

Securing BYOD: Plugging the Gaps in EMM

Personal devices expose your organisation to phishing, malware, and network threats that EMM can't prevent.

Mobile Threat Defence (MTD) fills these gaps, securing BYOD without compromising privacy.

Welcome to your new reality. Employees will always find ways to use their personal devices for work. It's more convenient, more productive, and sometimes, unavoidable. Whether it's responding to client emails on a personal phone, accessing company files from a tablet, or using WhatsApp to discuss work — **BYOD is happening, whether you officially allow it or not.**

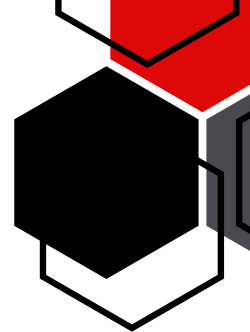
The challenge? These devices are outside your traditional security perimeters and are already exposing your organisation to new attack vectors.

In case you need a reminder, the most common BYOD security risks are:

- **Phishing attacks:** Traditional email security tools don't protect against SMS-based phishing (smishing) or malicious links opened in personal email accounts.
- **Malicious apps:** Employees may unknowingly install high-risk apps that request excessive permissions, record screens, or harvest credentials.
- **Unsecured networks:** Connecting to public Wi-Fi or compromised home networks increases the risk of man-in-the-middle (MITM) attacks.
- **Data leakage:** Even well-meaning employees might use unapproved apps or cloud services to store or share sensitive data, bypassing official security controls.

Despite these risks, many organisations lack visibility into **what threats their employees' personal devices are exposed to.** This is the security gap that needs to be addressed.

The business case for MTD in BYOD security.



1. Avoid Costly Data Breaches

In 2023, the average cost of a data breach reached **\$4.45 million**, with mobile devices becoming a **primary attack vector**. Without adequate protection, personal devices present a significant security risk.

82%
of phishing sites now
target mobile devices

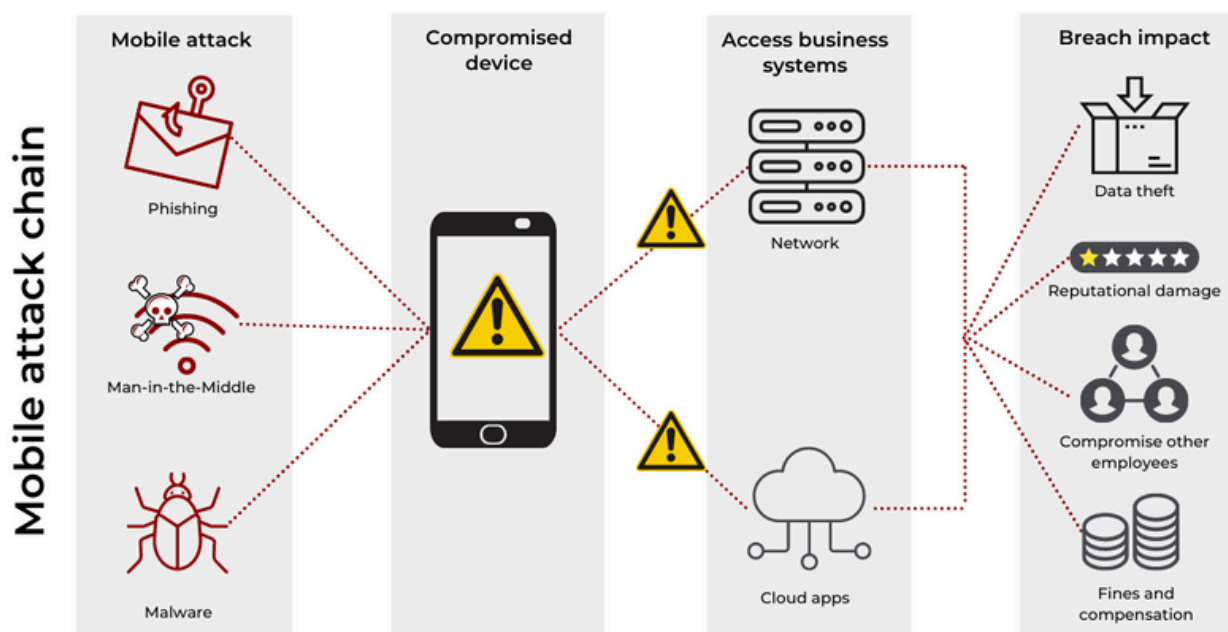
Zimperium 2024

2. Meet Regulatory Compliance

Compliance frameworks such as GDPR, FCA, and ISO 27001 increasingly require organisations to **demonstrate mobile security**, rather than just enforcing policies. Ensuring BYOD security is now a regulatory expectation. **Gartner** anticipates around 50% of regulated organisations to have MTD in 2025.

3. Address the Rising Threat Landscape

Cybercriminals actively target BYOD devices as the **weakest link** in corporate security. Without proactive protection, organisations risk becoming easy targets for **phishing, malware, and network attacks**.



Why **EMM alone** isn't enough.

Like many organisations, you may already use an EMM (e.g., Intune, Workspace ONE, MobileIron) or MAM solution to manage work apps on personal devices.

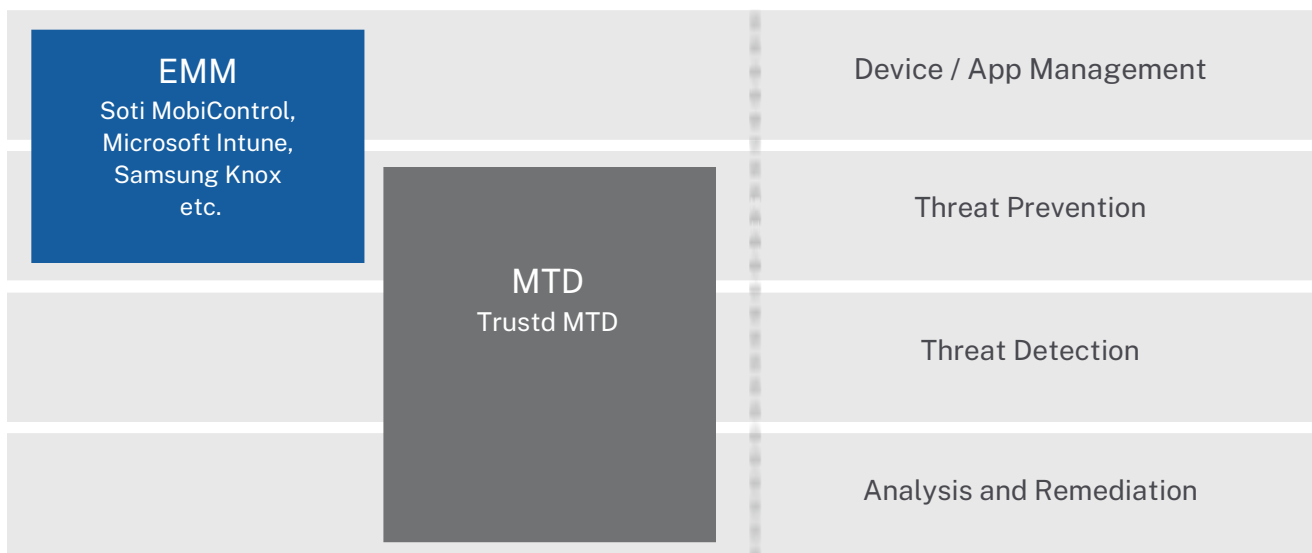
But EMM is not designed to detect and stop active threats.

Here's what EMM does well:

- ✓ Enforces security policies (e.g., requiring PINs, blocking certain apps)
- ✓ Controls access to corporate resources (e.g., ensuring only compliant devices can open work apps)
- ✓ Wipes corporate data if a device is lost or compromised

And here's what EMM doesn't do:

- ✗ Detect phishing attacks in personal email, SMS, or messaging apps
- ✗ Block malicious app installations or warn about risky app behaviour
- ✗ Secure network connections and protect against MITM attacks
- ✗ Provide real-time threat intelligence on emerging mobile threats



Which is why Mobile Threat Defense (MTD) is essential. Instead of replacing EMM, MTD complements it — **filling in the security gaps** that leave BYOD environments vulnerable.

How **MTD** secures BYOD.

Stops Phishing Attacks

Phishing scams now target **82% of mobile users**, often through credential-harvesting fake login pages.

✔ MTD detects and blocks phishing attempts, even when users access work content via personal email, messaging apps, or web browsers.

Detects and Blocks Malicious Apps

Mobile malware infections have doubled in the past year. Employees may install risky apps that request excessive permissions (e.g., camera and clipboard access, keylogging).

✔ MTD automatically flags apps with suspicious behaviour — before they can compromise data.

Secures Network Connections

Employees frequently connect to unsecured networks in cafes, airports, or hotels. Fake Wi-Fi networks can intercept sensitive information, even with VPNs enabled.

✔ MTD alerts users to risky network connections and protects against man-in-the-middle attacks.

Gives IT Teams Real-Time Visibility

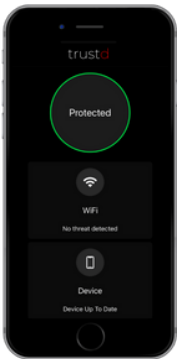
IT and security teams gain real-time insights into threats affecting BYOD devices — without invading user privacy.

✔ MTD dashboards show whether devices are at risk, allowing organisations to enforce conditional access policies based on real-time threats.



To achieve compliance and reduce risk, you need **employee buy-in** first.

Securing BYOD starts with employee trust. Once you overcome resistance, you can ensure **Cyber Essentials compliance**, **reduce the risk of breaches**, and **enforce security policies** without friction.



TOM'S *WHY NOW*

“A key reason for adopting MTD now comes from my own experience in IT. Employees were always asking, *“Why can’t I use my personal phone for work?”* In the past, the answer was simple — it was too difficult to secure, and privacy concerns made it a non-starter. But that’s no longer the case. Today, we have solutions that ensure compliance and security without compromising user privacy, making secure BYOD not just possible, but practical.”

Tom, [job title]

One of the biggest blockers to securing BYOD is employee resistance.

Many users worry that installing a security app on their personal phone means their employer will be able to see everything they do.

It’s a valid concern — but one that Trustd MTD has been specifically designed to address.

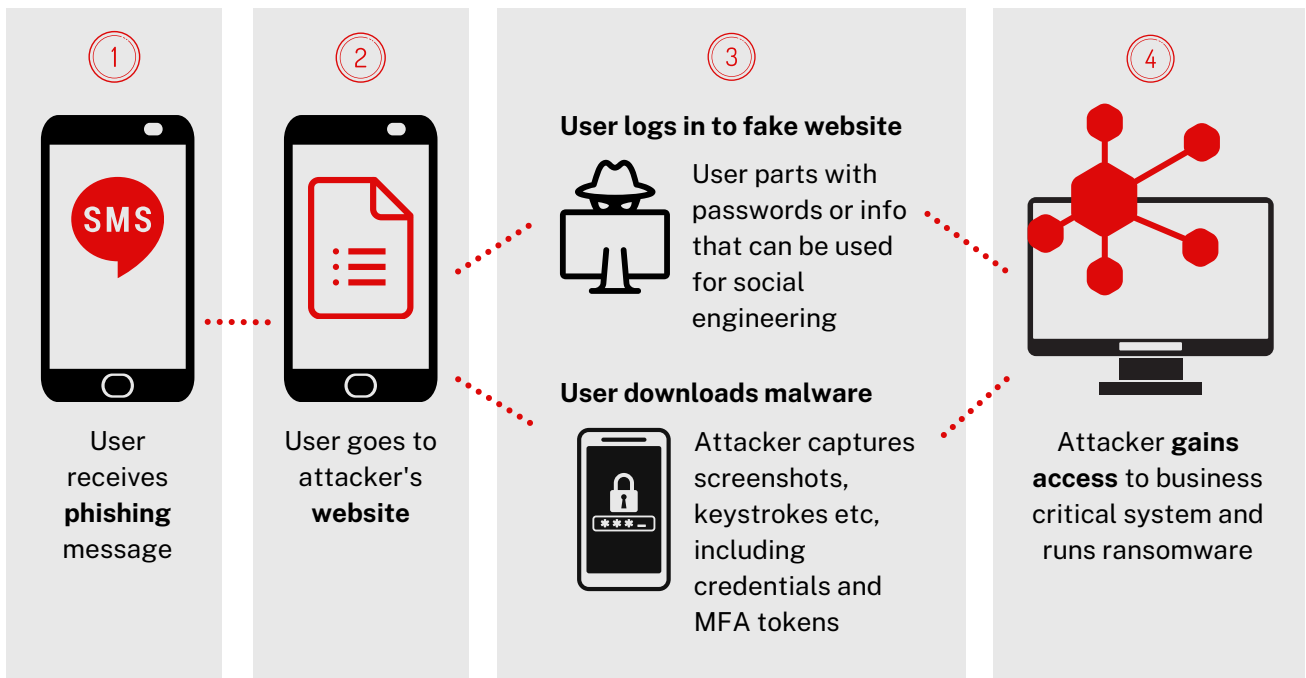
- ✓ **No access to personal messages, browsing history, contacts, or files**
- ✓ **No location tracking**
- ✓ **No ability to wipe personal data**
- ✓ **Only detects security threats — nothing else**

By respecting user privacy, organisations can achieve full employee adoption while maintaining strong security.

Something's **smishing**.

The Dangers of smishing (Mobile Phishing) via Personal Smartphones

QR codes, SMS, WhatsApp, and social media messages bypass any email protections you have in place. It needs an MTD to catch and block them at the point where the user tries to click through to the malicious website.



95%

of data breaches are due to human error

Mastercard

Why Your BYOD Users Are More Vulnerable to Attack

Mixing Work and Personal Use. Personal devices handle both work and private messages, making it easier for attackers to slip in phishing attempts. **Over 50%** of personal devices faced a mobile phishing attack each quarter in 2022.

Small Screens, Big Risks. Mobile users are **4 to 8 times** more likely to fall for phishing than desktop users because small screens hide full URLs and sender details, making scams harder to spot.

Unregulated Apps. Many mobile apps lack strict security checks, creating opportunities for phishing attacks. Mobile phishing incidents on personal devices have **risen over 20%** since 2021.

Trustd respects **employee privacy**

Your business remains protected against mobile threats without tracking employees. Web browsing, photos, videos, calls, contact, emails and messages stay completely private.

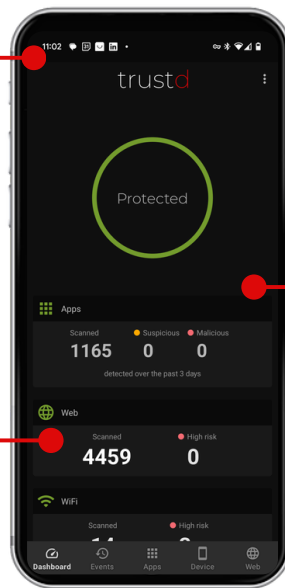
With the Trustd app on personal devices

Application threats

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

Device threats

- Vulnerability in OS
- System takeover
- Authorised unknown source



Network threats

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



In your Trustd MTD admin console

- See which devices are enrolled and protected
- Comply with data protection regulations
- High-level views ensure employee privacy
- Identify threats and remediate straight away
- Standalone MTD or integrate with your MDM



How to deploy MTD without disrupting users

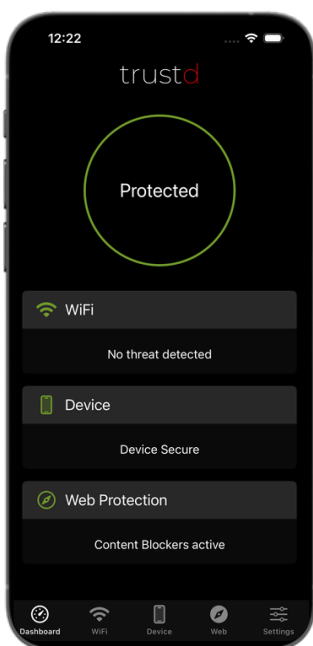
Rolling out MTD doesn't need to be complex. A well-planned deployment ensures seamless adoption and minimal impact on employees.

1. Integrate with existing EMM. Seamlessly deploy Trustd MTD alongside Microsoft Intune or any EMM with zero-touch installation. Gain full visibility into your BYOD, COPE, and hybrid setups while ensuring compliance and security.

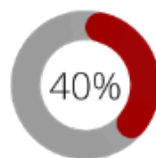
2 Define clear BYOD policies. Transparency is key to employee trust and adoption. Trustd ensures privacy-first security, helping UK businesses meet Cyber Essentials without intrusive monitoring. Clearly communicate what is (and isn't) monitored to build confidence.

3. Start with a pilot group. Roll out MTD gradually by testing with a small group before a full deployment. This approach helps fine-tune Zero-Trust policies, ensuring untrusted devices can't access Microsoft Cloud Apps or other sensitive data.

4. Automate compliance enforcement. Trustd enforces security policies dynamically, blocking threats like malware, phishing, rogue WiFi, and device exploits in real time - stopping known and unknown mobile threats before they cause harm.



What did CISOs say were their biggest security challenges?



employees using **personal devices** to access corporate data



employees using **unsecured WiFi** to access business resources

From an Ivanti survey of 400 CISOs across Europe.

Strengthening BYOD security without complexity



Blocks phishing and malicious websites



Detects Malware & Spyware apps



Supports Zero-Trust access to data



Reveals device vulnerabilities and outdated OS



Identifies compromised WiFi networks

BYOD is no longer an emerging trend - it's the **default way of working**.

But with mobile devices now the biggest cybersecurity blind spot, organisations can no longer rely on EMM alone.

Mobile Threat Defense closes the security gaps in BYOD environments - preventing phishing attacks, securing personal devices, and ensuring compliance without invading user privacy.

If your organisation is serious about mobile security, now is the time to take action.

Trustd is quick and simple to set up.

See for yourself with our 14-day, full-feature free trial. Enrol your own devices in 5 minutes and explore the console.

trustd mtd

**PARTNER
LOGO**

Partner contact details

traced

The creators of Trustd MTD



Coalition
Against
Stalkerware

Member of
Microsoft Intelligent
Security Association
Microsoft Security



National Cyber
Security Centre
For Startups
Alumni