

PREVENTIA

Forward Thinking Security Solutions



Your Information Security Ally™

introduces...

Remote Vendor Access™ (RVA)

Not All Access Should be Treated Equally

[WHITE PAPER]

Written by
Kris Zupan, CEO/CTO, e-DMZ Security, LLC

Remote Vendor Access™ (RVA): Not all Access Should be Treated Equally

The New Requirement and Issue at Hand

With an increase in IT cost cutting, and the development of more and more specialized technologies and services available to solve existing IT and unaddressed security issues, many organizations are making the choice to enlist the help of vendors and consultants who provide specialized solutions and services instead of relying solely upon internal resources. A new requirement has emerged as remote vendors require privileged access to the organization's infrastructure in order to fulfill their expectations. Since many companies have already invested heavily to provide remote access solutions (tokens, VPNs, etc) to their employees, they look to leverage existing solutions for their remote vendors.

This paper will focus on why not all access should be treated equally. Neglecting to treat Remote Vendor Access™ (RVA) differently from traditional remote access for employees can introduce security risks ranging from virus infection to unauthorized access and non-compliance. The mission critical differences between employee remote access and RVA are significant:

- Remote vendors should have access restricted so they are only able to access the areas of the company they support. A remote vendor contracted to administer specific Unix systems should not be connecting to other systems or resources at will.
- Remote vendors use their own client equipment to establish connectivity. This means that requirements around Personal Firewalls, Anti-Virus, platforms, etc. are difficult if not impossible to enforce.
- Requiring remote vendors to utilize specific VPN client software to access remotely may not be possible and can introduce remote vendor system liabilities and/or create incompatibilities with existing vendor client software.
- Remote vendors have staff that is outside the view of the company. Staff changes at the vendor company may result in challenges around accountability.

Compliance Drivers

While these differences alone seem significant enough, the introduction of additional laws and regulations has added significantly to the list of RVA issues:

If the company is to be compliant with the Gramm Leach Bliley Act (GLBA), how does the company know that the vendor has not violated customer privacy while performing their service?

Similarly, under the Health Insurance Portability and Accountability Act (HIPAA), can the company ensure no patient data has been compromised? Specific to the Sarbanes Oxley Act, can the vendor directly or indirectly affect financial systems?

Remote Vendor Access Deserves Distinct Requirements

Since the areas most often supported by remote vendors include: system management, desktop management, application management, development, and security, the above mentioned questions are extremely difficult to address. Therefore, we submit that RVA necessitates a new set of remote access requirements distinct from those belonging to traditional employees:

1. The solution must provide granular access control, to completely control the access of the remote vendor.
2. The solution must be clientless, since most companies can not dictate the remote client system or software.
3. The solution must provide a complete and robust session and access audit trail, so companies can answer the regulatory questions of who had access and what did they do.
4. The solution must provide protection to the customer network from network pathogens like worms and malware.

A Solution that Meets the Challenge

An appliance based solution exists today that satisfies all of the above requirements. Recognizing the unique demands driven by Remote Vendor Access, eGuardPost™ was developed.

- ✓ eGuardPost provides granular access control, not only to the system, but also to the protocol and userid used by the remote vendor. Multiple grouping functions make this scalable for thousands of systems.
- ✓ eGuardPost provides a clientless solution. The only requirement for the client is a browser that supports Java.
- ✓ eGuardPost captures and records the entire session in a space efficient manner, much like a keystroke logging mechanism works for a terminal. Since the entire session is captured, this solution works for Windows systems, Unix systems, applications and network equipment.
- ✓ eGuardPost proxies the connection between the remote vendor and the customer system, meaning that no system level connection exists. Even if the remote vendor is completely compromised, there is no chance for that system to introduce malware into the customer network. The remote vendor connection to eGuardPost is HTTPS and SSH, eliminating the ability to pass netbios or other network traffic.
- ✓ eGuardPost saves hours of event log review while providing 100% accuracy when looking at past events. For example, a single remote vendor patch load can create many thousands of system event logs. It could take hours or days of detailed log review to conclude an authorized patch was loaded. With eGuardPost session capture, a simple reply in minutes shows the patch command which was executed.

In addition, eGuardPost supports two factor authentication tokens, has High Availability capabilities, and is delivered as a purpose built appliance hardened with a commercial grade embedded firewall and AES encryption.

eGuardPost and PAR Combination

The one question that often arises when implementing eGuardPost as a RVA solution is how to force the connection through eGuardPost. There are three basic solutions:

1. Implement network level controls so that the traffic is directed to eGuardPost, and prevent direct communication to the device.
2. Use PAR to control the credential utilized on the device to ensure that the password or credential is only available via eGuardPost.
3. All of the above.

Every eGuardPost ships with a version of e-DMZ Security's Password Auto Repository™ (PAR). PAR securely stores and manages passwords, and ensures the passwords are changed after use. eGuardPost can retrieve the necessary password from PAR and make it available to complete the connection. Used in combination, the solution offers the following benefits:

- PAR ensures the password is changed after use.
- Depending on the proxy type, the vendor may never see the password used.
- The vendor is not in control of the password to the device. This means that even if the vendor has physical access to the device, they do not know the password needed to access the system.
- Assures the only way the vendor can gain access is by working through eGuardPost.

Conclusion

Remote Vendor Access (RVA) provides a unique set of challenges that the industry needs to address. As part of a company's layered defense, RVA is beginning to receive additional attention as the perimeter matures. The question of how Vendor Access control is implemented is going to be asked, the challenge will be how well you can respond. eGuardPost has been viewed as a complete solution for RVA, filling the gaps left by traditional SSL VPNs or gateways. eGuardPost does not require that you divest in your current remote access technology. It can work independently or in conjunction with your existing remote access solution providing enhanced access controls, full session audit, and password management.

Choose eGuardPost because not all access should be treated equally.

