deltaflare

CASE STUDY

Legacy Systems Encapsulation

at a glance…

When a leading UK utility operator was confronted with key operational technology obsolescence and the need to comply with cyber security regulations, they turned to the Phoenix platform.

This choice extended the lifespan of their assets and introduced vital cyber security controls. Remarkably, this solution was implemented within a similar budget to traditional industrial computers, while it seamlessly integrated numerous advanced security features that would have otherwise required substantial investments and the incorporation of multiple hardware and software systems.

The utility sector is reliant upon legacy hardware and software to operate systems safely. Current digital technologies being deployed do not apply secure-by-design principles, thus leaving the CNI utility systems vulnerable and exposed to cyber-attacks.

The industry heavily depends on software solutions running on outdated hardware and end-of-life operating systems, resulting in increasingly unsustainable maintenance costs. Moreover, the implementation of stringent cyber security regulations has substantially increased the long-term cost of ownership associated with these assets.

Challenge

Industrial computers had been deployed to facilitate a range of functions, from hosting engineering software (as Engineering Workstations) to carrying out advisory tasks, process calculations, regulatory reporting, and serving as the interface between operational equipment.

These industrial computers had reached the end of their operational life which necessitated their replacement. They were running unsupported Windows 98 or Windows XP operating systems, making an upgrade to modern operating systems unfeasible due to compatibility issues with legacy industrial software.

The utility operator faced the dual imperative of replacing the industrial PCs for continued operational reliability and achieving compliance with new cyber security regulations. The key cyber security requisites encompassed:

- Assurance of effectiveness of the security controls
- Management and maintenance of hardware and software assets
- Secure device management
- Securing stored and transmitted data
- Implementing Secure by Design and Least Privilege techniques
- Secure Configuration and central configuration management
- Vulnerability management
- System resilience and robustness through backup and recovery capabilities
- Security logging and monitoring

By employing conventional methodologies, meeting these cyber security requirements would have necessitated substantial capital and operational expenditure. This approach would have entailed the adoption of multiple new hardware and software solutions, significant alterations to the site's architectural infrastructure, extended periods of system downtime, the formulation of new policies and procedures, and the recruitment of additional resources to maintain and update the introduced systems.

Solution

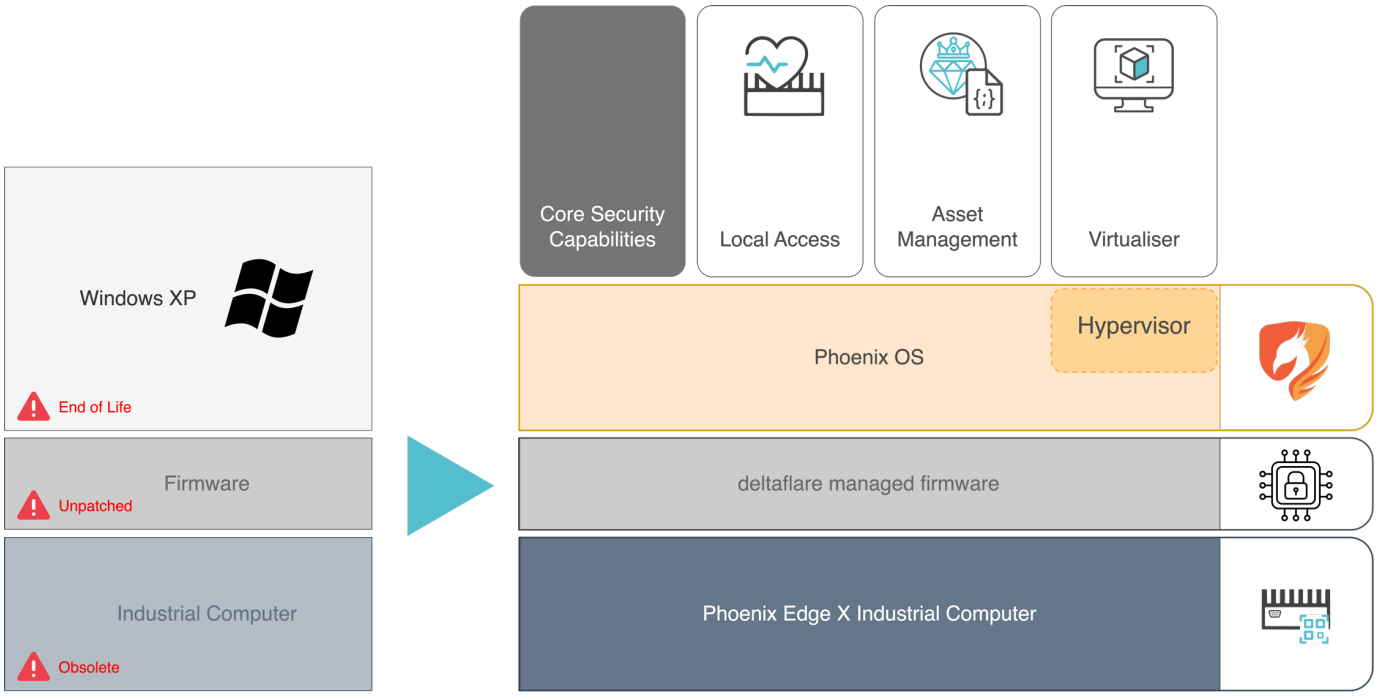
The utility operator selected the Phoenix platform to envelope the existing software systems while fortifying security measures around the legacy infrastructure.

To achieve this, new industrial hardware replaced the existing end of life hardware. Phoenix is hardware platform independent and so provided flexibility and cost reduction to the Operator. The selected hardware met the engineering and operational requirements and was assured for long term support.

The Phoenix platform with its ecosystem of services and apps is designed for seamless integration with Operational Technology. This solution was adopted intuitively by the operators and site technicians without a need for upskilling. Users were able to use existing tools and interfaces on site with transparent security provided by Phoenix.

The Phoenix Core provided security around the legacy software and whole system assurance. The Local Access app was utilised to deliver secure local access and diagnostic capability. The Phoenix Virtualiser app was used to encapsulate the existing software systems.

> *Applying cyber security to our legacy and distributed assets has been a major challenge for us and the wider industry.*
>
> *Phoenix has proven to deliver Critical National Infrastructure security without compromising on operation. The total cost of ownership has been compelling in comparison with any alternatives.*
>
> **OT Enterprise Cyber Security Architect** | UK Gas Network Operator



Leveraging the operator's backup procedures, the Virtualiser app delivered financial advantages and enhanced agility in transitioning to the Phoenix platform.
The Phoenix platform delivered central management of assets, and a method for offline Authorisation based on Operator's Identity and Access Management system (IDAM / IdP).

Notably, the Phoenix platform solution was implemented at an equivalent cost to that of a hardware-only replacement.

The Phoenix platform with Virtualiser app enables out-of-date computer systems running on obsolete hardware and un-supported operating systems to be transferred to a cyber-hardened, future-proof platform with minimal disruption and with the guarantee of replicated functionality

Your Roadmap with Phoenix

This solution is ideally suited for the secure maintenance of legacy critical systems. Its applicability extends to SCADA workstations, historians, engineering workstations, supervisory and reporting systems, and a diverse array of applications spanning multiple industries.

Reach out to our sales team to start the conversation and explore the possibilities.