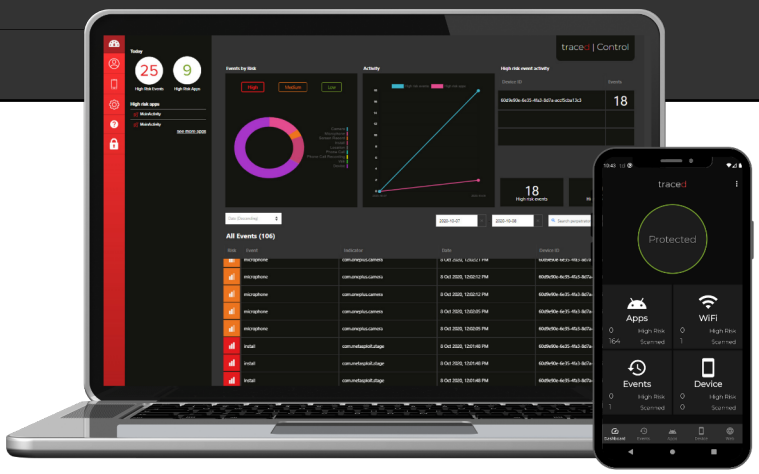
traced | Control

Mobile security, employee privacy



A robust, dynamic MTD with added app behaviour analysis and employee privacy baked in.

Every personal and business-owned mobile device is a gateway to sensitive business and personal data.

Threats on mobile devices can be at the device level, come via malicious apps, or from network connections - but all can be financially and reputationally devastating for your organisation. Traced Control is a groundbreaking MTD (Mobile Threat Defence) platform with additional app behaviour analysis and privacy that gives IT teams direct insight into the threats affecting employees' devices.

Control combines the Traced app that protects your employees' Android and iOS devices and cloud-based dashboard that provides immediate visibility and analysis of mobile-borne threats to your organisation's data.

They were built to work together to provide unparalleled protection against modern mobile threats like spyware, ransomware and phishing through vulnerable, compromised and malicious networks, apps, websites and software.

Key Benefits

Visibility of device security status

See which employees are protecting their devices, and which are undergoing security threats - all while maintaining your workforce's privacy. so you have complete reassurance you're protected against data loss and cyberattacks.

Dynamic protection against mobile threats

Real-time protection against viruses, spyware, phishing, surveillance and data loss , from both known and unknown malware using Deep Learning to enable you to adopt and secure your BYOD strategy.

Significant savings for security teams

Set up and enrollment is quick and simple, so you can start protecting devices immediately. Instant visibility of your mobile security status across your entire organisation means you can focus on other things.

What Threats Does Traced Stop?

Traced protects employee devices from application, network and device-based threats

Traced Control provides visibility of vulnerable mobile devices

App threats

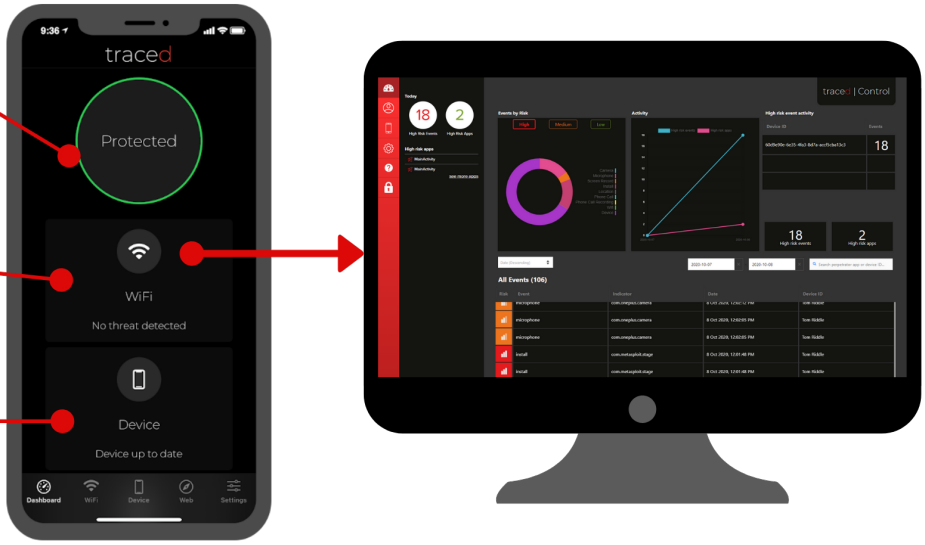
- Malware apps
- Known and unknown threats
- Screen recording
- Leaky apps
- Camera/Microphone access
- App permission abuse

Network threats

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

Device threats

- OS exploits
- Vulnerable configuration



Key Features

WiFi protection alerts both the device and in Control when a user connects to a compromised or insecure WiFi network.

Web protection ensures that users, devices and corporate data are protected against phishing attacks and malicious websites.

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

Deep Learning mobile malware protection protects you from modern Android malware, such as spyware and Trojans like Cerberus, Anubis and Joker.

Device health monitoring enables Zero Trust security and conditional access through the Control dashboard or the REST API.

Dynamic app behaviour monitoring (Android) detects indicators of attack, such as mobile app permission abuse, in real time.

Role-Based Access Control (RBAC) gives you granular control over access to the administrative cloud-based console.

Personal Privacy Mode reassures employees that you cannot see any personal information from their device, encouraging full adoption.

"One out of three enterprise attacks involves a mobile device... [and] those who invested in mobile security reported less than half of the breaches"
Verizon Mobile Security Index 2019