voices

CrowdStrike Customer Story

UNIVERSITY OF WESTMINSTER

U.K. University Gains 24/7 Protection, Visibility and Response with CrowdStrike MDR

The University of Westminster was established in 1838 as the first polytechnic institution in London and one of the first in the U.K. Founded to educate the city's working people, the university now enrolls over 19,000 students from 169 nations, offering many of them placements and work experience through partnerships with almost 200 organizations throughout the U.K. The university employs more than 2,000 people.

In 2021, the university faced a cyber threat landscape that was changing dramatically during the COVID-19 pandemic and included the following serious security challenges:

- **Legacy antivirus (AV) software.** The university lacked sufficient threat detection and response capabilities because of its reactive security posture and because its legacy AV could not keep up with increasingly sophisticated cyber threats.
- **Unacceptably high risk of attacks and reputational harm.** The university wanted to reduce the risk of cyber incidents and to protect its students and staff from the consequences of malicious attacks, which for the university could include damage to its reputation.
- **Surging threat of ransomware attacks**. Higher education was facing a particularly high risk of ransomware attacks.[1]
- **Limited security coverage.** Because higher education IT and security teams typically work 9 a.m.-5 p.m. on weekdays, the university's security leaders were concerned with the lack of coverage after hours when most ransomware is deployed.[2]
- **Rapidly evolving needs of remote working and learning.** The expansion of IT facilities to support remote employees and students during the pandemic, combined with decreasing capacity and increasing workloads caused by an evolving threat landscape, had led to a reactive security posture.
- **Major security visibility gaps and blindspots.** The university's legacy security solutions couldn't provide unified visibility across a variety of operating systems.

Because of the prohibitive cost of implementing an in-house security operations center (SOC) and the additional staffing burden a 24/7 security operation entails, the university's security leaders found the managed detection and response (MDR) service model to be appealing — cost-effective, scalable and resilient to meet the university's existing and future cybersecurity needs. One of the solutions the university considered, and the one it chose to provide a first line of threat defense and instant security posture improvement, is CrowdStrike Falcon® Complete MDR.

INDUSTRY

Higher Education

LOCATION/HQ

London, England

ENDPOINTS:

5,400

CHALLENGES:

- High risk of reputation-damaging ransomware attacks
- Lack of 24/7 threat detection and response
- A reactive security posture caused by capacity constraints
- No unified visibility across different operating systems

SOLUTION

The University of Westminster chose CrowdStrike Falcon Complete managed detection and response (MDR) to augment its in-house security team with responsive 24/7 coverage, expand visibility across all university systems and decrease the risk of cyber incidents and reputational harm.

"Falcon Complete MDR provides operational efficiencies and augments our in-house security operations with 24/7 coverage, responsiveness and a level of visibility we didn't have before."

Thierry Delaitre,

Head of IT Developments, Information Systems and Support

1 https://repository.jisc.ac.uk/8539/1/cyber-security-posture-survey-results-2021.pdf

2 https://www.mandiant.com/resources/blog/they-come-in-the-night-ransomware-deployment-trends

voices

CrowdStrike Customer Story

According to the university's security leaders, CrowdStrike meets and exceeds their expectations for what the expertly managed solution would deliver to the university every day.

"Falcon Complete MDR provides operational efficiencies and augments our in-house security operations with 24/7 coverage, responsiveness and a level of visibility we didn't have before," said Thierry Delaitre, Head of IT Developments, Information Systems and Support. "It also eliminates the need to build a fully staffed SOC, is highly effective at stopping intrusions and reducing risk, and provides a consistent cybersecurity platform across the entire university."

How the University of Westminster Chose and Deployed CrowdStrike MDR

In addition to CrowdStrike, the university evaluated MDR solutions from two other security vendors. The primary appeal of CrowdStrike, Delaitre said, was the speed, scalability and ease of deployment of Falcon Complete and the entire suite of tools the MDR team leverages across the CrowdStrike Falcon® platform. He also noted CrowdStrike's wide range of supported operating systems — including macOS, Windows and Linux — and the impressive maturity of Falcon Complete's MDR capabilities, both in terms of its security tech stack and its team of experienced, highly skilled security analysts.

"Falcon Complete's powerful combination of industry-leading security technology and elite MDR expertise are a match made in Heaven, because with security vendors we often get great products but not a great team or the team's great but not the product," said Russell Poole, Director of Information Systems and Support, adding that the CrowdStrike team was clearly experienced with working in a higher education environment.

Deployment was smooth and efficient, with the team installing the Falcon agent to more than 5,000 endpoints and 400 servers in four weeks. "The CrowdStrike team had a very well-oiled onboarding process, bringing us online in a very short period of time," Poole said.

Prior to the university-wide deployment, security leaders opted to phase in the security software, first running a proof-of-value trial with about 200 devices and servers. The success of this pilot program — which included 77 tests of Falcon Complete's deployment, management and threat detection, response and hunting capabilities — eased any remaining concerns and secured the decision to proceed with the full deployment.

Implementation of the lightweight Falcon sensor was quick and caused "absolutely no" performance issues, Delaitre said, and the transition from legacy AV to CrowdStrike's next-gen AV was "very smooth."

"Falcon Complete's powerful combination of industry-leading security technology and elite MDR expertise are a match made in Heaven, because with security vendors we often get great products but not a great team or the team's great but not the product."

Russell Poole,
Director of Information Systems and Support

RESULTS

Immediate visibility into threats previous legacy solutions could not detect

24h
1h

24/7 detection coverage that reduced response time from 24 hours to one

Unified view across endpoints and servers regardless of location or OS

Improved remediation and root-cause analysis of incidents

CROWDSTRIKE PRODUCTS

- Falcon® Complete managed detection and response
  - Falcon® Prevent next-generation antivirus
  - Falcon® Insight XDR endpoint detection and response
  - Falcon® Discover IT hygiene
  - Falcon® Discover for Cloud and Container
  - Falcon OverWatch™ managed threat hunting
  - Cloud Runtime Protection
- Falcon® Device Control
- Falcon® Firewall Management
- Falcon® for Mobile Standard

voices

CrowdStrike Customer Story

University Immediately Gains Expanded, 24/7 Coverage and Unprecedented Visibility

Falcon Complete MDR demonstrated its value from the start. In one instance during rollout, it detected malicious activity where an unapproved web browser had been installed on some endpoints. In another instance, it shut down malware initiating command-and-control attempts from endpoints in a student lab.

Overall, the university has better coverage for security protection than it had before, Delaitre and Poole said, with CrowdStrike protecting all of its operating systems on all of its endpoints and servers, and regardless if its assets are on-premises or remote.

"We have better visibility of detections, prompt remediation of security incidents and root-cause analysis of these incidents," Delaitre said. "And we have a unified view across our endpoints and servers regardless of OS, whereas previously we were using different technologies on different systems. In addition, with the Falcon Complete MDR team, we now have an incredibly responsive 24/7 SOC that rapidly analyzes and remediates every new inbound detection, regardless of the time of day or night."

The improved visibility and coverage extends to the university's Computer Science and Engineering School, whose servers are controlled outside of the Information Systems and Support department. In particular, the school is leveraging CrowdStrike cloud security modules for when staff and students do processing in virtual machines on AWS.

"CrowdStrike's ability to help us protect our on-premises systems and AWS workloads gives us an additional layer of security we did not have before," Delaitre said.

Crucially, with the 24/7 coverage of the Falcon Complete team, Delaitre said the university now enjoys a detection response time of one hour versus the previous "at best" 24-hour response time that was limited by the in-house security team's 9 a.m.-5 p.m. weekday schedule.

"CrowdStrike has given us a better understanding of what's happening across our IT estate, whereas before without a doubt things were happening that we never saw and therefore could never control," Poole said. "With our prior solution, what kept us awake most was the threat of ransomware and our ability to detect and respond to it. CrowdStrike has allowed us some extra hours of sleep."

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**

Start Free Trial

Learn more **www.crowdstrike.com**

CROWDSTRIKE

we stop breaches