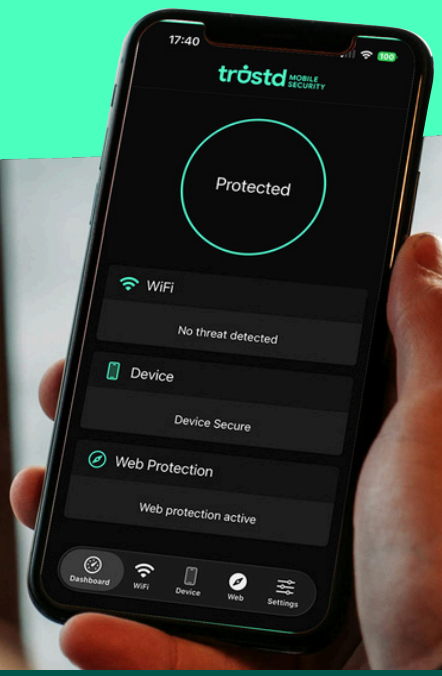
trustd
MOBILE THREAT DEFENCE

Trustd Mobile Threat Defence



STOPS MOBILE THREATS | PROTECT EMPLOYEE PRIVACY | KEEPS MOBILES COMPLIANT

Manage mobile risk without impacting users

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.

Security and compliance automation, Zero-Trust conditional access and Shadow AI detection ensures security policy compliance and breach prevention.

Standalone or integrates with MDM to plug crucial gaps in mobile threat detection, continuous compliance, remediation and analysis.

User-first experience

Protection without impacting users, Trustd MTD has a 4.7 star average user rating as it doesn't slow down mobile working.

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