



Wandera Mobile Security

Cloud services and mobile devices can make or break your business. Use them well and employees will work flexibly with great efficiency. Use them irresponsibly and criminals will make off with your data.

How can you manage the risks? What can you do against threats like mobile-based malware, cryptojacking, man-in-the-middle attacks and leaky apps?

It's surprisingly easy to defend yourself. You can protect your devices, your network and your data with Wandera Mobile Security.

Keep reading to find out what it does and how it works.

Secure mobile endpoints

Prevent your mobile endpoints from being compromised. Protect your data against the broadest range of threats.

- Monitor endpoints for vulnerabilities, from escalated privileges to outdated operating systems.
- Perform continuous app risk assessments for advanced detection of malware and risky applications.
- Detect man-in-the-middle attacks and open a failsafe VPN (virtual private network) tunnel to ensure business continuity.

Hold back attacks as they happen

Stop attacks from reaching your mobile endpoints in the first place with our dynamic SAL (Secure Access Layer).

- Protect against known and zero-day phishing threats.
- Stop malicious downloads and connections to third-party app stores. Prevent data exfiltration and command-and-control attacks.
- Monitor for data leaks and prevent sensitive data loss. Safeguard user privacy with added encryption.

Assess the risks while people use apps

Apply a continuous risk assessment of mobile endpoints before enabling access. If an endpoint is compromised or at high risk, access can be denied.

- Wandera's risk assessments are constantly updated, even between active user sessions.
- MI:RIAM, their advanced threat intelligence engine, monitors the broadest range of cyber risk indicators.
- Their numerous UEM (unified endpoint management) and SIEM (security information and event management) integrations enable you to automatically apply risk-based access policies for your mobile endpoints.

What makes Wandera Mobile Security special?

Advanced machine learning

MI:RIAM is an advanced machine learning and threat intelligence engine. It identifies and eliminates the widest range of known and zero-day threats.

In-network protection

Real-time security in the network, blocking zero-day threats like phishing sites and malicious domains at the source.

Unrivalled integrations

With more UEM and SIEM partnerships than any other mobile security vendor, as well as Wandera's own device risk API (application programming interface), you can maximize your existing security investments and easily take advantage of mobile threat insights.

User privacy

Safeguard online privacy with encryption and protection against personal data phishing. Ensure regulatory compliance with advanced privacy features.

Real-time insights

Our intuitive management portal provides real-time insights on mobile risks as well as the ability to configure automated policy actions.

Any mobile device, any ownership model

Accommodates all devices and ownership models, whether BYOD ('bring your own device'), COPE ('corporately-owned personally-enabled') or COBO ('corporately-owned business-only'), letting you work with your preferred model in a way that is best for your business.

“Wandera helped build on our UEM deployment to improve our security posture across our mobile devices.”

Dave Aston

Associate Director of IT,
Berkshire Healthcare NHS
Foundation Trust



Ask us about security today

Our 3,000 security experts are trusted with keeping the military, emergency services and government safe. They can do the same for you.

Offices worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.
© British Telecommunications plc 2020. Registered office: 81 Newgate Street, London EC1A 7AJ. Registered in England No. 1800000.
September 2020

