

Finding a Balance between Security and Convenience

Many banks have a limited number of IT employees on staff which means that they must often rely on outsourced assistance to help them keep their infrastructure and operations up and running. They may need assistance with their networking equipment, file servers, PCs, databases, security equipment, or their in-house core data processing system. Whatever the case may be, they need to provide secure remote vendor access to these systems.

One option is to provide vendor access via a Virtual Private Network (VPN). Unfortunately, this method is quite difficult to configure and virtually impossible to audit. Typically vendors have their own VPN software that is different and may conflict with what the banks uses, plus the bank typically has to interface with multiple vendors who need regular access. Unlike bank employees, banks do not have the same level of control or trust over remote third party connections.

While banks must trust their vendors, they still are required to closely monitor their activities. Their actions do not need to be malicious to cause damage – in fact in the majority of cases they are not – but they still need to be closely controlled. That is exactly why we designed our eGuardPost™ appliance to permit granular access that is recorded at every step of the way. You can think of eGuardPost™ as the equivalent of security cameras for your ATM – rarely used but invaluable when needed. Literally every keystroke, mouse movement and screen change is recorded and stored in an auto-archived, encrypted, and compact format for later review. Nothing could be more convenient for proving to auditors what outsiders are doing when they access your critical systems in addition to providing tremendous forensic value.

Just as important as the auditing capabilities of our solution are the password management and proxy access aspects of it. We include licenses to our Password Auto Repository™ (PAR) solution that permits IT administrators to automatically control access to their systems' passwords. This is especially important when you consider that vendors usually need high levels of authority (e.g., Root or Administrator) to do their jobs. In terms of proxy access for these accounts, the bank's IT staff can very easily limit each vendor to exactly the system that they are permitted to work on, unlike VPN access where once the remote user is on the network, they can view and possibly access the bank's entire IT infrastructure. The proxy also protects the bank from any viruses or mal-ware as the remote vendor does not have any direct connectivity to the back-end systems.

Banks need a seamless way to allow vendors to remotely assist them with ongoing issues, patches, updates, etc. Yet, auditors are taking a closer and closer look at this access as a potential serious security risk. The best solution by far of finding this balance is with our eGuardPost™ appliance because it requires no software to be installed at either end of the connection, and removes all of the headaches from managing remote vendor access in a secure manner that will satisfy the auditors.



Kris Zupan
CEO/CTO

Kris Zupan is CEO/CTO of e-DMZ Security and a CISSP. A seasoned veteran in the field of distributed security, Kris Zupan built and managed one of the largest Firewall and UNIX Security deployments while in tenure with a Fortune 10 Financial Services Organization. The UNIX Security Model he established there earned laudatory comments from Regulatory Agencies. Zupan founded e-DMZ Security on his visionary concept of Co-Managed Security Services, building on his extensive experience in providing the highest level of security for practical, 'real-world' applications. He has presented on the topic of UNIX Security and is active on various product advisory boards for security companies.

