WHY INTEGRATE TRUSTD WITH MICROSOFT INTUNE?

✓ Support zero-trust ✓ Protect employee privacy ✓ Stay compliant

Microsoft Intune is an **Enterprise Mobility Management** solution, meaning it is designed specifically for managing mobile devices.

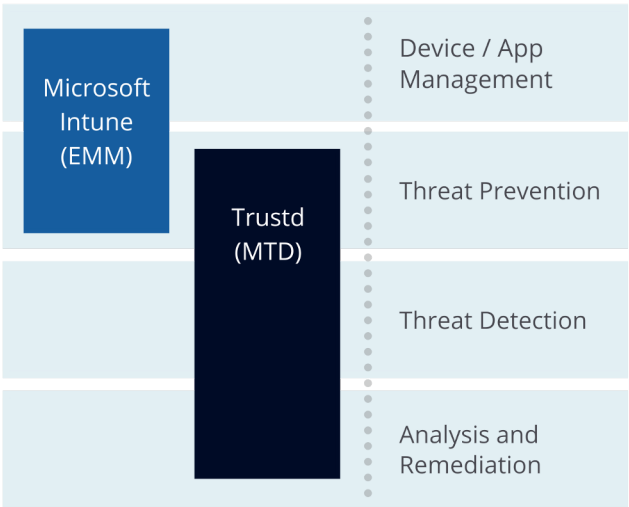
However, Microsoft Intune only deals with the management side of mobile devices, and can help to put a secure fence around sensitive data. It doesn't offer any means to detect or remediate mobile threats.

Intune doesn't provide any threat detection, analysis or remediation capabilities out of the box. It can't block phishing, stop malware, guide users to remove threats, identify permissions abuse on Android, or scan WiFi networks for attacks.

Organisations that have adopted some form of EMM or MDM have run into significant challenges, and that's led to the creation of MTD - to address those challenges and improve their mobile security.

Trustd MTD is a groundbreaking solution that works for Intune-managed devices *and* unmanaged devices (think BYOD). So you're ensuring every device that accesses business data is compliant with your security policies.

Trustd MTD supports zero-touch deployment through Intune and integrates with Azure Active Directory for zero-trust access to Microsoft Cloud App and deployment to unmanaged devices



Here are 3 key reasons to add trustd MTD to your mobility stack:

1 Mobile phishing

Often the first step in the ransomware chain of attack, increasingly sophisticated phishing scams remain the number 1 mobile threat to businesses. Trustd's protects against all forms of malicious content from websites and apps to guard against attacks.

2 Man-in-the-Middle

Employees connecting to public WiFi networks are at risk from Man-in-the-Middle attacks, where attackers intercept traffic to and from the device. This often leads to credential or identity theft that can result in a breach of your entire network.

3 Malware

More effective than signature-based malware detection, Trustd's AI-powered malware detection catches new and existing threats straight away, alerting the device user and admin before a costly data breach occurs.

© 2022 Traced Ltd. All rights reserved.