CASE STUDY

Banking on Airtight Protection

Institutions that handle and store money have always had to focus on security—and by now, they've become pretty good at it. Despite corporate America's rapidly increasing awareness of cyber threats and heavy investment in protective measures, turning banks' websites and mobile apps into the modern equivalent of Fort Knox remains a tricky proposition.

Trustwave®

Client Spotlight

With $400 million in assets and more than 90 employees across eight locations, this community bank has been serving local customers for a century. It recognized early on that cybersecurity had to be a top priority—and that it simply didn't have the in-house resources to protect its customer data. As a result, it has outsourced its protection to Trustwave for more than a decade.

The Challenge

A community bank on the Eastern Seaboard needed to establish the same elite security protocols as the country's mega-banks—but with only a sliver of the resources. This long-term Trustwave customer also wanted to help ensure that its safety measures, many of which were adapted years ago, remained cutting-edge.

> *"Over the years, Trustwave has kept up with security enhancements and made user-friendly changes for reporting. I can easily login to the Trustwave TrustKeeper portal to make a request for any needed changes, and it gets taken care of quickly."*
>
> – Senior vice president and COO, community bank

The Solution

The bank selected Trustwave Managed Security Services to provide cost-effective, 24/7 network monitoring, URL filtering, unified threat management, and intrusion detection. This broad threat-fighting arsenal can be easily accessed and customized by bank executives via the Trustwave TrustKeeper portal, which helps them stay abreast of security issues across multiple branches. Trustwave even secures the bank's email, siphoning off the whopping 70 percent of incoming messages that are identified as spam.

Industry Threat

Financial institutions suffer the highest cyber-theft-related costs of any industry: Banks and similar institutions spend a mind-boggling $18.3 million each year on cyber crime, according to Accenture. And while financial companies have long been leaders in managing risk and establishing consumer trust, the recent explosion in mobile banking introduces an entirely new set of problems. Executives must now contend with mobile malware, unsecured Wi-Fi networks, and third-party apps that can be compromised.

> *"A security model that includes continuous network monitoring and web security helps provide us with protection against any threats and was easy to accomplish."*
>
> – Senior vice president and COO, community bank

Trustwave®