XNOOVA

Scenario

Cloud

Regolamenti

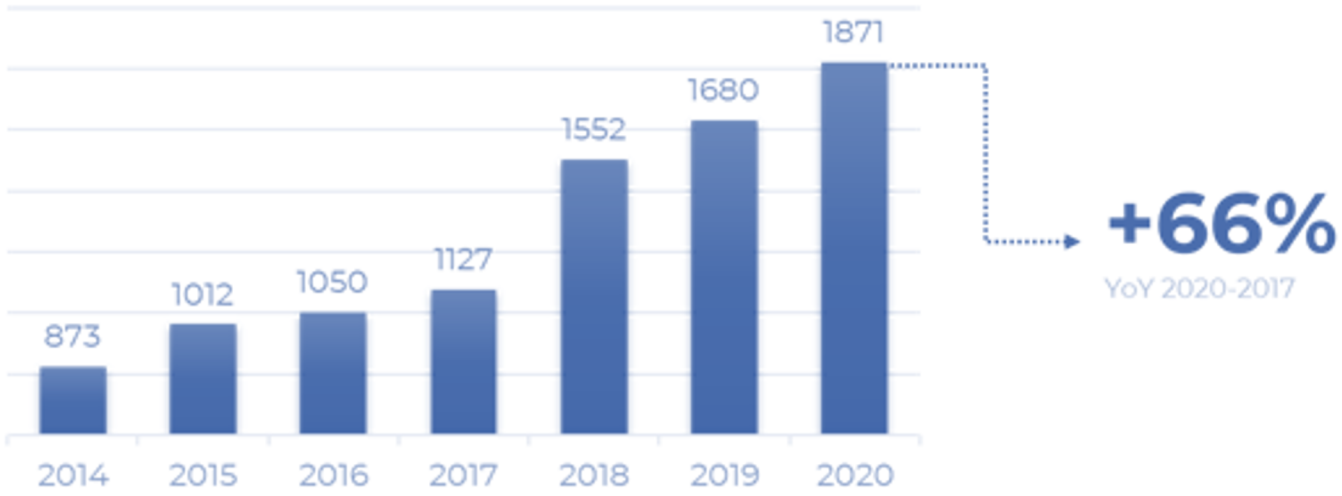
5G

Smart working

- Incremento della superficie d’attacco
- Domini eterogenei da difendere
- Stratificazione delle tecnologie
- Aumento degli accessi remoti
- Connessione di oggetti e loro controllo remoto
- Eterogenicità dei devices utilizzati

Aumento dell’adozione di dispositivi mobile e necessità di proteggerli

L’emergenza Cyber in Italia



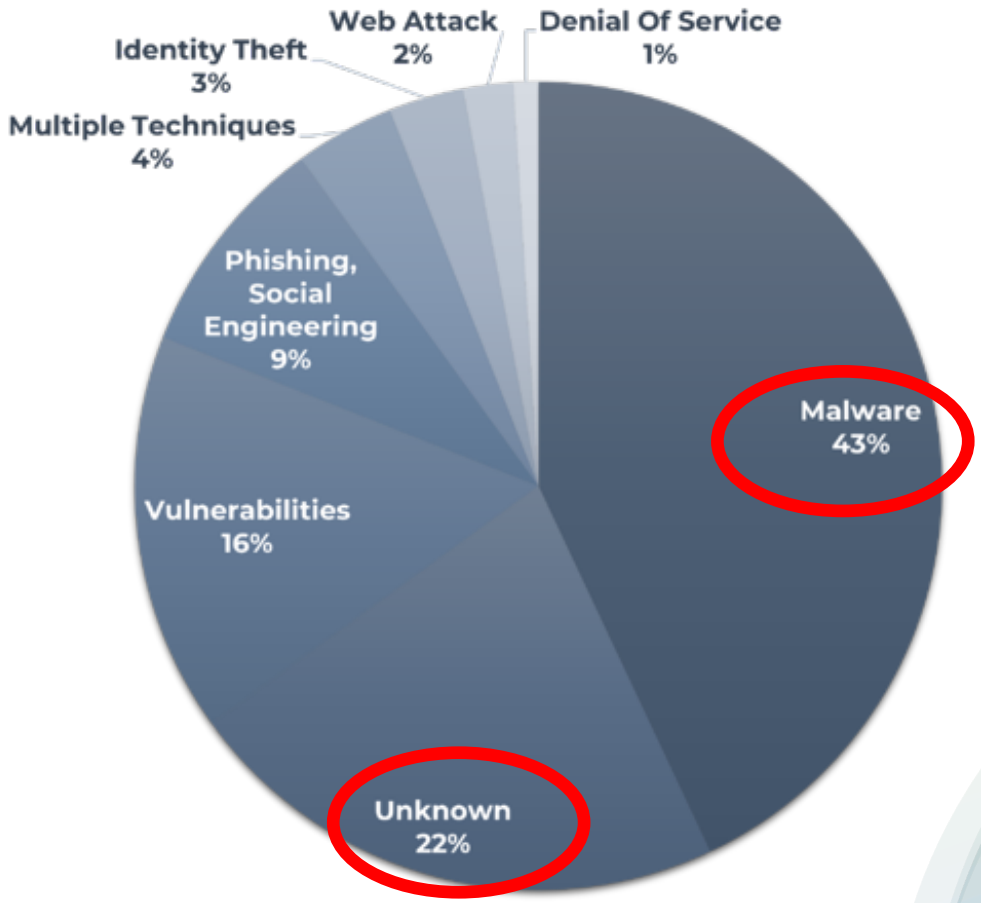
Un’emergenza globale concreta che incide per una percentuale significativa del GDP mondiale, con un tasso di peggioramento annuale a 2 cifre e un valore pari a **3 volte il PIL italiano.**
Per l’Italia, in questo scenario e ipotizzando un trend costante, nel 2024 **le perdite** potrebbero essere nell’ordine di grandezza dei **20-25 miliardi di euro all’anno**.

Tra i dati dello scorso anno ricordiamo che circa il 15% degli attacchi gravi noti erano a tema COVID; di questi Circa **il 61%**, sono stati condotti tramite campagne di **phishing,** (ingannevoli richieste di dati via email) e **social engineering**, talvolta anche in associazione a **Malware** (21%)**.**

L’emergenza Mobile Threat

Malware mobile in aumento: nel 2020, Check Point ha registrato un aumento del 15% dell’attività relativa ai cavalli di Troians bancari che potrebbero rubare le credenziali degli utenti. Gli hacker diffondono una varietà di malware per telefoni cellulari, inclusi i trojan di accesso remoto mobile (MRAT), i trojan bancari e i dialer premium. Spesso nascondono il malware nelle app che fingono di offrire informazioni relative a COVID-19.

Tipologie di attacchi



L'emergenza Mobile Threat

CVE : vulnerabilità conosciute

Apple » Iphone Os : Vulnerability Statistics

Vulnerabilities (**2573**) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules
Related OVAL Definitions : Vulnerabilities (127) Patches (154) Inventory Definitions (0) Compliance Definitions (0)
Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2007	1		1	1											
2008	2	2	2	1											
2009	11	2	3	2	2					2	3		1		
2010	20	11	9	5	3					4	2	1			1
2011	83	52	7	6	6		5			7	13	1			
2012	155	114	70	67	60		8			15	9	1			
2013	95	57	50	42	46		4			17	9	1			
2014	120	50	51	35	33			1		20	24	4			
2015	386	232	211	184	191			5		44	63	13	1		1
2016	168	113	79	81	81		3			8	42	11			
2017	388	241	222	210	194		14			39	63	5			
2018	125	63	63	55	50		1			19	19	2			
2019	354	9	101	90	167	2	14				25	5			
2020	305	17	141	49	60		8	2		6	13	5			
2021	[illegible]	15	[illegible]	35	41		6	3		11	9	9			
Total	2573	[illegible]	1185	863	934	2	63	11		192	294	58	2		2
% Of All		38.0	46.1	33.5	36.3	0.1	2.4	0.4	0.0	7.5	11.4	2.3	0.1	0.0	

Google » Android : Vulnerability Statistics

Vulnerabilities (**4083**) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules
Related OVAL Definitions : Vulnerabilities (7) Patches (88) Inventory Definitions (0) Compliance Definitions (0)
Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

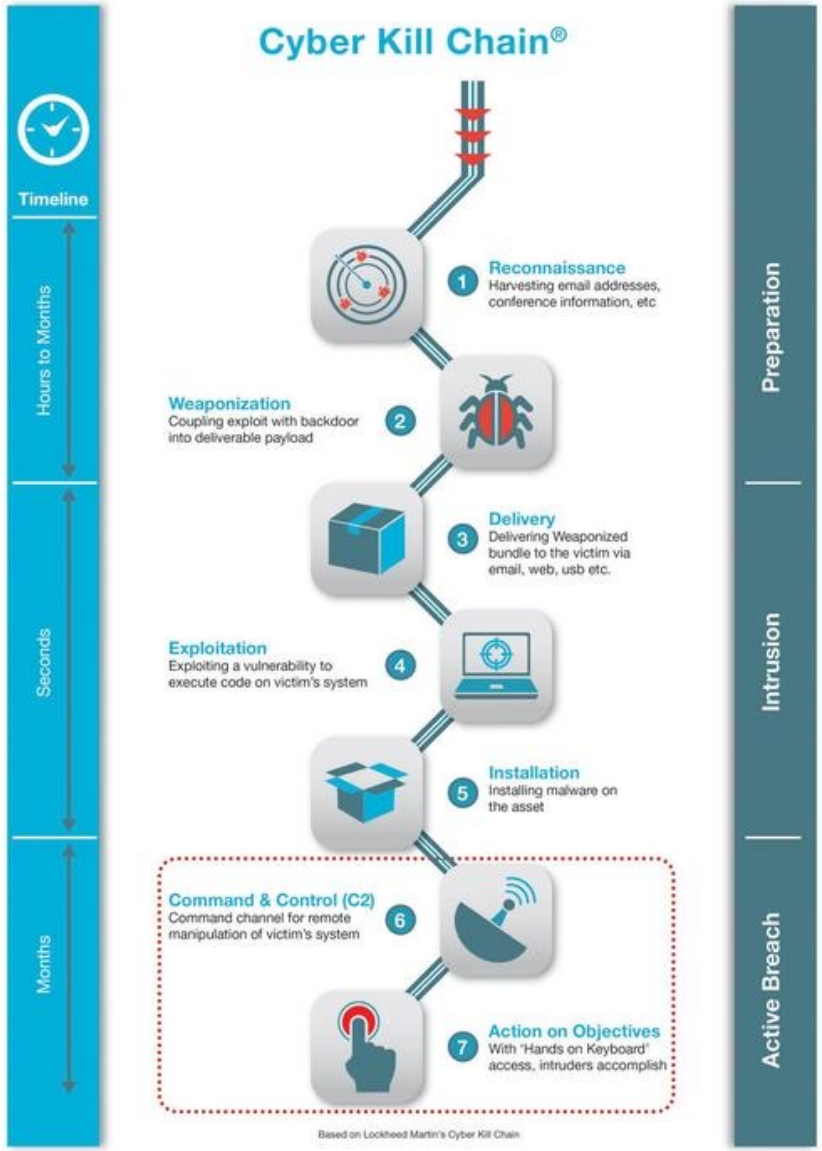
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2009	5	3								1					
2010	1	1	1												
2011	9	1	1		1		1			4	1	3			
2012	7	5	3	2							1				1
2013	4		1	1	1					1	1	1			
2014	12	2	4	1		1				1	2	1			1
2015	95	46	49	50	37					13	14	17			
2016	500	104	72	91	38					47	96	236			
2017	840	86	206	170	32			1		30	113	36			
2018	609	32	84	143	12	2	1	2		17	63	3			
2019	491	37	107	41	24	3		1		39	21	1			
2020	859	46	97	104	27	9		5		148	97	3			
2021	574	28	62	49	40	2		4		55	16	7			
2022	[illegible]	2	[illegible]	4						10	1	2			
Total	4083	[illegible]	693	[illegible]656	212	17	2	13		366	426	310			2
% Of All		9.6	[illegible]	16.1	5.2	0.4	0.0	0.3	0.0	9.0	10.4	7.6	0.0	0.0	

Oltre 2500 vulnerabilità note su iOS ed oltre 4000 su Android

Fonte : cvedetails.com

L’emergenza Mobile Threat

Le fasi di un attacco : la Cyber Kill Chain



Per ogni fase dell’attacco deve essere prevista una specifica line di difesa

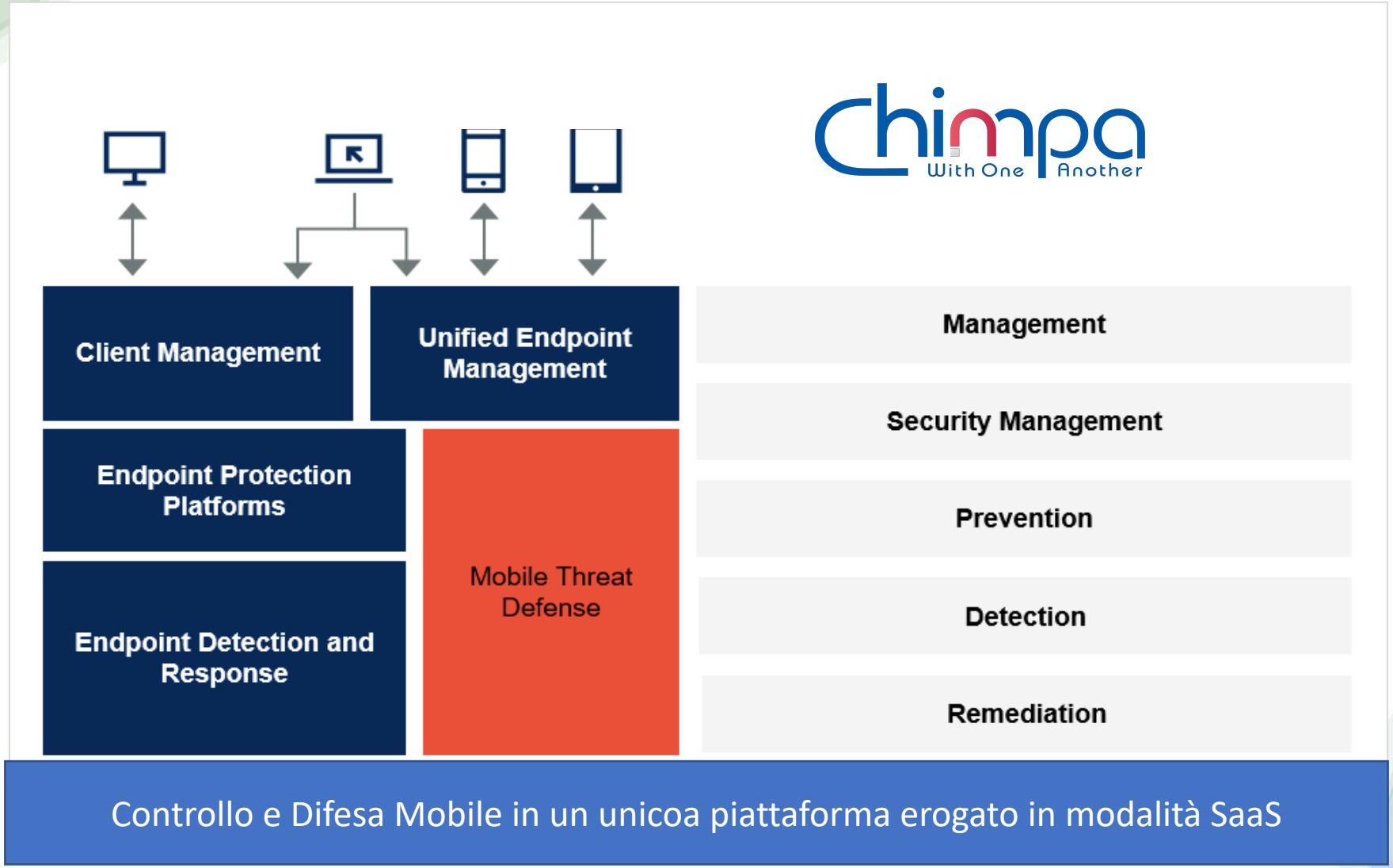
Cyber Intelligence OSINT (MTD)
- *Email*
- *Ip*
- *Domain*

System Hardening (MDM)
- *Passcode policies*
- *Use Restrictions*
- *APP restrictions*

Malware Detection (MTD)
- *Antimalware scan*
- *Anti phishing*
- *Web surf sicuro*

Cyber Threat Intelligence IOC (MTD)
- *IoC policies*
- *Correlazione*
- *Remediation*

La soluzione definitiva e complete MDM + MTD



Soluzione certificata

android enterprise
EMM provider

Validated by
SAMSUNG Knox

Consultants
Network

Sistemi operativi supportati

android

iOS

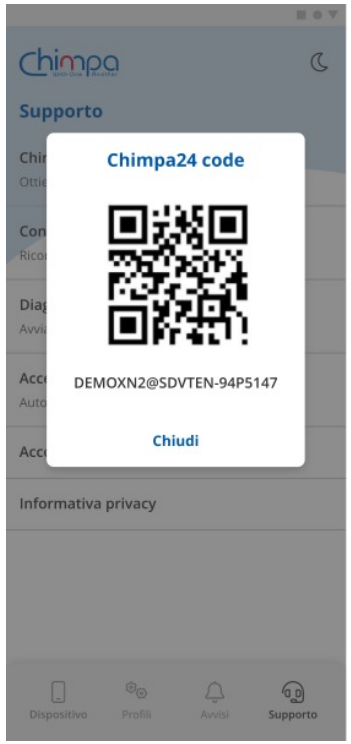
Windows 11

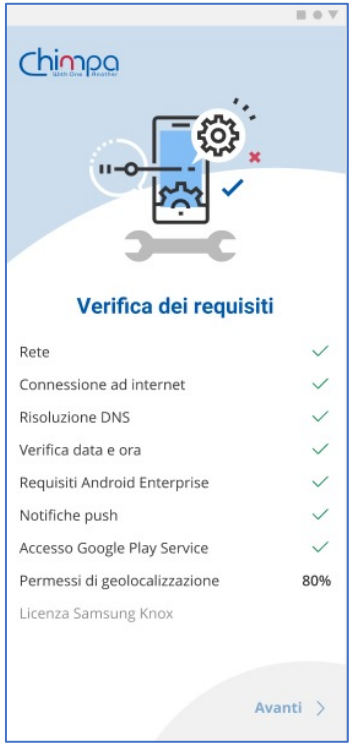
Windows 10

Caratteristiche principali

Configurazione automatica

Chimpa ha un sistema di installazione e configurazione totalmente automatico, grazie al quale l'utente , attraverso un semplice QRcode può far iniziare il processo di installazione e configurazione in maniera totalmente automatizzata e trasparente

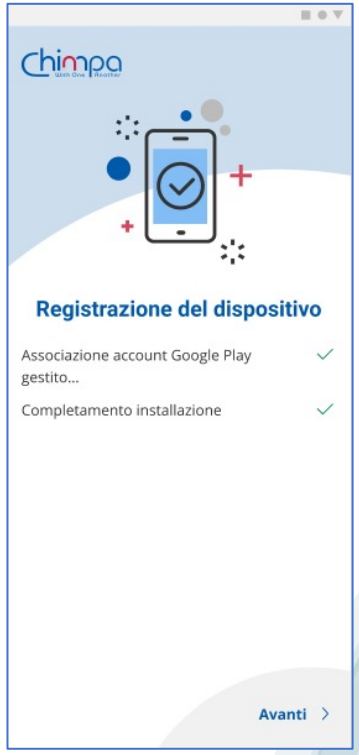




Caratteristiche principali

Facilità d'utilizzo

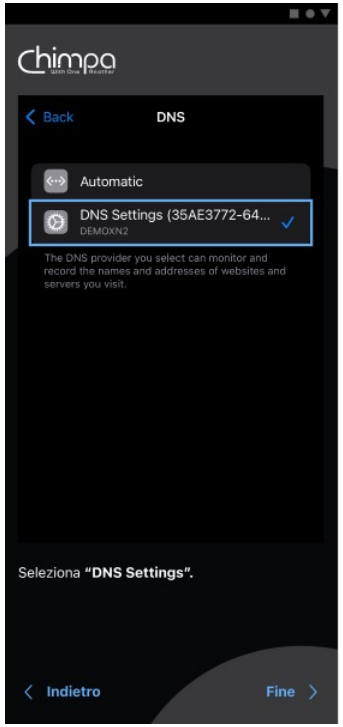
Chimpa dispone di un'interfaccia chiara ed intuitiva che facilità l'utente nella sua gestione . Inoltre grazie alla gestione di più profili di utilizzo , l'utente può gestire in maniera chiara e semplice le diverse funzionalità che Chimpa offre.



Funzionalità principali

Monitoring & Control

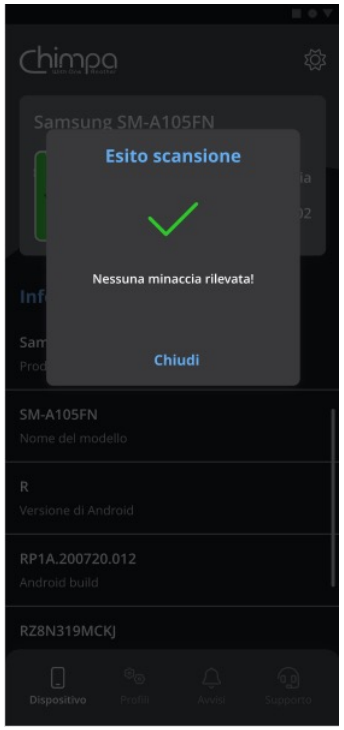
Chimpa ti offre strumenti per monitorare e controllare i principali parametri e l'utilizzo del tuo dispositivo , permettendoti di agire anche a distanza sui dispositivi per esempio in caso di smarrimento o furto

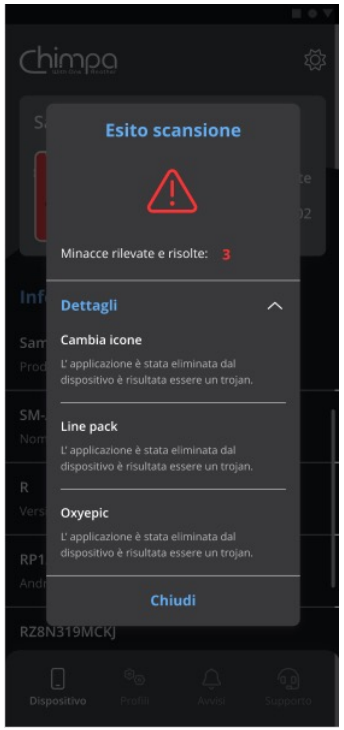


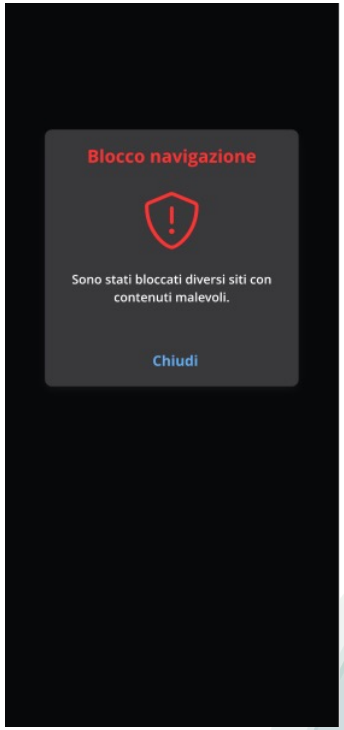
Funzionalità principali

Security

Chimpa protegge i tuoi dispositivi da attacchi di Trojan e Ramsonware grazie a sofisticati sistemi antivirus ed anti phishing. Inoltre rende sicura la tua navigazione , identificando e bloccando i siti malevoli , principale causa di molte truffe on line







Security : main features 1/2

Mobile Threat Defense & Intelligence

1	**Safe Web**	Modulo per la vavigazione sicura sul web capace di bloccare siti potenzialmente malevoli.
2	**Scansione antivirus ed anti malware avanzata**	Scansione di malwares, trojan e ramsonware multi sources
3	**Anti Phishing**	Verifica dell'attendibilità di URL digitati o inviati via sms , email , messaging quali potenzionali vettori di attacchi (pass steeling, phishing ecc) ed eventuale blocco di quelli ritenuti malevoli
4	**Smart Firewall**	Un firewall pre configurato in grado di bloccare le minacce più avanzate sul nascere

Security : main features 2/2

Mobile Threat Defense & Intelligence

5	**Check file hash**	Verifica dell'attendibilità del file scaricato, la verifica deve essere effettuata in maniera manuale (non presente nel continuous monitoring)
6	**TOR Node check**	Capacità di identificare un potenziale indirizzo ip quale TOR exit node
7	**OSINT check compromissions capability**	Ricerca informazioni di eventuali compromissioni da fonti aperte su : ip, files, emails nomi
8	**Creazione e gestione Patters di sicurezza (IOC)**	Permette di personalizzare , attraverso la scelta di indicatori di compromissione (IOC) , i pattern di sicurezza per device singolo , gruppi o tutti

Value proposition

Soluzione UEM basta su cloud che consente di gestire qualsiasi dipositivo basato su Android , iOS e Windows : monitorandoli , controllandoli e proteggendoli dalle intrusioni degli hacker e dal furto di dati atttraverso il suo modulo incentrato sulla difesa dalle minacce «mobile»

Unified endpoint manangement

Zero Touch deployment

Offera SaaS con data center in Italia

Sviluppato in Italia

Offerta modulare

Interfaccia UX web based chiara ed intuitiva

Una soluzione per dispositivi Apple , windows ed Android

La gestione di privacy, policies, apps/contenuti per gli amministratori IT.

Semplifica la distribuzione dei dispositivi iOS, iPadOS, tvOS ed Android anche in modalità ZERO Touch