



**Sheffield
Hallam
University**
Knowledge Applied

CASE STUDY

Connecting and safeguarding students and staff at Sheffield Hallam University

The single, unified Palo Alto Networks endpoint and network security portfolio is guiding Sheffield Hallam University towards improved security visibility; increased operational efficiency; and a connected, globally collaborative education framework.

IN BRIEF

Customer

Sheffield Hallam University

Partner



Industry

Higher Education

Featured Products and Services

Graduate education and research

Organisation Size

35,000 students; 4,500 staff

Location

Sheffield, UK

Challenges

Operating disconnected point cybersecurity meant low cybersecurity visibility with high risk and high costs.

Requirements

- + Prevent cyberthreats across cloud, network, and endpoint devices.
- + Protect staff and students' personal information and IP (Intellectual Property).
- + Deliver flexible remote access experiences at scale.
- + Accelerate the Zero Trust journey.
- + Streamline prevention, detection, and response by using orchestration and automation.

Solution

Palo Alto Networks ML-Powered Next-Generation Firewalls, Cortex XDR, Cortex XSOAR, and Panorama; KHIPU Networks Security Operations Centre

Ransomware threats rise 20-fold

Ransomware threats are up 20-fold at Sheffield Hallam University. These and other cybersecurity threats – such as breaches which could potentially compromise the personal information of students, faculty, and staff, or denial-of-service attacks that render learning management and other systems unavailable during important times – pose an increasing risk to the University.

CHALLENGES

Where learning and student experience come together

Sheffield Hallam University is one of the UK's largest and most diverse universities: a community of more than 35,000 students; 4,500 staff; and more than 295,000 alumni around the globe. Of those students, 53% are the first members of their family to attend university and 23% are from low-participation neighbourhoods.

Almost a decade ago, the University standardised on Palo Alto Networks ML-Powered Next-Generation Firewalls (NGFWs) to safeguard its network. However, the education sector has become increasingly vulnerable to ransomware since then. Jisc's Cyber Impact Report 2022 reveals that UK institutions spend an average of £2 million on responding to ransomware attacks – and ransomware is now the sector's top cybersecurity risk, with more than 100 institutions falling victim since 2020.

As lockdown struck, the University's remote connectivity also needed attention. "Almost overnight, we needed to scale remote access to 39,000 students and staff. Our Cisco VPN could do that but was expensive to operate and lacked the functionality to support a modern hybrid workplace," explains Dave Ainscow, Head of Cyber Security at Sheffield Hallam University.

Endpoint protection has also been a challenge in recent years. Ainscow explains, "The Sophos tool that protected our server estate required additional resources to manage exceptions. We also needed to extend EDR to support our new Azure estate."

With these increasing challenges in scaling remote access, upgrading endpoint protection, and – perhaps most critically – protecting itself against ransomware attacks, it was clearly time for the University to modernise its entire cybersecurity infrastructure.



We have seen a 20-fold increase in ransomware since lockdown. We host highly sensitive student, administrative, and research data. We work collaboratively across the world. And people are operating 24/7, so cyber protection needs to be highly resilient, proactive, and continuous.

Dave Ainscow, Head of Cyber Security at Sheffield Hallam University

REQUIREMENTS

Protecting staff and students' personal information

The University's next-generation cybersecurity strategy would be required to:

- + Prevent cyberthreats across cloud, network, and endpoint devices.
- + Protect staff and students' personal information and IP.
- + Deliver flexible, policy-driven remote access experiences at scale.
- + Accelerate the Zero Trust journey.

SOLUTION

One unified cybersecurity portfolio

The University has extended its existing Palo Alto Networks network security solution into endpoint protection and remote working. One unified portfolio comprising Palo Alto Networks ML-Powered NGFWs, Cortex XDR, and Panorama provides around-the-clock protection against new and existing threats.

Cortex XDR protects the University's 370 on-premises servers and Azure environment. It detects and responds across all data, regardless of origin or location. Complete visibility eliminates blind spots, while the management console offers end-to-end support for all Cortex XDR capabilities, including endpoint policy management, detection, investigation, and response.

Remote working has been similarly transformed. GlobalProtect is the University's exclusive VPN solution, enabling secure remote working for up to 34,000 staff and students. "The switch from Cisco during lockdown was a remarkable achievement. We had everyone live in less than two months," says Dave.

KHIPU Networks have played a vital role in orchestrating this cyber modernisation. Dave further explains, "KHIPU have been a long-term, trusted partner, providing higher education expertise, insight, and professionalism. Their engineers really understand our business too – they have become an extension of the University."

In 2022, the University began using the KHIPU Networks Security Operations Centre (SOC) to provide 24/7/365 cyberthreat monitoring, detection, and response. The SOC uses the Palo Alto Networks Cortex XSOAR platform to accelerate security orchestration, automation, and response. "Their SOC is staffed by cyber experts who are always available, their service integrates into our existing environment and doesn't just alert, it protects and prevents threats," says Dave Thornley, the University's Head of Digital Architecture.



We don't think there's any other solution on the market like Palo Alto Networks. The integration, simplicity of interface, visibility, and reporting outpace anything offered by other vendors. By utilising our existing Palo Alto Networks Next-Generation Firewalls we are to extend their capabilities by using their portfolio alongside KHIPU Networks as a low-risk, fully interoperable single partner.

Dave Ainscow, Head of Cyber Security at Sheffield Hallam University

BENEFITS

Connecting, collaborating, and learning globally

The benefits of this connected, agile cybersecurity portfolio include:

- + **Continuity of learning and research:** Despite the growing threat landscape – especially from ransomware – students and staff can connect, collaborate, and learn globally, confident that their data is protected and available.
- + **Student and staff security:** The portfolio prevents cyberthreats across cloud, network, and endpoint devices while protecting personal information and IP. It also safeguards highly sensitive research and government data.
- + **All-round visibility:** Ainscow explains, “Some people write risky PowerShell scripts. Cortex XDR identifies these among everything else so we can take action to close the threat.”
- + **Secure remote learning and working:** The portfolio delivers modern, flexible, policy-driven remote access experiences at scale – across any user, any application, any device, and any network.
- + **Increased efficiency:** The University requires fewer resources to manage its IT estate, despite relentless growth in data, applications, and users.
- + **Unified management:** There is a single cybersecurity solution across servers and services, driving simple, integrated security across cloud and SaaS workloads. For example, GlobalProtect supports SAML authentication in Azure Active Directory (AD).



In partnership, Palo Alto Networks and KHIPU Networks assess, protect, and manage the ever-increasing digital risks and threats posed to Sheffield Hallam University, ensuring our staff, students, and partners are protected throughout their education journey.

Dave Ainscow, Head of Cyber Security at Sheffield Hallam University

Learn more about Palo Alto Networks on the [website](#) where you can also read many more [customer stories](#).

To learn more about KHIPU Networks Security Operation Centre, please visit: <https://www.khipu-networks.com/join-khipu-soc-community/>



3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2023 Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. parent_cs_sheffieldhallam_010923