Unified Endpoint Management combined with the protection of Mobile Threat Defense

Overview

Chimpa is a solution based on cloud (Italian region located) which allows you to manage,control and protect any device based on **Android, iOS, iPadOS, tvos and Windows 10/11** , such as Smartphones, Handhelds, Tablets, Notebooks, PCs, Kiosks, Flat Panels: **monitoring** and **controlling** them remotely, **protecting** them from possible intrusions and the theft of the most valuable data, thanks to its module focused on defense against threats «mobile» (Mobile Threat Defense).

Smartphone & Tablet

Large format display

Windows devices

Interactive Flat Panel

Rugged devices

Single purpose devices

Focal points

- Cloud based **SaaS** EU located through a Tier 3 Data Center
- 100% source **code owned**
- **Cross platform** solution (Android iOS Windows) on different form factor devices such as : IFPs Smartphones, Tablets, PDAs Notebooks & PC
- Over **200 device restrictions** available through a web dashboard
- **Massive** Zero.Touch , Apple DEP and Windows Autopilot **deployment**
- **Full Device protection** through dedicated Firewall, Advanced Anti Virus/Malware , Mail & Messaging Anti phishing system , Advanced Threat Intelligence engine
- **MSSP** dedicated license available

Control features

Chimpa provides a series of a easy-to-use tools that can manage your devices in a granular and efficient way in order to prevent any inappropriate use.
The Chimpa Dashboard, available on a web browser from any device, allows you to create and manage policies and flows flexibly and quickly. All work profiles, including restrictions and policies, can also be scheduled on an hourly basis through the simple and powerful programming module

Momitoring features

Chimpa provides you with tools to monitor and track device usage, reporting any anomalies and allowing you to make more efficient the staff's work . Chimpa allows you , in case of device loss or theft to geolocate the device itself and performing for example the remote wipe of data.

Maintenance

Real-time alerts on hardware operation and any anomalies

Screen display

Thanks to the screen display you can see and control devices remotely

Usage data collection

Access logs, app usage, connection log, and network traffic

Geolocalization

Workflows based on position

Security features

Chimpa protects your organization from staff improper use, knowingly and/or unaware, of devices , with **GDPR compliance** , separating personal and business data.

Apps, data, information and business content are encrypted and protected by the MTD module, specially developed to protect data from threats such as **Malware, Trojans and Ransomware** that use the web (malicious sites), email (Phishing) or messaging (Smishing) as attack vectors.

Chimpa is also equipped with a dedicated **Firewall** for device data traffic rules management and an advanced **Threat Intelligence module**, which, through the Cyber correlation of **compromise indicators (IOCs)**, is able to detect even **"Zero Day"** threats based on. This module gives the possibility to do **Open Source Intelligence (OSINT)** activities on IP addresses, email and URL.

Distribution Control Monitoring Protection

Apple Integration

The Device Enrollment Program (DEP) and **Apple Business Manager** allow you to automate the registration of Apple devices massively and to speed up the initial setup.
The **Volume Purchase Program** allows schools and companies to purchase apps and books by volume and distribute them to their users, managed Apple IDs or devices.

Windows integration

Chimpa seamlessly integrates with the main Microsoft services: a strong point which gives a great easy-to-use and effectiveness to the management and enrollment phase and to the management and security of **Windows-based devices.** Thanks to the **Windows Autopilot** configuration, the devices can be configured massively and 100% automatically . The integration with Azure allows you a simple and authomatic management of users and groups, thus offering the ability to execute Single Sign On.

Android integration

Chimpa has a deep integration with **Android**, through **Google Play Managed** and **Google Play Protect services**, thanks to the multi-year technological partnership between **Chimpa** and Android, who certified Chimpa as **“Android Enterprise EMM provider”**. Mass recording of devices 100% automatized through Android Enterprise Zero-Touch, QR Code, NFC or EMM Token. Thourgh Chimpa you can Synchronize your Google Workspace (GSuite) domain accounts, access services, and import organizational units and users, while also offering the ability to run **Single Sign On**.

Samsung integration

Chimpa is a **Samsung Knox Validated** solution compliance to Knox Mobile Enrollment (KME), Knox Platform for Enterprise (KPE), Knox Service Plugin (KSP) and supports Knox integrated features such as Remote screen control, APN, Knox Attestation, SIM management.

android enterprise EMM provider

Consultants Network

Microsoft Partner

Validated by SAMSUNG Knox

Chimpa With One Another

Value proposition

The best for those companies that have a small "fleet" of devices, but need to be able to manage it homogeneously, ensuring the security of the data on the device thanks to its advanced **Antivirus**

chimpa

CORE

Advanced solution designed to automatically manage your "fleet" of devices to ensure their security with highly flexible configuration and customization levels based on your needs thanks also to the support of **Single Sign On**

chimpa

ENTERPRISE

For companies which want the best in both management and device security. Ideal for "fleets" of large devices, it is equipped with a **View Screen Remote and a Cyber Threat Intelligence** module among the most advanced on the market.

chimpa

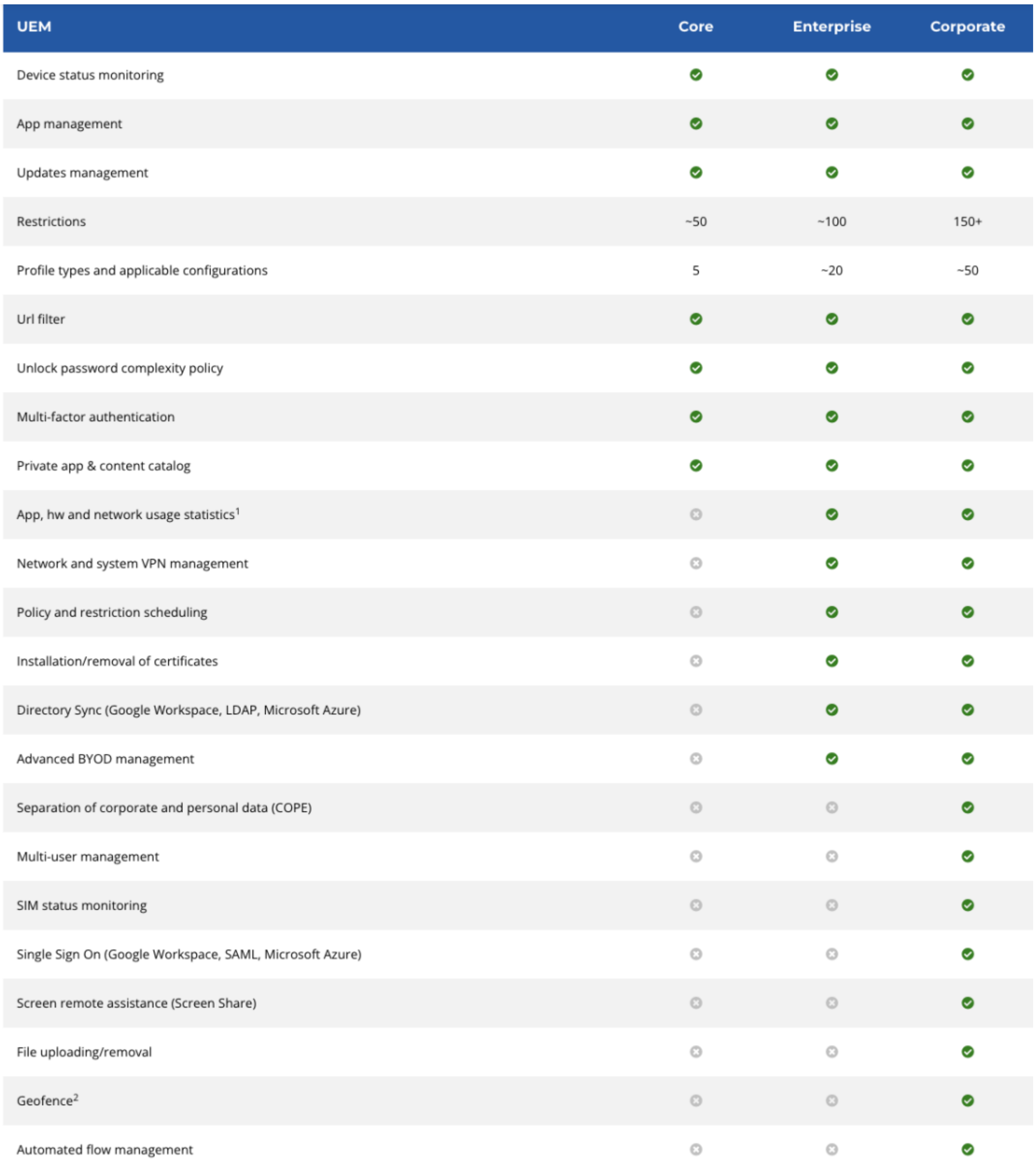
CORPORATE

+

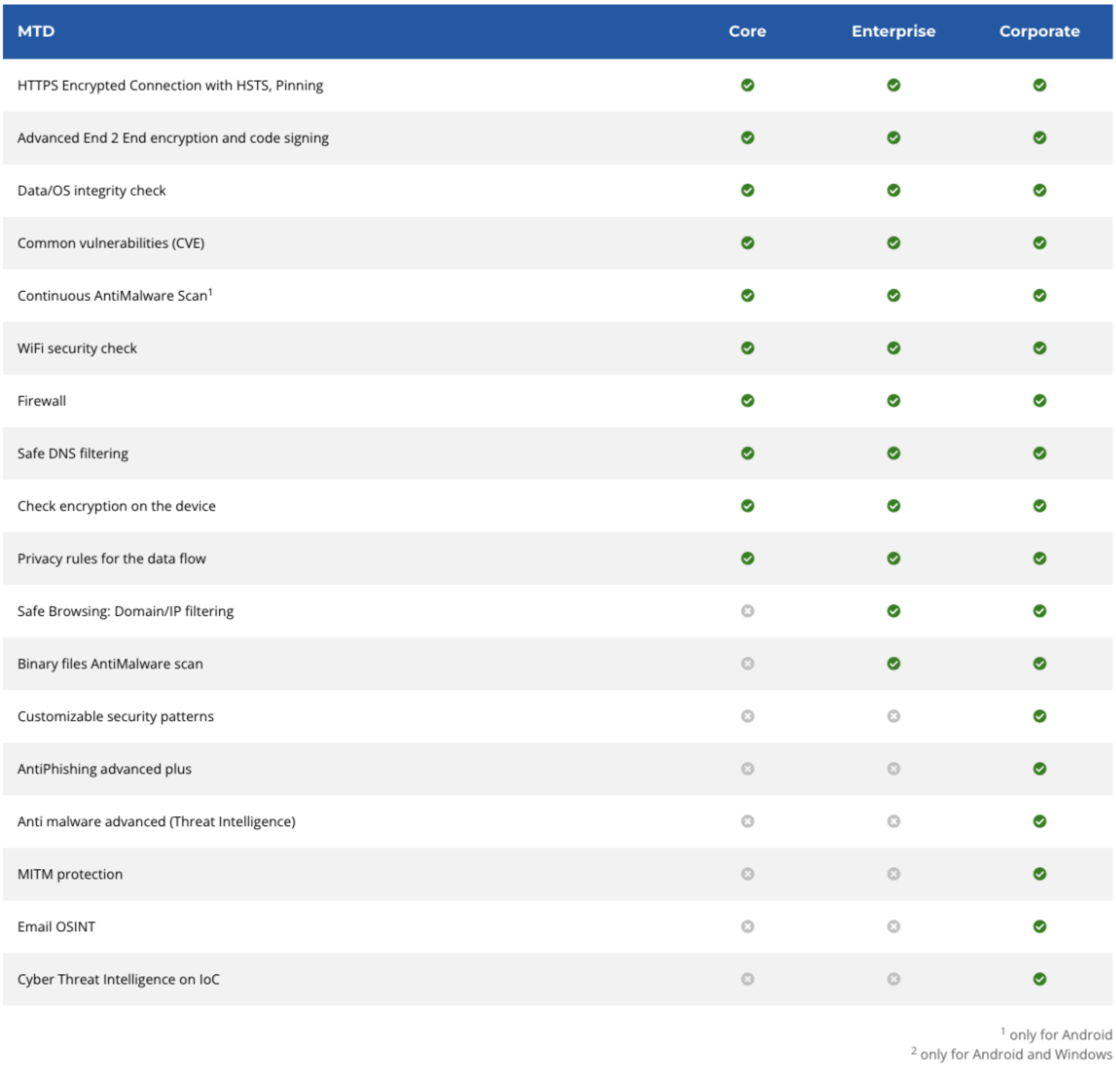
The Multi-instance version, also on premise, is dedicated to MSSPs wishing to complete their managed service offer also to the "Mobile" world, thanks to the Chimpa integration module that allows you to communicate with the most popular **SIEMs and SOARs.**

chimpa

MSSP



UEM	Core	Enterprise	Corporate
Device status monitoring	✓	✓	✓
App management	✓	✓	✓
Updates management	✓	✓	✓
Restrictions	~50	~100	150+
Profile types and applicable configurations	5	~20	~50
Url filter	✓	✓	✓
Unlock password complexity policy	✓	✓	✓
Multi-factor authentication	✓	✓	✓
Private app & content catalog	✓	✓	✓
App, hw and network usage statistics[1]	✗	✓	✓
Network and system VPN management	✗	✓	✓
Policy and restriction scheduling	✗	✓	✓
Installation/removal of certificates	✗	✓	✓
Directory Sync (Google Workspace, LDAP, Microsoft Azure)	✗	✓	✓
Advanced BYOD management	✗	✓	✓
Separation of corporate and personal data (COPE)	✗	✗	✓
Multi-user management	✗	✗	✓
SIM status monitoring	✗	✗	✓
Single Sign On (Google Workspace, SAML, Microsoft Azure)	✗	✗	✓
Screen remote assistance (Screen Share)	✗	✗	✓
File uploading/removal	✗	✗	✓
Geofence[2]	✗	✗	✓
Automated flow management	✗	✗	✓



MTD	Core	Enterprise	Corporate
HTTPS Encrypted Connection with HSTS, Pinning	✓	✓	✓
Advanced End 2 End encryption and code signing	✓	✓	✓
Data/OS integrity check	✓	✓	✓
Common vulnerabilities (CVE)	✓	✓	✓
Continuous AntiMalware Scan[1]	✓	✓	✓
WiFi security check	✓	✓	✓
Firewall	✓	✓	✓
Safe DNS filtering	✓	✓	✓
Check encryption on the device	✓	✓	✓
Privacy rules for the data flow	✓	✓	✓
Safe Browsing: Domain/IP filtering	✗	✓	✓
Binary files AntiMalware scan	✗	✓	✓
Customizable security patterns	✗	✗	✓
AntiPhishing advanced plus	✗	✗	✓
Anti malware advanced (Threat Intelligence)	✗	✗	✓
MITM protection	✗	✗	✓
Email OSINT	✗	✗	✓
Cyber Threat Intelligence on IoC	✗	✗	✓

[1] only for Android

[2] only for Android and Windows

Try Chimpa now for free !

Register for a free full trial to : chimpa.eu/en/contact