Enhance SOTI MobiControl with Trustd MTD

Employees' smartphones and tablets are a lucrative target for cyberattackers, exposing your organisation to the risk of a data breach.

While **SOTI MobiControl** provides excellent management and control for devices, only layering Mobile Threat Defence on top provides the threat detection and remediation capabilities you need to keep your organisation safe.

Trustd MTD is designed to work alongside SOTI to protect both personal and corporate-owned devices while protecting employee privacy, and reducing administrative burden with full deployment and protection with one-touch on iOS and zero-touch on Android.

Here are 3 key reasons to add Trustd to your mobility stack:

1

Mobile phishing

Phishing is often the first step in the ransomware chain of attack, and despite regular phishing training, employees are always vulnerable to increasingly sophisticated phishing scams. Trustd's AI-powered phishing detection engine protects against all forms of malicious content from apps and websites to guard against data breaches from phishing.

2

Man-in-the-Middle WiFi attacks

Employees connecting to public WiFi networks are at risk from Man-in-the-Middle attacks, whereby a threat actor intercepts traffic to and from the device. This eavesdropping often leads to credential or identity theft that can result in a breach of your entire network.

3

AI-powered malware protection

More effective than static malware detection, Trustd catches more never-seen-before threats because our threat detection is powered by AI. By identifying the common characteristics of Android malware, Trustd detects new and existing threats straight away, alerting the device user and administrator before they can do any damage.

traced

Mobile security, employee privacy