yubico

RWS protects their global workforce with YubiKeys

Enhancing security for hybrid & remote employees with phishing-resistant MFA

Case Study

RWS

Industry
- Translation Services

Benefits
- Enabled shift to remote work
- Smooth access to VPN
- Secures Microsoft 365
- No mobile device required

Protocols
- 2FA

Products
- YubiKey 5 NFC

Deployment info
- Office Workers
- Remote & Hybrid Workforce

An industry leader with an urgent need to raise the bar for security

RWS is one of the world's largest translation and localization agencies, utilizing the development of machine translation and artificial intelligence, as well as their team of skilled experts, to translate and localize content for companies all around the world. Headquartered in the UK, in recent years RWS has acquired many other translation agencies, including competitor SDL. Any merger of large companies also requires a merger of the technology they use. And as RWS acquired new companies, it became clear that not all parts of their business were at the same stage of technological developmen—this was especially true for cybersecurity.

Some parts of RWS supplied employees with phishing-resistant multi-factor authentication (MFA), while others had not implemented any MFA at all. Senior Project Manager Ben Donnelly, who previously worked at SDL, explains: "I'd been with SDL for a year or two and there was no MFA at all. That was unusual to me because from previous companies I was used to having MFA as part of my normal day-to-day process, whether it be a mobile application or some form of hardware. So for us, it was really about catching up. It was important to add extra layers of security, and MFA was part of that."

Donnelly is now part of the core IT team serving the entire RWS group. Shortly before SDL was acquired, he had been tasked with leading a project to deploy strong MFA to SDL employees around the world. While the long-term plan was to combine the Microsoft tenants used by RWS and SDL, it was decided that this SDL-only project was urgent and should continue.

Client request for strong multi-factor authentication (MFA)

A major driver in SDL's realization that they needed stronger MFA was the increasing number of clients who impose MFA policies not only internally but also to third-party contractors. "We are proud to build partnerships with clients all around the world across many industries. Today, part of delivering the high-quality service they expect is maintaining strong cybersecurity standards," explains Donnelly. Meanwhile, internal auditors also pushed for MFA to aid the protection of sensitive data and intellectual property.

Ben Donnelly
Senior Project Manager at RWS

> "From previous companies, I was used to having MFA as part of my normal day-to-day process, whether it be a mobile application or some form of hardware. So for us, it was really about catching up. It was important to add extra layers of security, and MFA was part of that."

RWS needed **secure authentication** for remote workers.

The rising tide of cybercrime globally provided further impetus for SDL to strengthen their defenses. Cybersecurity risks are certainly higher than five years ago, admits Donnelly: “We have offices all over the world, and as geopolitical tensions have risen, we’ve seen an increased number of attacks. To protect both staff and customers, we’ve taken steps to mitigate those risks and reduced our presence in certain countries.” The company also regularly reviews their vulnerability to attacks by sending out their own internal phishing emails to test which employees will click potentially dangerous links.

Legacy MFA failed to meet employee needs

As the need for MFA became clear, SDL, which was now part of RWS, chose their current VPN, Pulse Secure, as the first service for which they would demand a second factor of authentication. The next question was what form of MFA would be chosen as there are various MFA approaches available. Initially one form of legacy MFA, mobile authentication, was seen as the easiest option. “We came within days of pushing it out,” says Donnelly. “I’d even written and recorded the user guide for it! The convenience factor of having an app is why we ended up nearly pushing out a soft option. However, there was pushback from certain user groups who were not willing to use a personal device for a work function. By default we don’t give out smartphones to all users if there’s no business need for that in their role, so we struggled to get people to buy into the idea of using mobile authentication.”

It was quickly decided that as mobile authentication was unpopular among employees, hardware security keys were the best option. RWS turned to Yubico and purchased YubiKey 5 NFCs, which can be used on both laptops and, using contactless technology, on smartphones. The initial purchase was for all employees, and long-term contractors, who worked for the part of the company which had formerly been SDL. Additional spare YubiKeys were also purchased to be stored at various offices globally to service future employees.

> “We came within days of pushing out mobile authentication, but there was pushback from certain groups of users who were not willing to use a personal device for a work function. We struggled to get people to buy into the idea of using mobile authentication.”
>
> Ben Donnelly, Senior Project Manager at RWS

Enabling deployment to a remote workforce with “thousands of individual offices”

The timing of the project meant that deployment was more challenging than it would have been in ordinary circumstances. “The pandemic necessitated a shift to remote work,” says Donnelly, “which meant we essentially went from having 55 offices around the world to having thousands of individual offices in a matter of weeks. Our focus became supporting them and making sure they had whatever they needed to safely and securely keep doing their jobs and delivering a great service to customers, whether that was translating, doing the accounting or whatever else.” Even finding correct addresses for delivery proved challenging, as in many countries employees were working from home, often from different cities. The implementation of Brexit, while the project was in process, added further bureaucratic hurdles. Donnelly relied on office managers to distribute deliveries and ensure any new employees would receive YubiKeys. The full deployment took around three months and covered much of the globe, including Europe, the Middle East, North and South America, Asia and Oceania.

> MFA needs to be part of employees' day-to-day. If we can convey that message effectively, then the rest will be fine. The technical aspect of deployment was fairly simple, but we knew what was really going to make the project a success was user engagement."
>
> Ben Donnelly
> Senior Project Manager at RWS

Any IT deployment requires user engagement, but Donnelly knew this would be more challenging remotely: "Users just want to get on with their day job, right? We needed to find a way to make YubiKeys interesting and engaging, and to help employees understand why it's important."

To build enthusiasm, Donnelly created a series of videos, which he filmed with his daughter, to share on the company's internal social network: "I knew I'd have to do the normal email campaigns with PDF user guides because some people like learning that way. But we also know people ignore emails from IT. So I thought, 'let's see if we can make this funny'. We treated it like a movie marketing campaign, starting with a little teaser trailer. Then we created a clip where I start a mock presentation about how difficult everything is, but this is derailed by my daughter who immediately interrupts me and goes 'oh I've done it—easy!' I just used the iMovie app on my phone, and we dropped these sorts of videos every two or three weeks—they got a lot of engagement and comments from people who would have probably ignored an email."

A positive and secure experience—with more to come

It was decided to phase in the rollout of phishing-resistant MFA country-by-country. Employees were given a date by which their old VPN connection, which didn't require MFA, would no longer work. Any employees who were slow to switch to the new VPN link could be identified and given the support they needed. Following this, a subsequent phase could begin: requiring MFA to access all Microsoft 365 tools. This is now complete, and Donnelly is pleased with the results of the deployment: "The whole experience was overwhelmingly positive. We sent everyone this little key to look after with their lives and we didn't really get any complaints. I didn't ever want it to be something they constantly think about. I wanted the YubiKeys to seamlessly dive into their normal working day with minimal disruption, which I think they did. My bosses were delighted because the YubiKeys have done exactly what they had hoped. Ultimately, employees cannot get onto the VPNs without this extra layer of security, and it's important."

Contact us
yubi.co/contact

Learn more
yubi.co/yk5