IDC
Analyze the Future

I D C C U S T O M E R S P O T L I G H T

Enhancing Endpoint Security Efficacy: A Top 10 Global Financial Institution's CrowdStrike Experience

June 2018

Sponsored by CrowdStrike

Introduction

As Willie Sutton, a man with a 40-year robbery career, opined, "I rob banks because that's where the money is." IDC interviewed one of the biggest targets for today's cyber "bank robbers," speaking with the cybersecurity director for a top 10 global financial institution to develop this case study. A "Financial Institution"[1] is an investment bank and financial services company considered a "bulge bracket bank" (see the Solution Snapshot sidebar). Obviously, the cybersecurity needs in this segment are particularly acute.

This Financial Institution implemented CrowdStrike Falcon to improve its security architecture, replacing an existing endpoint detection and remediation solution with a solution that worked better with the IT architecture while better fitting within the budgetary envelope. This case study has been prepared by IDC to assess and articulate the experience and value achieved.

Solution Snapshot

Organization: A top 10 global Financial Institution in the "bulge bracket," which comprises the world's largest multinational investment banking firms whose clients are usually large corporations, institutions, and governments (These financial institutions facilitate the most global capital movement and underwrite most financial contracts.)

Operational challenge: Meet the cybersecurity requirement of an exceptionally demanding use case, providing the ability to evaluate the condition of endpoints, grab telemetry, and perform incident investigations

Solution: CrowdStrike Falcon Cloud-Delivered Endpoint Protection

Benefits: Significant commercial advantage while providing "mature code" and "high touch" support

Background

The Financial Institution cybersecurity team is likely similar to others of its kind. It is slave to three masters:

- **Security.** Frankly and obviously, a high-stakes task of keeping "bad guys" out exists.
- **Compliance.** Regulatory compliance is a fundamental requirement of doing business. The problem of which standard is relevant is exponentially compounded by the number of nations in which the institution does business.
- **Operations.** Banks are no different from other business entities. Business must get done. Obstructing the pace of commerce is not an option.

[1] The moniker "Financial Institution" is used to represent the reference for this case study. IDC interviewed the company's cybersecurity director to develop this case study. The identity of the subject company has intentionally been withheld to anonymize the organization because top 10 global financial institutions are understandably reticent to share the details of their security measures.

The timing of the selection of CrowdStrike was especially relevant. The cybersecurity director with whom we spoke actually chose CrowdStrike twice. In his previous role at a different financial institution, he chose CrowdStrike. That decision was in 2013. The existing solution was the result of a remediation tool put in place from a prior incident. However, when the solution actually ran, it was "disruptive" — that is, not something that would operate silently in the background. The result was that scans happened only every other month at best. Complaints and concerns with the product were not addressed in a timely manner. Moreover, from an efficacy perspective, the tool did not find anything.

The 2013 reality was that alternatives for endpoint visibility and response products were limited, making it worthwhile to evaluate a start-up. After several paper-based evaluations, CrowdStrike was deployed.

Interestingly, scalability was accidently tested very early. The deployment was supposed to be tested in 6,000 endpoint batches, but someone "fat fingered" the first batch and accidentally deployed 60,000 at once. The back end scaled without issue. Subsequently, the environment was found "quite riddled with a number of persistent infections," which was a real eye-opener. The uniqueness of the efficacy of the solution was telling.

Implementation

In 2016, the decision, as well as the use case, was quite different for the Financial Institution. The pain point was the need to evaluate the condition of endpoints, grab telemetry, and perform incident investigations. The Financial Institution had a solution in place from a managed security service provider (MSSP), but the solution was not "serving the need from either a commercial or a technical perspective." There were a couple of big challenges with the existing solution.

"The first challenge was [the existing solution] was terribly expensive."[2]

Functionally, the existing solution "just wasn't polished code." A number of challenges with integration arose. For example, particular elements of the agent caused I/O latency. If those elements of the agent were turned off, I/O would be fine, but that was about two-thirds of the agent's functionality. And working on debugging those elements was growing more difficult.

In terms of process, one of the large professional services organizations was hired to build a lab environment to test what were believed to be the top six or seven products. The top three options came from FireEye, Carbon Black, and CrowdStrike.

When it came to selecting a solution, the Financial Institution did not have "any stickiness with any of the vendors" because it was not using their products. The final selection of CrowdStrike came down to three factors:

- Good previous experience of the cybersecurity director with the CrowdStrike product
- A quick and favorable commercial negotiation
- CrowdStrike flexibility when it came to accommodating some of the unique requirements of a global financial institution (A great amount of focus is placed on privacy. The accommodating modifications requested were made in a very timely manner, including putting privacy features back into the main line code as a specialty version.)

[2] Whenever possible, direct quotations were used to transparently communicate the cybersecurity director's message. Such quotations were taken directly from a transcript of the conversation and not significantly altered.

Challenges

The implementation was not without challenges. For example, a strange race condition arose if an F# developer was doing a compile job and the load on the system was high. Another example was that when a network blip occurred, it caused all the CrowdStrike agents to attempt to re-establish a link. When that occurred, about 20,000 endpoints tried to squeeze out through the same proxy. According to the cybersecurity director, these types of issues happen. It is about being responsive, and CrowdStrike was very responsive. "And in the event of a Heartbleed issue, they now do a random retry. It's how you handle an issue. In each case, that's been handled quite gracefully."

Benefits

The initial benefit from the MSSP solution was a commercial advantage. "A significant amount of money was taken off our run rate in what was a fairly challenging financial time." The MSSP solution was *significantly* more expensive.

Functionally, a primary benefit and a secondary benefit were achieved. The primary benefit was mature code. "So there wasn't the 'Oh my God, this thing is causing an adverse interaction with the performance of a developer's machine.'" Rather, "it was mature and polished [code]." The reference to mature code is meant to imply the software product has demonstrated effective performance in demanding product environments with minimal need for IT intervention or support.

The secondary benefit was in the installation. Deploying CrowdStrike to an end-user environment was really "high touch." In the opinion of the cybersecurity director, high touch is important because users often attribute performance degradation or other defects of things to the installation when there is no causality, only inconvenient correlations. Managing performance engineering with IT operations and end users to ensure that "we were properly identifying performance and regression defects through the release management process" was critical.

After installation, no undiscovered, nasty infections were found. "It was more of the same." Given that the Financial Institution has an impressive security team, finding new infections was not expected, but confirmation of their absence was welcomed. What did change was "the fact that we were getting [fewer] complaints about the polish of the agent" and fewer agent conflict issues on endpoints, illustrating the maturity of the code base. "We were keeping our eyes focused on the actual state of security versus troubleshooting agent conflict issues."

Surprisingly, improving the ability to meet compliance standards was *not* mentioned as a benefit; compliance is "table stakes" for consideration. Even new standards such as GDPR were not relevant. Global financial institutions *know* privacy because they must adhere to the standards of countries such as the United States, Hong Kong, the United Kingdom, and Switzerland.

That being said, the Financial Institution did make a specific privacy request be implemented before installation: No personally identifiable information about customers was to be sent from the agent into the cloud. The request was quickly addressed. Equally interesting was that the CrowdStrike cloud-delivered endpoint protection methodology was also not a topic of conversation with the cybersecurity director. Once again, compliance is "table stakes" for consideration as a security vendor for a top 10 financial institution; any concerns about whether the cloud aspect of the delivery caused compliance issues would have eliminated the solution from consideration.

Other modifications were request by the Financial Institution. One of the improvements is that CrowdStrike automatically upgrades agents with how they bind to the kernel. When the Windows kernel changes, a new version of the agent that understands those changes is also released. Otherwise, it would act in what's called "reduced functionality mode" to avoid any incompatibilities within the new kernel.

A preview into what's coming next was included in the requirement so that CrowdStrike release engineering and Financial Institution release engineering could work in lockstep to ensure smoother agent upgrades. Another feature was an engineering portal to allow for a very "strict delineation so that engineers don't touch production unless they're debugging a broad issue, and all of their testing and preproduction work should be done against a separate environment all together." This best practice prevents modifications that may negatively affect production. There was a three-way arrangement between the Financial Institution, a systems integrator, and CrowdStrike to triage these issues. CrowdStrike did not require a lot of tuning, but, when needed, "CrowdStrike was always quite accommodating of tuning calls."

Methodology

Frank Dickson, research vice president with IDC's Security Products team, interviewed the cybersecurity director from the Financial Institution. This Customer Spotlight is a direct result of that interview. Direct quotations were used whenever possible to transparently reflect the opinions of the interviewee.
