



Mobile Threat Defence (MTD)

with M365 and Zimperium

Andrew Jones: BT Cloud Solutions Practice
Microsoft Technical Architect (Modern Desktop team)



The drive for partnership

Zimperium is a Microsoft Partner!

- IP Co-Sell (IPCS) status
- Enable Adoption & Usage of Microsoft workloads (e.g. Teams) on Mobile
 - 60% of all endpoints are now mobile devices (iOS; Android & ChromeOS)
- Are part of the Microsoft “Better Together” partner campaign
 - Mobile Apps are NOT at all like on-prem or web apps – we complement Defender
 - Together providing the most complete end to end solution.
- Zimperium are the only MTD Partner that runs natively on Azure - the others run on AWS
- Zimperium are a MISA Partner (Microsoft Intelligent Security Association)
 - Integrations into Defender; Sentinel and Intune/MEM

Zimperium supports Industry Priority Scenarios via strong Business Value

- Productivity - If the mobile device is secure Microsoft Workloads will be adopted faster
- Secure Employee; Customer; Patient and IP/Research data accessed on mobile
- Protect Factory Line and purpose-built devices to lower operational risk
- Secure the Supply Chain – we can protect Apps like Blue Yonder and SAP on mobile



Why Zimperium for MTD











BT Services

 **Microsoft**
Azure Services

 **Microsoft**
Productivity and Collaboration

 **Microsoft**
Modern Desktop services



	EPP/EDR	MTD
 CROWDSTRIKE		
 Microsoft		
 Microsoft +  ZIMPERIUM.		



Product Comparison

			Defender for Endpoint	Zimperium	MSFT + Z	CrowdStrike
Traditional Endpoints - Windows, Linux and MacOS	EPP/EDR	Threat & Vulnerability Management	✓		✓	✓
		Attack surface reduction	✓		✓	✓
		Endpoint detection and response	✓		✓	✓
		Threat Hunting	✓		✓	✓
		Automated investigation and remediation	✓		✓	✓
		Microsoft Secure Score for Devices	✓		✓	✓
Mobile Endpoints - iOS; Android; ChromeOS	Phishing	On-Device Mobile phishing detection		✓	✓	⊗
		Cloud based Mobile phishing detection	✓*	✓	✓	✓
		KNOWN Phishing URLs	✓*	✓	✓	✓
		UNKNOWN Phishing URLs (zero-day)		✓	✓	⊗
	Applications	Sideloaded App Detection		✓	✓	✓
		Enterprise App compliance and detection Policies		✓	✓	⊗
		KNOWN Malware	✓**	✓	✓	✓**
		UNKNOWN Malware (zero-day)		✓	✓	✓
	Network	Offline Malware detection		✓	✓	⊗
		Provide detailed app risk and privacy analysis		✓	✓	⊗
		Fine grained privacy controls (e.g., GDPR, BYOD)		✓	✓	⊗
		Network Attack detection (e.g. MITM)		✓	✓	⊗
		Reconnaissance scan detection		✓	✓	⊗
	Device	Insecure/Risky/Networks/Rogue Access Point Detections		✓	✓	⊗
		Offline Remediation w/o MDM/EMM		✓	✓	⊗
		Advanced Compromised / Elevation of Privilege Detection		✓	✓	⊗
		Detailed mobile threat intelligence and forensics		✓	✓	
		Device Risks (e.g. PIN, OS, Encryption, etc)		✓	✓	
		Malicious profile detection		✓	✓	⊗
		Protect devices across multiple UEMs in a single tenant		✓	✓	⊗
Provide advanced protection for Samsung KNOX devices (DLP)			✓	✓	⊗	
Personal info does not need to be pulled from the device and transferred to the cloud for analysis		✓	✓	⊗		

* Microsoft OEM from Bitdefender

** only Android

Business Use Cases

Business Alignment <i>Align IT investments with key priorities</i>	Operational Efficiency <i>Improve IT service delivery</i>	Operational Effectiveness <i>Improve business performance and productivity</i>	Capital Efficiency <i>Improve the return on Capital deployed</i>
<p>Protect the Brand:</p> <ul style="list-style-type: none"> • Ensure that Customer does not fall victim to Phishing or Social engineering via Mobile Attack Vectors <p>M&A Efficiency:</p> <ul style="list-style-type: none"> • Enable a faster time to market for integrating and securing acquisitions <p>Regulatory & Compliance:</p> <ul style="list-style-type: none"> • Support regulatory and audit compliance and issue remediation 	<p>Simplification:</p> <ul style="list-style-type: none"> • Enhance security, optimize performance, and drive service efficiency via correlation and integration into native Azure platform components <p>Standardization:</p> <ul style="list-style-type: none"> • Gain operational synergies through common standards (NIST and MITRE ATT&CK) and other best practices <p>Automation:</p> <ul style="list-style-type: none"> • Leverage tools to automate processes for monitoring and alerting <p>Innovation:</p> <ul style="list-style-type: none"> • Leverage modern technologies, such as threat analytics and machine learning, to improve prevention and detection, ultimately extending XDR to the mobile platform 	<p>End User Experience:</p> <ul style="list-style-type: none"> • The protection is transparent to the end users. They can focus on their work and not worry about their mobile device security <p>Workforce Mobility:</p> <ul style="list-style-type: none"> • Enable an anytime, anywhere workforce that can securely migrate across geos <p>First Line workers:</p> <ul style="list-style-type: none"> • Enable secure access to mission critical applications – even on purpose-built devices <p>Operational Risk:</p> <ul style="list-style-type: none"> • Minimize impact to operations through threat prevention as well as faster remediation 	<p>Reduce Fixed Assets:</p> <ul style="list-style-type: none"> • Utilize Software as a Service to reduce use of physical servers and maintained software <p>Eliminate Attacker ROI:</p> <ul style="list-style-type: none"> • Remove devices from the threat of attackers by making it extremely difficult, and therefore expensive to invest in compromising the customer’s mobile devices

Mobile Endpoint Security

Mobile Endpoint Security..... The challenge

'It is no longer a matter of if or when an enterprise's mobile endpoints are at risk of being attacked – – they already are'
State of Enterprise Report, 2019

- Mobile devices are now the dominant productivity platform in any organization with more than 80% of the daily work performed on a mobile device.
- In a typical organization today, 60% of the endpoints containing or accessing organizational data are mobile... most are without a security solution.
- Because of the current lack of visibility on mobile devices, most organizations never identify these portions of the attack
- The surge in remote working has made secure remote access a priority.
- Security leaders are challenged with protecting endpoints from attacks, while also providing access from any device company resources.

Why Hackers Target Mobile Endpoints

- Over 60% of enterprise endpoints are on iOS, Android or ChromeOS
- Mobile endpoints have access to the same information as traditional endpoints
- Mobile endpoints are critical to zero trust and two-factor authentication (2FA) initiatives
-
- Most mobile endpoints are unprotected and make easy targets

Mobile Endpoints Are Different

- **Users are the admins**; they decide when to upgrade OS's, what networks to connect to and what apps to install
- **Mobile apps are in containers**, limiting the capabilities of both malicious & security apps
- **Operating systems are locked down**, rendering EPP/EDR solutions like CrowdStrike (and Defender for Endpoints) ineffective because they rely on kernel access for detection

Security Laws Still Remain

- **Targeted attacks** against enterprises often use unknown, “zero day” attacks that require machine learning-based detection
- “**Land & expand**” campaigns target the weakest link for entry into the network-- unprotected mobile devices are hacker’s perfect starting point today
- To maximize the ROI of compromising any system (including a mobile endpoint), hackers’ want to establish a **persistent foothold** that remains even after reboot

How Hackers Are Attacking Mobile Endpoints

- **Device:** Attackers' primary goal on mobile is to fully compromise device in order to be persistent and weaponize it for "land and expand" lateral movements
- **Network:** Attackers use rogue access points (RAPs) and man-in-the-middle (MITMs) to steal data and also to deliver targeted exploits to compromise the device
- **Phishing:** Mobile phishing--especially via text/messaging apps and personal email--is a highly-effective way to steal credentials and deliver targeted exploits
- **Apps:** Malicious apps can create fraud, steal information and also deliver device exploits

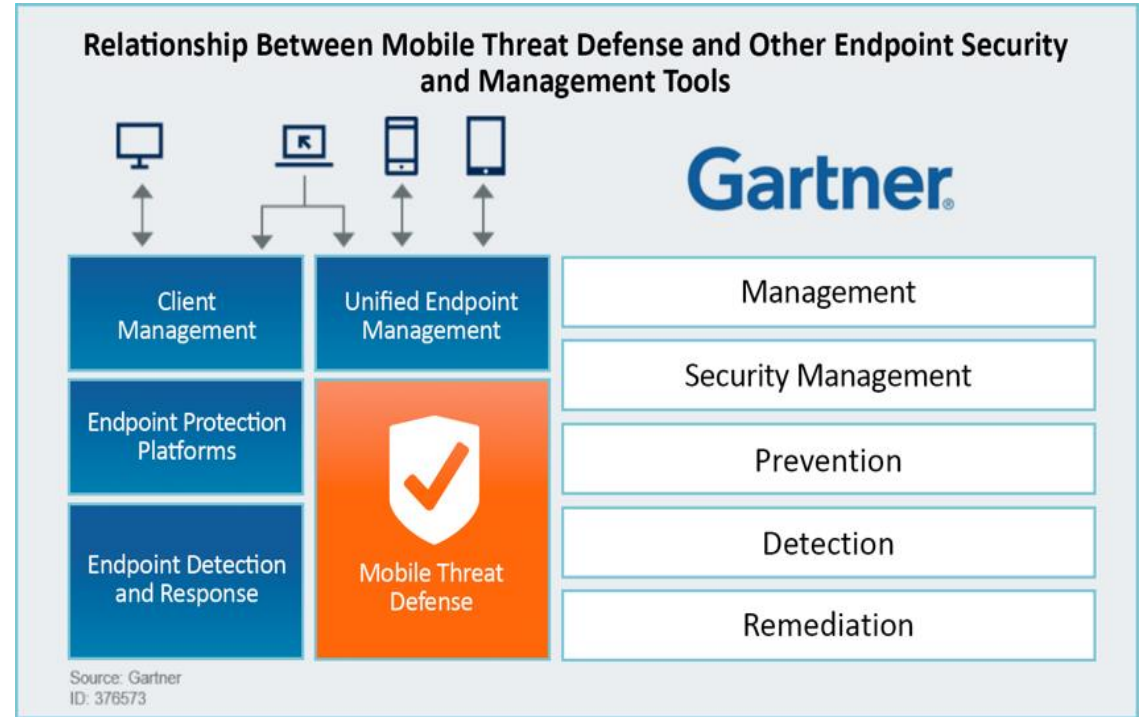
Why EPP/EDR Solutions Cannot Protect Mobile Endpoints

- Blind and ineffective due to locked down kernels in mobile OS's
- Have no ability to detect risky or malicious networks
- Cloud-based detection is disabled by network attackers and has privacy issues
- Cannot assess privacy and security risks in legitimate (non malicious) mobile apps

Mobile Endpoints Require A New Security Approach: MTD

Zimperium MTD Will:

- Detect threats even with locked down OS kernels
- Detect known and unknown (targeted) device, network, phishing and malicious app risks and attacks
- Deploy on-device detection to provide security when an attacker owns the network and will protect user privacy
- Will assess privacy and security risks in legitimate mobile apps



Zimperium Is The Global MTD Leader

- Absolute leader in Financial Services, Public Sector, Automotive, Healthcare/Pharma and others
- Demonstrated success in large scale implementations (e.g., U.S. Department of Defense)
- Only solution with on-device, privacy-protecting detection
- Proven, unmatched ability to detect known and unknown attacks across all threat vectors (device, network, phishing and malicious apps)
- Best ability to assesses privacy and security risks in legitimate mobile apps
- Unrivaled enterprise capabilities, e.g., multi-UEM, group-based policies, threat intelligence integrations)

Why Zimperium + Microsoft ?

- CrowdStrike has no ability to match our combined abilities and offerings
- Defender for Endpoints is very competitive against CrowdStrike for traditional EDR opportunities
- CrowdStrike Falcon for Mobile and Microsoft Defender are both early technologies, and primarily cover only known phishing and malicious apps
- Zimperium protects against risks and attacks not covered by either CrowdStrike Falcon for Mobile or Defender for Endpoints
- Zimperium is a leader in enterprise MTD
- Zimperium is only full MTD that can be hosted in Azure
- Zimperium's unrivaled mobile forensics are already being delivered to both Defender for Endpoints and Azure Sentinel

Changing The Game



	Known Attacks	Zero Day Attacks
Device		
Network		
Phishing		
Apps		



	Known Attacks	Zero Day Attacks
Device		
Network		
Phishing		
Apps		

Changing The Game



	Known Attacks	Zero Day Attacks
Device	Grey	Grey
Network	Grey	Grey
Phishing	Grey	Grey
Apps	Grey	Grey

	Known Attacks	Zero Day Attacks
Device	White	White
Network	White	White
Phishing	Grey	White
Apps	Grey	White

Zimperium Mobile Security Report 2019 (Semi-annual report with 45 million endpoints)

Network Threats and Attacks

- Over half of all enterprise mobile endpoints encountered risky networks.
- Network attacks accounted for 92% of all attacks covered in this report.
- 94% of network attacks were man-in-the-middle (MITM) variations wherein attackers hijack traffic to steal credentials/data or deliver exploits to compromise the device












Device Threats and Attacks 2019 State of Enterprise report

- Mobile OS vendors created patches for 1,161 security vulnerabilities.
In 2019, Apple patched 306 **Common Vulnerabilities and Exposures**, 64% of which were considered “critical” security threats.
In 2019, Google patched 855 CVE’s, the majority of which (54%) were considered “critical” or “high” security threats.

At the end of 2019, 48% of iOS devices were more than four versions behind the latest and 58% of Android devices were more than two versions behind.

App Threats and Attacks

- 85% of iOS apps and 21% of Android apps failed to receive a passing privacy grade.
- 71% of iOS apps and 68% of Android apps failed to receive a passing security grade.

VECTOR	KEY FINDINGS
	Mobile OS vendors created patches for 1,161 security vulnerabilities.
	24% of enterprise mobile endpoints were exposed to device threats not including outdated operating systems.
	68% of malicious profiles were considered “high-risk”, meaning they had elevated access that could lead to data exfiltration or full compromise.
	Over half of all enterprise mobile endpoints encountered risky networks.
	Zimperium detected over 3 million risky networks in 2019.
	Network attacks accounted for 92% of all attacks covered in this report.
	19% of enterprise mobile endpoints experienced network-based attacks.
	13% of enterprise Android devices detected malicious apps. Of all enterprise endpoints with malicious apps, 86% were Android-based and 14% were on iOS.
	48% of the Android devices had sideloaded apps versus 3% of iOS devices.
	85% of iOS apps and 21% of Android apps failed to receive a passing privacy grade.
	71% of iOS apps and 68% of Android apps failed to receive a passing security grade.

MTD and Zimperium

MTD and Zimperium

What is MTD or Mobile Threat Defence

According to Gartner, 'Mobile Threat Defence is defined as a mix of vulnerability management, anomaly detection, behavioural profiling, code emulation, intrusion prevention, host firewalling and transport security technologies to defend mobile devices and applications from advanced threats. Advanced threats in this case are threats that go beyond the capability of Enterprise Mobility Management (EMM) and Mobile Device Management (MDM) solutions. MTD extends both these solutions with additional security capabilities'

Reasons to offer MTD

- MTD solutions continue to add user cases which reduces Enterprise Risk
- Security and Risk Management continue to become more important within organizations
- Enterprises are looking to consolidate administration of platforms
- Continued emphasis using Office 365 opens opportunities for BT with existing/New customers
- Not surprisingly, the continual rise in mobile adoption and usage is compelling companies to pursue “mobile-first” strategies
- **Targeted attacks** against enterprises often use unknown, “zero day” attacks that require machine learning-based detection

MTD and Zimperium

Zimperium is positioned in the Leaders category of the 2020 IDC MarketScape for mobile threat management software. It is regarded as a global leader in mobile device and app security, offering real-time, on-device protection against Android and iOS attacks.

Founded in 2010 with Headquarters in Dallas, Texas.

The flagship offering - zIPS product, is an on-device MTM app with:

- on-device machine learning,
- threat detection, and
- remediation capabilities.
- zIPS uses the company's z9 machine learning engine

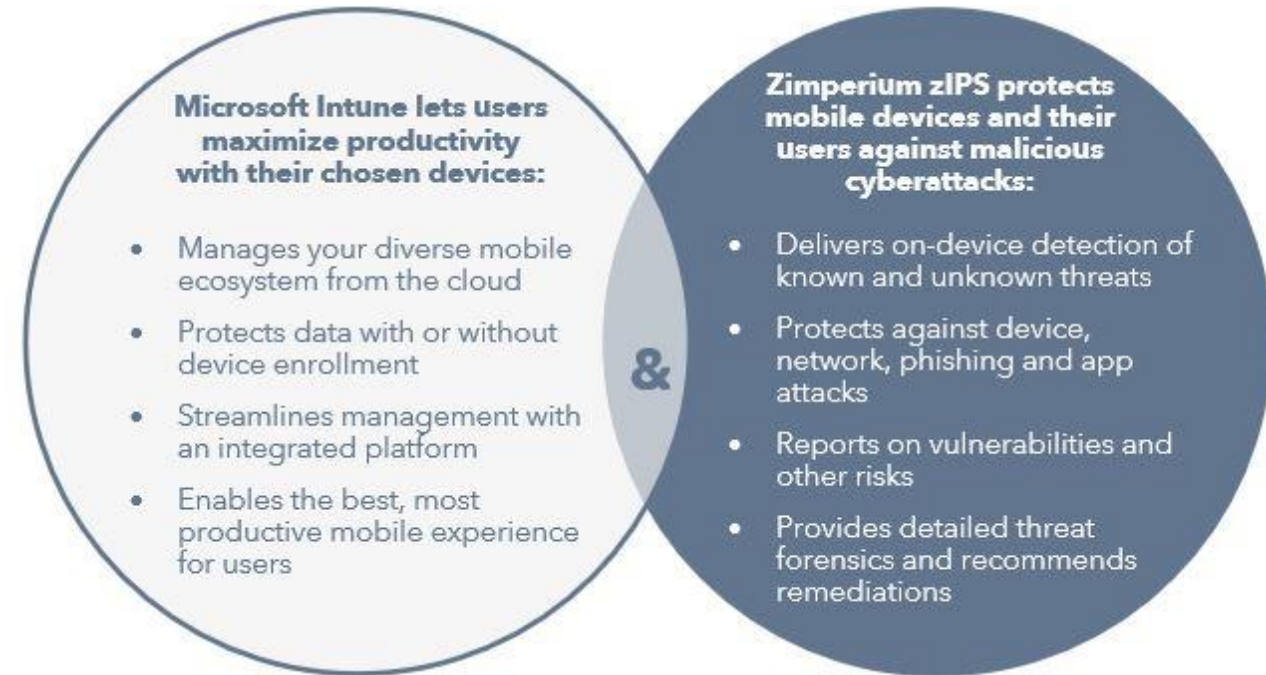
As a business, Zimperium has two major partnerships,

- With EMM/UEM vendor MobileIron (Where zIPS is the underlying technology behind the MobileIron Threat Defense — the vendor's integrated UEM/MTM security offering.
- White label partnership for zIPS with McAfee, which uses the Zimperium technologies in its broader McAfee MVISION Mobile security portfolio.

Zimperium & Microsoft Intune Integration

Zimperium and Intune Integration – Complete Mobile Security

- Together, Microsoft Intune and Zimperium enable enterprises to manage and secure mobile devices against the broadest array of device, network, phishing and malicious app attacks.
- Zimperium continuously detects and analyses risks and threats and provides Microsoft Intune with the visibility to enact risk-based policies to protect mobile devices.
- The integrated solution provides IT Security Administrators with a way to safely enable corporate and BYO device initiatives. The combination enables a balance between empowering mobile employees to be more productive with the device of their choice, while at the same time securing mobile devices and the enterprise against advanced threats



‘Together, Intune and zIPS enact risk-based policies to prevent a single mobile device from compromising the enterprise’

Zimperium and Intune – How It Works



Deployment / Activation

- Intune deploys Zimperium App to devices
- Zimperium authenticates via AAD SSO
- Device activates after authentication and reports to Intune



Risk based Detection and Reporting

- Zimperium utilises Microsoft EMS device threat levels to define risk posture threshold
- Device threat level and threat data are reported to Intune
- Intune designates compliant devices by using Zimperium threat data



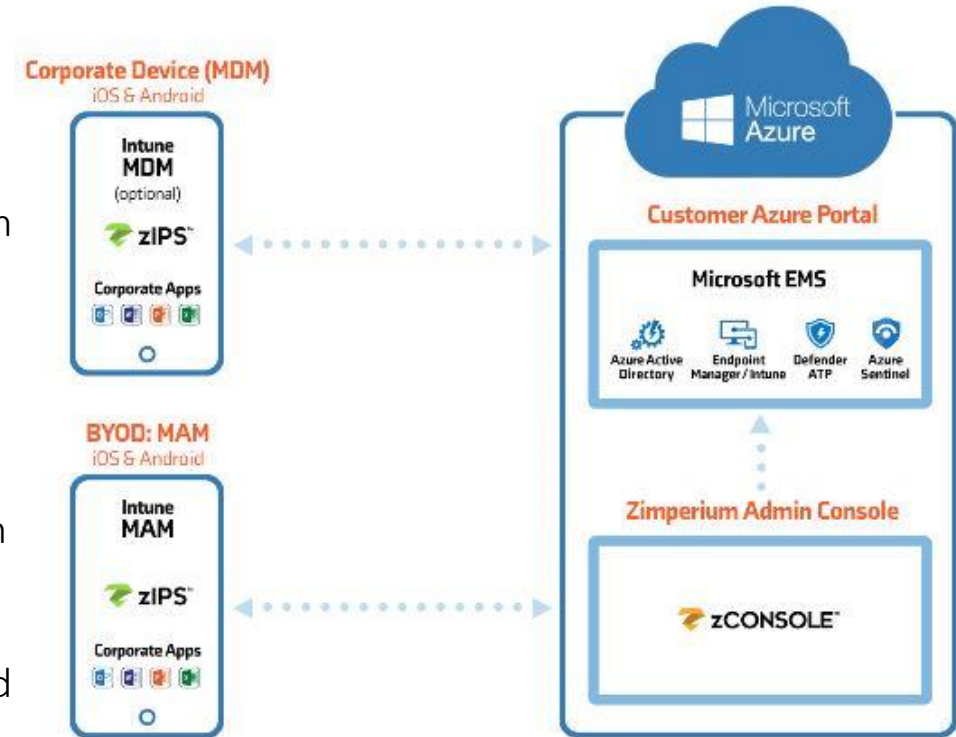
Remediation

- Intune enforces conditional access policies for noncompliant devices like removing access to Exchange or Apps.
- Zimperium notifies Intune when the threat is mitigated in order to reinstate device and user access.

Why BT with Zimperium + Microsoft

BT + Zimperium + MS Intune

- BT have chosen the best products in the market to deliver UEM and MTD to their customers and are a Microsoft Co-sell partner.
- There has been a major shift towards Microsoft 365 E3 and E5 licensing together with usage of Microsoft Endpoint Manager (MEM)
- More recent trends for remote working and BYOD demands more robust mobile security.
- Companies are looking to fully utilise their investments in licensing, with moving from MS E3 to E5 licensing seen as the natural progression.
- BT have extensive experience and knowledge with end to end device provisioning and deployment projects. This includes working with Intune and Zimperium MTD.
- With the establishment of MEM, Microsoft is now a leader in the UEM Magic quadrant and offers the most used UEM tool on the market, with significantly more devices under management than its competition.
- The combination of toolsets supports consolidation of management and administration within the Microsoft Cloud.



Microsoft now leaders in UEM

Magic Quadrant

Figure 1. Magic Quadrant for Unified Endpoint Management



Source: Gartner (August 2020)



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.

◆ Free Mobile Risk Assessment ◆

For organisations who are unsure about 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.

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:

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**

BT

Mobile Threat Defence with Microsoft 365 and Zimperium

Free Mobile Risk Assessment

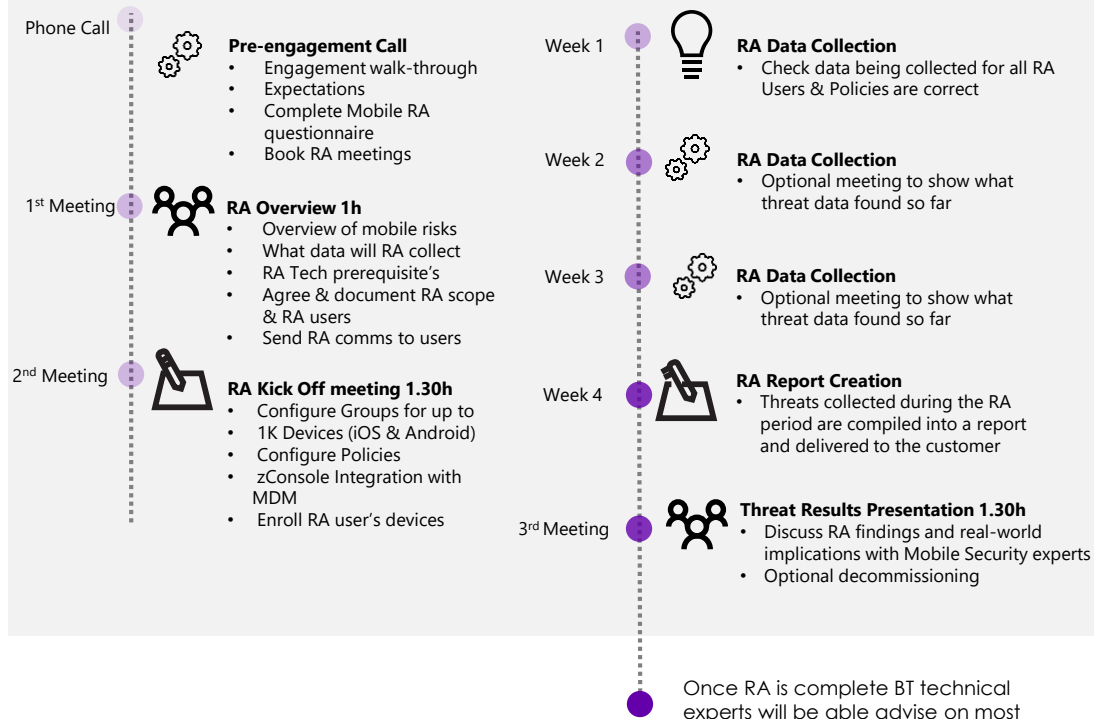


“Mobile devices were the biggest hole in our security.”

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)



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

