American National Bank

Protecting thousands of customers and employees from advanced threats

Overview

The need

American National Bank wanted to stay ahead of fraudsters and better protect its customers and employees against advanced threats.

The solution

The bank deployed advanced fraud prevention solutions from IBM that help detect, block and remediate malware and phishing threats across both customer and employee endpoints.

The benefit

The solutions protect more than 10,000 customers and employees, stopping malware that traditional antivirus software has missed, to help avert fraud losses and increase customer confidence.

A subsidiary of American National Corporation, American National Bank provides a full range of banking, treasury management and wealth management services to businesses and consumers. With USD2.1 billion in assets, the bank has 32 locations in Nebraska and Iowa.

Staying ahead of fraudsters

How can we best protect our customers from today's security risks? It's a common question for all banks, and at American National Bank, the answer lay in expanding its visibility to the customer endpoint.

Customers appreciate the bank's fraud prevention efforts. "Over 100 customers attended a recent security seminar, and customers are thankful when we contact them about a malware report," says Andy Bingham, Product Development and Client Liaison, Treasury Services, American National Bank. "The solution has turned out to be more straightforward than we expected."

Solution components

Software

- IBM® Security Trusteer Rapport®
- IBM Security Trusteer Apex™ Advanced Malware Protection

Bank customers remain a prime target for fraudsters, and without insight into end user systems, bank staff had to rely on customers to report problems—such as strange email requests for banking information or peculiar web application behavior when banking online. When malware was suspected as a result of these calls, bank staff couldn't help the customer resolve the issue.

"The goal is zero losses," says Andy Bingham, Product Development and Client Liaison, Treasury Services, American National Bank. "We want our customers to have confidence that we're on top of things. At American National Bank, protecting our customers is our primary responsibility. We're actively working to stay ahead of fraudsters."

"To have visibility of the endpoints is critical," adds Amanda Klug, desktop and applications support manager in the bank's IT department. "And we wanted to provide support to our customers without having to take over their PCs."

Proactively identifying known and emerging threats

To help prevent phishing and malware attacks on customer endpoints, the bank implemented IBM® Security Trusteer Rapport® software.

Using behavioral algorithms to uncover anomalies in web application behavior, the software can detect, block and remove both known and emerging threats. When malware is detected, customer support representatives receive alerts and immediately contact the customers—often within minutes—to inform the customers that malware was detected on their computers and to ask them to take remediation action. The software is delivered via a software-as-a-service (SaaS) model, helping ensure customers are continuously protected against new threats.

> *"Trusteer Apex has alerted us to threats on employee systems."*
>
> —Amanda Klug, Desktop and Applications Support Manager, American National Bank

In evaluating solutions, bank staff spoke with colleagues at other banks who use Trusteer software. "We were comfortable after talking to other banks with the solution's capabilities and its ability to meet our goals," says Bingham.

Because small businesses are frequent targets of financial fraud, bank staff decided that use of Trusteer Rapport software would be mandatory for its commercial customers. The bank's retail division offers the software as an optional benefit to consumers. Currently, more than 10,000 commercial and retail customers are protected.

Getting started quickly

To help educate customers regarding its new fraud prevention program, the bank launched a comprehensive communications campaign that included a promotional brochure, new web content and targeted "splash" messages. Treasury Services staff also sent emails to commercial customers at regular intervals to remind them that downloading the software was mandatory. Internal training prepared bank staff to answer any customer questions.

The bank drew heavily from the planning guides and marketing content provided by IBM. "We used the materials IBM provided to help us plan our deployment, maximize acceptance, and market the software to our end users," says Bingham. "The documentation is extremely good and the materials helped us move forward very quickly."

Achieving nearly 100 percent adoption in only four months

A best practice that enabled the bank to complete mandatory adoption with nearly 3,500 commercial users in only four months was its early adopter program.

"We're actively working to stay ahead of fraudsters. The goal is zero fraud losses."

—Andy Bingham, Product Development and Client Liaison, Treasury Services, American National Bank

"We thought that the path to acceptance might be a little longer for some of our largest commercial customers, so we reached out to our top 50 corporate customers before we rolled Rapport out," says Bingham. "We let them know what we were doing, offered to meet with them individually, and suggested they download the software early. Some of these customers did need to go through an approval process and appreciated the early warning."

Protecting employee endpoints with Trusteer Apex software

As part of its fraud prevention efforts, the bank is also expanding endpoint security to employee desktops. The bank is currently deploying IBM Security Trusteer Apex™ Advanced Malware Protection software across nearly 600 employee PCs.

The software provides a multi-layered defense architecture that helps the bank detect and mitigate advanced malware, protect employee credentials, disrupt the exploit chain and prevent malicious communication.

"The logic behind getting Trusteer Apex was very similar to why we deployed Rapport," says Klug. "It gives us peace of mind, providing an added layer of security above and beyond what our current antivirus software gives us. It's not fully deployed yet, but where it is deployed, Trusteer Apex has alerted us to threats on employee systems."

Averting fraud losses

For Bingham, the solution has been fundamental in helping the bank mitigate risk for both itself and its customers.

"It's very likely that we have averted loss of funds," says Bingham. "Since implementing Trusteer software, we have been alerted to many active malware infections on customer machines. Trusteer gives us confidence that we are helping to protect our customers during their online banking sessions and averting potential financial losses. Our focus has been on loss prevention and staying ahead in the anti-fraud game."

Cybercriminals are constantly changing tactics, which creates significant challenges for security teams. Working with IBM Security staff, Bingham says, also gives the bank vital insight into what's happening and what may be coming next.

"We recently had a situation with the Neverquest malware in which several of our customers and employees were hit at the same time," says Bingham. "The ability to have access to expertise at IBM to better understand what was happening and why it was happening was a time saver and certainly made us more knowledgeable."

For more information

To learn more about IBM Security Trusteer® software, please contact your IBM sales representative or IBM Business Partner, or visit the following website: **ibm.com**/security

For more information about American National Bank visit: www.anbank.com

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
March 2015

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.