voices

CrowdStrike Customer Case Study

BerkshireBank

Berkshire Bank Accelerates Digital Transformation and Multi-Channel Customer Services with CrowdStrike

As Berkshire Bank grows and focuses on digital transformation, the main cyber challenges it faces, according to SVP and CISO Ryan Melle, are API security, rising zero-day vulnerabilities, third-party risk management as banking systems and services are moved to the cloud, and the increasing sophistication and frequency of cyberattacks. "Our job is to enable customers to access the services they need and allow the business and employees to operate while maintaining a secure environment," Melle said.

Security Infrastructure Built on Unified, Cloud-Native CrowdStrike Falcon Platform

Berkshire Bank has built a unified cybersecurity infrastructure upon the cloud-native CrowdStrike Falcon® platform. The bank initially deployed a range of Falcon® modules including CrowdStrike Falcon® Discover IT hygiene, CrowdStrike Falcon® Insight XDR endpoint detection and response (EDR), CrowdStrike® Falcon OverWatch™ managed threat hunting, CrowdStrike Falcon® Prevent next-generation antivirus (AV) and CrowdStrike Falcon® Device Control.

The bank started using CrowdStrike several years ago when it only had AV tools and needed to strengthen its EDR capabilities. "In the old days when we had only AV tools, everything was a thick client with power-hungry agents," Melle said. "Managing that was time-consuming and we had some challenges with resources on workstations — whereas CrowdStrike is cloud-based and has just one agent for all the different solution modules compared to competitor products that need multiple agents."

Melle was "very happy" with the security capabilities of the Falcon platform. "We did a proof of concept and rolled out 50 agents in seconds and that was a good selling point, making it frictionless especially for IT," he said. "With CrowdStrike, you do not even know it is running."

Identity Protection Integrated Easily and Seamlessly

After its initial CrowdStrike deployment, Berkshire Bank started to build a Zero Trust security strategy focused on remote access, moving away from legacy systems like VPN and implementing a stepped approach for identifying applications, user-level access and network segmentation. Regular monitoring and penetration testing helped enhance visibility, particularly around identity access such as by a compromised account. The bank was getting information and identity logs, but it took time and effort to spot vulnerabilities. Another security enhancement the

INDUSTRY
Financial

LOCATION/HQ
Boston, MA, United States

CHALLENGES
- Supporting digital transformation and online banking services
- Growing threat and risk of identity attacks
- Increasing cost and time needed to manage traditional AV tools

SOLUTION
Berkshire Bank uses a portfolio of CrowdStrike solutions, including identity protection, to protect the business, users and customers, and to ensure safe and secure access to digital banking services.

"After deploying Falcon Identity Threat Protection, we did another penetration test and immediately saw the benefits of the enhanced visibility. CrowdStrike worked as intended and gave us the granular visibility we did not have before. CrowdStrike has moved the bank from detecting identity vulnerabilities to protecting against them."

Ryan Melle
SVP, Chief Information Security Officer
Berkshire Bank

voices

CrowdStrike Customer Case Study

bank sought concerned multifactor authentication (MFA) for privileged users; the bank uses Okta for authentication and authorization and wanted the best way to enforce MFA.

As part of its Zero Trust strategy, Berkshire Bank has deployed CrowdStrike Falcon® Identity Threat Protection. "We chose the CrowdStrike identity protection solution because we could easily and seamlessly integrate it with our existing CrowdStrike platform," said Melle. "One of the key benefits was the improved security and user experience by triggering MFA only when the risk increased. We were able to turn on identity protection in minutes."

Falcon Identity Threat Protection has provided the bank with enhanced visibility and greater prevention and policy enforcement. "After deploying it, we did another penetration test and immediately saw the benefits of the enhanced visibility," said Melle. "It was great to use CrowdStrike to take screenshots, report back in real time to the team as they were doing the pen test, and map the attack path. CrowdStrike worked as intended and gave us granular visibility we did not have before. CrowdStrike has moved the bank from detecting identity vulnerabilities to protecting against them."

As with the other Falcon modules, Falcon Identity Threat Protection was deployed in only a few hours. The CrowdStrike solution now protects 2,000 user and system endpoints at the head office and in branch locations, as well as remote workers.

Security Improves Through More Visibility, Less Effort

One of the key benefits of deploying CrowdStrike has been a significant cut in security management time. The bank has also experienced reduced alert fatigue, fewer false positives, and improvements in security operations center (SOC) efficiency and in detection and incident response times.

"It is comforting to know that if there is an alert, it is likely to be legitimate and we can deal with it," said Melle. "In our true/false positive analysis, false is usually zero so we are not spending time chasing unnecessary alerts. We do not need a dedicated CrowdStrike manager — we just set up CrowdStrike and the data flows into our security information and event management (SIEM) tool."

Berkshire Bank has a monthly "health check" with CrowdStrike to review its environment and ensure that the bank is operating effective and efficiently. Otherwise, Melle said, "CrowdStrike is a hands-off product because things like updates run automatically, and in the seven years since the first install, we have not had any significant problems."

Identity Protection Helps Maintain Insurability

One area in which CrowdStrike, and Falcon Identity Protection in particular, can help an organization is improving its insurability by shrinking the identity attack surface, enabling continuous visibility into the risks and providing confidence to the cyber insurers that the organization can stop identity-based attacks.

RESULTS

Achieves a dramatic improvement in overall security

Delivers a significant cut in alert fatigue and fewer false positives

Improves SOC efficiency by decreasing detection and incident response times

ENDPOINTS

2,000

CROWDSTRIKE PRODUCTS

- Falcon Device Control
- Falcon Discover IT hygiene
- Falcon Identity Threat Protection
- Falcon Insight XDR endpoint detection and response
- Falcon OverWatch managed threat hunting
- Falcon Prevent next-generation antivirus

voices

CrowdStrike Customer Case Study

"Today insurers ask far more stringent questions because of the increased risk of attacks. We need to show we have comprehensive controls in place, so it is good to have CrowdStrike to demonstrate our security posture with risk-based MFA. CrowdStrike helps improve our risk posture and subsequently our insurability because of its strong reputation and leadership in the space."

For Berkshire Bank, the partnership with CrowdStrike is important for the future. "CrowdStrike is continuously investing in technology," Melle said. "It is good to see different enhancements coming to further strengthen the platform for features like Zero Trust and identity because the threats keep evolving. Our security policy is using best-of-breed technology, and it is important that our tools integrate in one single pane of glass. CrowdStrike continues to invest in and understand the cyber environment and future threats. That is a win for us."

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/