Mobile Security for Recruitment

Protecting client data and employee privacy

trustd

The challenge for recruiters

We built Trustd for businesses like yours.

Recruiters carry a treasure trove of confidential data around on their mobile phones and tablets - from private candidate and client information, to CRM and payroll credentials. This makes the recruitment sector one of the hottest targets for phishing attacks and data theft by malware, and it makes their phones the front line in the battle against criminal hackers.

A data breach, whether accidental or via cyberattack, can put your employees, your clients and candidates at significant risk, and can result in heavy GDPR fines and long-lasting reputational damage.

Trustd protects employees against phishing attacks and exploitative, web-based threats; malicious apps on Android, while WiFi protection is designed to protect employees against data loss and theft whilst working remotely. It also checks for device vulnerabilities from out of date patching, lack of passcodes, and device rooting.

"We looked at several mobile security vendors but they didn't provide the WiFi or web protection we needed and was still more than twice the cost."

LUKE SEAMAN

Managing Director, IN2 Consult
Recruitment Consultants

Security The free Trustd app is designed to protect employees' personal and business information from phishing, compromised WiFi and device vulnerabilities on iOS and Android. The Android app also detects malicious apps and permissions abuse, which can be abused to steal credentials and plant malware.

Privacy Trustd MTD is ideal for privacy-conscious recruiters concerned about GDPR compliance. Unlike some mobile security solutions, the Trustd app doesn't share any personal information about users, their browsing behaviour, or their devices with the console, other than their email address.

Compliance Trustd reduces the risk of data breaches and associated legal, reputational and financial costs, supporting GDPR compliance. It supports your Zero-Trust mobile strategy by restricting access to company data from untrusted devices, whether they're managed by an EMM such as Microsoft Intune or unmanaged.

Security, privacy and data protection

Company-owned devices
(used by employees, managed by you)

Staff-owned devices
(BYOD, accessing business data)

Enrol both company-owned and BYOD mobile devices in **Trustd MTD** to protect them against malware, spyware, compromised WiFi networks, OS vulnerabilities and phishing attempts.

View the security status of your entire organisation's mobile devices at a glance, while maintaining user privacy.

- Receive alerts when your device is connected to a compromised or insecure Wi-Fi network.
- Monitor your device health and enable Zero Trust security and conditional access.
- Ensure user devices and corporate data are protected against phishing and malicious websites.
- Gain granular control over access to the administrative cloud-based console.
- Defend against modern Android malware, including spyware and Trojans.

What does Trustd MTD protect against?

Administrative dashboard

- High-level view ensures user privacy
- Set up Zero-Trust access policies
- See which devices are enrolled and protected
- Identify threats and remediate straight away
- Deploy quickly via MDM, bulk user upload or email

On-device security

App threats (Android)

- Malware apps
- Known and unknown threats
- Screen recording
- Leaky apps
- Camera/Microphone access
- App permission abuse

Network threats (iOS & Android)

- Man-in-the-Middle attacks
- Phishing
- Malicious scripts
- Malicious proxies
- Unsecured WiFi
- Weak WiFi security

Device threats (iOS & Android)

- OS exploits
- Vulnerable configuration

Set up a free trial today. Find out more at traced.app/trustd-mtd

traced