



Perimeter, Host and Endpoint Security – Finding the Right Mix

In the past, security at the perimeter and network edge took precedence, but the balance has gradually shifted over the years. While it is still important to secure the perimeter because the old attacks featuring scripts, bot-nets, port scanning, etc are continuing unabated, the inner edge and the core of the network are gaining more attention. Unfortunately the inside and outside threat levels are blurring and banks must work hard to protect against all types of threats regardless of where they originate.

In many regards there is a 'perfect storm' brewing: hackers now have easy access to the tools, networks and specialized knowledge that they need to launch complex attacks. There is a whole new world of attack methodologies and techniques, and many of them involve lodging themselves inside the bank's network with remote control, root kit, and/or keylogging software. This means that banks must do a better job of securing individual systems such as file and database servers that hold sensitive data, as well as individual workstations. It is critical for IT Departments to always know who is accessing their systems and from what location.

Host-based Intrusion Prevention Systems are gaining popularity as a result of these new inside attacks. Many of our clients now are using a layered Intrusion Prevention strategy – one that combines Network Intrusion Prevention with a full featured Host-based Intrusion Prevention implementation. We design these systems to work in concert to deliver a defense in depth solution.

Additionally, we can obtain a contextual view of the flow of data through the bank's network which allows us to enforce security controls and policies from a central location. It is always important to strictly enforce the bank's policies and we accomplish this with our Policy Compliance service. This service utilizes a comprehensive series of system security tests to measure various security aspects of the computers located on the bank's network and compares the results with Perimeter's Recommended Security Policy.

With so many different layers of defense needed today such as e-mail, user, network, system, vulnerability, and intrusion; it can be quite difficult for banks to decide where to start. Virtually all banks have at least two or three layers of defense in place, so the big question becomes what should I do next? At Perimeter eSecurity, we have helped thousands of banks answer that question and focus their efforts in the most risk-appropriate areas. With over fifty different security products, our goal is to tailor the right solution to each bank's specific needs. We call this 'complete security on demand,' and Perimeter makes this world class security easily available and affordable for banks of all sizes.



Kevin Prince
Chief Security Officer

Kevin Prince

is the Chief Security Officer (CSO) at Perimeter eSecurity™. In this role, Kevin assists with the company's strategic plan and is responsible for many of its strategic relationships. A well known expert in the security industry, Kevin has been asked to train national and federal organization employees on relevant security issues over the years. Topics that Kevin has spoken on include firewall security, remote access, virtual private networks, intrusion detection and prevention systems. Perimeter eSecurity™ is the leading provider of multi-threat, managed "Security in the Cloud" services to financial institutions and other firms with high data security and regulatory requirements.

