

### *Protecting Member Data at Rest and in Motion*

One area that is growing in importance right now is remote vendor access. It is absolutely critical to control where vendors go and know what they did. While every credit union has a firewall and VPN (virtual private network) in place to help control outside access, these technologies do nothing to monitor where people go and what they did once inside the credit union's network. This issue is only growing in importance during these tough economic times when more and more credit unions are turning to outsourcing as a way to reduce costs and affordably support their IT operations.

Auditors are also starting to take a much closer look at vendor and consultant access into the credit union. They want to make sure that credit unions are adequately controlling and monitoring their vendor actions. There is a concerted effort on their part to make sure that credit unions vet their vendors more closely and put mitigating controls in place. This must be an ongoing effort because staff changes at the vendor may result in challenges around accountability. Whether it is the core system or other important software applications, it is simply not acceptable to turn over complete – and unsupervised – control to an outside party regardless of trust.

At e-DMZ Security, we have tackled this problem head-on with a powerful solution: eGuardPost™. eGuardPost is a stand-alone easy-to-install remote vendor access management appliance that allows for very granular fully recorded access control to specific servers or systems inside the credit union. At the other end, it is clientless since credit unions can not dictate the remote client system or software of their outside support teams. Our solution can also be used internally to capture and record access to important systems that contain member, HR and/or financial data. Credit unions gain peace of mind knowing that eGuardPost delivers 100% accuracy when looking at past events with DVR-like session playback. eGuardpost is like having a video camera in a parking garage, it is not looked at everyday, but in the event something happens, there is peace of mind knowing you can "review the tape".

Another important point to consider is that every eGuardPost appliance can be shipped 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. If a credit union has fifty or more systems to manage, this solution is the most efficient and cost effective way to manage passwords. eGuardPost and PAR are designed to work in conjunction to provide "auto-login" of remote vendors ensuring account credentials are not exposed to outside vendors. This provides the highest level of remote vendor access security possible – end to end accountability with no intervention from the credit union's IT Department.



**Kris Zupan**  
CEO/CTO



#### Contact Info

[www.e-dmzsecurity.com](http://www.e-dmzsecurity.com)

**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.