

# Value for the Dollar—Network Protection and PCI Compliance

## Amarillo National Bank

### Overview

Amarillo National Bank (ANB) was founded in 1892 and is now one of the largest family-owned banks in the nation and voted the #1 bank in Amarillo, TX for seven years in a row. The IT staff at ANB work hard to ensure their network is secure and compliant with the latest banking industry regulations.

### The Quest for PCI Compliance

The Payment Card Industry Data Security Standards (PCI DSS or simply, PCI) are a set of worldwide information security regulations for all merchants that accept credit cards. The standards are intended to protect cardholder data. Among those standards is a directive to regularly monitor and test networks for rogue wireless devices.

Bill Davis, Data Security Administrator for ANB, was tasked with making the bank's network PCI compliant. In researching products to fulfill this PCI requirement, Bill looked into wireless scanners, point solutions that discover rogue wireless devices by tracing a wireless signal. As an IT department in a privately held bank, the ANB IT staff works to derive optimal value from each expenditure. Wireless scanners could fulfill the rogue access point detection requirement, but could only perform that single function. Davis decided to continue his investigation and discovered eTelemetry's Locate.

### Network Visibility with Locate

Locate is a plug-and-play network appliance that correlates people on your network with their IP address, MAC address, and switch port in real time and historically. Locate's rogue access point detection feature enables administrators to identify, locate, alert, and disable rogue access points on the network. Locate continuously applies its proprietary access point scoring algorithm to all people, devices, and switch ports discovered on the network to identify potential rogue access points and tag known access points as approved. Immediate access point identification for Davis and ANB protects his network better than the quarterly scans required by PCI. "With Locate, we don't have to wait to find a problem," commented Davis. This coupled with the ability to shut down a rogue device's access by switch port, provides Davis with a solution for his PCI needs that was much more robust than a hand-held wireless scanner.

Davis also considered purchasing a more expensive and extensive network monitoring system, but realized that he, "got the same information from Locate, a 'pizza box' appliance that I plug into my network and spend 15 minutes configuring." Locate's additional functionality, and its low cost—less than that of a single hand-held wireless scanner—made Locate the clear choice. "It was really a no-brainer decision to buy a product that would provide a wireless access report, and also IP, MAC, and switch port address information so that I can validate my current infrastructure

#### PCI Requirements for Wireless Access Points

11.1 Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.

11.1.a Verify that a wireless analyzer is used at least quarterly, or that a wireless IDS/IPS is implemented and configured to identify all wireless devices.

11.1.b If a wireless IDS/IPS is implemented, verify the configuration will generate alerts to personnel.

11.1 c Verify the organization's Incident Response Plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.



and turn it into a forward protection device to show me what's on my network," said Davis. "The ability to disable by switch port is a great feature!"

In addition to PCI compliance and validating infrastructure, Davis plans to leverage the person to switch port visibility provided in Locate to be proactive in the unending fight against viruses. "Antivirus is good," he said, "but it's reactive not proactive—with Locate you log on, find the infected machine, find its switch port and shut it down."

IP Address	Hostname	MAC Address	Switch Port	Manufacturer	Manuf. Score	MACs	IPs	Accounts	Total Score
Hide 192.168.201.204		00:08:74:2d:9f:95	192.168.10.254.4/46	Dell Computer Corp.	n/a	n/a	n/a	13	65
Hide 192.168.100.219		00:08:74:2d:e3:0a	192.168.10.254.5/16	Dell Computer Corp.	n/a	n/a	n/a	12	60
Hide 192.168.100.194		00:0c:0b:5b:e5:e9	192.168.10.253.3/12	Dell ESQ PCBA Test	n/a	n/a	n/a	5	25
Hide 192.168.100.93		00:08:74:ab:ad:02	192.168.10.243.3/59	Dell Computer Corp.	n/a	n/a	n/a	5	25
Hide 192.168.101.160		00:04:56:ed:53:7b	192.168.10.254.2/32	Dell PCBA Test	n/a	n/a	n/a	5	25
Hide 192.168.200.76		00:08:74:2d:9e:35	192.168.10.254.3/43	Dell Computer Corp.	n/a	n/a	n/a	5	25

Locate's Rogue Access Point Detection feature provides the IP and MAC addresses, switch port, and manufacturer information for potentially suspicious devices.

To further increase the proactive defense of his network, once Davis identifies all devices on the network, creating a baseline of devices on the network, he will utilize Locate's new MAC address alerting functionality to receive notifications for every new MAC address that appears on his network. This will enable Davis to investigate potentially suspicious devices before they become a threat.

### Rolling Out Access

Davis plans to roll out access to Locate beyond his IT staff. Its ease of use makes it possible for even non-technical bank employees to gain value from the information Locate provides. Davis will eventually grant access to auditors to enable them to monitor changes to the network and get an auditable network change report, freeing his staff from spending time usually spent tracking and documenting such changes themselves. With Locate, Davis has been able to not only meet PCI compliance requirements, but also get network endpoint visibility and control he had previously not had before. Said Davis, "Locate provides value for our dollar and protection for our network."

Contact eTelemetry



Turning Network Traffic into Business Intelligence

41 Old Solomons Island Road • Suite 202 • Annapolis, MD 21401  
Phone: 888-266-6513 • Fax: 410-266-0796 • www.eTelemetry.com

