CWSI: Providing South Lakeland and Eden District Councils with CESG security compliance

South Lakeland and Eden District Councils required a new Mobile IT security platform to protect their mobile phones and tablets in accordance with CESG guidelines (now part of the NCSC).

The Solution

The councils issued an RFP and invited a shortlist of applicants to demonstrate their proposed solutions. CWSI were chosen based on their ability to successfully implement protection on device, application and network levels with all solution components being orchestrated through a single administrative console.

For a fully CESG compliant solution, CSWI integrated MobileIron, Wandera and Check Point Sandblast to protect all elements of the mobile device fleet, as well as VPN access to internal SharePoint resources and many other internally hosted web based applications for mobile users.

MobileIron

The MobileIron platform combines traditional mobile device management (MDM) capabilities with comprehensive security, mobile application management (MAM), and mobile content management (MCM) capabilities.

SANDBLAST

SandBlast Mobile uses malicious app detection to find known and unknown threats. Its dynamic threat response prevents compromised devices from accessing the organization's network, while enabling it to set adaptive policy controls.

wandera

Wandera provides a Mobile Data Gateway to control and analyse mobile traffic, with the added benefit of expense control. Not only does Wandera prevent users from accessing inappropriate sites, but also checks that no sensitive data is being leaked by apps.

The solutions provided by CWSI have enabled the use of both tablets and phones in a way that was not previously possible.

The configuration has allowed us to give secure access to corporate data and systems on a device of choice, giving our staff and district councillors much more flexibility in how they operate.

Ben Wright
IT Services Manager and Senior Supplier for Digital Innovation
Eden and South Lakeland District Councils

"A clear separation between personal and business data can be created."

Intuitive, secure and reliable solutions

MobileIron's MDM capabilities enable IT administrators to secure and manage mobile devices across multiple operating systems, providing secure corporate email, automatic device configuration, certificate based security, and selective wipe of enterprise data.

IT administrators can apply granular controls based on a variety of parameters such as device type, device ownership and employee role.

This reduces the councils' burden of complying with a wide range of privacy laws as well as alleviating end-user privacy concerns.

The solution implemented by CWSI involved integrating the MobileIron MDM with SandBlast Mobile so that riskbased policy adjustments can be made on compromised devices, such as blocking access to a secure container

Administrators can manage the lifecycle of each device and its applications, from registration to retirement. It also has a security and management engine that enables IT to set policies for mobile devices, applications and content.

MobileIron integrates with the councils' backend enterprise IT platforms such as Active Directory and enables access to applications within a "secure container" which is password protected and encrypted.

Lastly, the councils now no longer have to worry about inappropriate websites being accessed or sensitive data being leaked thanks to Wandera, which can be effortlessly deployed from the MobileIron console. Wandera further secures the councils' device fleets through its leading web gateway for mobile architecture.

CWSI's mobile project has helped SLDC/Eden in many ways:

► Provided secured access to company applications from anywhere.
► Complied with CESG guidelines around device and data management and protection.
► Devices are used to access various Internet-based services, both for official and limited personal use.
► Protection against lost/stolen devices through encryption and remote wiping.
► Devices connect to a range of trusted networks to access official information.
► 3rd party networks are verified as secure whenever a device connects and all data in transit is protected.
► Devices can be de-provisioned when the device no longer needs access to official information, and all sensitive information is automatically removed.

Benefits:

► Risk reduction for the councils with encrypted secure devices that can be wiped remotely.
► Productivity is enhanced with instant access permitted on any authorised device, anywhere.
► Phones and tablets are protected at device, application and network levels, with security insights and automated playbooks for various scenarios.

Key Benefits

Mobile Devices secure – encryption, VPN

Detection and protection against network and SMS phishing attacks

Restrictions on accessing inappropriate content and cost control

Remote access to SharePoint resources and Skype

App risk evaluation

Why CWSI?

Our team at CWSI are unrivaled in their depth of knowledge and technical expertise to create tailored solutions to clients' requirements.

We provide MDM support as well as professional services and solution architecture, working across all industry sectors for many of Ireland and the UK's most respected organisations. Our solutions are leading edge and we stand by the quality of the work we deliver and our operational management.

"Mobility is at the core of everything we do"