
Case Study

Client Profile

Leading regional financial institution.

A New Approach to an Old Problem

webApp.secure™ uses unique web/insite™ technology to automatically recognize and enforce the Web site's Intended Use Guidelines™ (IUG). Any activity that does not meet the IUG is automatically blocked and reported.

Approaches based on signature recognition are, by definition, reactive since they need to know what an attack looks like before they can protect against it. Evaluating activity based on the IUG ensures prevention of both known and unknown attacks.

Limited IT Resources. Unlimited Exposure.

The client offers their customers the advantage of viewing check images over the Web. While this is extremely convenient for the account-holder, and reduces costs for the financial institution, it makes compliance with federal regulations like the Gramm-Leach-Bliley Act difficult.

In their environment, the on-line banking system requests check images from a Web server hosted by the client. Previously, their network firewall did not allow incoming traffic of any kind. They were justifiably concerned about opening even one TCP Port (443) to allow check image retrieval.

They selected webApp.secure because it offered superior protection without the complexity of other solutions. It held up flawlessly to independent 3rd-party penetration testing, but does not strain their already taxed internal IT resources.