

XNOOVA

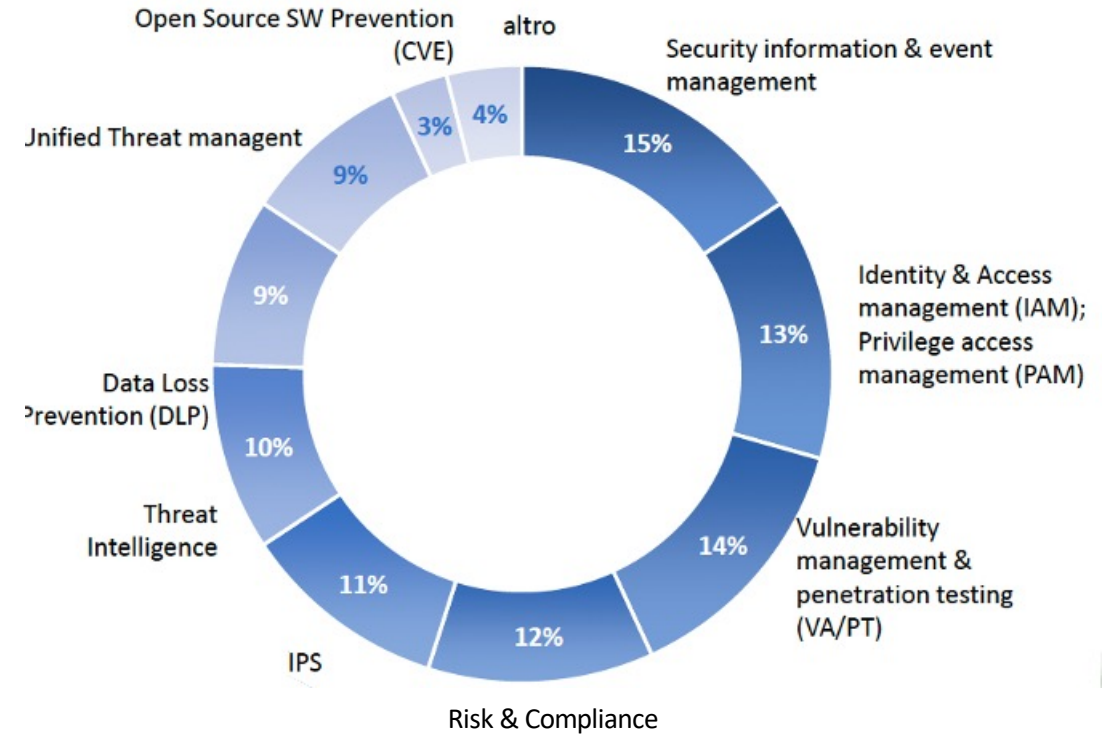
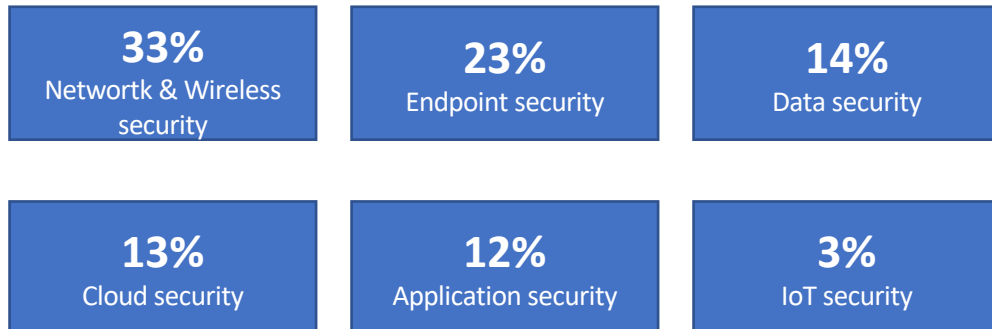
Chimpa
With One Another

Cyber market

In 2020 the Cyber Security market in Italy has reached 1.37 billion in value, with an increase of 4% compared to 2019

The expenditure components are 52% in services while 48% in solutions.

The main "types of security" adopted by companies are:



Enviroment



Cloud

- Increase of the attack surface
- Heterogeneous domains to defend
- Stratification of technologies
- Increase of remote logins



laws



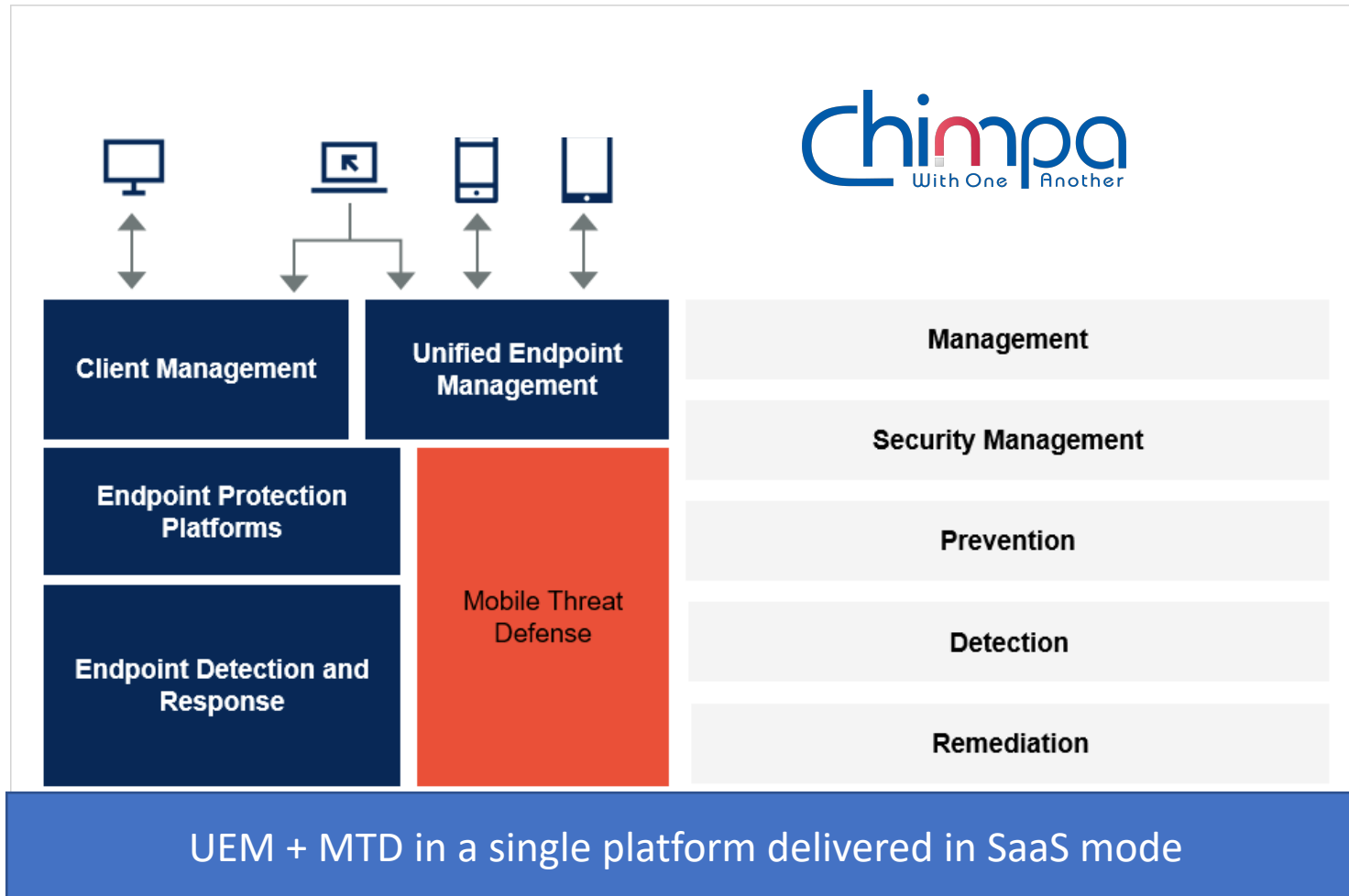
5G

- Connection of objects and their remote control
- Heterogeneity of the devices used



Smart working

Increased adoption of mobile devices and the need to protect them



Certified solution



android enterprise
EMM provider



Validated by
SAMSUNG Knox



Consultants
Network

Devices & OS



INTERACTIVE
DISPLAYS



LARGE FORMAT
DISPLAYS & DIGITAL
SIGNAGE



MOBILE DEVICES



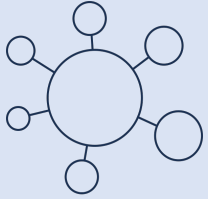
PDA



ROOM BOOKING &
SMALL FORMAT
DISPLAYS

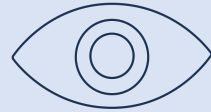


Main features



Distribution

Chimpa allows you to distribute and manage settings, policies, Apps, and updates in a uniform way.



Monitoring

Chimpa offers you tools to monitor the use of devices, allowing you to remotely act on the devices, for example in case of loss or theft



Control

Chimpa provides you with tools capable of granularly managing device restrictions at different levels



Security

Chimpa protects your devices from Trojan and Ramsonware attacks using vectors such as emails, messages and surging URLs and from ZERO DAY attacks thanks to its Threats Intelligence capability

Distribution

Chimpa offers you tools to efficiently use and manage apps, settings, content and updates, along with the certainty that each individual device will be configured according to its specific purpose.



Control

Chimpa offers you a wide range of tools (70+) for a granular management of the restrictions applied to the devices used in your organization, preventing any misuse. All profiles, including restrictions and policies, can be scheduled on an hourly, daily, weekly and monthly basis

Time Range

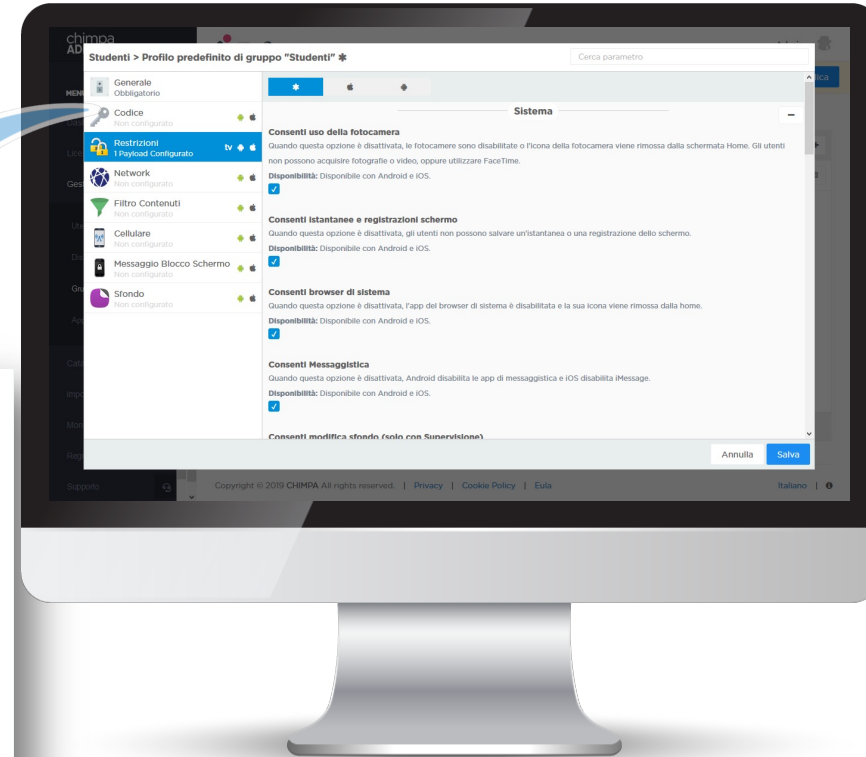
From To

Sun Mon Tue Wed Thu Fri Sat

Exclusion Dates

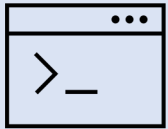
Time Slot
If not specified, will be applied 24h for each day selected in the time period

From hour (minutes) To hour (minutes)



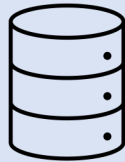
Security : 4 levels

Chimpa, acting on several levels, is able to guarantee all-round protection of the devices



Application Level

- OS
- Apps
- Systems configuration
- Processes



Storage Level

- In transit Data
- Stored Data
- External Data
- Logs



Communications

- Email
- Instant messaging
- SMS
- Internet browsing



Connectivity

- Wifi
- Bluetooth
- NFC

Security : main features 1/2

Mobile Threat Defense & Intelligence

1

Safe Web



Anti malicious Website module

2

Scansione antivirus ed anti malware avanzata



Anti imalwares, trojan e ramsonware multi source scan

3

Anti Phishing



eMail and Messages analyzer for searching malicious url

4

Smart Firewall



A Pre configured Smart Firewall able to analyze and block the most common cyber attacks

Mobile Threat Defense & Intelligence

5

Check file hash



Verification of the reliability of the downloaded file, the verification must be carried out manually (not present in continuous monitoring)

6

TOR Node check



TOR exit Node search module

7

OSINT check compromissions capability



Search for information of any compromises from open sources on: ip, files, emails, names

8

Security patterns and Indicators of compromission (IOC) threat intelligence approach



Allows you to customize, through the choice of indicators of compromise (IOC), the security patterns for single device, groups or all
Allows you to customize, through the choice of indicators of compromise (IOC), the security patterns for single device, groups or all

Value proposition

Cloud-based UEM solution that allows you to manage any device based on Android, iOS and Windows (from April 2022), such as Smartphones, PDAs, Tablets, Kiosks, Flat Panels and VR: monitoring , controlling and protecting them from hacker intrusions and theft of data thanks to its module focused on mobile defense (Mobile Threat Defense)

In particular, the protection of the device is provided by specific algorithms which, thanks to the use of artificial intelligence are able to block even exploiting ZERO DAY threats based on.

Unified endpoint
management

Zero Touch
deployment

SaaS providing
infrastructure

100% developed
in Italy

Modules offering
based on

Very clear UX
Web interface



A solution for Apple, windows and Android devices



The management of privacy, policies, apps / contents for IT administrators.



It simplifies the distribution of iOS, iPadOS, tvOS and Android devices even in ZERO Touch mode



Management supporting BYOD (Bring Your Own Device), COBO (Company Owned / Business Only), COPE (Company Owned / Personally Enabled)