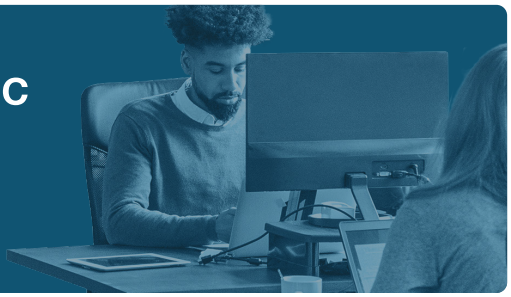
yubico

Phoenix Software protects the public sector supply chain with YubiKeys

Transforming workplaces across the UK public sector



Case Study

PHOENIX

Industry

- IT for Public Sector

Benefits

- Protects high security environments
- Unified tool for smartcards and other platforms
- Simplifies multi-user accounts
- Reduces reliance on passwords

Protocols

- FIDO2
- PIV

Products

- YubiKey 5Ci

Deployment info

- Privileged user accounts
- Accounts accessing customer environments

Phoenix Software enables digital transformation in the workplace, empowering UK organisations to innovate and transform with cloud technology, data, AI, security, and collaboration tools. By understanding the individual goals of its customers, Phoenix delivers strong, outcome focused IT solutions and services that allow UK organisations to make a difference to the lives of their employees, service users, and communities. As a reseller with direct access to customers' IT systems, Phoenix is part of the supply chain, which means the company has an important role in protecting critical infrastructure—not just by offering clients high-assurance security services, but also by securing its own IT infrastructure.

Shaun Tosler, Infrastructure Manager at Phoenix, works closely with the Phoenix CTO and Bytes Technology Group CISO to look after all IT infrastructure internally and those that run managed services. His challenge is to maintain a high-level of security while ensuring ease of access and usability for both their own systems and customer environments. "There's an increased risk in working with the public sector," admits Tosler. "Any breach, whether within our own organisation or to one of our suppliers, could affect, for example, the many hospitals we deal with. Our first priority is making sure that our access to customers' systems is safe."

According to Tosler, Advanced Persistent Threats (APTs), where intruders lurk undetected in a network for extended periods of time, are "few and far between but they are probably the biggest threat because of the knowledge, funding and backing they have. While some attackers actively try to cause harm, we also have to deal with opportunists seeking to sell credentials and access."

Tosler sees the end user as the biggest vulnerability: "The days of simply having to protect your network boundary are gone. Of course, you still need to have firewalls in place, but it doesn't matter how strong your firewalls are if a user gives out their credentials to a phishing attack. All it takes is for someone to be tired and make one bad decision. They may have all the anti-phishing training in the world. Everyone's human."

Shaun Tosler
Infrastructure Manager,
Phoenix Software

> "It's about balancing between security and usability. We can have the most secure environment in the world, and that's great, but not if no one can do anything. The YubiKey allows us to maintain that high level of security while still giving high levels of usability."
>
> —Shaun Tosler, Infrastructure Manager at Phoenix Software

Seeking an alternative to passwords

Historically, Phoenix relied on passwords and legacy mobile MFA. Passwords had to be complex and rotated often, but Tosler found that users' passwords quickly became predictable: "If you've got five passwords, all the user is going to do is add a number or a symbol at the end. Human nature will take the easiest route, and the easiest route is just to increment."

Determined to enhance security for privileged users, Phoenix saw weaknesses with mobile authentication: "It could be that multiple people have thumb prints on the phone and that's all they need, really. I know you need to put in code but I have no trust in terms of who's actually got the phone and is doing the authentication." Phones also rely on battery and cellular reception: "One of the reasons we don't use smartphones for MFA is that they are just one more thing to go wrong. We don't like having to rely on the mobile."

Time-based One Time Passwords (TOTP) also didn't appeal to Tosler: "You still need a password. It's still 'Password MFA'. The main driver for us is we want to be passwordless, or at least passwordless where it makes sense to do so. And the reason for that is if the user doesn't have a password, they can't get phished.

Phoenix began testing FIDO2 with YubiKeys: "We needed a solution that was simple enough to manage, simple enough for end users and provided the right level of security. FIDO was that tool. With the YubiKey the user has to be connected to their device, they have to put in a six-digit pin and they have to touch the key."

> "The biggest low hanging fruit for attackers is the end user. YubiKeys allow us to get rid of the human factor. If you don't have a password, you can't get phished."
>
> —Shaun Tosler, Infrastructure Manager at Phoenix Software

Deploying YubiKeys to privileged users

Phoenix chose to purchase the YubiKey 5Ci for all users with administrative access into either internal systems or customers' tenants. Phoenix use YubiKeys with multiple providers who support FIDO, including Microsoft 365, Twilio, and Cloudflare. If a user loses a key they can request a replacement from the administrator.

Deployment was aided by the simplicity of the technology. According to Tosler, "We already knew that FIDO isn't rocket science. You don't have to set up a full PKI environment. You literally just plug a key in, set your PIN, register with the systems you want to use, and you're done. On Day One, it only took 30 seconds." Tosler is pleased with how the keys have performed: "It really did simplify multi-user management. I've got five accounts – now to access any of those accounts all I need is one six-digit pin and to touch my key." A user can use a single YubiKey across multiple work and personal accounts and the secrets are never shared between services.

Phoenix have also been able to utilise YubiKey's Smart card/PIV functionality for internal support: "When someone logs into an end user's machine through our new support tool, this can pass through smart cards. We still do need to have a legacy approach in place for smart cards and this is a better way of managing it because I don't need to give users a physical card and a YubiKey. YubiKeys provide us with a unified platform for both our smart card and FIDO-based authentication processes."

> At the end of the day, we're happy. There's not a challenge we've had that YubiKeys themselves can't provide the solution to. Whenever we've asked 'Do YubiKeys work in this situation?', the answer has always been yes."
>
> —Shaun Tosler, Infrastructure Manager at Phoenix Software

YubiKeys deliver a fast and easy user experience and drive productivity

The response from end users has also been positive. Kieron Stone used the YubiKey in his role as a technical support analyst at Phoenix: "The YubiKeys have been really beneficial to our way of working and when you've got a multi-user account it really does simplify things. The YubiKey gets rid of any time spent trying to remember your passwords or having to reset everything because you've forgotten it. That was all time wasted that you could be doing something else and that time has monetary value. In that way they drive productivity, as well as making life easier."

Down the line, Phoenix plans to extend their requirement to use hardware security keys to all third-party consultants. According to Tosler, consultants have already seen how YubiKeys are used internally and have been keen to learn more: "They wouldn't necessarily use them in the same way we do, but people see how easy it is to secure both their personal and professional accounts. Even if they just use the keys for a password manager, it can give them added protection and save them time."

Any MFA is better than a password, but not all MFA is created equal

Phoenix are not just happy customers–they have also begun selling YubiKeys themselves to their clients in the UK public sector to help them establish phishing-resistant MFA in their environments and raise the bar for security beyond basic legacy MFA. Tosler explains, "Our requirement for highest-assurance security is shared by our clients. We look after the emergency services, local governments and others for whom security is absolutely critical." YubiKeys meet the requirements for public sector organisations set out in the Government Cyber Security Strategy and, for healthcare, recommendations put forward by NHS Care Identity Service 2 (NHS CIS2).

However, Phoenix sees YubiKeys being valuable even for clients outside the public sector: "The level of security they provide is suitable for small companies all the way up to much larger enterprises than us. They don't just solve for very specific things for a particular sector – they are just very good at securing everything. They provide that level of trust, since the password is offline, and there's not a challenge they can't handle. So any organisation could roll them out."

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
5201 Great America Pkwy
Suite 122
Santa Clara, CA 95054
USA