

Full protection. Zero surveillance.

Most mobile security asks people to trade privacy for protection. Corrata doesn't. Every threat check runs on the phone itself, so personal data never has to leave it.



WHY IT MATTERS

Phones are personal. If security can see location, messages or browsing, staff push back, works councils block it and DPOs slow it down. **Privacy now decides whether mobile security gets deployed at all.**

Two ways to inspect a phone

THE COMMON APPROACH

Send it to the cloud

Traffic is tunnelled through a vendor VPN or cloud proxy to be checked. Activity leaves the phone, adds latency and lands on someone else's servers.

CORRATA

Check it on the phone

Deep packet inspection runs inside the Corrata agent. Threats are blocked in place. Only the security verdict reaches your console.

What that means in practice

The privacy questions users, DPOs and works councils ask first, answered plainly.

THE CONCERN	HOW CORRATA HANDLES IT
Location tracking	Never collected. No GPS, no location history, no movement data. Not a setting you switch off. It was never built in.
Files, photos and messages	Never scanned. Corrata inspects network traffic only. Nothing else stored on the device is touched.
Browsing history	Never touched. Corrata does not read, scan, store or analyse browsing history in any way. It is not something we use.
Traffic routing	No VPN backhaul and no cloud proxy. Traffic goes where the user sends it, once it has been checked on the phone.
Battery and connectivity	No round trip to a remote server. No added latency, no dropped connections, no extra battery drain.
Personal use on BYOD	Personal life stays personal. Your console sees risk and posture, not what someone does with their phone.

100%

of threat inspection happens on the device itself.

Zero

user traffic routed through Corrata infrastructure.

#1 of 20

Highest overall score in the GigaOm Radar for MTD 2025.

Exactly what we see. And what we don't.

Data minimisation by design, not by policy. If we never collect it, it can't be misused, breached or requested.

STAYS ON THE DEVICE

- Location and movement
- Messages, emails and texts
- Photos, files and documents
- Browsing history, never scanned or used
- Personal app data on BYOD and mixed-use phones

SHARED WITH YOUR CONSOLE

- Security events and verdicts
- Device risk and posture
- OS version and compliance status
- Risky app alerts

Why privacy wins the deal

Works councils say yes

No location, no content, no monitoring of staff. A clear story for employee representatives, without months of back and forth.

DPOs sign off faster

Minimal data leaves the device, so the DPIA is shorter, the legal basis is simpler and GDPR obligations are easier to meet.

BYOD becomes possible

Staff install the app because it can't see their personal life. Higher enrolment, fewer opt-outs, real coverage.

Users don't notice it

Fast, quiet and light on battery. Nothing to see until it blocks an attack. No helpdesk tickets about slow phones.

Five privacy questions worth asking any MTD vendor

We are happy to answer every one of these in writing.

1. Is traffic inspected on the device, or routed through your VPN or cloud?
2. Do you collect location data? Can it be removed entirely, not just hidden?
3. Does your agent access files, photos or message content?
4. Exactly what data leaves the device? Can we see the full inventory?
5. Where is that data hosted, and who can access it?

EU

Data residency as standard

ISO 27001

Certified platform and operations

GDPR

Privacy by design, Dublin HQ

MISA

Microsoft Intelligent Security Association

Security without surveillance.

Stronger protection than the cloud approach, with none of the privacy trade-offs.

corrata

CORRATA.COM