Mobile Threat Defence for **Accounting Firms**

Secure confidential information accessed from employees' phones and tablets.

trustd mtd

VALUABLE TARGETS FOR ATTACKERS

Accounting firms are a gateway to vast amounts of sensitive data, making your staff a highly attractive target to attackers.

In fact, PwC estimates that financial institutions are over 30% more likely to be targeted than other businesses, and smaller firms are seen as a soft target. Due to the volume of financial data you process and store, your company needs to take extra measures to secure devices that access that data.

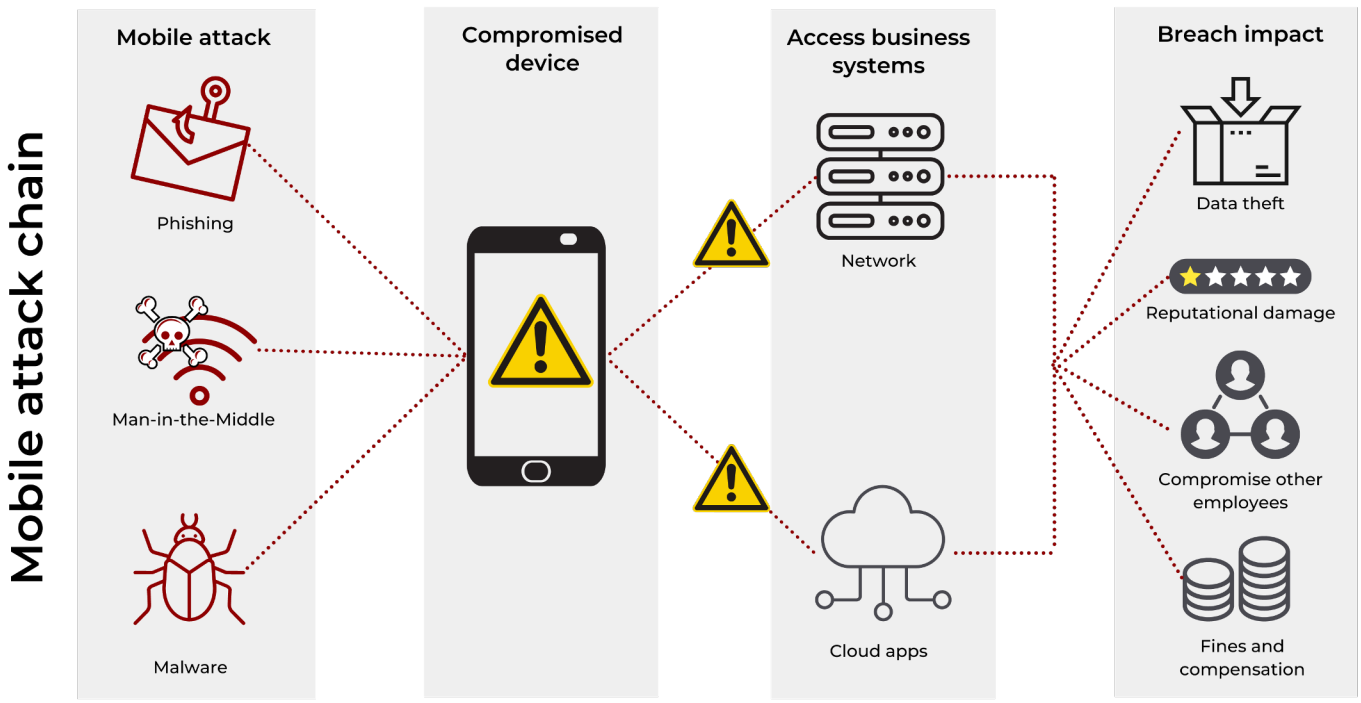
But balancing security with productivity is no easy task, particularly when employees also demand their own privacy. It's vital that you ensure regulatory compliance, and can demonstrate appropriate security measures when it comes to safeguarding personal and financial information on all devices.

45% of organizations have reported mobile-related breaches - that is twice as many as in 2021.[1]

VISIBILITY OF DEVICES

"With Trustd MTD on all of our devices, we know exactly who is protected and who isn't protected, and, more importantly, where the threats are coming from."

Matthew Bonfield
Executive Chairman, Huntswood



THE TOP 3 MOBILE THREATS TO ACCOUNTING FIRMS

Phishing attacks

Reports of smishing in the UK grew nearly 700% in the first six months of 2021 compared to the second half of 2020[2]. Accountants are particularly at risk from phishing because a successful attack can be so financially lucrative. From invoice fraud and purchase scams, to fake Linkedin job offers and parcel delivery SMS scams - your employees are under constant attack from phishing attacks via all devices. The aim of phishing is varied, and includes downloading malware, parting with credentials, transferring funds, or divulging personal information that can assist in social engineering attacks on other staff.

> ***95% of losses from cyberattacks result from human error, with each successful cyberattack on SMEs resulting in an average loss of £35,000.***

Hybrid working

86% of UK cybersecurity professionals said attacks increased due to employees working remotely.[3] Connecting to public WiFi exposes devices to Man-in-the-Middle attacks that harvest traffic to and from the devices. It leads to an increase use of personal devices that may not have the latest security patches or harbour malware.

Supply chain compromise

With our growing digital interconnectivity it opens up your organisation to malware and data breaches that originate from outside of your company. Clients, suppliers and third-party software can inadvertently compromise your data, introduce malware into your systems and leave you exposed to ransomware, reputational damage, and regulatory fines.

> ***A client's system was hacked and a fake email requesting a payment was sent to their accounting firm. The accountant complied as the request wasn't unusual, but the client held the accounting firm responsible.***

YOUR CHALLENGES

Full, frictionless employee adoption

You can't protect all devices if you don't know about them, so how do you balance the risk of personal devices accessing sensitive data with both employee privacy and the need for productivity?

Protect every device from evolving threats

You're particularly at risk from phishing and ransomware. Every device needs to be protected, including any personal phones and tablets that can access company-stored PII.

Comply with regulatory standards

You need to demonstrate appropriate security measures across your organisation, protecting every device.

WHAT THREATS DOES TRUSTD 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 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)

WHY TRUSTD MTD?

One-touch enrolment

Full deployment and protection with one-touch on iOS and zero-touch on Android makes it simple to get all devices set up.

Standalone or layer on MDM

Take your first mobile security step, or plug the gaps in your existing EMM/MDM solution with threat detection and remediation.

BYOD-friendly

Keep employee activity private, leading to higher adoption, happy employees, and a significantly lower risk of a data breach.

Your duty of confidentiality

Trustd MTD supports your Cyber Essentials application, and compliance with PCI-DSS and GDPR, and ACCA and ICAEW guidance.

Zero Trust access to data

Trustd can restrict access to your company's data from untrusted mobile devices, whether they're managed by MDM/MAM or unmanaged.

Mixed mobility environment

Save money on distributing corporate devices to all employees by adopting a BYOD policy, or easily manage a mix of both.

Sources
1 Data from Proofpoint's Cloudmark data of scams reported to 7726 from H2 2020 to H1 2021
2 Verizon, 2022 Mobile Security Index
3 Trend Micro, Q1 2020 Threat Report
4 WMWare, UK Security Insights Report 2021