Mastering Mobile Security in Education

Securing devices while respecting student and employee privacy

trustd

The challenge for further education

The education sector faces a unique and difficult security challenge. Universities and colleges need to operate and defend enterprise-scale networks against sophisticated cyberattacks like ransomware, Trojans and phishing.

They need to do this with lean budgets, in a climate of tightening regulation, while onboarding and securing huge numbers of new users each year.

The days of only having to worry about issuing and securing standardised devices are gone. Educational establishments must find ways to protect data, detect threats and manage security policies on the operating systems and devices their users own, as well as the ones they're given.

> “34% of educators say that data loss is one of the biggest areas of concern for their school's IT security
>
> *YouGov, Geekileaks*

Privacy

Trustd MTD is well suited to both privacy-conscious students and organisations concerned about GDPR compliance. Unlike some solutions, the Trustd app doesn't share any personal information about app users, their browsing behaviour, or their devices with the Trustd console, other than the email address used to connect the two.

Security

Working together, the Trustd app and console provide a sophisticated, low cost MTD solution that can detect and analyse threats to your network, prevent data breaches and ensure compliance. The app protects iOS from phishing attacks, compromised WiFi and device vulnerabilities, while the Android app also detects app permission abuse.

Safety

The free Trustd app is designed to safeguard mobile device users by detecting novel mobile threats like stalkerware. By monitoring unauthorised access to screens, address books, cameras, microphones and more, the Trustd app can give students the tools they need to keep themselves safe as they learn and start to investigate the world.

Security, privacy and safeguarding with Trustd

Device ownership	Management status
Business-owned devices (used by staff and students).	Our **Mobile Threat Defence** solution, Trustd, can operate as standalone software, or integrate with an existing EMM like Microsoft Intune to allow conditional access to sensitive data based on the risk status of the device and ensure full adoption with zero-touch deployment. In either case, the security status of your entire organisation's mobile devices is presented at a glance, while maintaining your employees' privacy.
Staff-owned devices (Staff accessing private data on school systems)	
Student-owned devices (Not accessing private data on school systems)	No need to enrol in Trustd MTD, but recommend students download the **free Trustd app** to protect their devices from phishing, malware, stalkerware, spyware and rogue WiFi.

What does Trustd MTD protect against?

On-device security

App threats

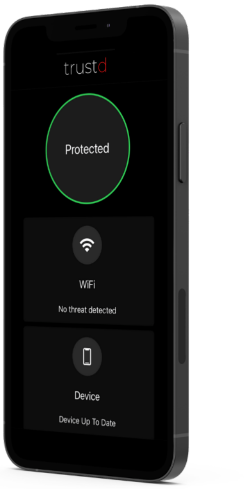
- Malware apps
- Known and unknown threats
- Screen recording
- Leaky apps
- Camera/Microphone access
- App permission abuse

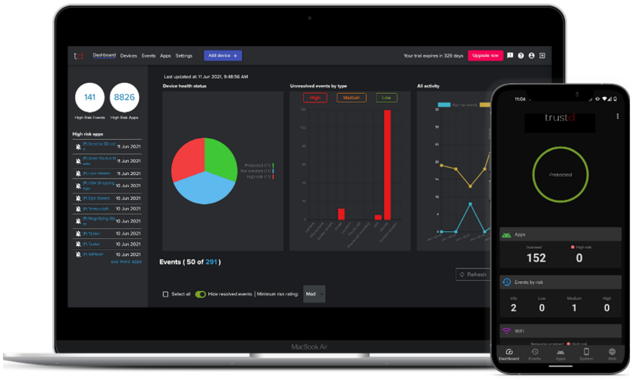
Network threats

- Man-in-the-Middle attacks
- Phishing
- Malicious scripts
- Malicious proxies
- Unsecured WiFi
- Weak WiFi security

Device threats

- OS exploits
- Vulnerable configuration





Administrative dashboard

Visibility. Security. Privacy.

- See which devices are enrolled and protected
- Set up Zero-Trust access policies
- High-level view ensures user privacy
- Identify threats and remediate straight away
- One-touch enrolment for devices in MDM

Set up a free trial today. Find out more at traced.app/trustd-mtd

traced