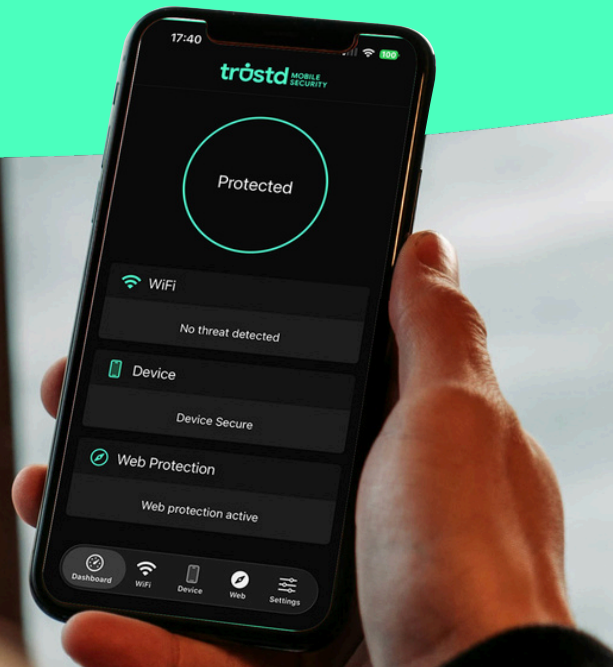


# Mobile Threat Defence from Trustd Mobile



STOP THREATS  PROTECT EMPLOYEE PRIVACY  STAY COMPLIANT

## Manage mobile risk without invading employee privacy

Trustd Mobile Threat Defence prevents costly breaches by managing the risks of mobile cyber threats and continuously ensures employees' mobile devices' compliance with organisational policies. It combines the Trustd Mobile Security app, that protects Android, iPadOS, iOS and Chrome OS devices, and the cloud-based dashboard that provides immediate visibility of mobile-borne threats, discovers Shadow AI and integrates with your existing security stack.

Mobile threats are on the rise, with 73% of UK organisations experiencing a mobile-related breach in the past year and 85% saying improving mobile device security is a critical or high priority for the year ahead. As mobile phones and tablets are now used for a mix of personal and business activity, they are a lucrative and easy target for attackers. At the same time, the biggest concern for IT Security Leaders when implementing mobile threat defence is employee/user impact, making user-friendly protection essential.



### AI-powered protection

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

**Device health monitoring**, Zero-Trust conditional access and Shadow AI detection ensures security policy compliance and breach prevention.

**Standalone or layer on top of MDM** to plug crucial gaps in mobile threat detection, remediation and analysis.



### User-first experience

Simple, non-intrusive alerts and guided actions for employees, and at-a-glance, actionable reporting for admins.

**Privacy-first design** keeps employee activity private, leading to higher adoption, happy employees, and a significantly lower risk of a data breach.

**Zero-touch protection** for MDM-managed devices and quick protection for unmanaged devices.

## Mobile threats blocked by Trustd MTD

### Web threats

- Phishing
- Malicious websites
- Malicious scripts

### Network threats

- Man-in-the-middle attacks
- Unsecured networks
- Weak WiFi security

### App threats

- Malware apps
- Screen recording
- Shadow AI
- Spyware apps
- App permission abuse

### Device threats

- OS exploits
- Vulnerable configuration