

# TRACED CONTROL MOBILE THREAT DEFENCE

- ✓ Stop threats
- ✓ Protect employee privacy
- ✓ Stay compliant



## MANAGE MOBILE RISK WITHOUT INVADING EMPLOYEE PRIVACY

Traced Control is a ground-breaking Mobile Threat Defence platform that gives IT teams direct insight into the threats affecting employees' mobile devices. It combines the Traced app that protects Android and iOS devices and the cloud-based dashboard that provides immediate visibility and analysis of mobile-borne threats. You can deploy Traced as a standalone MTD, or integrate with an EMM such as Microsoft Intune.

Every personal and business-owned mobile device is a gateway to sensitive business data. Mobile-borne threats rose 1,400% between 2016 and 2020 and with mobile phones and tablets now used for a mix of personal and business activity, they are a lucrative and easy target for attackers. Traced's privacy-friendly, lightweight security app for iOS and Android blocks mobile threats before they can harm your business.

**User-friendly mobile security** for iOS and Android phones and tablets to alert admins and guide users to remediation.

**Phishing protection** ensures that users, devices and data are protected against mobile phishing and malicious content.

**Device update alerts** identify vulnerable devices, while the Traced app reminds and guides users to patch their OS.

**WiFi protection** to alert users and admins to a compromised WiFi network and active Man-in-the-Middle attacks.

**Device health monitoring** supports Zero Trust conditional access and ensures security policy-compliance.

**Unique AI-powered protection** against malware and phishing that outperforms other vendors' out-dated detection methods.

**Deep Learning malware detection** protects you from modern Android malware, like spyware and Trojans.

**Employee privacy-first design** means higher adoption rate, happy employees, and you significantly reduce the risk of a data breach.

## WHAT THREATS DOES TRACED STOP?

### Network threats (Android & iOS)

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

### Device threats (Android & iOS)

- OS exploits
- Vulnerable configuration

### App threats (Android)

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

