SECTOR: RECRUITMENT / CASE STUDY

In2Consult + Trustd MTD

IN2 CONSULT

SECTOR:

Recruitment

MOBILITY SETUP:

BYOD

DEVICES:

iOS

KEY RESULTS:

Protection of employees' mobile phones against phishing and compromised WiFi.

Compliance with regulations in safeguarding confidential PII data

traced

SECURING BUSINESS DATA ON STAFF MOBILE DEVICES

As a recruitment company specialising in the IT and Financial Services sectors, IN2 Consult handles PII (personally identifiable information) on their clients and candidates, and securing this data is of the utmost importance.

As IN2 Consult's employees regularly work from home our the move between meetings, ensuring that their mobile phones were secure was an increasing concern.

With access to the company's CRM and emails on their devices, a data breach would put the company at risk of regulatory fines and reputational damage.

With the increasing reliance on mobile devices within the company, IN2 Consult were looking for a security solution that protected the data on those devices, but that was affordable for their growing business.

"We looked at several mobile cybersecurity vendors, but it became obvious that they didn't offer the WiFi or web protection we needed, and were still more than twice the cost of Traced's MTD."

LUKE SEAMAN, Managing Director, IN2 Consult

PROTECTION FROM PHISHING AND ROGUE WIFI

The web and WiFi protection offered in the Trustd iOS app were critical features for In2Consult, who need to protect staff against phishing and compromised WiFi networks while they're out and about and accessing sensitive business and client data on mobile devices.

REGULATORY COMPLIANCE

The Trustd Mobile Threat Defence console provides visibility the protection status of employee devices, as well as high risk events on those devices, so staff can take steps to educate users about potential threats.