Arrow Global Case Study

Arrow Global Group PLC is a leading European credit and asset management business with teams operating across the UK, Ireland, Portugal, Netherlands, Italy and Albania. Processing credit and debt information, data protection is at the heart of Arrow Global's business. The Group Information Security Team reports into the Group Chief Information Security Officer and is made up of a team of multi-disciplinary Information Security professionals, each having responsibility for a geographical region.

THE CHALLENGE

Arrow works across multiple markets under a range of operating companies that all share the 'One Arrow' ethos. Creating a connected Group with enhanced cohesion was a top priority for Group CEO, Lee Rochford. In 2019, this priority led to the requirement to find a solution that would allow colleagues across the multiple geographies to communicate and collaborate in a modern and more effective way. This, in turn, would enable employees to forge better working relationships and unlock the full potential of the 'One Arrow' culture.

Led by its Group Corporate Communications Team, Arrow considered a number of platforms and after a detailed evaluation working with consultancy partner Generation Digital, selected Workplace by Facebook for its intuitive user interface, excellent mobile user experience, and familiar features and functionality. It was determined that this familiarity with the platform among users would drive greater utilisation and better employee engagement throughout the organisation.

The support of Arrow's Group Information Security Team was critical to ensure that the implementation complied with the Group's minimum information security requirements. Matthew O'Neill (Group Information Security Manager) was tasked with devising and leading Arrow's Workplace security strategy and then, with support from Andrew Mallin (Technical Project Manager and Infrastructure Architect), completing its technical implementation across the Group.

Arrow Global operates under a strict financial regulatory regime across all of its geographies, including the Group's regulatory and contractual obligations with regard to data protection. Matthew's initial review of native security within Workplace found that in several areas additional security controls were required to make it suitable for Arrow Global.

He explains, "I didn't know much about Workplace, however upon researching its default offering, I found that there were a number of areas in which the platform wouldn't meet our stringent security requirements if it was to be used in the way we wanted."

ARROW GLOBAL

PROFILE

INDUSTRY
Credit and asset management

REGION
Europe

CHALLENGES

- Adoption of Workplace by Facebook across the organisation but need to ensure acceptable use policies and regulatory compliance
- Insider threat–prevent a staff member inadvertently or maliciously sharing sensitive information
- Financial regulatory compliance under PCI-DSS
- Identify malware in user posts and chats

BENEFITS

- Mitigate exposure of PCI data via Workplace by Facebook by collections agents
- GDPR compliance for all users

SOLUTIONS

- API Protection for Workplace by Facebook to enforce GDPR and PCI DLP policies
- Using Netskope steering client to enforce GDPR and PCI DLP policies
- Threat protection and remediation in Workplace by Facebook posts

netskope

Matthew determined that Arrow would need a layered, strength-in-depth approach to security, with multiple measures serving as fail-safes.

"As well as ensuring that Workplace didn't become a free-for-all for internal visibility of confidential documents, we also needed to maintain security controls to remove the risk of sensitive data going outside of our perimeter," he concluded.

THE SOLUTION

Matthew identified two viable security approaches and outlined both to the Workplace project team: "We had a choice; proceed within the agreed timeframe, but only use the platform for public content or, maintain the goals from the original brief of allowing free collaboration, but push back the launch date until we could ensure that all content and data was secured in compliance with both internal and external data regulations. In the end, it was agreed that extending the timeframe was both necessary and valuable to ensure the project met the original brief."

After assessing the additional security requirements and evaluating vendor options suggested by Generation Digital, Matthew recommended the use of two security vendors to support the enhancement of the platform's security:

1. Okta was selected as the Cloud Identity Solution providing identity and access management to Workplace via Single Sign-On and Adaptive Multi-Factor Authentication; and

2. Netskope was selected for content management and data protection:

   a. Netskope's End Point Agent was to be installed on all corporate devices, physically preventing unapproved data and files from ever reaching the Workplace cloud;

   b. Netskope's Reverse Proxy would provide an additional layer of security to support users who wanted to use their own access device (including iOS devices). With the Reverse Proxy, all traffic to Workplace would first go through the Netskope private Security Cloud; and

   c. The final safety guard in the Netskope platform would come from the API integration. Netskope is physically built into the Workplace platform so if all else fails and something inappropriate does somehow manage to get posted to Workplace, it will be automatically removed within the platform in seconds.

In addition to designing and implementing the aforementioned technical security controls, Matthew also opted to draft a new Acceptable Usage Policy specifically for Workplace; this would be used to complement the existing Arrow Information Security policies.

THE IMPLEMENTATION

Matthew's first action was to prepare the Acceptable Usage Policy. This would not only inform the project team and users of what was allowed within the platform but would also drive the Netskope implementation—instructing the platform of Arrow's security policies.

Matthew: "The policy creation was a big task, and while many policies are pre-programmed into Netskope, we wanted to tailor specifics to optimise both security and usability. For instance, Netskope has an existing profanity blocker, but we wanted to ensure that we were capturing local dialects... and researching local Glaswegian profanities was eye opening! Personally Identifiable Information (PII) blockers can also be problematically heavy-handed without tailoring because they can block full name use, which prohibits users from tagging colleagues by name on Workplace."

Although securing the Workplace platform added three months to the project timeframe, the Netskope implementation went smoothly, with Netskope team

"As well as ensuring that Workplace didn't become a free-for-all for internal visibility of confidential documents, we also needed to maintain security controls to remove the risk of sensitive data going outside of our perimeter"

Matthew O'Neill | Group Information Security Manager

members collaborating with Matthew and Andrew to ensure that Arrow received the required customisation.

Matthew: "The Netskope team was great, working collaboratively with us to achieve our goals in the tight timeframe. They were knowledgeable as well as supportive of our intention to launch in a very short timescale. Our needs were specific, we required extensive tailoring, and we were not prepared to compromise on our minimum-security standards, which was something they fully supported."

"As a company responsible for data belonging to nearly 3 billion people, Facebook takes security very seriously. Workplace adheres to the highest security standards with globally recognised compliance and security certifications. The project team at Arrow Global also take security very seriously and invested a significant amount of time with us to ensure the security solution was world class." Graham Mackay, Managing Partner at Generation Digital.

THE RESULTS

The Workplace platform is now up and running on corporate devices for employees in all geographies, and usage figures are looking very strong. Arrow's Information Security Team has enhanced the security of the platform without compromising on usability and adoption has been so positive that the Group Corporate Communications Team is already pulling back on its use of email which is, in turn, further driving company-wide dependency on Workplace.

FUTURE PLANS

With the Netskope End Point Agent now installed on corporate devices, Arrow is working to provide access to Workplace via personal devices with the same level of security controls.

Finally, with the end in sight for the initial Workplace project, the Group Information Security Team is looking forward to being able to make full use of the much broader functionality of Netskope, including the discovery and management of unsanctioned cloud use as well as DLP across Arrow Global's wider IT infrastructure.