Next-generation, On-device Mobile Security

Mobile devices are now the dominant productivity platform in any organization with more than 80% of the daily work performed on a mobile device. These devices have access to the same information and applications that a traditional endpoint does but without the same security controls.

Enterprise IT organizations are under pressure to deliver a robust mobile experience to employees. In order to realize these goals with mobility initiatives there is a need for robust security against the ever-increasing threats facing mobile devices.

Secure your Mobile device investment

BT has harnessed the capability from Zimperium for Mobile Threat Defence (MTD) on iOS and Android deployed devices to provide a comprehensive mobile security solution that protects against both known and unknown mobile network, application, device OS and phishing threats.

Zimperium's MTD has been developed with Microsoft as an integrated solution with Microsoft's Enterprise Mobility + Security (EMS) providing the only Azure native solution:

Free Mobile Risk Assessment

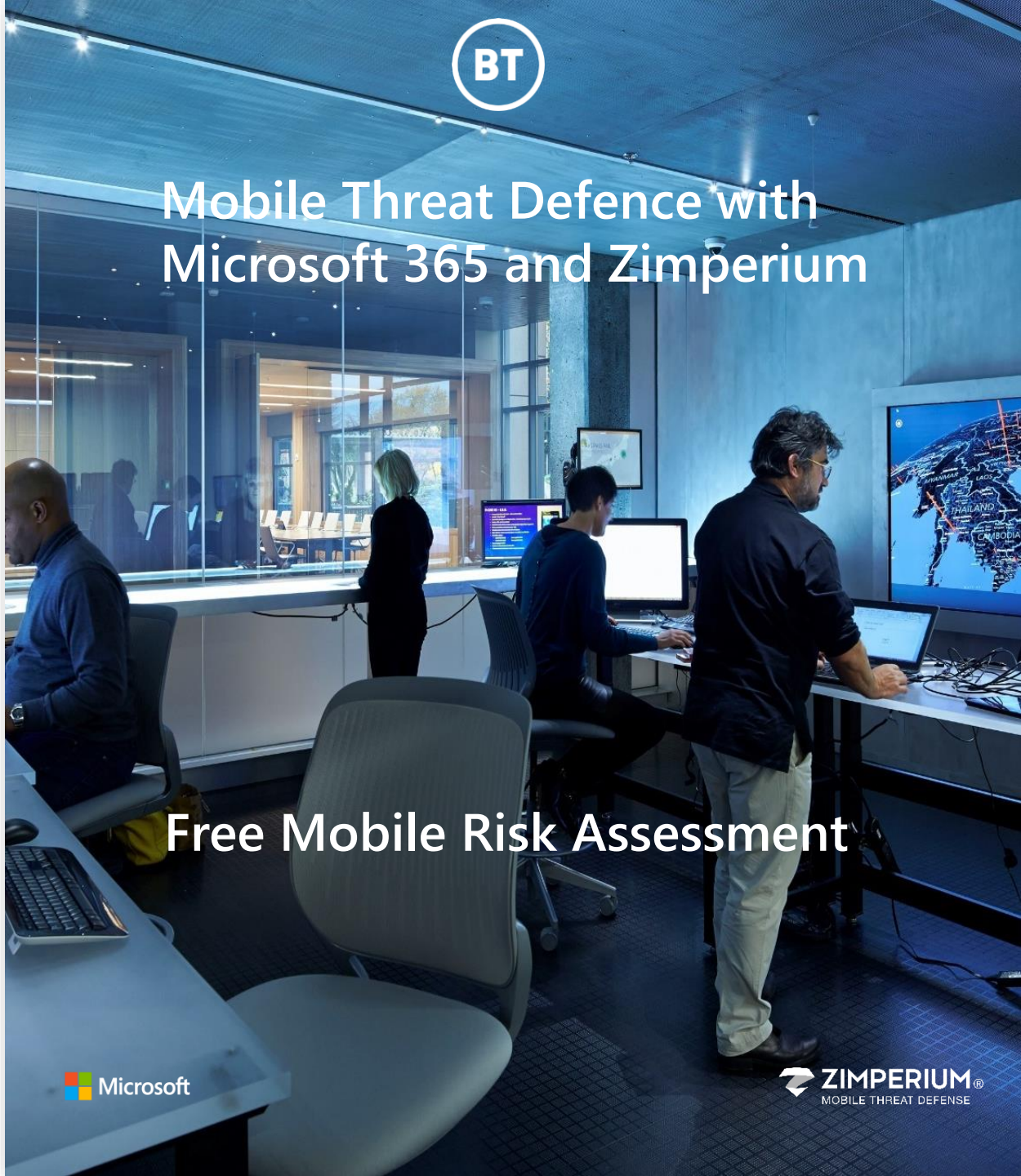
For organisations who are unsure about the the need for Mobile Threat Defense or who wish to understand what threats exist on the iOS & Android devices connecting to their network, BT offer a Mobile Risk Assessment.

The Risk Assessment involves using your MDM to push the Zimperium MTD zIPS app to a cross section of your mobile devices. The MTD app will then run in 'listening mode' only so as not to alert the end user and send anonymised threat data back to your own secure management console.

After 3-4 weeks you will receive a report of all mobile threats found on your mobile devices.

The Risk Assessment Report will detail the following broken down by iOS & Android:

1. Number of compromised devices:
   - devices with HW & SW vulnerabilities
   - devices with critical risks
   - devices that should have OS updated
2. Devices running risky apps
   - apps with high privacy & security scores
   - side-loaded apps detected
   - unmanaged profiles installed
3. Devices exposed to rogue or risky networks
4. Devices experiencing Phishing attacks



Mobile Threat Defence with Microsoft EMS and Zimperium zIPS

"Mobile devices were the biggest hole in our security."

A large regional power utility serving more than 13 million customers over 50,000 square miles currently enables over 10,000 mobile workers. The security team realized the information on the mobile devices contained critical data on the nation's infrastructure and electrical grid diagrams.

What you will get

Mobile Risk Assessment (RA)

Phone Call

Pre-engagement Call
- Engagement walk-through
- Expectations
- Complete Mobile RA questionnaire
- Book RA meetings

1st Meeting

RA Overview 1h
- Overview of mobile risks
- What data will RA collect
- RA Tech prerequisite's
- Agree & document RA scope & RA users
- Send RA comms to users

2nd Meeting

RA Kick Off meeting 1.30h
- Configure Groups for up to
- 1K Devices (iOS & Android)
- Configure Policies
- zConsole Integration with MDM
- Enroll RA user's devices

Week 1

RA Data Collection
- Check data being collected for all RA Users & Policies are correct

Week 2

RA Data Collection
- Optional meeting to show what threat data found so far

Week 3

RA Data Collection
- Optional meeting to show what threat data found so far

Week 4

RA Report Creation
- Threats collected during the RA period are compiled into a report and delivered to the customer

3rd Meeting

Threat Results Presentation 1.30h
- Discuss RA findings and real-world implications with Mobile Security experts
- Optional decommissioning

Once RA is complete BT technical experts will be able advise on most appropriate mobile security strategy and move to MTD POC or Pilot if appropriate.

Microsoft

Next steps: For more information about how to Get Modern, contact your Account Manager or Sales Specialist.

BT