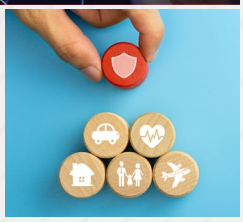

University of Sunderland

UK University Turns to CrowdStrike for Managed Detection and Response After Legacy Endpoint Solution Fails to Stop Ransomware Attack

In October 2021, the University of Sunderland fell prey to a ransomware attack, like so many organizations before it. Questions swirled: How did the attackers get in? What systems were compromised? What data may have been exfiltrated?

Needing answers fast, as well as critical services restored, the university turned to CrowdStrike's incident response (IR) service.

"CrowdStrike worked with us to take control of a situation, which we'd never previously encountered, and guide us through the entire remediation process," said David Conway, Deputy Technical Director at the University of Sunderland.

The CrowdStrike IR team determined an individual's login credentials had been compromised, allowing the attacker to gain access to a specialist learning environment, then move laterally to other systems. The endpoint solution from a native OS security vendor in place during the attack failed to stop the breach. This is an all-too-common occurrence: When CrowdStrike's IR team investigates a customer that's been breached, Microsoft Defender has been bypassed more than 75% of the time.

The university was acutely aware it needed an ever-stronger cybersecurity posture. However, its ability to provide around-the-clock support was an issue. With only 50 IT staff responsible for securing a global network supporting 28,000 students across three campuses, the university lacked the resources to effectively run a modern security stack on its own.

Continuing to rely on endpoint protection from the previous solution was insufficient, given its limited ability to respond to complex attacks. The IT department looked at several other security vendors, and based on technical evaluations, business value assessments and a competitive procurement process, the university chose the superior protection of CrowdStrike.

"We were all incredibly impressed with how CrowdStrike handled the incident response. Most vendors offer a good product or service, but CrowdStrike offers both," said Conway. "We had the utmost confidence that CrowdStrike would deliver the high level of security we needed."

Security as a Service: Strong Protection 24/7

The University of Sunderland selected CrowdStrike Falcon® Complete, a 24/7 managed detection and response service designed to stop modern breaches through a unique combination of technology, threat intelligence and skilled expertise. The university saw it as a perfect way to secure its 5,000 endpoints with little administrative overhead.

INDUSTRY

Higher Education

LOCATION/HQ

Sunderland, UK

CHALLENGES

- After a breach, the university needed to modernize its security systems
- But headcount was an issue — no new security staff members could be added
- The university needed to expand protections from endpoints to cloud and identity

SOLUTION

The University of Sunderland adopted CrowdStrike Falcon® Complete, a 24/7 managed service designed to stop modern breaches through a unique combination of technology, threat intelligence and skilled expertise.

CrowdStrike achieved 99% detection coverage in the first-ever closed-book MITRE ATT&CK® Evaluations for Security Service Providers — **outpacing every vendor in the test.**

The plan, according to Conway, was to assess Falcon Complete after one year to determine if any changes were needed. CrowdStrike passed the test.

"Senior leadership gained significant confidence in CrowdStrike during management briefings. And from a technical side, it's rare that I'm this impressed with a vendor, but I'm immensely impressed with CrowdStrike's technical ability, knowledge, skills and ability to execute," said Conway.

While initially focused on protecting endpoints, the University of Sunderland expanded its managed protections in 2022 to include CrowdStrike Falcon® Complete Identity Threat Protection and CrowdStrike Falcon® Complete Cloud Security. As the ransomware incident in 2021 demonstrated, adversaries often leverage identity-based attacks to bypass legacy security solutions. Increasingly, these adversaries are using the endpoint as a perch to pivot to cloud infrastructure. By unifying endpoint, identity and cloud protection through a single platform, the university now has managed protection across all steps of an adversary's attack path — from exploitation, to the delivery of malware or exfiltration of data, all the way through stolen credentials and compromised identities.

CrowdStrike makes security convenient for the University of Sunderland. For example, Falcon Complete proactively identifies and responds to threats on behalf of the university, reducing noise and administrative burden. And when further action is needed, Conway and his team can easily view the details in the Falcon platform — one command console that covers every module.

"CrowdStrike filters out the noise incredibly well," said Conway. "We get very few escalations, and when we do, CrowdStrike makes it easy for us to take action."

Scouring the Dark Web for Threats

For a university, continuity of service isn't the only thing at risk when a security incident occurs. Reputational damage is also on the line, both for the university and its senior leaders.

The CrowdStrike 2023 Global Threat Report highlights a startling trend that puts this risk into perspective. Advertisements for access broker services, in which malicious hackers steal identities and sell them on the dark web, were up 112% in 2022 over the previous year. Higher education is the most targeted industry.

"We have a duty to protect not just our infrastructure but our people as well," said Sam Seldon, Data Protection Officer at the University of Sunderland. "Our senior leaders are on social media and websites where adversaries are actively hunting for their information. For these executives, a compromise in life could lead to a compromise at work."

To monitor potentially malicious activity across the dark web, the University of Sunderland uses CrowdStrike Falcon® Intelligence Recon. The threat intelligence module, which is delivered as a managed service, scours the dark web for threats to the university and its senior leaders. When a threat is identified, an alert is generated, allowing the university to take preventative action and use the intelligence to train employees on active threats.

"If you look at security as a whole, it's pointless to have only one piece of protection because threats are coming from every direction," said Seldon. "As a relatively small IT team, there's no way we could dedicate the resources to scour the dark web ourselves. If the firewall is our door, Falcon Intelligence Recon is our surveillance."

RESULTS

- Zero breaches with CrowdStrike
- 10-12 headcount saved by outsourcing security to CrowdStrike
- 99% of threats stopped automatically by CrowdStrike

ENDPOINTS

5,000

CROWDSTRIKE PRODUCTS

- CrowdStrike Falcon® Complete managed detection and response
- CrowdStrike Falcon® Prevent next-generation antivirus
- CrowdStrike Falcon® Insight endpoint detection and response
- CrowdStrike Falcon® Identity Threat Protection
- CrowdStrike Falcon® Cloud Security
- CrowdStrike Falcon® Discover IT hygiene
- CrowdStrike® Falcon OverWatch™ managed threat hunting
- CrowdStrike Falcon® Intelligence Recon
- CrowdStrike Falcon® Device Control
- CrowdStrike Falcon® Firewall Management
- CrowdStrike Falcon® Spotlight vulnerability management

"Most vendors offer a good product or service, but CrowdStrike offers both."

David Conway,

Deputy Technical Director,
University of Sunderland

Leaving Security to the Experts

Since adopting Falcon Complete in 2021, the University of Sunderland has suffered zero cybersecurity breaches. It's also been able to avoid a headcount increase of 10-12 employees who would have otherwise been needed to run a self-managed security stack to this level.

"We'd have to increase our headcount significantly to get anywhere near what CrowdStrike does for us," said Conway.

Looking forward, the university is focused on expanding its digital business while balancing other IT priorities, including user education, bring-your-own-device protocols and supporting research contracts — all made possible by outsourcing cybersecurity to CrowdStrike.

"There are areas where we invest our time and money in security experts, so we can focus on what we do best," concluded Conway. "We know we're in safe hands with CrowdStrike."

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