Enhancing Data Security: Trusted Technology Partnership Ltd.'s Port Control and Data Loss Prevention Solution for South East Coast Ambulance Service

Summary

With over 25 years of experience, Trusted Technology Partnership (formerly Healthcare Computing) are experts in delivering exceptional IT services. This case study highlights Trusted Technology's role in providing South East Coast Ambulance service with a successful port control and data loss prevention solution. SECAmb sought to enhance data security and meet DSPT requirements whilst working alongside pre-existing security solutions.

Client Background

South East Coast Ambulance Service (SECAmb) SECAmb is one of the largest ambulance services in England, serving a population of approximately 5.8 million people across Kent, Surrey, Sussex, and parts of London. As a healthcare organization, SECAmb handles sensitive personal data regularly and has a legal obligation to protect patient confidentiality.

The Problem

SECAmb were facing challenges with the management and control of storage devices. They wanted to control all removable devices and enforce encryption across all endpoints used by staff that held or allowed access to personal data. In addition, SECAmb needed a solution that was easy to deploy and compatible with existing management and security products already being used.

The Requirement

Trusted Technology faced many challenges whilst strengthening data security at SECAmb…

I. **Controlling Ports and Managing Removable Device Usage**: The organisation lacked control over the use of removable devices such as USB drives. Removable devices can often be insecure and offer significant risks of data breaches to organisations. This an issue for all organisations but Healthcare organisations like SEACAmb who have access to particularly sensitive information.

II. **Endpoint Encryption**: SECAmb aimed to enforce encryption on all endpoints that held or allowed access to personal data to mitigate the risks associated with potential data theft or loss. For example, paramedics and other ambulance staff are provided with body worn camera's during their shifts. If the footage ever needed to be passed on to other authorities, then that data must be encrypted to preserve security and maintain the privacy of all those involved.

III. **DSPT Requirements**: Healthcare organisations like SEACAmb are held to standards when it comes to keeping their information systems secure. If they do not meet these standards, confidential data is deemed at risk. SEACAmb needed a solution that allowed them to implement device control whilst also meeting data security and protection toolkit requirements.

"Requirement 9.52 – Are all removable devices that hold or allow access to personal data, encrypted?" – DSPT Standards"

IV. **Compatibility and Ease of Deployment**: Perhaps most importantly, SECAmb needed a solution that seamlessly integrated with their existing management and security products, ensuring a smooth deployment process with minimal disruption to their operations.

The Solution

With our extensive experience of providing IT solutions in the Healthcare sector, Trusted Technology understood the specifications and solutions that SEACAmb required. By using this knowledge, alongside utilising interorganisational partnerships Trusted Technology was able to provide SEACAmb with Endpoint Protector.

Endpoint protector is an industry-leading solution provided by CoSoSys that ensures data-loss prevention, which is easy to manage, enabling granular access policies for users and devices to be deployed, enforcing device security.

Trusted Technology provided SECAmb with an innovative solution that met all their needs and provided complete control over their ports and removable storage devices. This solution was integrated seamlessly, providing SECAmb with the ability to enforce encryption to keep sensitive data secure, whilst complying with DSPT standards.

Outcome

- **Control:** Implementing granular polices and access restrictions, Trusted Technology's solution allows SEACAmb complete control over peripheral devices and storage.
- **Encryption:** Endpoint Protector was provided to our customer to integrate robust encryption capabilities, ensuring all data stored or accessed on those devices remains protected. This solution enforced encryption protocols to meet industry standards and compliance requirements, keeping personal data secure.
- **Integration:** Trusted Technology's fast, powerful and cross-platform solution with flexible deployment options was effortlessly integrated to compliment SECAmb's existing security products.

Testimonial

"SECAmb came to Trusted Technology Partnership with a very specific requirement that we needed to manage storage devices and keep data secure. Not only were Trusted Technology able to provide the perfect product to meet our needs but we could also deploy it alongside pre-existing security measures which minimised disruption in our organisation. With Trusted Technology's support we now have complete control over ports and can minimise data loss."

Stewart Edwards

IT Security Manager at SEACAmb