the enterprise faces is "time vs. process" since following the established process to grant temporary access to critical resources can take time – and for most enterprises, production downtime is money! It is not uncommon for it to take hours from initial requirement/request to approval and actual access when working through established SoD and access procedures. Certainly, no enterprise has established policies that are intended to bypass. But the reality is, in many cases the established policy and controls are bypassed albeit with good intention, creating security, compliance and operational concerns.

The Solution:

The need is for a solution that can grant secure, controlled and audited resource access in a timely fashion and cannot be bypassed.

For a growing number of companies, the solution is eDMZ Security's eGuardPost with Password Auto Repository (PAR) as part of an internal access control architecture providing the level of security, fine-grain control and audit demanded when granting limited "fire call" or other access to critical production resources and/or applications.

As depicted in *diagram 1* below, eGuardPost provides a trusted controllable gateway between specific authorized users and specific production resources and accounts. Providing a secure yet automated gateway allows organizations to respond to critical resource issues more quickly, efficiently and affectively saving significant time and money while gaining in security, audit and compliance.

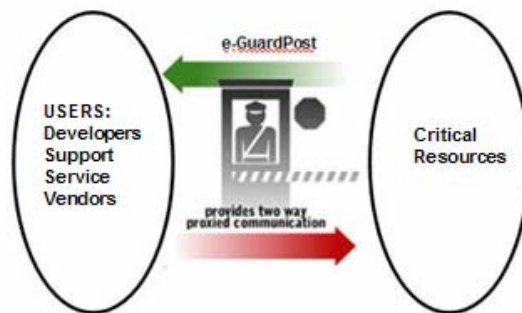


diagram 1

Driven by the needs and requirements of our customers and prospects, the session controls of eGuardPost combined with the password management of PAR delivers across all key security and compliance requirements associated with granting temporary access to critical resources. The table below provides a summary of how e-DMZ Security's solution meets the common requirements associated with granting this access:

Action	eDMZ Solution	Time	Issues
Request Access	<p>eGuardPost supports strong two-factor authentication.</p> <p>Authorized users can request connections only to specifically allowed resources.</p> <p>Requestors must specify resource, connection time required and reason for request all of which are part of audit record.</p> <p>Full audit of all connection requests, approvals and/or denials including who, when and why.</p>	1 – 2 min	None.

Approve Access	<p>Authorized connection requests can either be auto-approved or configured to require dual connection authorization. This is configurable on a per user, resource and/or account basis.</p> <p>All activities, approvals, denials, etc. are fully audited.</p>	0 – 2 min	None.
Grant Access	<p>Once approved, the authorized user is allowed to connect to the specific resource/account.</p> <p>eGuardPost creates a proxy connection to specific resource – so NO direct resource access.</p> <p>eGuardPost if configured with PAR can also obtain the account password from PAR and auto-log the user into the resource account – NO exposure of account passwords!</p>	0 – 1 min	None.
Terminate Access	<p>eGuardPost grants access for the specified connection request time. If time is over-run, administrators are notified and can immediate terminate the connection or take other actions.</p> <p>Administrative roles can terminate any active connections in “real-time”.</p>	0 min	None.
Audit	<p>eGuardPost not only keeps a full audit of all requestor, approver, auditor and/or administrative activities, eGuardPost RECORDS the entire session – Every keystroke, mouse movement, application access, etc. is recorded for future playback in VCR-like fashion!</p> <p>You have a complete record of everything done while access was granted.</p>		None.

With eGuardPost, you not only enhance the security, audit and automation of your existing SoD and access process, you save TIME! With eGuardPost secure, approved, controlled and audited access to key resource/application(s) can be delivered in minutes versus hours with existing controls –delivering a strong ROI!

eGuardPost provides full control over who can connect, when they can connect and how long they can connect – add to this a secure proxy connection for protection against viruses, malware or other items and you have a secure trusted gateway. eGuardPost includes full session recording, you have an audit/forensic record of EVERYTHING done through eGuardPost! You can easily and quickly search for recorded logs based on user, system and/or time – and replay the log with VCR-like controls.

Below is an example of eGuardPost session log listing and a snap-shot of an actual replay of a session to a windows server.

The screenshot displays the eGuardPost interface. At the top, it says "Session Logs Listing" and "Selected Session: 1526". Below this is a table with columns: Username, User Full Name, Start Date, Request, File Size, Duration, System, and Account. The table contains 8 rows of session data. Below the table are navigation buttons: "Filter", "Layout", "Listing", "Export to Excel", "Export to CSV", and "Replay Session". A red circle highlights the "Replay Session" button, with a red arrow pointing to a window titled "Replay Session". This window contains text: "This is a recorded session from eGuardPost. With eGuardPost you get fine grain access controls, session proxy and FULL session recording. Every keystroke, mouse movement, application access is recorded with VCR like playback. This is an actual remote connection session reply." At the bottom of the replay window, there is a status bar with "WindowsB1 user1" and "883-888811" highlighted with a red circle. Below the status bar, it says "VCR-Like Controls".

Username	User Full Name	Start Date	Request	File Size	Duration	System	Account
reqB1	Req, Test	1/15/2008 10:50:42 AM	1398	526	0:02:09	WindowsB1	user1
reqB1	Req, Test	12/19/2007 7:09:01 PM	1391	1791	0:02:23	WindowsB1	user1
reqB1	Req, Test	12/17/2007 3:47:59 PM	1380	111	0:35:38	WindowsB1	user1
reqB1	Req, Test	11/27/2007 5:30:09 PM	1366	347	0:01:03	WindowsB1	user1
reqB1	Req, Test	11/14/2007 12:59:19 PM	1354	1247	0:06:13	WindowsB1	user1
reqB1	Req, Test	11/8/2007 10:42:58 PM	1348	551	0:02:38	WindowsB1	user1
reqB1	Req, Test	11/7/2007 3:35:26 PM	1341	908	0:17:38	WindowsB1	user1
reqB1	Req, Test	10/31/2007 4:27:22 PM	1335	364	0:09:18	WindowsB1	user1

The integration of eGuardPost with PAR (either on the same appliance or separately) brings the level of password management and control demanded when providing critical resource access. You no longer have to manage the process of providing support, service of developers temporary ID's, passwords and access. eGuardPost can automatically retrieve the required account password from PAR and "auto login" the authorized connection – the password is NEVER exposed to the user. Thus there is no risk of password exposure and no risk of future unapproved access. For added password protection, PAR can be configured to change the

password after the authorized connection (even though not exposed, still changed) and/or change passwords every X days based on your specific password policy.



Contact info@preventia.co.uk today to discuss your specific requirements in more detail or to arrange a webex and/or product evaluation.