How Anglia Ruskin University Slashed IT Workloads And Improved Security Maturity Through Automated Email Protection And Increased Resilience

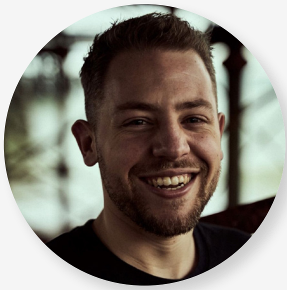
INDUSTRY	HEADQUARTERS	COMPANY SIZE
Education	Cambridge, United Kingdom	4,000+ staff, 35,895 students

OVERVIEW

Anglia Ruskin University (ARU) is a modern public university with campuses in Cambridge, Chelmsford, Peterborough and London. With over 35,000 students and more than 4,000 staff, ARU is known for its commitment to inclusive education, innovation and employability. The university continues to invest in digital transformation to support its academic and administrative communities.

OUR SOLUTION

Harmony
Email & Collaboration



> The most tangible improvement is the dramatic reduction in security incidents. Our Microsoft 365 team is handling a much lower level of threats that need to be remediated, compared to before. This improvement is particularly significant given the - increasing sophistication of email-based attacks targeting educational institutions.
>
> *Kyle Strudwick, Head of User Infrastructure at ARU*

CHALLENGE

Facing rising security and operational challenges, Anglia Ruskin University (ARU) found its email security platform increasingly lacked the flexibility the team needed to implement the security policies necessary to deliver effective protection while also providing users with the quality user experience they expect.

The inflexibility of their legacy email security platform also brought significant operational inefficiencies, forcing the IT department to spend excessive time manually handling security incidents. That stole time away from team members being able to focus more on strategic initiatives. As a substantial educational institution, ARU's technology team supports approximately 4,000 staff members and over 35,000 students across its multiple campuses. During peak academic periods, ARU needs to protect tens of thousands of active email mailboxes.

When it came to improving cyber security maturity, the ARU technology team set three primary objectives: strengthen protection against advanced attacks, raise the university's security maturity levels through automation, and improve user experience.

As cyber criminals increasingly leverage generative AI to create more convincing and sophisticated attacks, ARU found that its existing email defenses were falling behind against these threats. As Kyle Strudwick, head of user infrastructure at ARU, explained, the university "wasn't getting the level of protection that they wanted against complex threats and phishing attacks."

Concerning the maturity of the security program, Mladen Kirilov, information security manager at ARU, added that the team wanted to protect all user accounts evenly. Previously, they considered student accounts as a lower risk due to lower potential breach impact, compared to administrative accounts. Not anymore. "Even a student account can give an attacker a foothold in our network. A foothold they can then use to start doing malicious things," he said.

By improving the resilience of all the university's mailboxes, the security team aimed to reduce the time spent on remediation and attack investigations, thereby increasing the time allocated to maintaining proactive defenses. This improvement would enhance security and lead to cleaner mailboxes, ultimately improving the email experience for everyone across the university.

a.r.u.

> Positive feedback came from internal IT staff, lecturer staff, to senior executives consistently reporting reduced spam volumes and easier email management.
>
> *Mladen Kirilov, Information Security Manager, ARU*

SOLUTION

To meet their goals, ARU undertook a comprehensive evaluation that ultimately led the team to select Harmony Email & Collaboration. Working closely with their technology partner Softcat, together they developed a rigorous selection methodology designed to identify the optimal email security platform for their environment.

The methodology proved thorough. The evaluation began with extensive market research, followed by architectural reviews conducted through their technical design authority. "We ended up with a proof-of-concept that included four vendors. We trialed their four products within our environment," Strudwick explained.

The ARU technology team's criteria focused on several key areas, including Microsoft 365 integration, advanced threat protection, the ability to detect sophisticated attacks — particularly impersonation and spoofing attempts — optimal user experience and automation, and the quality of the security vendor's support.

Softcat was crucial in this process. Softcat helped ARU navigate the complex vendor landscape and ensured that they considered all viable options. "Softcat helped us in the initial discovery and in narrowing down potential vendors. They pointed out things that we needed to consider that we hadn't," noted Strudwick, citing how the partnership was instrumental in giving ARU confidence that they had thoroughly evaluated the market before making their decision.

Softcat made sure Harmony Email & Collaboration would be an excellent technological fit and that it aligned well with our architecture and requirements," added Kirilov.

Harmony Email & Collaboration distinguished itself from competitors through several key differentiators that directly addressed ARU's specific requirements. First, the seamless integration of Harmony Email & Collaboration with Microsoft 365 proved to be crucial, as ARU operates predominantly within the Microsoft ecosystem. This native integration eliminated the need for complex third-party plugins or additional user training, as Kirilov explained. "Everything's integrated, and Harmony Email & Collaboration comes with first-party email reporting functionality for our users. You don't have to install any Outlook plugins," Strudwick said.

For a university with limited security resources, these efficiency gains were crucial for maintaining effective protection without overwhelming the IT team.

OUTCOME

Harmony Email & Collaboration delivered significant improvements. These results demonstrate both quantifiable operational benefits and qualitative improvements in user experience and security posture.

The most tangible improvement is the dramatic reduction in security incidents. "Our Microsoft 365 team is handling a much lower level of threats that need to be remediated, compared to before," Strudwick said. This improvement is particularly significant given the increasing sophistication of email-based attacks targeting educational institutions," he said.

The implementation has yielded substantial operational benefits for ARU's IT organization. Support ticket volumes related to email security issues decreased by approximately 10-15 percent, freeing up valuable IT resources for strategic initiatives rather than reactive security management. The transition, from proof of concept to full implementation, went seamlessly. Kirilov noted how well Check Point managed this transition: "There was no gap between our trial and our implementation," he said.

However, the decisive factor in ARU's selection was the self-service user capabilities provided by Harmony Email & Collaboration's digest functionality. This feature enables end users to review quarantined emails and release legitimate messages themselves, eliminating the need for IT intervention with every request. Strudwick described this as a game-changing capability: "Having the digest available to enable users to release emails they need themselves is invaluable. These communications may be invaluable to them, and they don't want to wait for us to release them."

Harmony Email & Collaboration has also impressed the ARU team with its administrative efficiency features, providing easier configuration, clearer visibility into security events, and streamlined incident response capabilities. For a university with limited security resources, these efficiency gains were crucial for maintaining adequate protection without overwhelming the IT team.

Perhaps most rewarding was the unprecedented positive feedback from users across the organization garnered by the ARU technology team. "Positive feedback came from internal IT staff, lecturer staff, to senior executives consistently reporting reduced spam volumes and easier email management," Strudwick said.

Harmony Email & Collaboration enabled the university to provide a more reliable, always-available email experience while simultaneously strengthening its security posture. "Ultimately, it helped us to deliver a safer, more reliable experience," Strudwick said.

The success of ARU's implementation demonstrates how the proper email security can simultaneously strengthen an organization's security posture while reducing operational complexity and improving user satisfaction. For educational institutions facing similar challenges with sophisticated email threats and resource constraints, Check Point Harmony Email & Collaboration offers a proven path to enhanced security without sacrificing operational efficiency or user experience.

About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading protector of digital trust, utilizing AI-powered cyber security solutions to safeguard over 100,000 organizations globally. Through its Infinity Platform and an open garden ecosystem, Check Point's prevention-first approach delivers industry-leading security efficacy while reducing risk. Employing a hybrid mesh network architecture with SASE at its core, the Infinity Platform unifies the management of on-premises, cloud, and workspace environments to offer flexibility, simplicity and scale for enterprises and service providers.

LEARN MORE

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065

www.checkpoint.com

December, 2025