

MTD

Mobile Threat Defense

Installed in a few seconds, the **TEHTRIS MTD** application offers a unique protection by detecting and neutralizing in real time any types of attacks and suspect behaviors on your smartphones.

Gartner

TEHTRIS recognized as a Representative Vendor in the 2021 Market Guide for Mobile Threat Defense 2021*

Your cell phone, the neglected vulnerability of your information system...

Access to emails, directories, downloading files, mixing private and professional uses... information inside your smartphones are sensitive. As an underestimated access point to your IT assets, your mobile fleet needs to be protected more than ever.

Mobile Detection & Response in **REAL TIME**

Android, iOS, iPadOS, Chrome OS



- ↓ Quick installation (Cloud)
- ↓ Centralized control & unified console
- ↓ Control your applications from installation to update
- ↓ Available on Android, iOS, iPadOS and Chrome OS
- ↓ Access to the TEHTRIS XDR Platform

TEHTRIS MTD

detects and responds to attacks on your mobile fleet in real time.

Its threat knowledge base - connected to the TEHTRIS CTI (Cyber Threat Intelligence) - is updated 24/7 to identify, detect and respond to all types of threats: from the installation of a malicious application to its update (including system applications), brute-force attempts and man-in-the-middle attacks, or the discovery of

A real-time protection combined with vulnerability hunting: security flaws are immediately detected on iOS, iPadOS, Android and Chromebook. Remediation is performed automatically and preserves your mobile fleet by reducing the attack surface, notably by DNS isolation of corrupted devices.

vulnerabilities in the local configuration, thanks to its low-level scanning library.



Full visibility on your mobile fleet

TEHTRIS MTD can be installed and deployed quickly to ensure 360° protection & vision of your mobile fleet.

With BYOD or MDM, the application is deployed without any modification of the mobile settings and without any action required from the user. The protection of your fleet is operated remotely in SaaS, including configuration, integration, deployment, and maintenance in operational conditions. You benefit from a dedicated virtual machine to manage your fleet, deployed in the fully secured TEHTRIS cloud.

BENEFITS

EFFICIENCY

- ▶ Fast deployment
- ▶ Compatible and complementary with EMM/MDM
- ▶ Automatic remediation

CUSTOMIZABLE

- ▶ Customizable settings for security policies
- ▶ Application blacklisting
- ▶ Remediation scenarios (Playbooks)

AUTONOMY

- ▶ Security scans performed in the background
- ▶ Centralized monitoring from the console

As a TEHTRIS customer, you are informed in real time through TEHTRIS MTD of attacks on your fleet by receiving security alert notifications from the TEHTRIS XDR Platform.

Centralized vision of your mobile fleet for a complete visibility

Control of the mobile fleet's devices

- ▶ Access to collected Alerts & Events
- ▶ Customizable interactions with each mobile device

Unified Console for Device Management, Alerting, Remediation & Reporting

Take advantage of the unified **TEHTRIS XDR Platform** interface and its extensive detection and response capabilities via CTI (continuously updated knowledge base), Hunting, Compliance, and Incident Management, combined with integrated SOAR orchestration.

Benefit from a dedicated or mutualized XDR deployed in the TEHTRIS trusted cloud to ensure the cybersecurity of your mobile fleet as well as a single console to ensure compliance with your security policy !

Automatic detection & neutralization in real time 24/7 monitoring of your mobile devices

Anti-Jailbreak
Anti-smishing
Security compliance

- Monitoring** of applications, from installation to updates
- Analysis** of applications rights and permissions
- Analysis scan** Low-level (jailbreak, alternative stores, ports)
- MAST Analysis*** (static & dynamic code security analysis) of applications installed on your fleet or under development in your services

- ✓ **Removal** of malicious applications from the console
- ✓ **Easy Wipe/Reset** of the mobile from the console in case of loss or theft
- ✓ **Blacklist and remote uninstall** of applications
- ✓ **TEHTRIS DNS Firewall protection** (customizable as an option)
- ✓ **Targeted DNS isolation** in case of mobile compromise
- ✓ **DNS Blacklist** (configurable)

TEHTRIS MTD

detects and neutralize all types of attacks including brute-force & TLS interceptions called man-in-the-middle attacks.

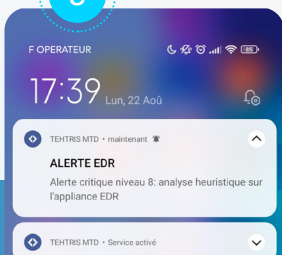
Push Notification stay informed in real time and optimize your reaction time to alerts

Get notified directly on your cell phone by the TEHTRIS XDR Platform in case of a critical alert on your fleet.

When and at what level of alert to get notified?
You decide!

Your SOC analysts
can contact you directly with a personalized push notifications !

3



KEY FUNCTIONALITIES

REAL TIME DETECTION

24/7 Monitoring

- ▶ **APK:** Detection of malicious or unknown applications
- ▶ **Access:** Events related to the enrollment of a device and alerts related to the connection to a new Wi-Fi spot
- ▶ **DNS:** DNS Firewall notify connection attempts to a malicious domain name
- ▶ **Event Log:** Tracking of actions performed remotely on the phones
- ▶ **Brute-force** attacks
- ▶ **TLS Interception** detection (Man-In-The-Middle Attacks)

Investigation & IOC Hunting

- ▶ CVE Applications & targeted hunting

Security scan

- ▶ Rights allowed and authorizations of applications analysis
- ▶ **Static and dynamic code analysis** (MAST - Automated Mobile Application Security Testing)
- ▶ **Low-level analysis:** 50+ continuous security tests
- ▶ Detection of an illegitimate debugging process
- ▶ **Rootless Jailbreak** detection
Unwanted third-party blind detection
Malicious library injection detection

COMPLIANCE

- ▶ Adaptability of the bruteforce
- ▶ Customization of the minimum security for unlocking the device
- ▶ Applications & DNS Blacklist / Whitelist
- ▶ GPS location
- ▶ List of WI-FI networks used

AUTOMATIC REMEDIATION

- ▶ Remote wipe of the mobile
- ▶ Uninstalling applications via MDM
- ▶ Removing applications via MDM
- ▶ Application and domain names blacklist
- ▶ Targeted DNS Isolation

DASHBOARDS & REPORTING

Unified console for a complete visibility 24/7

- ▶ Rooted / Jailbroken Mobiles
- ▶ Compromised Mobiles
- ▶ Non-Compliant Mobiles
- ▶ TEHTRIS MTD deployment indicators
- ▶ OS mapping

Historization of security data for better traceability

- ▶ DNS
- ▶ Geolocation
- ▶ Security scan history

Security Checks

- ▶ Low-level analysis reports
- ▶ Operating system reports

ALERTS

- ▶ Alerts & Events
- ▶ Event qualification
- ▶ Send customized push notifications
- ▶ Critical security alert through our integrated SOAR

Continuous maintenance
operated by TEHTRIS in
SaaS mode

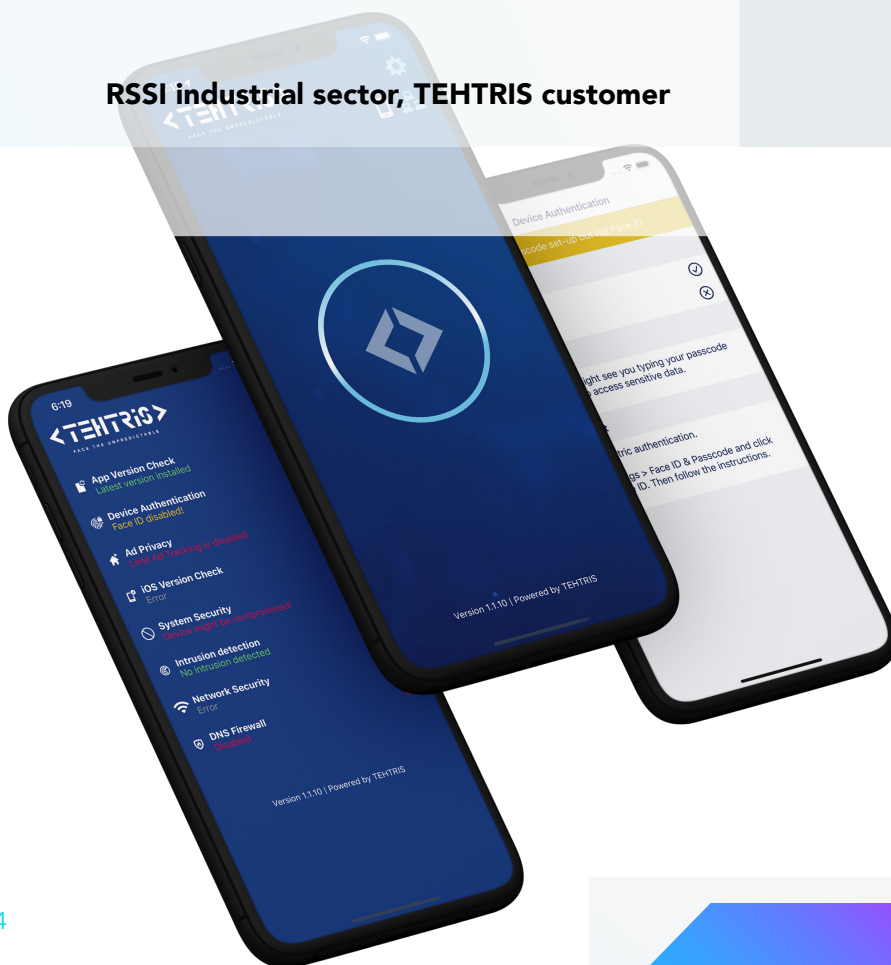
Services available
from 3G/4G/5G
Wi-Fi



TEHTRIS MTD saved us from an attack on a Jailbreak device. The attack was stopped immediately, and all cell phones continued to work without interruption. Day to day, our work is simplified. Central mobile management has become a must for our team.



RSSI industrial sector, TEHTRIS customer



From
Android 8.0



From
iOS/iPadOS 14

**MITRE |
ATT&CK®**

TEHTRIS XDR Platform
is 100% compatible with

* Gartner and Market Guide are registered trademarks of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Gartner Market Guide for Mobile Threat Defense, Dionisio Zumerle, Rob Smith, 29th March 2021

Ask for a
demonstration

TEHTRIS XDR Platform



EDR



EPP



MTD



SIEM



NTA



Deceptive Response



DNS Firewall



Zero Trust



CWPP



Email Protection



Identity Access Management

CONTACT US

business@tehtris.com
tehtris.com