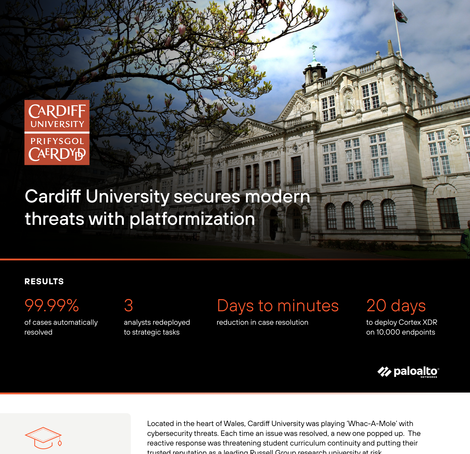


Cardiff University secures modern threats with platformization

RESULTS

99.99%
of cases automatically resolved

3
analysts redeployed to strategic tasks

Days to minutes
reduction in case resolution

20 days
to deploy Cortex XDR on 10,000 endpoints

INDUSTRY
Higher education

COUNTRY
United Kingdom

WEBSITE
cardiff.ac.uk

PRODUCTS & SERVICES

- Cortex® XDR
- Cortex® XSOAR
- Unit 42® MDR
- Unit 42 Proactive Services
  - Tabletop Exercises
- Unit 42 Retainer
- Hardware Firewalls
- Prisma Browser™
- Cloud-Delivered Security Services:
  - Advanced Threat Prevention
  - Advanced DNS Security
  - Advanced URL Filtering
  - Advanced WildFire®
  - Advanced SD-WAN
  - Enterprise Device Security
  - GlobalProtect®
- Professional Services

Located in the heart of Wales, Cardiff University was playing 'Whac-A-Mole' with cybersecurity threats. Each time an issue was resolved, a new one popped up. The reactive response was threatening student curriculum continuity and putting their trusted reputation as a leading Russell Group research university at risk.

In efforts to create a secure, compliant learning programme and foster a positive user experience, the University replaced four separate, overlapping endpoint security tools with a single, connected network and endpoint security platform from Palo Alto Networks. This forward-thinking architecture is augmented by 24/7 managed detection and response (MDR) services from Unit 42.

CHALLENGE

Higher risk in higher education

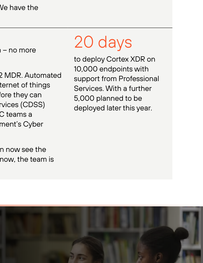
Cardiff University was walking a cybersecurity tightrope, balancing security against user experience. On one side, it needed to protect more than 15,000 different user personas – students, academics, professional services, and research – from every type of threat across its campuses in Wales and Kazakhstan. On the other, it was necessary to ensure that those same users could learn and work with a consistently flexible and rewarding user experience.

The University needed to:

+ **Modernise the security infrastructure:** Security across 15,000 access points was enforced using four separate, disconnected endpoint security tools, which created complexity and delayed response.
+ **Minimise risk:** The legacy fragmented architecture provided poor visibility, and the in-house security team only performed monitoring during working hours.
+ **Increase operational efficiency:** The small IT security team was flooded by manual security tasks, limiting the time available for strategic security initiatives, such as threat hunting.
+ **Protect brand reputation:** Alongside the user disruption and cost implications of a potential breach, there were concerns regarding the reputational damage a cyberattack might cause the University.

"We needed to move to a mature cybersecurity model with a well-defined technology roadmap," says Lee Evans, Assistant Director of IT Infrastructure, Cardiff University. "This included a strategy to streamline the security tool sets and move to a fully automated, proactive platform providing 24/7 cybersecurity protection."

> The things I like the most about this platform are: the high degree of automation, the excellent dashboard reporting, and the speed of response to detected cases.
>
> **Lee Evans**
> Assistant Director of IT Infrastructure
> Cardiff University



Path to platformization

Network security
Next-Generation Firewalls (NGFW)
Prisma Browser™
Cloud-Delivered Security Services:
Advanced Threat Prevention
Advanced DNS Security
Advanced URL Filtering
Advanced WildFire
Advanced SD-WAN
Enterprise Device Security
GlobalProtect™

Proactive and incident response services
Unit 42 Retainer
Unit 42 Proactive Services
Unit 42 MDR

AI-powered SOC platform
Cortex XDR
Cortex XSOAR

SOLUTION

Secure by design models across a global campus

Cardiff University standardised on a single, unified security architecture, with Palo Alto Networks at its core. A connected suite of AI-powered network, browser and endpoint security platforms, together with MDR services from Unit 42, enable the University to stay ahead of threats in an agile, automated environment across every stage of the attack lifecycle.

"We've implemented a secure by design model across our entire IT infrastructure," says Lee. "We can now comfortably prevent and disrupt advanced threats such as ransomware and AI-driven spear phishing. Unit 42 also provides the contingency and reassurance that we can bring in experts if required to help us recover as soon as possible."

Secures uninterrupted learning and research

Cardiff University now has the defence in depth to safeguard both the educational institution and its users' personal information across cloud, network, and 15,000 endpoint devices. For example, Prisma Browser ensures secure browsing across the University's broad user base to stop evasive threats, secure generative AI (GenAI) use and safely enable work from anywhere for students and staff.

By embracing 'trust nothing, validate everything' zero trust cybersecurity, the University is reducing risk, simplifying its hitherto complex infrastructure, and freeing up resources.

"It's like we've moved from owning a mid-range car to driving a Ferrari. We have the security speed, visibility, and control we never had before," says Lee.

4-to-1
Four siloed endpoint security tools replaced by 1 platform, providing single, unified management across 300 buildings – from Cardiff to Kazakhstan.

Maximises security visibility

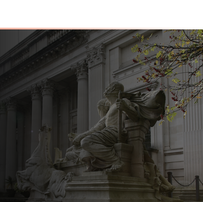
The single platform provides a 360-degree view of the security situation – no more delayed toggling between screens to reach the root cause of a case.

The control is augmented by 24/7 monitoring and remediation by Unit 42 MDR. Automated data collection across the University's endpoints, network, cloud, and internet of things (IoT) provide the critical insight and context needed to block attacks before they can impact the campus. Network Security and Cloud-Delivered Security Services (CDSS) boost Cortex XDR visibility, using Enhanced Application logs to give SOC teams a complete picture. Furthermore, it supports compliance with the Government's Cyber Essentials scheme.

Mike Kennard, Cyber Security Programme Manager, comments, "We can now see the entire attack surface. On average, we're attacked every 10 seconds and now, the team is poised to block those attacks."

20 days
to deploy Cortex XDR on 10,000 endpoints with support from Professional Services. With a further 5,000 planned to be deployed later this year.

> The platform sees everything, giving us the insights to act immediately and strengthen our defences.
>
> **Mike Kennard**
> Cyber Security Programme Manager
> Cardiff University



Increases operational efficiency

Expert threat detection and response are now significantly faster, more accurate, and more complete with Cortex and Unit 42 MDR. Over a two-month period, more than 99.99% of 468,000 security cases were rapidly triaged and resolved through AI-driven analytics, automation, and expert-led MDR workflows, dramatically reducing manual workload and accelerating response at scale.

Cortex XSOAR integrates seamlessly with Cortex XDR as well as third-party products to orchestrate and automate incident response via prebuilt and custom playbooks. This Cortex platform automation, combined with Unit 42 MDR and its proactive threat hunting, has enabled the University to redeploy three team members from reactive alert management to more strategic security initiatives.

Executive-ready reporting and security insights from Cortex XDR and Unit 42 MDR are regularly presented to the University's board to validate the work undertaken by the security team and make the case for further investment. Furthermore, the University is using its Unit 42 Retainer credits to run Tabletop Exercises with its senior leadership team to remain prepared in case of an incident.

This blueprint for modern cybersecurity is being used to train the next generation of cybersecurity talent in Wales.

99.99%
of cases automatically resolved

'Whac-A-Mole' is now all in the past for the University. Today, it benefits from an agile, scalable security platform, augmented by trusted experts from Unit 42. As part of its 5-year plan, the University will start work on a phased Cortex XSIAM® rollout this year.

> We hope never to need to use the Unit 42 Incident Response team to recover from a cybersecurity incident or data breach. However, it provides the reassurance that we can bring in experts if required to help us to recover as soon as possible.
>
> **Lee Evans**
> Assistant Director of IT Infrastructure
> Cardiff University

Find out how platformization and Unit 42 experts can put your organisation ahead of tomorrow's threats.

GET IN TOUCH

© 2026 Palo Alto Networks, Inc. Palo Alto Networks and the Palo Alto Networks logo are registered trademarks of Palo Alto Networks, Inc.