FireEye
SECURITY REIMAGINED

Citizens National Bank of Texas increases advanced cyber attack protection with FireEye

CUSTOMER STORY

KEY COMPONENTS

- FireEye Network Threat Prevention Platform

Citizens National Bank of Texas takes great pride in retaining a personal touch to meet the needs of local customers and communities. Wade Jones, CIO and senior vice president at the bank explained how this impacted his own role. "Because we see most of our clients face-to-face each day, there is a much closer relationship compared to the way the national and global banks interact with their customers. If we don't fiercely protect data with the latest data security measures, a single breach could damage our reputation."

The bank previously relied on a firewall for application-level blocking,an email gateway, and an anti-virus solution to protect its infrastructure. Jones noted, "The existing combination was capable of identifying certain malware activity but we found we were always reactively responding to attacks. We were never in a position to proactively address the threats."

COMPANY	Citizens National Bank of Texas
INDUSTRY	Financial Services
DESCRIPTION	Founded in 1868, Citizens National Bank (CNB) of Texas is the third oldest independent bank in the state. Headquartered in Waxahachie, Texas, with 150 employees spread across thirteen branches, the bank holds combined assets in excess of $550 million. CNB of Texas has a stated commitment to invest in the best technologies to safeguard information and advance the capabilities offered to its customers.
CHALLENGE	• Maintain its commitment to protecting sensitive client data against increasingly sophisticated Web-based attacks • Identify a proactive and preventative approach to handling threats that addresses shortcomings in existing security portfolio • Protect against attacks launched from Web browsing and malicious URLs in email messages • Avoid impact to employee productivity caused by having to take desktop devices offline to resolve security issues
SOLUTION	• FireEye Network Threat Prevention platform
BENEFITS	• Malicious threats proactively countered without the need to take users offline • Multi-vector protection for Web-based and email weaknesses • Defenses implemented against exploits that elude the bank's other security measures

"With our FireEye Network Threat Prevention Platform we don't have to worry about malicious threats to our systems and we can now proactively block malware from reaching desktops. And because the computers are now truly locked down, users don't experience downtime anymore."

— **Wade Jones,** CIO and senior VP, Citizens National Bank of Texas

FIREEYE LOCKS DOWN INFRASTRUCTURE

Following a recommendation by an independent security consultant, the bank performed a detailed evaluation of the FireEye platform. "The inherent intelligence of FireEye's solution was immediately evident and we felt that our purchase of the FireEye® Network Threat Prevention Platform represented the final piece in the puzzle to lock down our infrastructure," recalled Jones.

The FireEye Network Threat Prevention Platform is deployed inline between the firewall and Internet gateway; preventing malicious multi-protocol callbacks and blocking inbound Web exploits that elude the bank's other security measures.

As an integral component of the FireEye Network Threat Prevention Platform, the FireEye Multi-Vector Virtual Execution™ (MVX) engine confirms zero-day attacks and captures callback destinations to dynamically prevent users from accessing a malicious channel. The signature-less FireEye MVX engine executes suspicious binaries and Web objects against a broad range of browsers, plug-ins, applications, and operating environments to determine the true intent of the malicious code.

"The FireEye Network Threat Prevention Platform not only protects our users when they visit websites but also when they receive email with malicious attachments or links: having both levels of protection is absolutely critical to us. The whole banking industry is subjected to a huge variety of very sophisticated attacks that exploit both Web and email weaknesses. We see many spear phishing attacks in which malicious emails disguise themselves as coming from legitimate business partners. If users click on a bad link or attachment that initiates a callback, the FireEye Network Threat Prevention Platform blocks it every time," stated Jones.

BETTER PROTECTED AND MORE PRODUCTIVE BECAUSE OF FIREEYE

Several Citizens National Bank of Texas employees recently received an email that appeared to come from a trusted business partner. Jones elaborated, "Five users tried to open an apparently innocuous attachment but the FireEye Network Threat Prevention Platform detected that it included embedded malware and immediately started blocking the approximately 200 callbacks each machine tried to generate. If any of these reached their intended target they could have severely compromised the bank's systems but the FireEye solution just doesn't allow this type of data to leave our network."

Jones declared, "FireEye has placed us in the position to proactively counter malicious threats; we now don't have to take a user offline in order to rebuild their PC following an attack. We're better protected and more productive!"

"Cybercriminals grow smarter all the time, that's why our use of the FireEye next-generation security platform is now mandatory throughout the bank's infrastructure."

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**