ZIMPERIUM®
ADVANCED MOBILE SECURITY

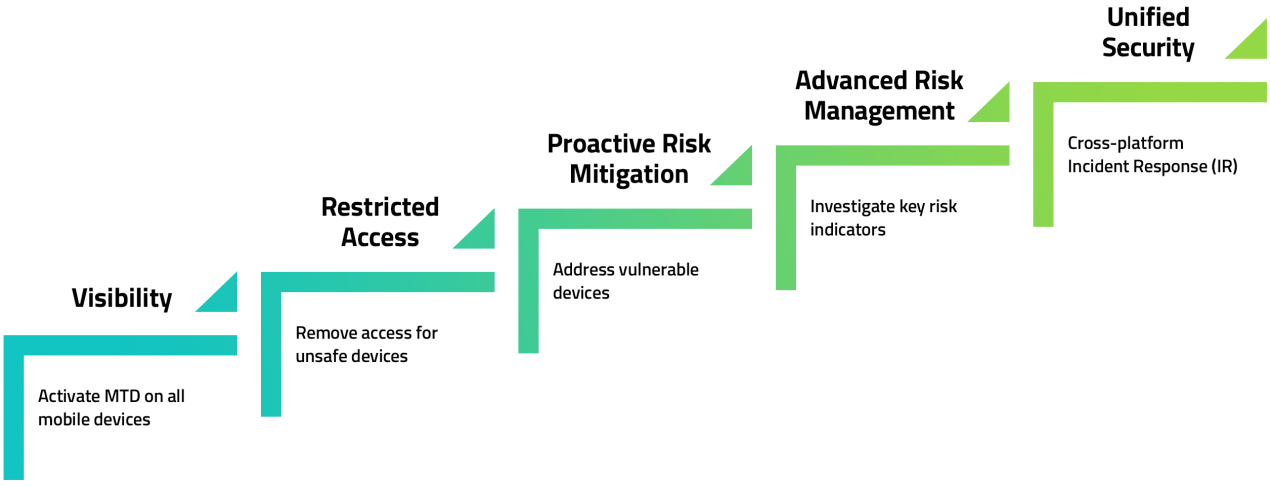
Mobile Threat Defense (MTD) Maturity Model

Enabling Enterprises to Effectively Manage Mobile Risks

Zimperium's Mobile Threat Defense (MTD) solution provides enterprise customers effective and scalable security controls. It efficiently monitors and mitigates advanced mobile threats while respecting enterprise policy and privacy requirements.

But security professionals know better than most that having the proper tooling is essential but is only the first step and that deriving holistic value quickly is critical in cybersecurity. And with the pace at which cyber threats are evolving, Zimperium understands that enterprise customers need help accelerating their mobile security positioning more than ever.

Zimperium provides a MTD Maturity Model to help customers build effective Mobile Threat defense capabilities based on best-practices.



The goal of the model is simple: provide a path forward and enable enterprises to periodically assess security postures and defensive opportunities. The model has five maturity levels: Visibility, Restricted Access, Proactive Risk Management, Advanced Risk Management, and Unified Security.

Each maturity level contains critical focus areas such as threats, policy recommendations, milestones to achieve the intended protection level. The higher the maturity, the higher the security efficacy against mobile attacks and threats. Once a level of maturity is determined, the following steps include measurements, metrics, and specific outcomes. The model is a valuable tool to strategize, execute and communicate across the organization to address mobile risks.

Below is a high level view of the maturity level and their focus areas:

Level: **Visibility**

Focus Areas

- Activate MTD on all mobile devices
- Start defining processes and policies based on visibility
- Enforce compliance policies on unprotected devices

Customer Case Study:
Global Conglomerate | 50K Devices

Working to activate MTD on 100% of devices across 20+ diverse companies to achieve visibility.

Level: **Restricted Access**

Focus Areas

- Remove access to devices in a critical state
- Enable user alerts and admin notifications

Customer Case Study:
Automotive Manufacturer |180K Devices

Restricted access to corporate apps for rooted devices, jailbroken devices, devices with suspicious profiles and malicious apps.

Level: **Proactive Risk Management**

Focus Areas

- Implement risk-based access
- Customize policies by users groups and access levels
- Begin integrating into existing security ecosystem

Customer Case Study:
Large Utility | 10K Devices

Limit enterprise access to devices with apps from third party stores, no device pin, side-loaded apps, risky profiles.

Level: **Advanced Risk Management**

Focus Areas

- Periodic review of risky App and Profiles
- Review advanced threat chains & patterns

Customer Case Study:

Global Consulting | 35K Devices

Security Operations (SOC) experts are leveraging Zimperium's Threat Advisory services to proactively and iteratively search through threat chains, risky apps and risky profiles to detect and isolate advanced threats.

Level: **Unified Security**

Focus Areas

- Enrrich and correlate threat data
- Orchestrate remediation across endpoints

Customer Case Study:

Large Australian Bank | 35K Devices

Automated end to end threat log integration with their SIEM (ArcSight). Their Incident Response(IR) team monitors and remediates all critical threats 24X7.

IN SUMMARY

Zimperium's goal is to support customers as they **embrace mobile platforms** to drive **productivity** and **growth** while minimizing security risks. The Maturity Model provides guidance on how to plan, adapt and integrate Mobile Threat Defense platforms into the enterprise ecosystem. If you want to learn more, please contact us.

ZIMPERIUM®