

Perimeter, Host and Endpoint Security – Finding the Right Mix

It is a fact of life that today's network perimeter is breaking down and becoming more porous. The traditional "moat approach" simply is not applicable anymore. That is because there are so many areas within the bank that need to be secured now. Plus there are quite a few departments within the bank— Human Resources, Marketing, IT, etc – that require various levels of secure access to critical data. This makes even role-based access difficult to configure and enforce.

The traditional "circle the wagons approach" is not practical and is being replaced by what I like to call the "Kevlar approach." When you circle the wagons, you go nowhere, but with the Kevlar approach you are agile and using a layered system that provides for much more flexibility. This is particularly important when it comes to online banking and electronic services.

At Arcot, we offer a complete line of industry leading Strong Authentication and Risk-based Authentication solutions. Our 100% software solutions satisfy FFIEC requirements for strong authentication for online banking. Many banks start with our risk-based authentication system (RiskFort) and then later move on to our more advanced system that uses the PKI-based software (WebFort). They can also choose our SignFort solution for their digital loan documents and e-statements.

Our goal is to provide multiple layers of authentication as unobtrusively as possible. Banks need to be able to dynamically adjust the level and method of authentication based on each situation due to the fact that fraud is a constantly moving target. Our software protects against phishing, man-in-the-middle and spyware attacks, all while keeping the user experience for the customer as simple as possible.

All of this becomes much more important as banks offer more sophisticated online services to their customers such as account-to-account transfers, wire transfers, business banking, etc. These types of advanced online functionality demand a more robust risk-based approach that is above and beyond simple login authentication. It is important to remember that any fraud fighting system must not only keep the bad guys out, but also must be as seamless as possible for legitimate online bankers to use.

Every bank must take into account their customer base when implementing a system, but the intent should always be to make it as user friendly as possible. Users simply sign up for our system at their bank's online banking site, then they receive a token that comes through the Web page itself and is placed on their machine as a file that the authentication engine recognizes as unique to that particular user. Essentially it is as straightforward as what they are already used to: a username and password. That is the beauty of all of our software solutions - they are very foolproof and designed from the ground up to be user friendly.



R. 'Doc' Vaidhyanathan
Vice President

R. 'Doc' Vaidhyanathan is Vice President of Product Management at Arcot. Prior to Arcot, Mr. Vaidhyanathan was Vice President at Majesco Software where he was responsible for global outsourcing. Doc previously held management and development positions at TDICI and Tata Unisys. Doc holds a B.Tech from the Indian Institute of Technology and an M.B.A. from the Indian Institute of Management. Arcot Systems, Inc. is a leading provider of software-based digital signatures and identity solutions. Arcot's solutions combine the ease-of-use, scalability, and cost-effectiveness of a software format with a breakthrough technology approach that offers maximum online protection.

