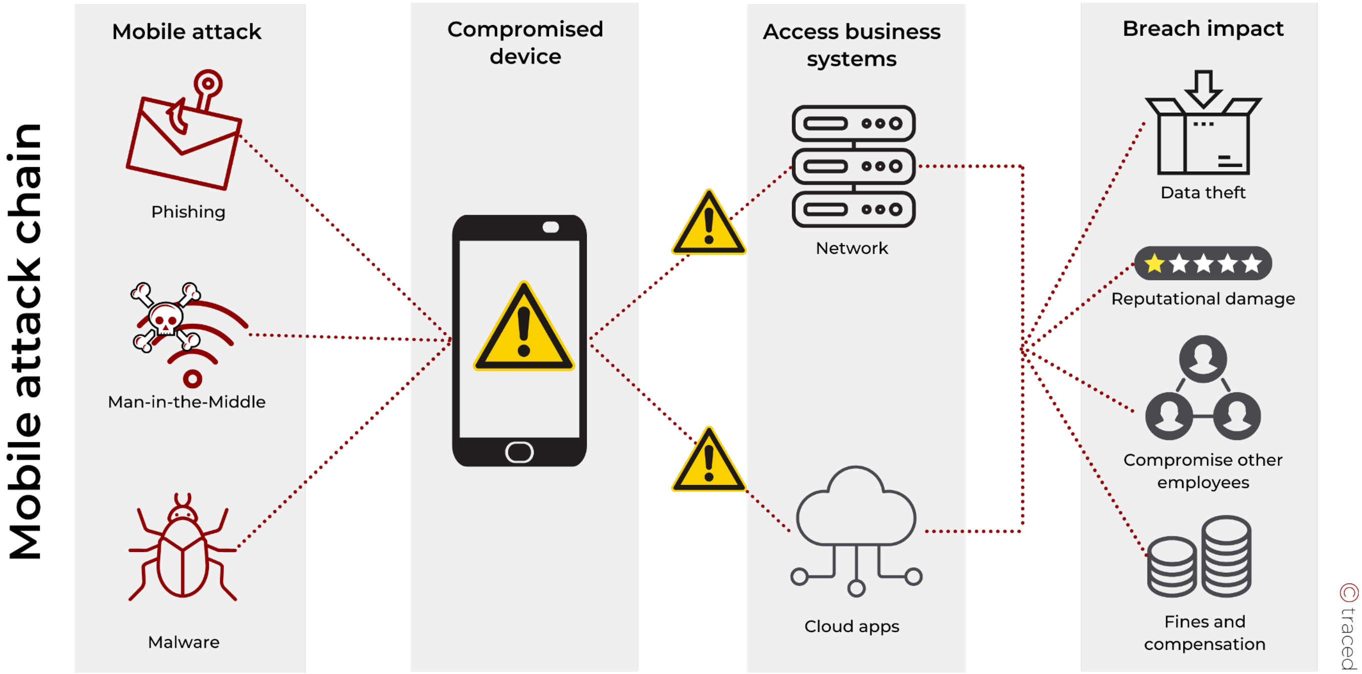
Trustd MTD Sales Deck

Trustd Value Proposition

Trustd is an AI-driven Mobile Threat Defence solution to secure smartphones and tablets from a range of mobile-borne threats, including mobile phishing, compromised WiFi and malicious apps and websites. This will reduce your cyber-threat surface and mitigate the risk of a costly data breach.

The Chain of Attack



What is the Risk?

According to IBM the **average cost of a data breach in 2021 was $3.6 million** (includes ransoms, down time, fines and reputational damage). When adequate security was implemented this was lowered to $2.4 million but ***when security was seriously lacking this increased to $6 million***. Protecting mobile endpoints has become key to prevent and lower the risk of data breaches, as mobile threats like ***malware increased 500% between Feb and March of 2022*** (Proofpoint), and ***mobile phishing rose 700% in 2020*** alone (Symantec).

Scenario:

- Customer is subject to a data breach and has not secured all endpoints adequately.
- This increases the threat of a ransomware attack and potentially ransom payment.
- Increased incident exposure/time to remediate data breach increases costs.
- Regulatory bodies may impose large fines due to inadequate security posture.
- Reputational damage may be incurred and may affect future earnings.

traced
AUTHORISED PARTNER

Why Trustd MTD?

Trustd MTD's privacy-friendly, lightweight security app for iOS and Android blocks mobile threats before they can harm your business. Trustd MTD solves the challenges of other mobile security solutions by combining AI, to catch more threats more quickly, with simple deployment and absolute employee privacy.

AI-powered protection

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

Device health monitoring supports Zero-Trust conditional access and ensures security policy compliance, blocking access to business data from untrusted or unsafe devices.

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.

Quick and easy set up with zero-touch deployment and one-touch enrollment for MDM-managed devices.

Sales Scenarios and Opportunities

Standalone – Organisations can sidestep resource-heavy MDM solutions and implement Trustd MTD as a low-touch option. This will secure their users and corporate data whilst proving compliance to auditors.

MDM Up Sell – MDM provides management and controls with limited security features. It does not secure against phishing, compromised WiFi and other mobile threats.

	MDM only	Trustd MTD	MTD + MDM
Protection against phishing	-	✓	✓
AI-powered malware protection	-	✓	✓
Cyber Essentials mobile compliance	-	✓	✓
Zero-Trust access to company data	-	✓	✓
Remote configuration of mobiles	✓	-	✓
Remote app management and installation	✓	-	✓

Endpoint Cross Sell – 61% of corporate data breaches result from credential theft (Verizon 2021). By not securing mobile devices you are leaving a huge part of the attack surface vulnerable to exploitation that could lead to broader attack. If you're buying an endpoint solution, secure ALL endpoints.

User Awareness Training – When selling user awareness training suggest organisation takes a layered approach by securing against mobile threats. Yes, ideally users wouldn't click on a link after training but realistically this hasn't stopped the problem yet and probably won't in the future. Layer up with MTD on mobiles.

BYOD and Zero Trust – BYOD offers great benefits for organisations. Financially it is very attractive with potential to save organisations up to $2,300 per device. However, it does represent a great security risk if not dealt with appropriately. The challenge is balancing corporate responsibility for data security with the user's right for privacy on their personal device. Traced offers a novel solution, balancing these requirements with either corporate or personal device enrolment, offering the same security but limiting PPI returned to employers.

What threats does Trustd MTD guard against?

Trustd MTD App

Application threats

- Malware
- Known and unknown threats
- Stalkerware
- Screen recording
- Leaky apps
- Camera/Microphone access

Network threats

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

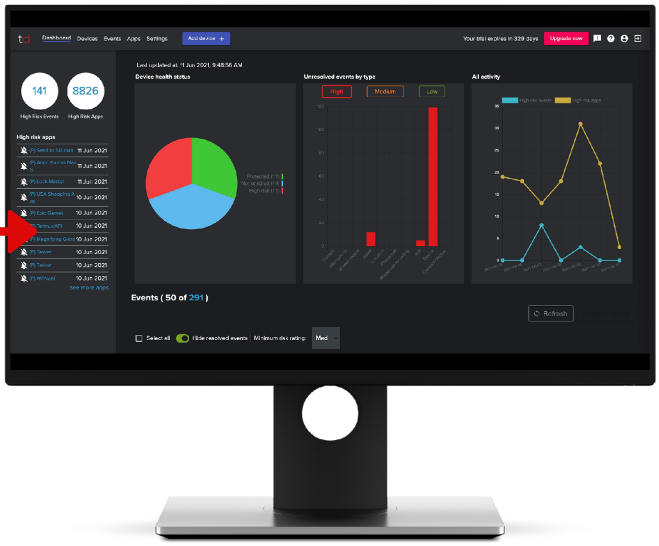
Device threats

- Vulnerability in OS
- System takeover

trustd
Protected
WiFi
No threat detected
Device
Device Up To Date

Trustd MTD Admin Console

- See which users and devices are at risk
- Set up policies and conditional access
- Download compliance reports
- One-touch device enrolment (zero-touch with MDM)



Common Objections

We haven't had any security issues from mobile devices	MDM and EMM provide management of devices. Only MTD provides threat detection, analysis and remediation so you are protecting the device and know the device is safe before it connects to business data.
	If not, how do you know they haven't been compromised?
	It is your responsibility to know, and Trustd can help you.
Mobile Threat Defence isn't a priority.	Do you have anti-malware on your computers? Mobile devices are handheld computers with access to corporate data and it is corporate responsibility to secure them.
We already have MDM or EMM - we don't need MTD	MDM and EMM provide management of devices. Only MTD provides threat detection, analysis and remediation so you are protecting the device and know the device is safe before it connects to business data.

Deal Registration

Send the following info to *ben@traced.app*

- Customer Name
- Customer Address
- Need
- Device Count
- Timescale