voices

CrowdStrike Customer Case Study

Healthcare Solutions Provider

Healthcare Solutions Provider Rolls Out CrowdStrike Falcon to Secure Extensive Global Interests

"Security is not just about the technology, it's really about having the right people and processes in place to respond appropriately when the need arises," said the company's information security (IS) manager. A long-time cybersecurity industry veteran, he had been brought in to help define and further enhance the company's defense strategy. A key element of his approach has been to strengthen the security of thousands of endpoints spread across the global environment.

Top of the Table

The security team created a detailed set of evaluation criteria and scored prospective contenders on a scale of one to five in categories such as ease of deployment and ongoing management, threat detection prowess, breadth of functionality and impact on endpoint performance.

The selection process narrowed the field to three competing solutions. "CrowdStrike was our favorite," said the IS manager. "It scored highest on our evaluation matrix, and we could clearly see how everything tied together to maximize team efficiency and enable us to respond quickly to any alerts."

Having decided to proceed to the next phase with CrowdStrike, the team conducted a comprehensive proof of concept (POC) with the modules that had been selected to populate the CrowdStrike Falcon® platform, including Falcon Discover™ IT hygiene, Falcon Insight™ endpoint detection and response, Falcon OverWatch™ managed threat hunting and Falcon Prevent™ next-generation antivirus.

Confidence in Making the Right Decision

Following the successful completion of the POC, a phased rollout to approximately 6,500 endpoints was completed across offices in one region. "The proof of concept verified the compatibility and effectiveness of the CrowdStrike solutions in our

INDUSTRY

Healthcare

LOCATION/HQ

Asia Pacific region

CHALLENGES

- Requirement to improve protection of endpoints
- Desire to enhance intelligence associated with alerts
- Lack of a comprehensive view into status of distributed facilities

SOLUTION

The healthcare solutions provider selected a portfolio of CrowdStrike offerings to strengthen its security posture and gain centralized visibility and control across a geographically distributed network of endpoints

"Protecting the endpoint is fine, but I need intelligence to really understand who is behind each attack and then have the context and tools to facilitate a swift and effective response. This is why we chose CrowdStrike."

Information Security Manager
Healthcare Solutions Provider

voices

CrowdStrike Customer Case Study

environment," said the IS manager. "And it gave us the confidence to undertake the large-scale deployment and then add additional countries in subsequent phases."

"The implementation went really smoothly, with no discernible impact on users or network resources," said the IS manager. "The initial rollout was deemed a great success, especially considering the magnitude of the project."

The IS manager recalled several situations where the CrowdStrike agent was deployed on a device before the legacy endpoint solution had been removed. "CrowdStrike immediately demonstrated that it was able to detect potential threats that weren't being picked up by our incumbent product," he said. "This was another very positive validation of our decision to make the change."

Together As One

Traditionally, each country in the company's network has had the autonomy to define its own strategy and select individual products. A consequence has been inefficiencies in sharing critical cybersecurity resources between entities and the absence of a fully unified, global approach to protecting the company's digital assets.

"We feel very confident that CrowdStrike is the right answer to many of our challenges," said a senior member of the global security team, whose responsibility is to communicate to the individual countries the findings and learnings of the headquarters' security team. "We're collaborating with the regions and using CrowdStrike to show the benefits of having centralized control across the entire global environment."

"We've been able to demonstrate that having the ability to see exactly what's occurring anywhere in the environment enables us to respond quickly and effectively. When we experience any type of malware attacking one of our systems, we can rapidly equip the other offices to defend themselves against that specific threat."

A Picture is Worth a Thousand Words

The Falcon platform's comprehensive reporting capabilities also have proved to be an asset even outside of daily operations for the security team. "Most executives typically don't have an understanding of what a specific threat actually means to the company," the IS manager said. "The CrowdStrike dashboard enables us to consolidate and summarize incidents, and then depict the risk profile of individual entities in a graphical, color-coded report that even the most non-technical manager can understand. "We also use the reports from the Falcon platform to demonstrate how CrowdStrike, and the investment we've made in CrowdStrike, is helping mitigate risk."

RESULTS

Centralized visibility and control across global infrastructure

Accelerated ability to detect, contain and remediate threats

Rapid deployment across thousands of endpoints immediately elevated protection

ENDPOINTS

6,500

CROWDSTRIKE PRODUCTS

- Falcon Discover™ IT hygiene
- Falcon Insight™ endpoint detection and response (EDR)
- Falcon OverWatch™ managed threat hunting
- Falcon Prevent™ next-generation antivirus

voices

CrowdStrike Customer Case Study

The Right Tool for the Job

"Technology will always be king, but it's the people behind the technology that make the difference," said the IS manager. "We have a finite number of security professionals spread around the regions, but CrowdStrike delivers what we need to coordinate an effective and swift response to threats occurring anywhere we have Falcon deployed. Despite the sophistication and comprehensive functionality, CrowdStrike has been really convenient to deploy and very easy to use."

He concluded, "Protecting the endpoint is fine, but I need intelligence to really understand who is behind each attack and then have the context and tools to facilitate a swift and effective response," he said. "This is why we chose CrowdStrike."

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (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.**