A New Breed of Mobile Security for the Legal Sector

Secure every employee phone and tablet without compromising privacy.

trustd

YOU ARE A VALUABLE TARGET FOR CYBERCRIMINALS

You are a gateway to vast amounts of confidential client information and financial transactions, making your employees a highly attractive target to attackers.

But balancing security with productivity is no easy task, particularly when those employees also demand their privacy. It's vital that you ensure regulatory compliance across your entire organisation, and can demonstrate appropriate security measures when it comes to securing every device in your organisation.

Remote working and a merging of work and personal activity on the same device means IT teams are struggling to keep track of devices and deploy budget appropriately, while mobile-borne cyberattacks are increasing.

> *The need for everyone to remain cybercrime vigilant has never been higher. Law firms should make sure that they have effective cyber security policies in place, and, crucially, that everyone in the firm understands and follows these day-to-day.*
>
> Paul Philip, SRA Chief Executive[1]

WHERE DO MOBILE THREATS COME FROM?

- Phishing, malicious or spoof websites
- Malicious or compromised apps
- Misconfigured or unpatched devices
- Unsecured and intercepted WiFi networks

It makes sense that the cost of preventing cyberattacks is much lower than the cost - not to mention the reputational damage - of a successful attack. As well as being a regulatory requirement, it therefore makes good business sense to protect your own and your clients' data and money.

In the first half of 2020, nearly £2.5m of money held by law firms had been stolen by cybercriminals.[2]

One law firm lost £150,000 worth of billable hours after an attack.[3]

Sources 1 SRA, Greater than ever need for law firms to remain cybersecure, 2020
2 SRA, Information and Cybersecurity, Nov 2020
3 SRA, Cybercrime thematic review Press Release, 2 September 2020

MOBILE SECURITY FOR YOUR STRATEGY

BYOD (personal devices)

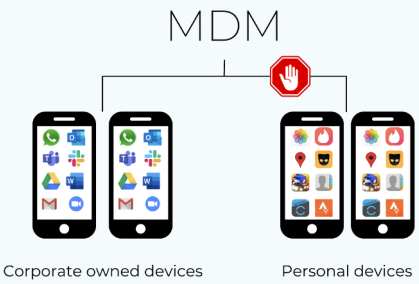
You need productivity, to allow your employees to use personal mobile devices for work, but you also need to protect the confidential and personal data stored on and accessed by those devices. The security program needs to be sustainable and every single device needs to be accounted for so you can be sure there are no weaknesses, and to remain compliant with your own policies and data security regulations.

COPE and COBO (company owned devices)

A common answer to the mobile security problem is for companies to purchase hardware for employees and install policy management and security software on the device. But inevitably these devices are used for a mix of personal and business, and employees frequently object to invasive device management. In response to this, they turn to their own devices and you're faced with a tri-fold issue of huge hardware costs, unpredictable bills, and still more holes in your security. Locking down your devices with MDM to "business only" use can reduce your mobile attack surface, but it doesn't address risks such as phishing and network threats.

MDM vs MTD

Quite simply, MDM has been around longer, but it doesn't provide detection and remediation of threats. Employees often object to intrusive MDM policies, making full adoption difficult.



Trustd MTD offers full protection and employee privacy built in

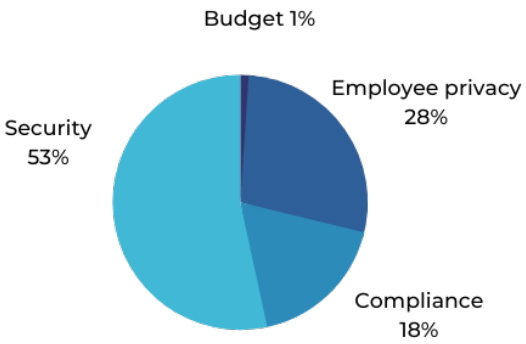
For full device coverage where privacy and complexity is a concern, you can use Trustd with your MDM for corporate-managed devices, and MTD only on BYOD. Your business remains protected against mobile threats without impacting employee privacy.

DYNAMIC, PRIVACY-FIRST DEFENCE

Unlike other mobile threat defence solutions, Trustd combines AI-powered mobile protection technologies, straightforward user guidance and accessible pricing to protect organisations against mobile malware, phishing and data theft on both BYOD and COPE/COBO devices.

It can support Cyber Essentials, compliance with SRA, PCI-DSS and GDPR guidelines, and enforce your duty of confidentiality. Enable your Zero-Trust mobile strategy by restricting access to company data from untrusted devices, whether they're managed by an MDM/MAM or unmanaged.

What concerns were your top blocker to implementing a BYOD strategy?



Traced poll of 191 IT Governance professionals May 2021

trustd mtd

A new MTD that manages the risk of your mobiles without invading your users' privacy.

- See which devices are enrolled and protected
- Comply with data protection regulations
- Standalone or use with an MDM/EMM
- Identify threats and remediate straight away
- Zero-touch deployment and one-touch enrolment
- Protect employee privacy