Consistently ranked as one of the top higher education institutions in the world, this university faced mounting challenges keeping sophisticated attackers at bay. CrowdStrike's reputation within the close-knit academic community led to a speedy deployment of the Falcon Platform across a very broad set of semi-autonomous organizations operating within the university system. The customer quickly gained the visibility and prevention capabilities they needed to thwart ongoing attempts by advanced adversaries to target their systems and data.

The Challenge

This sprawling university houses a widely dispersed collection of entities, many operating their own IT infrastructure in a decentralized fashion. While this provides a tremendous amount of autonomy to the faculty and staff of various colleges and organizations within the university, it also results in a lack of standardization across the endpoints of numerous interconnected IT systems. This creates the potential for innumerable attack vectors that can be exploited to gain access to valuable information. As part of a broad security improvement initiative taking place throughout the university and its affiliated organizations, the institution’s security team recognized the need to confirm the integrity of their environment and ensure that they were not at risk of exposing sensitive privacy or research data.
The university deployed Falcon on all endpoints (Windows, Linux and MacOS) in faculty and central server locations, including associated colleges and business operations. Immediate alerting capabilities from the deployment resulted in Falcon OverWatch quickly identifying multiple potential vulnerabilities — ranging from commodity malware to sophisticated tactics, techniques and procedures (TTPs) consistent with nation-state and hacktivist/activist threat actors — which the university was able to address and resolve promptly with the direct help of the OverWatch team.

The Results

Due to the ease with which the Falcon Platform deployed across a large and diverse environment, the university is continuing to expand its use of Falcon technology and services across its infrastructure. The exceptional visibility this enables into endpoint activity has provided a much better understanding of the threats the environment is exposed to on a regular basis. Close interaction with the Falcon OverWatch and CrowdStrike Intelligence service teams has provided more color and context into their threat environment. As a result, the university’s IT security organization has transitioned from simply triaging and treating symptoms to identifying and actively addressing the causes, eliminating vulnerabilities before they can be exploited.