ENDPOINT SECURITY - MTD

Mobile Threat Defense

| HOW CAN TELEFÓNICA TECH HELP?

We guarantee the highest level of security for your company's mobile devices thanks to rigorous comprehensive protection measures

Mobility is becoming increasingly prevalent and has profound business implications: numerous benefits such as increased productivity, but also an increased risk surface for cyber-attacks. **The mobile device is a key element in mobility.** It connects to any corporate service, accesses any corporate data the employee needs to work, can be connected 24 hours a day, and **attacks on this device have become increasingly sophisticated.** And all this while still being the least protected endpoint in organisations.

Mobile security has therefore become one of the **main concerns for companies.** The adoption of enterprise mobility requires maximum protection of sensitive information, providing secure mobile access to data and keeping mobile devices safe from threats.

Telefónica Tech's Mobile Threat Defense (MTD) is our security solution to protect your company's mobile terminals from cyber threats, thanks to comprehensive and specific protection for mobile devices.

To provide a unique experience we rely on our partner Check Point, and its leading Harmony Mobile technology, which provides advanced, comprehensive protection, the highest detection rate and unified management.

| WHO IS THIS SERVICE FOR?

Suitable for **corporations of any size,** as employees in **any company today have mobile devices** and use them to access corporate information.

It is particularly recommended as an add-on for **customers who already have an MDM/UEM solution for management and an EDR/MDR solution for solution for desktop/laptop protection.**

OUR VALUE PROPOSITION

Our service

Telefónica Tech's Mobile Threat Defense (MTD) service protects mobile terminals (iOS & Android) from risks and cyber threats, both known and more sophisticated attacks such as zero-day.

It is easy to scale and simple to manage and deploy. No impact on end-user experience or privacy and rapid adoption.

MTD is comprehensive protection as it provides protection against all three mobile attack vectors: application attacks, on-device attacks, and network attacks. Also, acting in conjunction with SMDM, it enables response mechanisms to be triggered on compromised devices. Corporate information is thus protected and so, prevents the threat from spreading to other enterprise systems and lateral movements.

What does it allow you to do?

This service will allow you to:

› **Provide the highest level of corporate security specifically for mobile devices.**

› **Protect sensitive information accessed from the device as well as the device itself.**

› Protection against **the device's three attack vectors:** applications, devices and network.

› Protection against **known and advanced threats** such as 0-day attacks using behavioural algorithms.

› Obtain **advanced correlation of information** from the device, installed applications and network usage.

› Risk and threat alerts enable **incident response.** Faster if integrated with SMDM.

› **Minimise the economic impact of cyber-attacks.**

Telefónica Tech's differential value

We provide the highest level of corporate security for mobile devices thanks to our strategic agreements with the best market-leading protection platforms and our team of cyber security experts.

Telefónica's SSPP specialists in security and device management provide expert advice and the possibility for the customer to delegate the management of the service to Telefónica.

We give the customer the power to decide the desired speed of deployment and provide the peace of mind of having contracted a fully scalable service as billing is done per activated device (pay-per-use). You are billed only when the service has been deployed on the device.

Benefits

Comprehensive cyber threat protection

Provides protection against all three attack vectors on mobile devices: application attacks, device and O.S. attacks and network attacks. Protection against MitM, Anti-Phishing, Anti-Bot, URL Filtering, Safe Browsing, Conditional Access, Device Configuration Analysis, Advanced Rooting Analysis, Application Malware Detection, O.S. exploits, etc.

Advanced protection technology

Employing the № 1 technology on the market. Detection of all types of cyber threats, both known and advanced 0-day attacks: use of algorithms based on device, network, cloud and behavioural analysis; use of the largest collaboration and knowledge network offering real-time dynamic security intelligence; use of sandboxing; advanced code flow analysis, among other techniques.

Security Status visibility

Console-based management of the entire fleet of devices. Generation of relevant information to know the real situation of risk exposure and attacks on the mobile device fleet: number of devices at risk and risk level, device deployment status, detected security events, rating of detected threats, etc.

User experience

No impact on user experience. Low consumption of device resources. Background activity. Protects user privacy as it does not collect or examine content or files. Facilitates BYOD adoption. When integrated with SMDM, deployment is quick and easy.

EQUIPMENT, TEAMS AND ACHIEVEMENTS

Our team

› Certifications: ENS and ISO 20000 (Management) / 27001 (Security).

› **+1,500** security certifications.

› Certified technical team.

› Constant certification of new versions, OS and platform functionalities.

Achievements

› **900K** micro devices managed (workstation), **+150** customers.

› **150K** managed devices (MDM service), **+450** customers.

› **60K** DaaS (Desktop as a Service), **+100** customers.

BUSINESS MODEL

The MTD service can be customised according to the customer's needs. It is billed monthly per device on a "pay-as-you-go" basis. There are three different methods:

› **Stand Alone:** Resale of licences (service subscription).

› **Add-on** in standard service "Managed Mobile DWP".

› **Stand Alone + DOC Management** (management within Managed Security / Device Management services).

RELATED PARTNERS

 CHECK POINT

| RELATED SERVICES

Secure Mobile Device Management (SMDM)

Business mobility platform providing end-to-end security and management service for devices, applications, documents, email and web access.

→

Managed Detection & Response

Comprehensive endpoint security monitoring through 24/7 detection, containment and rapid response to security breaches with continuous Proactive Hunting and expert cyber-crisis support, based on the leading EDR and XDR technologies.

→

Secure M365

Comprehensive cloud security services solution specifically designed to harden your Microsoft 365 environment.

→

Contact us to start the digital transformation of your organization.

→