



CrowdStrike Customer Case Study



Texas Bank Raises Its Cybersecurity Capabilities to the Next Level with CrowdStrike

As a financial institution, Central National Bank of Waco is an attractive target for cyberattacks — it surpassed \$1 billion USD in assets in 2021. The community bank is owned by eight families who serve on the board of directors and has four locations in central Texas. With over 15,000 customers and 100 employees, it also is a commercial bank serving small-to-medium-sized businesses. In addition, as a national bank, Central National Bank is heavily regulated and audited.

Rusty Haferkamp is chief information security officer (CISO) at Central National Bank of Waco. No stranger to cybersecurity, he is laser-focused on protecting customers' assets. Overall, the bank was doing a good job in this area, but Haferkamp knew more could be accomplished.

CrowdStrike Elevates Security by Providing “Emergency Room” Service

A couple of years ago, Haferkamp contacted CrowdStrike after an incident occurred in the middle of a forensics audit of the bank's security system. Luckily it did not require any mitigation, but it was enough for the CISO to step in. To close the gap, Central National Bank of Waco partnered with CrowdStrike for the deployment of CrowdStrike Falcon Complete™ managed detection and response (MDR) throughout the organization.

This cloud-based service represented an elevation in cybersecurity for Central National Bank of Waco. “CrowdStrike is the emergency room for 2022,” Haferkamp said. “Falcon Complete has given us the ability to clean up the network and trim down the noise. Now, our attack simulations are correlating with CrowdStrike's findings, and we get single-page, easy-to-read reports with phenomenal information.”

Small Businesses — and Cybersecurity — Have Evolved

Haferkamp once owned a small computer consulting business. Those years of experience, coupled with the knowledge gained in his current position, provided the skillset to recognize the need for elevated security. “We are in a new phase of technology,” he said. “Small businesses used to have an IT person on staff who fixed any problems, or perhaps a generalist who knew how to update the system. However, that person was not trained to replace a firewall or SQL server. They had an antivirus agent running, and they hoped everything worked out because they did not have reporting or logging capability.”

However, as the frequency of cyberattacks has surged, small businesses — including banks — have needed to adapt and increase spending on cybersecurity tools to protect customers' assets. “We have progressed a lot when it comes to being proactive instead of reactive, but we can't do it overnight,” he explained. “There is employee training and customer training, for example.” And they could not do it alone.

INDUSTRY

Financial Services

LOCATION/HQ

Waco, Texas

CHALLENGES

- Reactive, labor-intensive cybersecurity strategy
- Manual threat management
- High cost of cybersecurity services

SOLUTION

Central National Bank of Waco uses CrowdStrike Falcon Complete™ managed detection and response to ensure customer data is protected by cloud-delivered, next-generation endpoint protection.

“CrowdStrike is the emergency room for 2022. Falcon Complete has given us the ability to clean up the network and trim down the noise. Now, our attack simulations are correlating with CrowdStrike's findings, and we get single-page, easy-to-read reports with phenomenal information.”

Rusty Haferkamp

Chief Information Security Officer
Central National Bank of Waco



CrowdStrike Customer Case Study



"Falcon Complete MDR has taken all the granular tools we have been running for years and added a whole other layer that up-levels our protection — and it did this with zero impact on users," Haferkamp said. "Since bringing in CrowdStrike, there haven't been any high-severity issues. Falcon Complete MDR identifies any low-severity issues that could have easily slipped under the radar in the past."

Once Central National Bank of Waco started using CrowdStrike, Haferkamp's team began seeing the alerting and reporting features and everything else CrowdStrike was doing. "It was such a relief," he said. "I am much more comfortable with my network now. If we have an incident, I am confident that we will not have a problem thanks to CrowdStrike."

"CrowdStrike gives me the ability to go home and relax. Any time we have an alarm, the hair on the back of my neck rises if I see failed authentication attempts in our Active Directory. However, with CrowdStrike I can tell very quickly what is going on. The process tree in the MDR portal delivers all the information within a matter of seconds, instead of someone here spending a couple of days working on it. With the automatic remediation it delivers, I don't have to worry that someone has accessed our systems."

Close Working Relationship with CrowdStrike Provides Peace of Mind

Haferkamp wants to be able to call the bank's cybersecurity resource and feel confident he's talking to someone who is educated and knowledgeable about his environment and about cybersecurity in general. He has that level of confidence with CrowdStrike, he said. "Every time we've had an incident — like when somebody tries to plug in a USB drive — I receive an email from one of our dedicated CrowdStrike support team members, warning, 'Hey, check your portal, this does not look like it's caused an issue, but please check it.'"

"CrowdStrike performs as if I have someone onsite 24/7 monitoring our assets all the time, even at three o'clock in the morning," he continued. "We cannot work every three-day weekend to patch or update servers. I've seen trends where hackers will strike during holidays or after hours. CrowdStrike makes me feel a lot more comfortable about going fishing."

ABOUT CROWDSTRIKE

[CrowdStrike](#) (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities. Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more: <https://www.crowdstrike.com/>

Follow us: [Blog](#) | [Twitter](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

Start a free trial today: <https://www.crowdstrike.com/free-trial-guide/>

© 2022 CrowdStrike, Inc. All rights reserved.

RESULTS



Improved visibility into security operations



Facilitated compliance and auditing operations



Instilled confidence in protection of customers' assets

ENDPOINTS



CROWDSTRIKE PRODUCTS

- Falcon Complete™ managed detection and response
- Falcon Discover™ IT hygiene
- Falcon OverWatch™ managed threat hunting
- Falcon Insight XDR™ endpoint detection and response
- Falcon Prevent™ next-generation antivirus
- Falcon Device Control™
- Falcon Spotlight™ vulnerability management