



Perimeter, Host and Endpoint Security – Finding the Right Mix

IT Departments have been focusing for years on the perimeter, but it has only been recently that they have begun to turn their attention to the inside of their networks. Statistics show that more than fifty percent of security issues – both accidental and intentional - originate from the inside. Of course the perimeter still needs to be protected, but now more focus is being placed on the local area network and data leakage problems. This extends all the way down to the end-point, e.g., what USB devices, MP3 players or cellular phones are being plugged into the bank's desktops.

The vast majority of banks don't have dedicated security teams or even any extra IT resources available to closely monitor their infrastructure. There is so much at stake today with security breaches: sensitive customer data can be compromised; money can be moved out of the bank; and the bank's credibility can be brought into question by customers and the general public. However just adding more and more layers of security and point solutions is not enough. What banks really need is visibility across their network.

At TriGeo, our goal is to protect the entire network environment, from perimeter to endpoint, with a comprehensive, integrated solution that responds to threats in real time. The TriGeo Security Information Manager (SIM) sits in the middle of the bank's network – collecting and analyzing logs from firewalls, switches and routers - and delivers a crystal clear view of all network activities in an easy to understand format. Our product arrives with hundreds of preconfigured rules and reports that provide IT Departments with the ability to automatically quarantine, block, route and control services, processes, accounts and privileges. After installing our system, many clients immediately discover items such as unusual network traffic, misconfigured routers, and prohibited devices. Many of them tell us that they have a feeling of control over their systems for the first time.

Last year we added some powerful new products to complement the TriGeo SIM. We introduced TriGeo InSight™ which is the first business intelligence (BI) product for network management and security. Combined with the TriGeo SIM, this robust BI software allows IT Departments to isolate and analyze data at a granular level, and fine-tune their security posture via a simple point-and-click interface. We also rolled out TriGeo InDepth™ an IT search solution powered by Splunk™ technology. Designed to complement the TriGeo SIM, InDepth aggregates and archives log data in real time, with patented data collection, storage and indexing technology that delivers secure and repeatable searching across terabytes of data.

Most banks think that an investment in a Security Information and Event Management (SIEM) solution will cost hundreds of thousands of dollars, but we have turned that assumption on its head with our affordable SIEM solution that is specifically designed for small and medium-sized organizations. Our pricing, functionality and commitment to customer service are why we have enjoyed so much success with community banks.



Michelle Dickman is president and chief executive officer of TriGeo Network Security. Ms. Dickman has spent over 20 years in the software and financial industries combined. Much of her extensive management, sales and marketing experience has been focused on the midsize enterprise which is TriGeo's core market. Dickman also brings considerable business development and management skills to TriGeo. As the co-founder and President of an ERP software company, Dickman grew that organization from ten to nearly one hundred employees, with four regional offices, and annual growth ranging from 20 to 60 percent. Her leadership ultimately led to the organization's acquisition by a public company.