

Perimeter, Host and Endpoint Security – Finding the Right Mix

Before banks purchase any additional security-related hardware, software or services, they should step back and evaluate where they are, what is required to protect customers (FFIEC mandates/guidance), and how their decisions will fit into their Information Security Program. In order to have an effective Information Security Program with excellent reporting, all systems must be able to communicate and collaborate.

In the past, banks often used only a few security products, but today some may have up to ten or fifteen when you look from the perimeter all the way down to the host. While this arrangement is good for a defense in depth strategy, it is nearly impossible to effectively integrate, manage, and report on numerous disparate systems. Banks need to be able to integrate these diverse layers from the perimeter all the way down to the endpoint.

While on the surface it may seem that 'best of breed' systems are always preferable, this isn't always the case. You can have the best airbag in the world, but if your car's front impact sensor isn't integrated to tell the airbag to release and protect you during a front impact, then best of breed doesn't keep you safe. This is the same when it comes to end point security solutions communicating with the perimeter. All of the various security systems and network devices – firewalls, routers, switches, IDS, IPS, VPN, log management, etc – must be able to communicate with each other in order to effectively detect and prevent attacks.

At HEIT, we made a conscious decision from our inception years ago that we would only offer banks integrated solutions that are speaking the same language. That is why we chose to partner with the largest security company in the world: Cisco. And in recognition of our solutions and customer satisfaction at banks, we earned Cisco's prestigious "Financial Services Partner of the Year" 3 times running.

The key to our approach is the HEIT Self-Defending Network for Banks which means that all systems from the perimeter to the endpoint are identifying, preventing, and adapting to threats from both internal and external sources. We offer the Cisco Adaptive Security Appliance (ASA) which is the number one selling firewall and IPS appliance in the world. Then we make sure that the Network IPS is collaborating with the Host IPS to give the right risk rating.

On the desktop and servers, we offer the Cisco Security Agent (CSA) which is a critical component of multi-layered security strategy, protecting banks from data leakage and zero day attacks. Additionally, CSA ties into the Cisco Self-Defending Network by collaborating with Cisco ASA and Cisco Monitoring, Analysis and Response System (MARS). The security monitoring capabilities that are built into MARS greatly reduce false positives by providing an end-to-end view of the network. Our FFIEC based reporting is like no other in the industry, because we have the ability to report on a holistic point of view in regards to your Information Security Program. At HEIT, we deliver a true end-to-end integrated solution that meets banks' operational, security, and strategic IT needs.



Dan Holt
CEO

Dan Holt is co-founder and CEO of HEIT, Inc. Mr. Holt is responsible for all aspects of the corporation including management, company development, strategic partnerships, and overall corporate strategy. Under his leadership, the company continues to expand nationally earning numerous accolades including: Cisco's Financial Services Partner of the Year; ReymannGroup Certified Enabler; and a leading Industry Solutions Provider for Banks and Credit Unions. Additionally, Holt is a leading information technology expert for the financial services industry and specifically delivers thought leadership at Bank seminars, speaking engagements, and provides expertise on the Federal Financial Institutions Examination Council (FFIEC) guidance.

