Coventry University

Coventry University Achieves First-Class Results with Enhanced Endpoint Security Strategy

Stability and predictability are the cornerstones of an effective security program. Steve Rogers, Enterprise Cloud, Infrastructure and Security Architect at Coventry University, had neither. "On any given day, we support about 40,000 stakeholders, spread around the world, and due to the various courses we offer, we spike by thousands of users every few months," said Rogers. "We also have a 'bring your own device' (BYOD) policy that means we have limited control over the diverse range of technologies that connect to our networks. To further complicate the situation, the university has a dynamic portfolio of over 600 applications, running on a distributed pool of 600 servers and cloud-based environments."

With its main campus located in the West Midlands, England, Coventry University can trace its origins back to 1843. Today, the university provides innovative teaching — and a focus on impactful primary research — for 29,000 students in Coventry, London and Scarborough, and internationally in China, Singapore and Rwanda.

The university has won numerous awards and accolades for student satisfaction and teaching quality, including being shortlisted for University of the Year, a gold rating in the UK government's Teaching Excellence Framework, and a top 15 placement in a prestigious national newspaper ranking.

The Price of Success

The university creates substantial amounts of proprietary research and high-value intellectual property (IP), much of it resulting from partnerships in healthcare, engineering and the automotive industry. Coupled with holding significant volumes of sensitive personal information, Coventry University has become a prized target for cybercriminals around the world.

The volatile nature of the environment had resulted in Rogers and his team being forced to take a very reactive stance in protecting the university's digital assets, frequently relying on complete disk reimaging to address compromised machines. "Despite the measures we had in place, it was taking us several days to identify a security incident before we even began remediation procedures," said Rogers. "We were having to completely overwrite around 20 disk drives each week. The resource drain on the team was enormous."

Plugging the Holes

An independent audit and gap analysis from a long-time IT partner confirmed that the weakest link in the university's defenses was endpoint security, and this vulnerability was being amplified by the highly diverse and unknown nature of devices connecting to the global network.

INDUSTRY

Higher Education

LOCATION/HQ

Coventry, England (main campus)

CHALLENGES

- Eliminating existing reactive, inefficient approach to endpoint security
- Securing a highly diverse, volatile global environment
- Attaining infrastructure-wide visibility and control

SOLUTION

Coventry University leverages CrowdStrike Falcon® Complete managed detection and response (MDR) for comprehensive protection of a dynamic campus environment.

"Since deploying CrowdStrike, the time spent by the infrastructure team on resolving cyber threats went from over 80 hours in a measurement period, to under five hours. This is almost a 94% drop."

Steve Rogers

Enterprise Cloud, Infrastructure and Security Architect, Coventry University

A multi-vendor proof of concept enabled Rogers to determine that the CrowdStrike Falcon® platform was the optimal solution to address the university's endpoint challenges. To create a world-class set of endpoint protection capabilities, the Falcon platform was deployed with CrowdStrike Falcon® Device Control USB security, CrowdStrike Falcon® Complete managed detection and response (MDR), CrowdStrike Falcon® Discover IT hygiene, CrowdStrike Falcon® Insight XDR extended detection and response, CrowdStrike® Falcon OverWatch™ managed threat hunting, CrowdStrike Falcon® Prevent next-generation antivirus, CrowdStrike Falcon® Intelligence automated threat intelligence, CrowdStrike Falcon® Firewall Management and CrowdStrike Falcon® Spotlight vulnerability management.

Immediate Benefits

Implementation of the CrowdStrike suite enabled Rogers to reduce the number of vendor solutions maintained by the security team from seven to three. In addition to reducing the burden of managing this number of applications, the effectiveness of the team showed significant improvement: "Since deploying CrowdStrike, the time spent by the infrastructure team on resolving cyber threats went from over 80 hours in a measurement period, to under five hours," said Rogers. "This is almost a 94% drop!" CrowdStrike protects the university's hybrid environment, securing Microsoft Azure and additional AWS services, as well as the numerous physical servers and connected devices. CrowdStrike consultants customized existing protocols and interfaces to enable the Falcon modules to seamlessly integrate with physical and virtual firewalls and the network segmentation security methods that were already in place.

"Very soon after going live we were hit by a string of zero-day attacks," Rogers said. "CrowdStrike identified the threats and isolated the impacted machines in a matter of minutes. Prior to Falcon, this would have knocked us offline for multiple days."

Moving the Needle

As befitting Coventry University's reputation as a global and transformational educator, Rogers and his team operate within a comprehensive metrics framework that tracks key parameters relating to the performance and effectiveness of the security infrastructure.

Measurement	Pre-CrowdStrike	With CrowdStrike
Number of user machines needing reimaging due to malicious threats	18 per week	Zero
Number of malicious files found in network	56 per month	Zero
Average time to resolve security incidents (P1) end to end	2-3 days	44 minutes (longest incident)
Service Desk FTEs needed to manage/ mitigate security incidents	2 FTEs	No recorded incidents since CrowdStrike implementation
Number of security-related incidents on network in six-month period	350 incidents [user-, desktop- and server-related]	Zero incidents
Number of out-of-hours security-related threats discovered in six-month period	113 threats identified	>230 threats identified

RESULTS

- Average time to resolve security incidents decreased from 2-3 days to under one hour
- PCs needing reimaging due to malicious threats dropped from 18 per week to zero
- 94% decrease in time spent on resolving cyber threats

ENDPOINTS

9,000

CROWDSTRIKE PRODUCTS

- Falcon Complete managed detection and response (MDR)
- Falcon Device Control USB security
- Falcon Discover IT hygiene
- Falcon Firewall Management
- Falcon Insight XDR
- Falcon OverWatch managed threat hunting
- Falcon Prevent next-generation antivirus
- Falcon Spotlight vulnerability management
- Falcon Intelligence automated threat intelligence

Notable statistics include:

"The visibility we have now is a powerful asset in keeping the university secure," said Rogers. "We're able to use the detailed reports to show our senior management team threat and risk levels across the entire environment. In addition, we utilize these accurate metrics to create a compelling business case to ensure that we can secure the appropriate levels of investment to continue protecting the university."

People Make the Difference

One of Rogers' team's biggest challenges was having an unmanageable workload. "With CrowdStrike now handling key aspects of our security responsibilities, we're able to focus on being proactive across both the security and infrastructure domains," he said. "And rather than having to ask team members to work unsociable hours, CrowdStrike's 24/7 support desk provides us with the reassurance that everything will get appropriately handled. Everyone is happier!"

"Many vendors in the security space are just anonymous, faceless organizations, but with CrowdStrike, we've come to know the people we work with," Rogers continued. "They've become an extension of our workforce and the way we do business."

For Rogers, the impact of CrowdStrike has been significant. He said: "CrowdStrike is a crucial long-term partner for Coventry University. It may sound clichéd, but knowing that the university's infrastructure is protected gives us peace of mind and lets us sleep well at night."

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.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Start Free Trial →

Learn more **www.crowdstrike.com**