

Perimeter, Host and Endpoint Security – Finding the Right Mix

Perimeter security devices like firewalls, Intrusion Prevention and Intrusion Detection Systems have been around for many years have reached quite a mature level. At this point, the vast majority of banks have solid perimeter security defenses in place, and now they are starting to look inward where there is still much work to be done on the local area network, servers and desktops.

Increasingly banks are taking a look at NAC (network access control) to help lock down their internal networks. They are also considering new ways to secure databases – both for access and encrypting critical personal data. Another area that is garnering quite a bit of attention right now is application level security. Essentially many organizations are searching for ways to add effective layers of control from the inside.

A bank's core system holds their crown jewels: customer information. Any bank with an in-house data processing system has to take extreme care to guard the access to their core system. It is a fact of life that issues will always arise that require outside assistance from the core system vendor's support staff, consultants, and outsourcing partners. This access represents a significant security and compliance risk for banks because they are basically asked to turn over complete – and unsupervised - control of their core system to an outside party.

At e-DMZ Security, we have developed a unique solution to this Remote Vendor Access problem: eGuardPost™. eGuardPost™ is a stand-alone Security management appliance that delivers complete control over incoming connections using a proxy approach. There is no carte blanche access to a bank's internal network with eGuardPost™ because it is easily configured to only provide access to specific servers or systems inside the bank. Add the option of dual authorization connection control and you have a solution that is unmatched in providing secure granular remote access.

While some organizations may say that they offer their vendors secure access with a VPN (virtual private network), unfortunately a VPN only controls who accessed a network and when they accessed it. They leave out the most important part: what they did when inside the network. Keystroke logging has been popular for many years in Unix environments, but now eGuardPost™ extends this powerful capability to Windows systems, terminal services and more. eGuardPost provides a complete recording of internal support activities, plus it includes end-to-end session recording, logging and playback of every keystroke, mouse movement and application accessed for event reconstruction purposes.

Now IT Departments – and the auditors that monitor them – can be 100% confident that they are aware of exactly what happened on their systems. They can be assured that no one uploaded any confidential information, downloaded any malware, or turned on a sniffer. With the ability to incorporate dual control, password management, enhanced reporting, and secure storage, eGuardPost™ provides a world class tool for helping to control consultants, vendors, or the bank's own employees.



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.

