

## *Managing Risk and Security Efficiently and Affordably*

Given the current economic situation, banks are incessantly looking for ways to make their IT Departments more efficient and productive, while maintaining high levels of security. When administrators spend time changing passwords on servers, routers, switches and other network devices, they are being diverted away from working on projects that could help the bank with their core competencies such as gathering more deposits, adding new customers, funding new loans, etc. Every bank with more than a handful of servers and network devices should strongly consider boosting their productivity by implementing a password management package that will provide them with fully compliant life-cycle management of share/privileged accounts.

To address these concerns and automate these tedious password controls, we developed our Privileged Password Management (PPM) module which is part of Total Privileged Access Management (TPAM) solution suite. This solution includes out-of-the-box integration with Active Directory and eliminates the need for troublesome and time consuming manual password changes. Busy IT professionals will appreciate the fact that our solution is a secure, agent-less "drop-in" appliance with no additional software required for deployment. In addition, the appliance is secured with full disk encryption, expandable with other modules to control privileged sessions and infinitely scalable.

Another area that banks are currently concerned with is third party vendor due diligence. The FDIC auditors have made this a top auditing area in 2009 and they will continue to do so into 2010. No bank can afford to allow any vendor laissez-faire access to their network and systems. It is not a matter of trust, it is a matter of verification. Our Privileged Session Management (PSM) module, also part of our TPAM suite, solves this issue completely by delivering full session management, control and recording. Bank IT Departments can individually set access controls levels for each and every vendor that needs access to their servers, core data processing system, routers and other network devices.

With our optional Privileged Command Management (PCM) module, vendors can be restricted to running only certain applications that they need to perform their duties. On UNIX and Linux, we can control individual commands, while with Windows they can be restricted to specific programs or commands. Not only can we limit access to specific resources on a very granular level and eliminate exposure to potential vendor PC virus and malware infections, IT admins can easily view active connections, record all activity, configure connection approval workflow, be alerted if connections extend beyond allowed time and even terminate connections as required. Internal auditors and external examiners love the fact that we provide full session recording for a complete audit trail that is easily reviewed at any time.

Since 2001, e-DMZ Security has focused on securing IT infrastructures, tackling issues like Privileged Password Management and Remote Vendor Access and Monitoring. Over the years, we have continually updated our product suite and it has now evolved into the Total Privileged Access Management (TPAM) Suite. Banks that want to resolve all of their privileged identity, access and audit requirements can be assured that TPAM will provide a flexible, modular and affordable solution.



**Kris Zupan**  
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.

