CrowdStrike Customer Case Study

CBC Commercial Bank of California | 20 years

Commercial Bank of California Consolidates Cybersecurity with CrowdStrike

What compels a bank to replace its cybersecurity tools? For some, it's the complexity of juggling multiple point products. For others, it's cost. For most, it's the need to extend security beyond compliance in order to secure the business and client data. For Commercial Bank of California (CBC), it was all three.

CBC is a full-service, FDIC-insured, business bank headquartered in Irvine, California. Thousands of businesses rely on CBC for things like business loans, lines of credit, and sending and receiving payments. This pushes the bank to deliver in two key areas.

"Everything we do is absolutely critical in terms of speed and security," explained Kevin Tsuei, SVP Information Security Officer at CBC.

Heightened Risk

In 2021, CBC was growing increasingly concerned about cyberattacks. Ransomware in particular was making headlines as banks worldwide succumbed to costly and damaging attacks. Financial regulators were taking notice, as was the CBC board of directors.

The bank decided to run a ransomware simulation to test its legacy endpoint solution. The results were shocking: The solution blocked only a fraction of the scenarios tested.

CBC immediately began shopping for a replacement. The first endpoint solution it tested blocked everything in the simulation — which unfortunately included legitimate activities. The solution also required a lot of configuration, which didn't appeal to CBC.

The bank then evaluated CrowdStrike. "We decided to test CrowdStrike because it's known in the industry to stop cybersecurity breaches. CrowdStrike blocked all simulated ransomware attacks … the best results of every vendor we tested," said Tsuei.

Consolidating with CrowdStrike

CBC licensed the CrowdStrike Falcon® platform along with several product modules and services, including CrowdStrike Falcon® Insight XDR for extended detection and response, CrowdStrike Falcon® Cloud Security, CrowdStrike Falcon® Identity Protection and CrowdStrike Falcon® Complete for 24/7 managed detection and response (MDR).

The bank started with Falcon Insight XDR for endpoint detection and response. But just a month after deployment, Tsuei received a Falcon platform alert late one Friday night about a possible security incident affecting one of the company's web applications. When he couldn't reach the application engineer or head of security operations, he questioned how fast CBC could respond to a potential incident.

INDUSTRY

Financial Services

LOCATION/HQ

Irvine, California

CHALLENGES

- In light of heightened ransomware risk, CBC needed modern endpoint security to replace its legacy tools
- It also needed robust cloud security to protect its growing public cloud infrastructure
- With a lean IT and security team, the bank also needed managed detection and response to provide 24/7/365 security

SOLUTION

CBC licensed the CrowdStrike Falcon® platform along with several product modules and services, including CrowdStrike Falcon® Insight XDR for extended detection and response, CrowdStrike Falcon® Cloud Security, CrowdStrike Falcon® Identity Protection and CrowdStrike Falcon® Complete for 24/7 managed detection and response.

RESULTS

- Zero breaches with CrowdStrike
- 100% ransomware protection
- 34% reduction in cyber insurance premiums
- 24/7 managed detection and response
- Unified security from endpoint to workload

> "With CrowdStrike, we can remediate any cloud intrusion in less than 16 minutes, which puts our minds at ease, while ensuring a great user experience for our clients."
>
> **Kevin Tsuei**
>
> SVP Information Security Officer,
> Commercial Bank of California

At the time, both CBC and its subsidiary VCI (formerly Vericheck) used a different MDR for SOC-as-a-service. But there were two problems: it required a separate instance for each company, which added cost and complexity, and the solution lacked remediation. CBC found the performance it needed in Falcon Complete.

"While the previous vendor claims to be MDR, they simply alert us if they detect a threat and guide us on the remediation. In contrast, Falcon Complete will try to remediate the threat before escalating it," explained Tsuei. "From a cost and feature perspective, it was a no-brainer to consolidate our MDR with Falcon Complete and add VCI's assets to it."

Security from Endpoint to Cloud

As a bank built for the speed and scale of modern business, CBC runs a number of customized web applications and APIs hosted in AWS and Microsoft Azure. Initially, these environments were protected only by endpoint security. But as the bank shored up its endpoint security in light of heightened risk, the team realized it also needed visibility across its cloud infrastructure.

"We looked around the industry and started to see more web application attacks, API libraries being compromised and client information being stolen from cloud environments. That's when we realized endpoint security wasn't enough," said Tsuei.

For CBC, security is more than a checkbox item. "We care about our client's data and the funds they entrust us to hold. We needed a solution that could monitor our multiple cloud environments in AWS and Azure, and provide the tools to harden these environments so we can avoid any data loss or potential compromise."

CBC learned it could quickly and easily deploy Falcon Cloud Security to protect its cloud environments using the same lightweight Falcon sensor it uses to protect other attack surfaces. With Falcon Cloud Security, CBC can better understand risks based on criticality, while fortifying its multi-cloud environments against breaches. CrowdStrike also made it easy for CBC by providing precise guidance to its IT engineering team on how to remediate risk.

"Falcon Cloud Security helped us harden our cloud environments. We can now quickly identify and fix cloud misconfigurations, secure our containers and protect our Linux servers in both AWS and Azure," said Tsuei. "This was a godsend because that infrastructure hosts critical information and impacts the availability of our payment platform. With CrowdStrike, we can remediate any cloud intrusion in less than 16 minutes, which puts our minds at ease, while ensuring a great user experience for our clients."

Saving on Cyber Insurance

CBC found yet another compelling reason to further consolidate on the Falcon platform when its cyber insurance premiums skyrocketed in 2021. That year, the bank's premiums grew by 300%. It shopped around for other insurers but couldn't escape the high premiums. The culprit: lack of multifactor authentication (MFA) in key areas.

"We protected our VPN, email and our Citrix environment with MFA, but the cyber insurers were looking for MFA protection across our workstation servers, cloud applications and various networking devices," explained Tsuei.

CBC tried a MFA solution with an existing vendor, but after spending $60,000 USD for professional services and the infrastructure needed to support that environment, the project failed after two years. Meanwhile, the bank's cyber insurance premiums had increased another 300%.

CROWDSTRIKE PRODUCTS

- Falcon® Insight XDR for extended detection and response
- Falcon® Cloud Security
- Falcon® Identity Protection
- Falcon® Discover for IT hygiene
- Falcon® FileVantage for file integrity monitoring
- Falcon® Prevent next-gen antivirus
- Falcon® OverWatch™ managed threat hunting
- Falcon® Complete for 24/7 managed detection and response
- Falcon® Threat Intelligence

Eventually, CBC found Falcon Identity Protection. “It was everything we were looking for,” said Tsuei. The Falcon module stops identity-based attacks in real time with the industry’s only unified platform for endpoint security and identity protection. For CBC, Falcon Identity Protection not only extends MFA across the key areas required by insurers, it provides risk-based conditional access using dynamic risk scoring to prompt MFA in risky scenarios while ensuring worker productivity when risk is low.

For CBC, Falcon Identity Protection has increased security and performance, while lowering costs. According to Tsuei, the bank saved $20,000 USD on identity security the first year with CrowdStrike, and $22,000 each year after that, compared to the previous solution. All told, the bank’s cyber insurance premiums have dropped 34% since switching to CrowdStrike.

“Falcon Identity Protection has been a lifesaver for us. For the first time in history, our cyber insurance premiums have actually gone down,” said Tsuei.

Better Security, Fewer Distractions

Much like the small and medium-sized businesses it serves, CBC is challenged to do more with less. Before switching to CrowdStrike, the bank’s limited IT and security team struggled to manage more than 12 security tools — each with its own sensor, user interface, contract, etc.

“Even as the person who oversees this department, I struggled with security information overload,” said Tsuei. “Our team was paralyzed by the number of alerts from the various systems and the daily challenge of using each system and security tool effectively.”

Consolidating cybersecurity with CrowdStrike has simplified things for CBC.

“The Falcon platform has allowed us to consolidate our security toolbox. It yields big savings for us, but more importantly, it allows us to focus. When an alert hits from the Falcon platform, we're able to address it without being distracted by other tools,” concluded Tsuei. “We’ve been more than delighted with CrowdStrike.”

Start Free Trial

Learn more **www.crowdstrike.com**

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.

CrowdStrike: **We stop breaches.**

Follow us: **Blog** | **Twitter** | **LinkedIn** | **Facebook** | **Instagram**

CROWDSTRIKE

we stop breaches