NTT DATA

SERVIZI E SOLUZIONI PER LA SICUREZZA DEI DEVICE E LA PREVENZIONE DELLE FRODI IN AMBITO MOBILE

ABI - Banche e Sicurezza 2014

28 Maggio 2014

ALBERTO PAGANINI

GIORGIO SCARPELLI

AGENDA

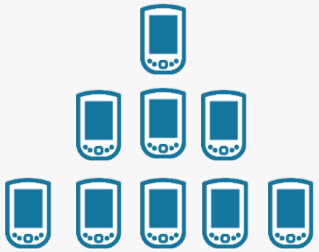
- «MOBILE» SCENARIO
- I RISCHI COMPORTAMENTALI E TECNOLOGICI DA PRESIDIARE IN AMBITO «MOBILE»
- STRATEGIE E SOLUZIONI PER LA SICUREZZA «MOBILE»
- MOBILE APPLICATION RISK MONITORING

DIGITAL & MOBILE TREND

ESPLOSIONE DEI CONNECTED DEVICE

+ 2 Miliardi

L'utilizzo di smartphone nel mondo entro il 2015



+ 3,5%

Il **traffico web mensile** generato da **Mobile**

NUOVE OPPORTUNITA' SUI CANALI DIGITALI

73,9 %

tempo medio speso su un tablet per navigare in internet

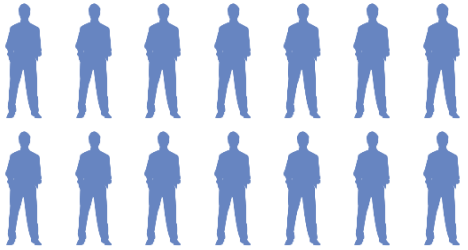
TABLET

25% **Prodotti online acquistati via Tablet da un utente italiano nel 2013**

53%

Popolazione italiana è multicanale

La multicanalità è diventata un fenomeno di massa



78 %

degli utenti utilizza la rete per **confrontare i prezzi** e **cercare informazioni** su prodotti e servizi

90%

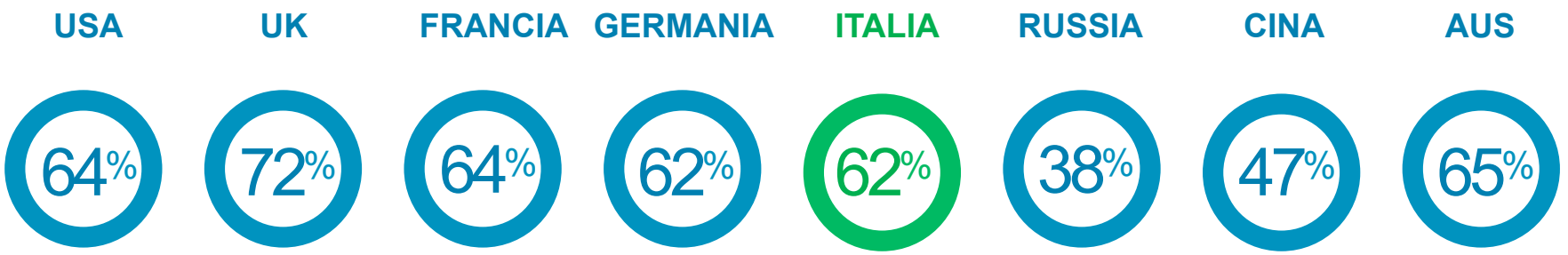
degli **«smartphone shoppers»** utilizza il mobile nelle **attività pre-shopping**

Fonti: Bloomberg.com, Forbes.com, Emarketers.com, Reuters.com, PWC Total Retail 2013

SMARTHPHONE PENETRATION PHENOMENON

Gli ultimi anni sono stati caratterizzati dall'esplosione dei *connected device*.

Penetrazione smartphone nel mondo – Anno 2013



l'Italia vanta medie di penetrazione comparabili a quelle dei principali paesi nel mondo.

Evidenze smartphone penetration

- Miglioramento delle funzionalità mobile per le applicazioni retail
- Adozione di nuove tecnologie mobile da parte dei retailers
- Diminuzione "*Barriers to use*"

Diffusione accessi online in Italia - 2013

- 2,7% PC

Il canale web registra una flessione dell'audience online

+ 28% SMARTPHONE
+ 127% TABLET

Il canale mobile conquista il primo posto della total digital audience

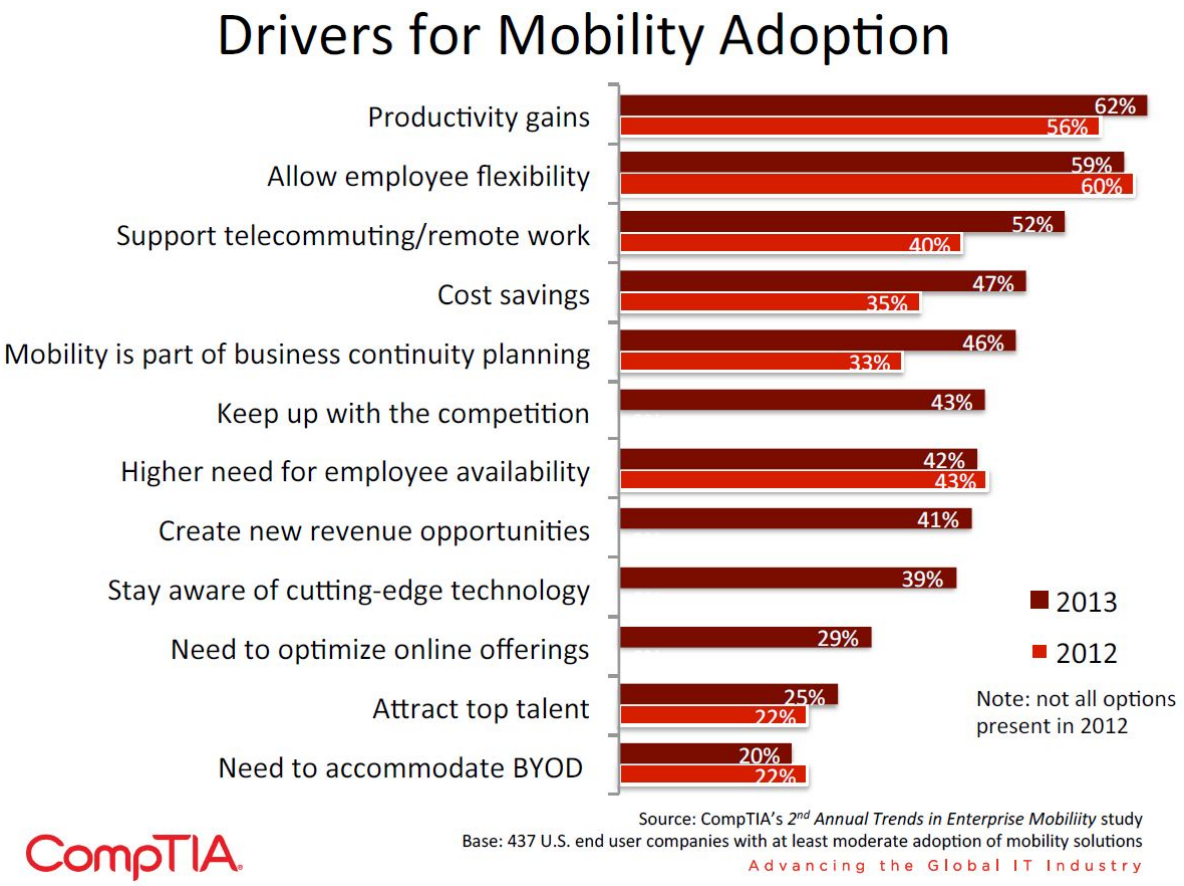
Fonte : Deloitte Digital, The Down of Mobile Internet , Nielsen, Settembre 2013

L'UTILIZZO DEI MOBILE DEVICE ENTRA NEI PROCESSI DI BUSINESS CON NUOVI PARADIGMI

Il **15%** della **forza lavoro** ha **accesso** alle **informazioni aziendali "anytime, anywhere".** Questo numero **triplicherà entro il 2016**. (Forrester Research)

Entro il 2015, I progetti di **sviluppo di mobile app sorpasseranno quelli su PC** in rapporto di 4 ad 1 (Forbes)

Il **valore** percepito per le **enterprise apps andrà sempre più aumentando** (OVUM)



NELLE AZIENDE VENGONO UTILIZZATI I MOBILE DEVICE PERSONALI E AZIENDALI RENDENDO PIU' COMPLESSA L'IMPLEMENTAZIONE DI MISURE DI SICUREZZA EFFICACI

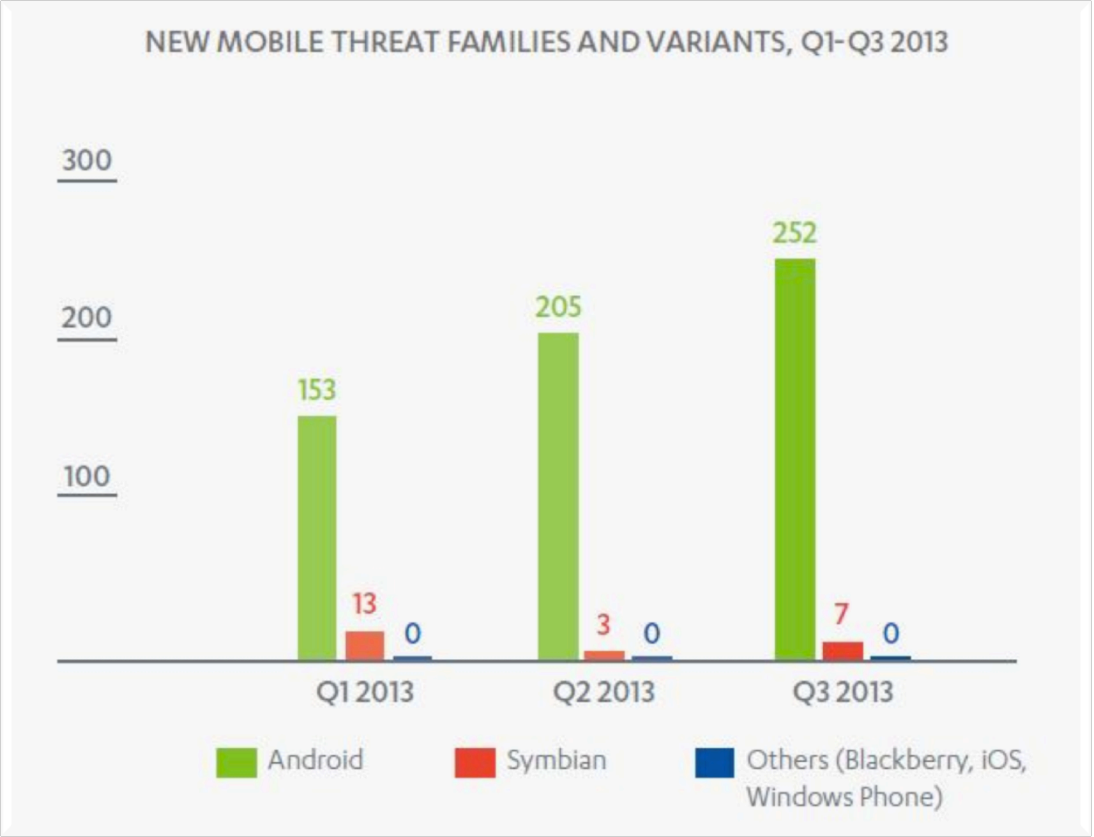
Aumento utilizzo device mobili nel contesto aziendale:

- ***BYOD***
- ***COPE***

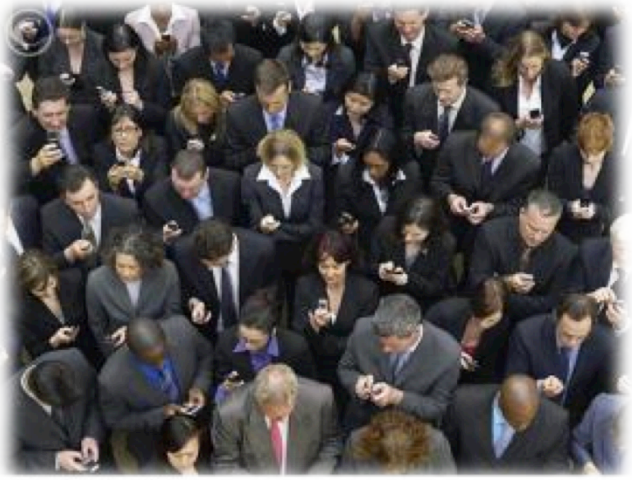
Opportunità VS Rischio per le Aziende

IL CYBER CRIME PUO' FAR LEVA SU VULNERABILITÀ TECNOLOGICHE DEI MOBILE DEVICE PER VIOLARE LE DIFESE AZIENDALI

- **Aumento** dei **Malware per mobile platforms** (in particolare Android)
- Incremento **black / grey markets per dati utente rubati** che porterà ad una crescita di information stealing Malware (ENISA threat landscape - 2013)
- **Più del 20 % delle App** in circolazione presentano **vulnerabilità nell'accesso a dati personali** (Kaspersky)



ALLE VULNERABILITÀ TECNOLOGICHE SI AGGIUNGONO QUELLE «COMPORTAMENTALI» DEI MOBILE USERS



Il **comportamento** dei Mobile end-users diventa **sempre più destrutturato**

Le **vulnerabilità "comportamentali"** rappresentano spesso il **punto di innesto di attacchi** cyber-criminali

VULNERABILITÀ COMPORTAMENTALI - VISUALITY

"superficialità" nell'analisi dei contenuti, perdita dell'abilità di analizzare i dettagli

Ridirezione del mobile **browsing** dell'utente verso malware web sites

Istallazione inconsapevole di **App fake** (repackaged)

Fake advertising

Mascheramento di **codice malevolo** all'interno di immagini o filmati

VULNERABILITÀ COMPORTAMENTALI - IMPATIENCE

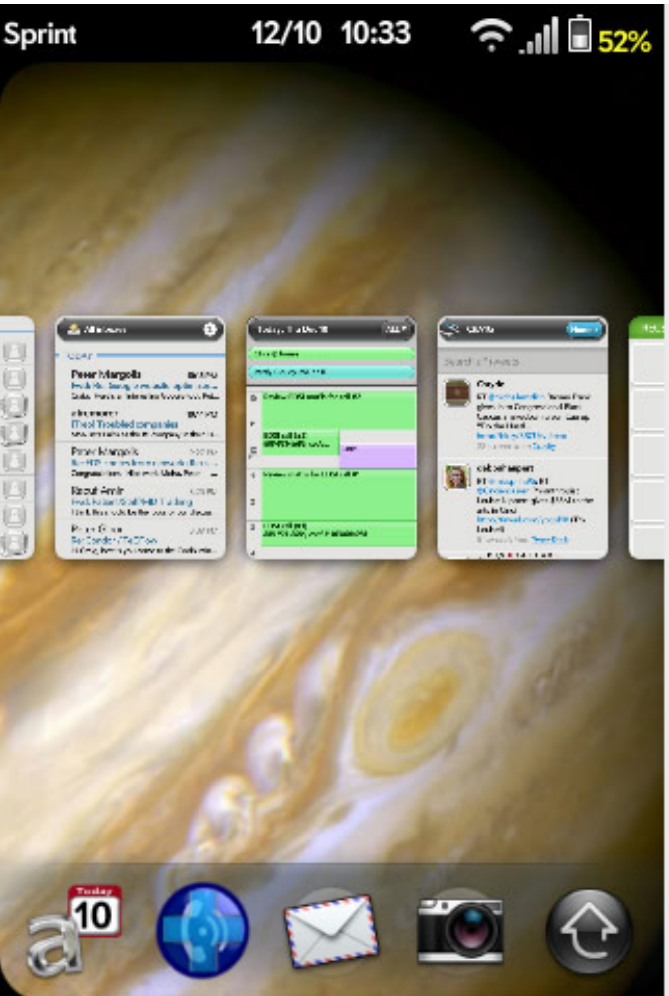
Aspettativa di una gratificazione istantanea

Esecuzione di **malicious code** indotto dal **desiderio di concludere rapidamente un'operazione**

Sottomissione di **molteplici form** per registrarsi ad un servizio per **indurre** l'utente a **rivelare informazioni non necessarie**, che vengono fornite pur di arrivare velocemente alla fine del processo

VULNERABILITÀ COMPORTAMENTALI - MULTI TASKING

Minore focus ed attenzione a cosa si sta facendo



Background Apps lasciate «girare» senza controllo e «dimenticate»

Decisioni prese o azioni eseguite **inconsciamente**

VULNERABILITÀ COMPORTAMENTALI - COMPLUSIVITY

Acquisizione di comportamenti compulsivi da assuefazione all'uso

Gestualità «inconscia» che potrebbe essere sfruttata per indurre l'esecuzione inconsapevole di malware

Decisioni prese «**on-the-fly**» senza comprendere esattamente cosa si stia realmente facendo (es. a fronte della ricezione di un SMS di Spamming)

VULNERABILITÀ COMPORTAMENTALI - ANONYMOUS AND IMPERSONAL RELATIONS

de-responsabilità, diminuzione dei limiti etici

Maggiore apertura ed «estroversione», minor controllo dell'informazione trasmessa

Diminuzione del livello di **controllo**

Crescenti attitudini ad assumere rischi

Sensazione di libertà nel fornire valutazioni e informazioni confidenziali, diventando inconsapevolmente «confidenti» dei criminali informatici

VULNERABILITÀ COMPORTAMENTALI - OVEREXPOSURE

Desiderio di visibilità

Divulgazione «volontaria» di informazioni personali / confidenziali, non importa «chi può vedere»

Contributo a rendere efficace **«l'open-source intelligence»**

VULNERABILITÀ COMPORTAMENTALI - TRUST

Fiducia eccessiva negli altri

Si **crede** che le persone stiano esprimendo le loro vere attitudini quando si dichiarano

I criminali informatici stabiliscono una **relazione di fiducia** con la **vittima** da cui ottengono informazioni personali

VULNERABILITÀ COMPORTAMENTALI - IGNORANCE

Mancanza di conoscenza delle policy di sicurezza

Conoscenza inadeguata di policy di sicurezza e difficoltà nell'implementazione di adeguate contromisure

Pigrizia e noia nel leggere e studiare procedure di sicurezza online

VULNERABILITÀ COMPORTAMENTALI - DEALS

Entusiasmo ad ottenere riconoscimenti gratuiti

Tentazione di fare un **grande affare**

Inserimento di informazioni relative a **dati sensibili** quali il numero di carta di credito o password

Molte volte dietro un grande affare si nasconde un **inganno**

VULNERABILITÀ COMPORTAMENTALI - COMPASSION

Desiderio di essere utili

Molti inganni sono fondati sul sentimento di **compassione**

Creazione di campagne di **sensibilizzazione** da parte di pirati in cui sono richieste donazioni

Contributi di **beneficienza** col fine apparente di **aiutare** persone in difficoltà sono sfruttate per frodare o carpire informazioni sensibili

VULNERABILITÀ COMPORTAMENTALI - AUTHORITY

Eccessiva fiducia nelle autorità

Senso del dovere verso le “autorità” che possono essere istituzioni finanziarie o governative, ecc.

Concessione di dati personali in risposta ad email inviate da (**false**) **autorità**

VULNERABILITÀ COMPORTAMENTALI - FEAR

Eccessiva paura di incorrere in perdite

Paura di essere truffati durante una connessione Web

Molti criminali informatici **fingono di proteggere** l'utente

L'utente è indotto a **fornire dati personali** e confidenziali su se stessi o istallare misure di sicurezza «fake»

QUESTO INNESCA ESIGENZE SPECIFICHE LEGATE A TEMI DI SICUREZZA E CONTROLLO …

Le minacce **coinvolgono tutte le tipologie di end-users**

...MA ANCHE ESIGENZE DI SEMPLIFICAZIONE DEGLI STRUMENTI DI GESTIONE E CONTROLLO

Elevata complessità e **frequenza** delle azioni necessarie per mantenere sicuro un end-point.

Anche gli **utenti più sensibili** corrono il rischio di **compromissione dei device**

Device compromessi possono diventare inconsapevolmente parte di **sofisticati** schemi di attacco **cyber-criminali**

IMPATTI SUL CONTESTO BANCARIO: LE FRODI MOBILE

Target primario:
Indurre l'istallazione di software malevolo

Possibili Attività malevole:

- OTP SMS Stealing
- Invio di SMS «premium rate» per conto dell'utente
- Furto dei «Transaction Authentication Numbers»
- Impersonificazione dell'utente
- Partecipazione a BotNet
- Pubblicità ingannevole
- Controllo completo del device

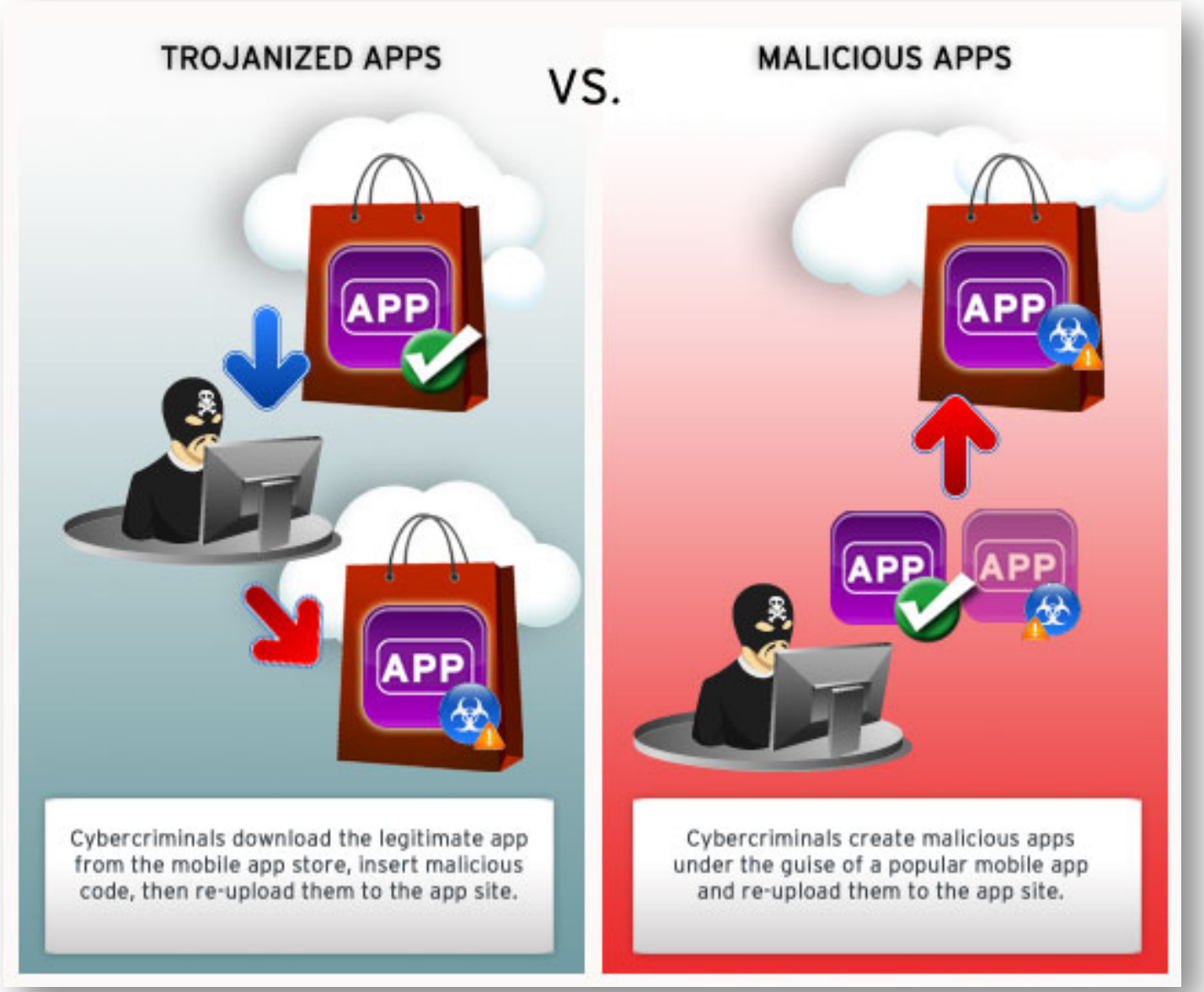
Example

France - Oct 2012 - 20-year-old hacker using fake Android apps, established a virus on 17,000 users' smartphones to send premium rate SMS messages. $650,000 (€ 500,000) within 8 months.

http://www.frandroid.com/actualites-generales/117583_six-mois-de-prison-ferme-pour-notre-hacker-national-damiens/

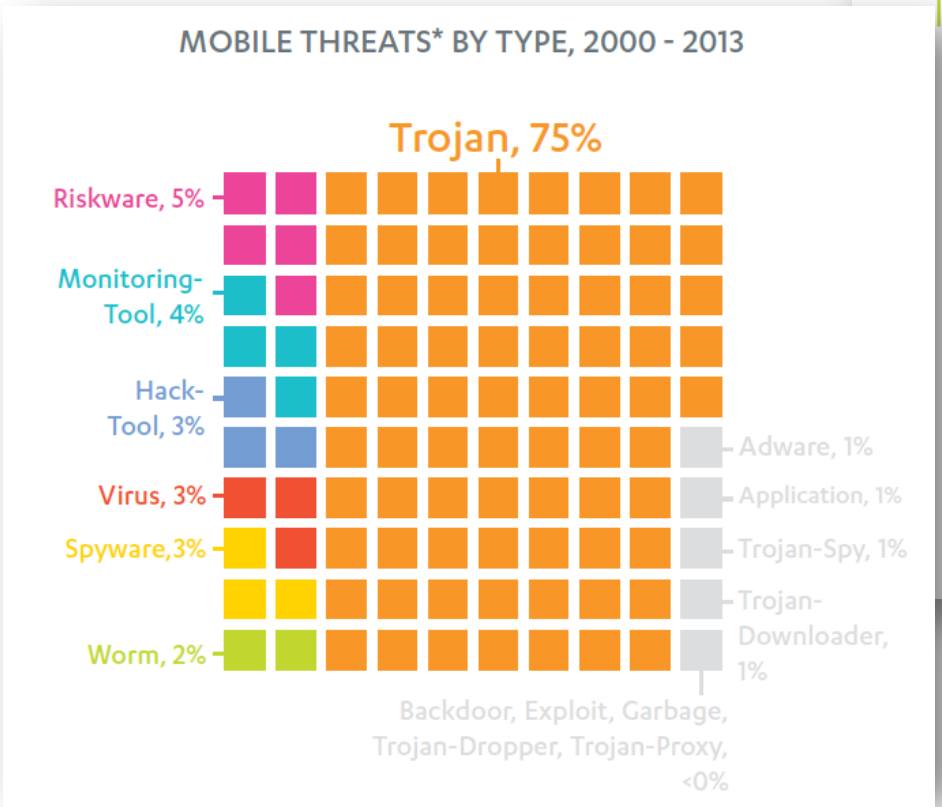
Source: *APWK: Mobile Threats and underground marketplace – May 2013*

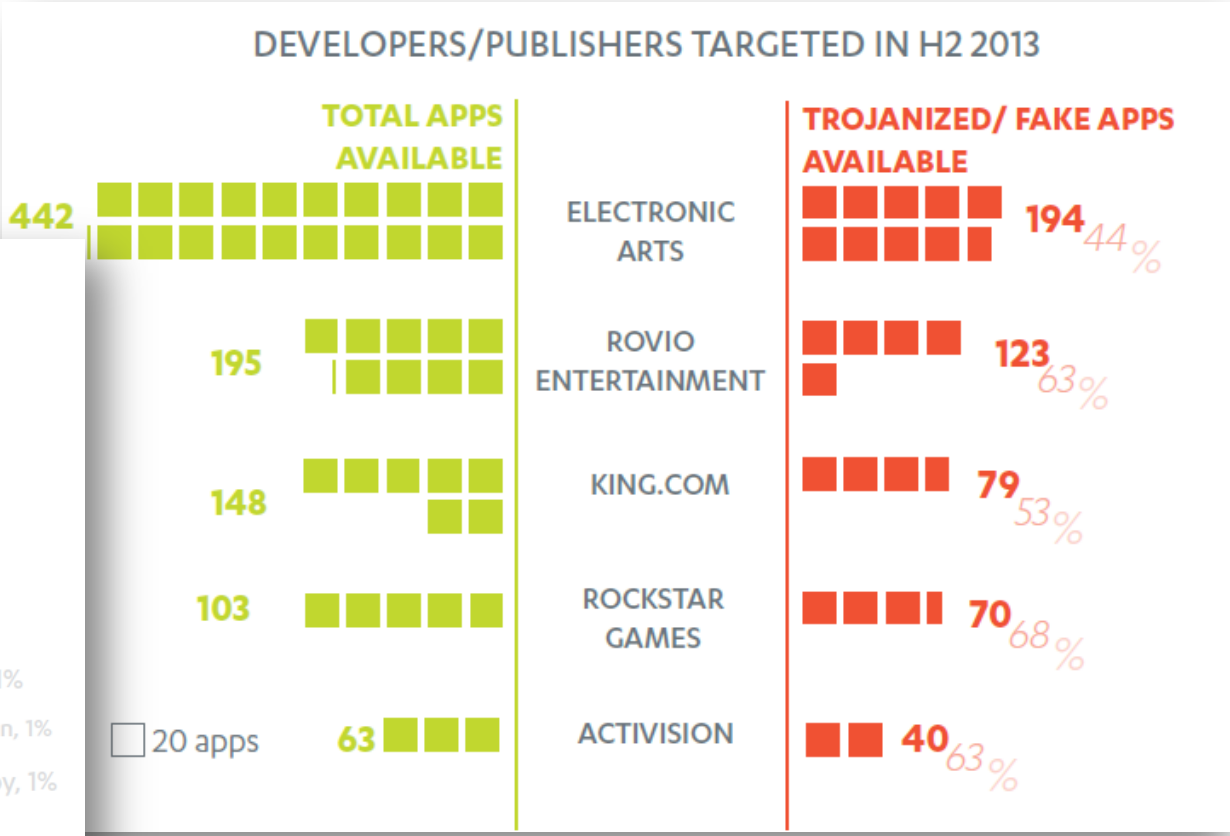
LE MINACCE SI ANNIDANO NELLE APP...



...IL FENOMENO HA UNA RILEVANZA SORPRENDENTE...

I produttori di malware puntano sulla popolarità delle App per allargare il target di potenziali vittime (soprattutto giochi, scommesse, ecc) ma spesso **sviluppano azioni mirate sulle App di un particolare istituto di credito, puntando sulla «credibilità» del brand**





Source: F-Secure Threat Report 2H 2013

... E RIGUARDA UN'AMPIA TIPOLOGIA DI APP

TOP 8 PLAY STORE APPS TARGETED FOR REPACKAGING

CANDY CRUSH SAGA
package: com.king.candycrushsaga
Signed by *King.com* — 17%

CLASH OF CLANS
package: com.supercell.clashofclans
Signed by *Supercell* — 10%

SLOTOMANIA – FREE SLOTS
package: air.com.playtika.slotomania
Signed by *Playtika* — 23%

POCKET EDITION
package: com.mojang.minecraftpe
Signed by *Mojang* — 12%

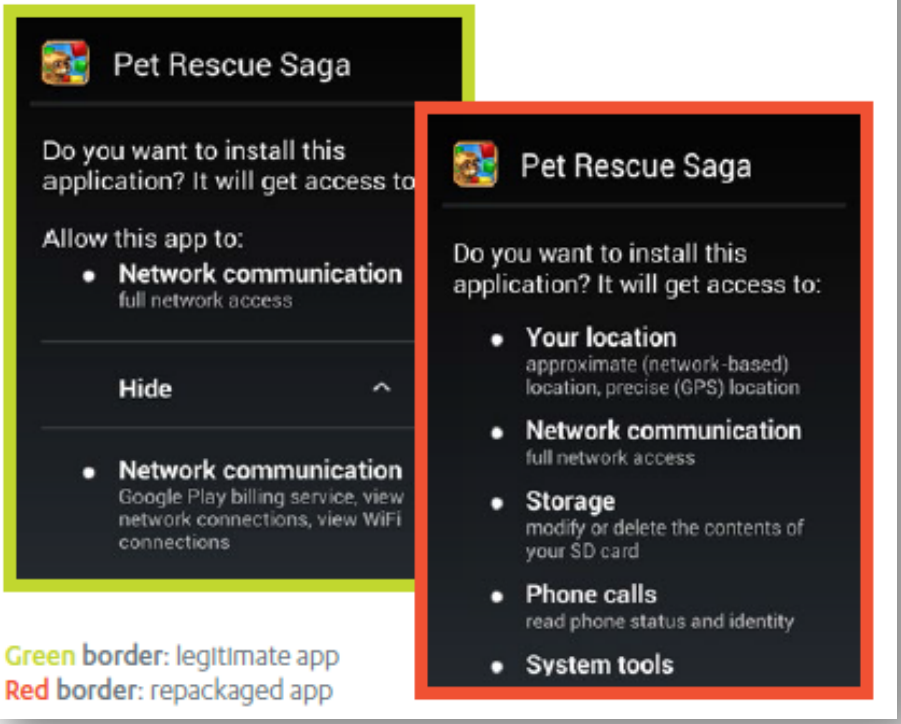
CASTLE CLASH
package: com.igg.castleclash
Signed by *Kabam* — 11%

DOUBLEDOWN CASINO – FREE SLOTS
package: com.ddi
Signed by *Double Down Interactive, LLC* — 33%

KNIGHTS & DRAGONS
package: com.iugome.lilknights
Signed by *Gree, INC* — 8%

PET RESCUE SAGA
package: com.king.petrescuesaga
Signed by *King.com* — 8%

PERMISSIONS REQUESTED BY A REPACKAGED APP, VERSUS THE LEGITIMATE APP



Green border: legitimate app
Red border: repackaged app

% of samples of this app found in H2 2013 that are repackaged versions distributed in third-party martkets

Source: F-Secure Threat Report 2H 2013

GLI STRUMENTI MALWARE SONO DISPONIBILI SUI BLACK MARKETS A PREZZI ACCESSIBILI ...

Sample Toolkits & Service	Price (US$) - March 2013	Example Descriptions
Mobile intrusion (keyloggers)	Open Source - 400	Java & Python Keyloggers, Mobistealth,
Mobile Intrusion (surveillance)	500 – 5,000	Re-engineered Finfisher, Finfisher Lite & FlexiSpy extended copies
Mobile malware for banking theft	10,000 – 30,000	Eurograbber, ZitMo, Tinba Trojan, DroidCleaner, Citadel (inc. PtH capabilities)
Mobile botnet (rental)	50 - 400	Hourly rates
Mobile botnets (operational & tailored source code)	4,000 - 30,000	Mobile ISP service, SMS, & Drive by
Mobile malware for black SEO and underground partnership programs	5,000 – 10,000	Used to traffic redirects, J2ME midlets, or standard applications for the popular platforms.
Mobile traffic by targeted country	10 – 30 per 1,000 hosts	Can be bought through special underground services (by area, by country)
Mobile SMS spam service	2-8 cents per 1 SMS	Mobile spamming
Mobile SMS spamming tool	30-50	SMS spamer by klychev v0.3
Mobile flooder (Skype or SIP)	30-80	Skype Flooder

Source: *APWK: Mobile Threats and underground marketplace – May 2013*

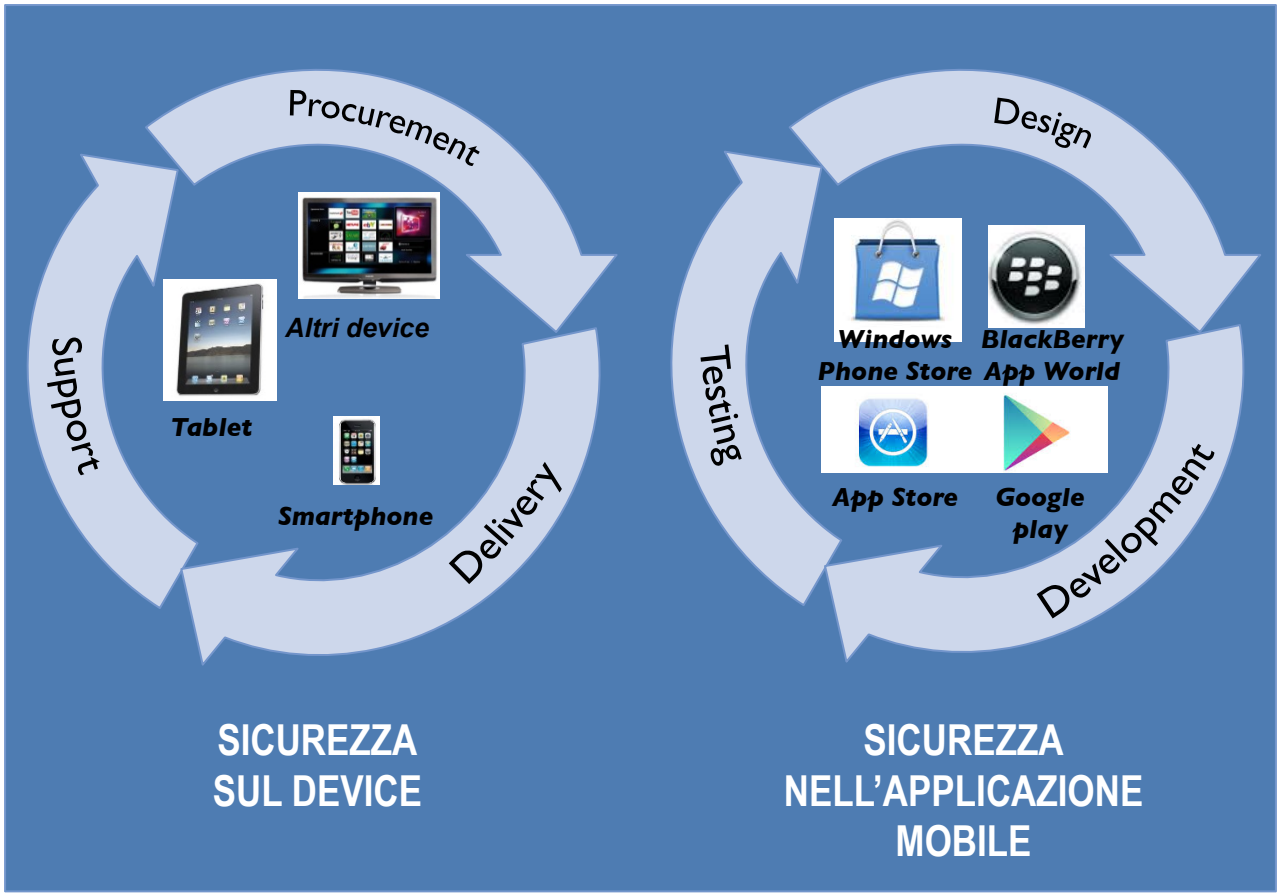
IMPLICAZIONI E RESPONSABILITÀ DEGLI ISTITUTI BANCARI

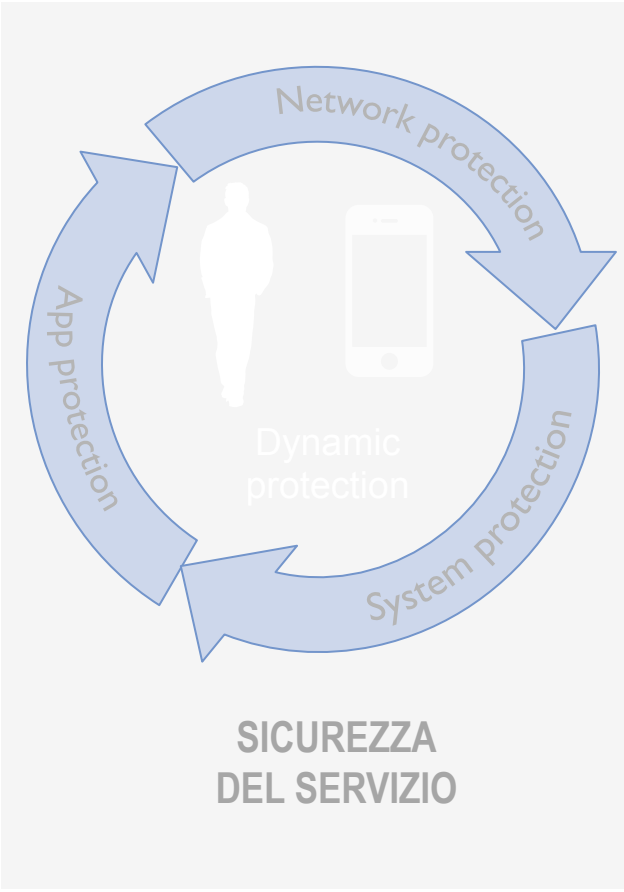
In base alle normative vigenti, gli Istituti di Credito quasi sempre sono costretti a **risarcire i danni a meno che non riescano a dimostrare** inequivocabilmente **la negligenza o la fraudolenza del cliente**. Che comunque parte sempre in vantaggio e con la legge dalla sua parte.

Recenti sentenze giudiziarie su casi di controversia fra banca e cliente per operazioni non autorizzate o fraudolente hanno quasi sempre dato ragione a quest'ultimo, riconoscendo d'ufficio la responsabilità dell'istituto di credito. Nel dubbio, si presume sempre che la responsabilità sia a carico della banca.

Lo dimostrano le **sentenze** del tribunale di Nicosia per u**n caso di pharming**, quella del tribunale di Palermo in un **caso di sottrazione di credenziali di accesso** e della Corte di Cassazione in un **caso di furto d'identità**, nonché il provvedimento del Garante Privacy nei confronti di un istituto di credito in un caso di **accesso non autorizzato a dati personali**.

STRATEGIA DI SICUREZZA «MOBILE»





QUALE RISPOSTA DARE

E’ necessario lo sviluppo di un modello di difesa integrato , che operi su tutti i fattori di rischio

Per un’efficace strategia di sicurezza Mobile è necessario:

Sviluppare Apps applicando criteri di **Secure Development**

Proteggere i dati e segregare le App critiche all’interno di **blinded execution environment**

Evitare che l’**utilizzo promiscuo** dei device possa **estendere ad App critiche le vulnerabilità** indotte **dall’utilizzo privato** del device

Monitorare la **diffusione di fake apps** nei black markets

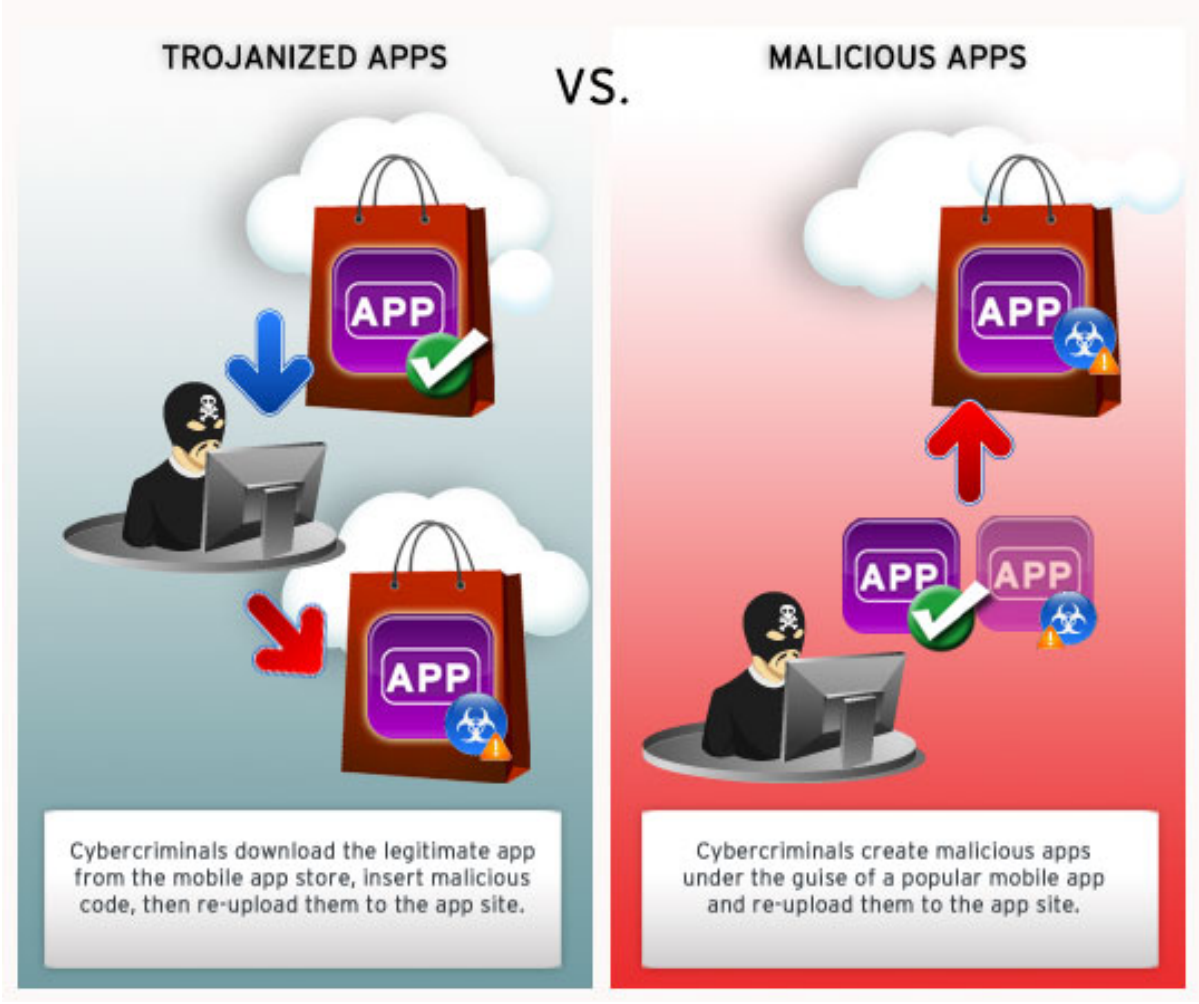
Supportare l’End-users per accrescere la sua **Security Awareness** ed il rispetto delle **Security policy**

Source: OWASP/ENISA Mobile Security Project

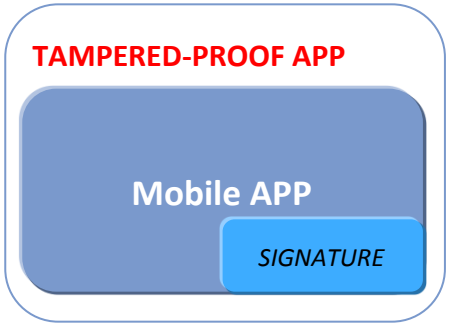
STRUMENTI PER LO SVILUPPO DI «MOBILE» APP SICURE

Le **vulnerabilità** delle **APP** dipendono **solitamente** da:

- **Sviluppo** APP **non corretto** o che **non tiene conto delle Security best practice**
- **Tampered APPs / Origine non controllata**

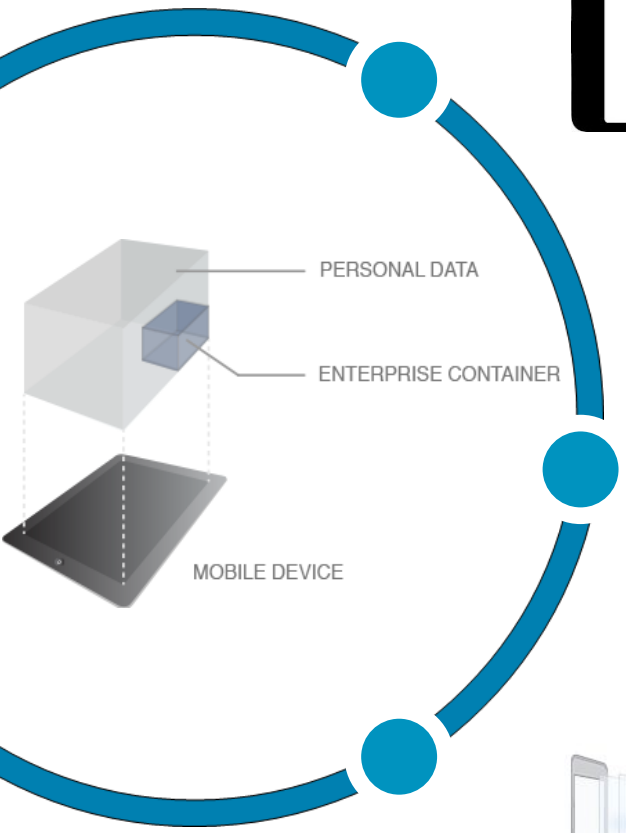


Possibili contromisure



- Anti-tampering libraries
- Anti reverse-engineering libraries
- Obfuscation
- Secure Coding / Secure App deployment

UTILIZZO DELLA CONTAINERIZZAZIONE PER PROTEGGERE I DATI CRITICI

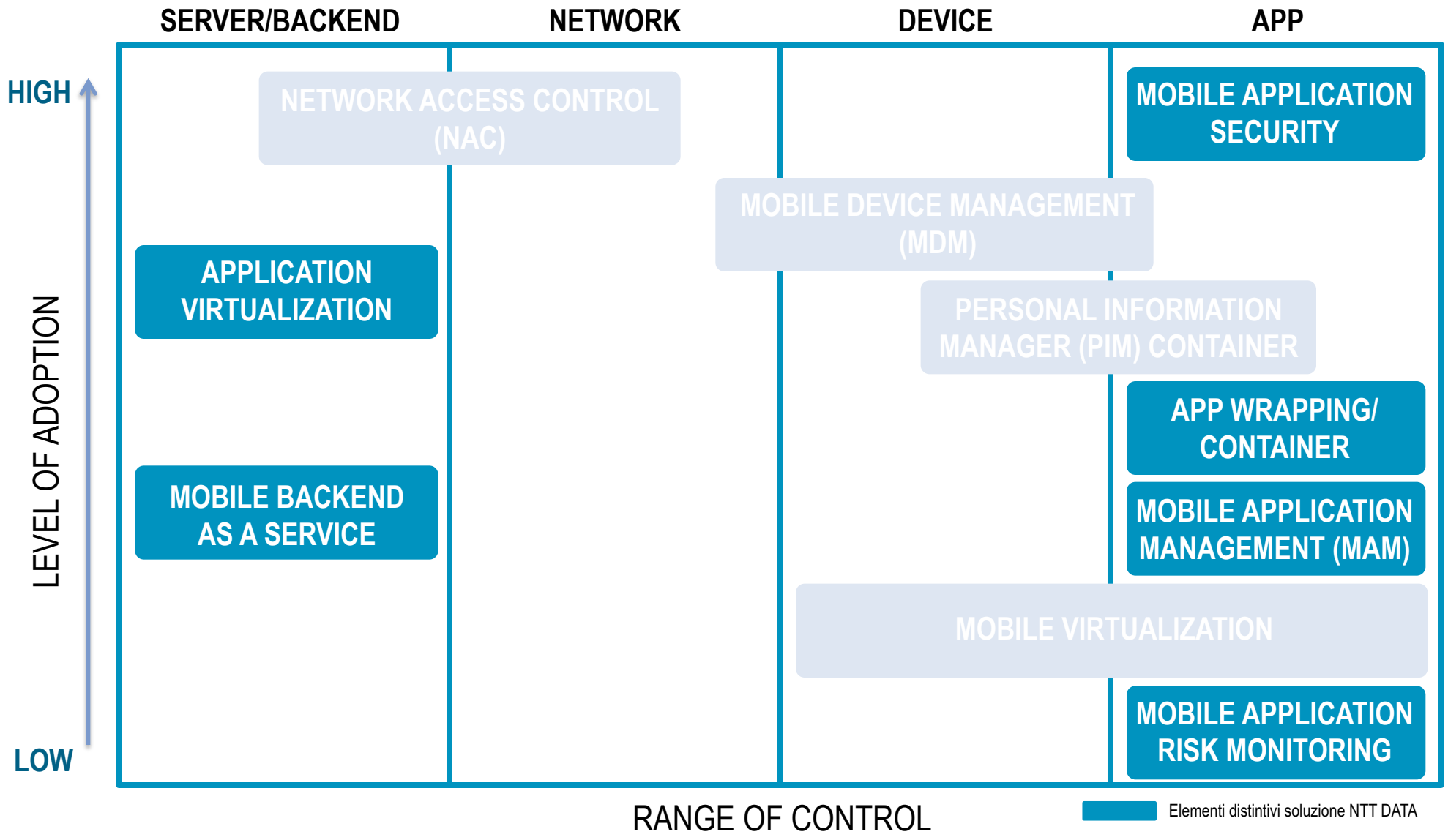


Creazione di uno ***spazio criptato***, o folder, in cui i dati di alcune applicazioni possono essere conservati

Creazione di un ***protective "app wrapper"*** che crea una “bolla sicura” intorno a ciascuna applicazione ed ai dati associati da proteggere

Sviluppo di un ***mobile hypervisor***, che crea un container virtuale sul device dove possono risiedere e cooperare molteplici applicazioni

SOLUZIONI DI SICUREZZA «MOBILE»



Fonte: 451 Group

LA SOLUZIONE NTT DATA: DYMORA

DyMoRA

NTT DATA

Dynamic Mobile Resource Access

- *Flexible Mobile Privileges Management*
- *Policy Engine for mobile resources utilization*
- *Context-aware Policy enforcement on mobile devices and Apps*
- *Protected running environment for Mobile Apps and Data, separated by private area*
- *Enterprise authentication and authorization integrated with already in place IT security infrastructures and processes*

IL LIVELLO DI CONTROLLO RICHIESTO

GESTIONE INTEGRATA DELLE POLICY

IMPLEMENTAZIONE PERVASIVA E CONTESTUALIZZATA DEI CONTROLLI

PARAMETRI CONTESTUALI CHE DETERMINANO L'APPLICAZIONE DELLE REGOLE

COSA SONO ?
A CHI APPARTENGONO ?
PER QUALE UTILIZZO SERVONO?
COS'HANNO ISTALLATO ?

CHI È ?
CHE MOMENTO È ?
COSA VUOL FARE ?
COSA E' AUTORIZZATO A FARE ?
QUALI SONO LE SUE ABITUDINI ?
CHE COMPORTAMENTO ASSUME ?
QUANTO E' ATTENTO ALLA SICUREZZA ?

DOVE CI SI TROVA ?
A COSA SI E' CONNESSI ?
CHI C'È VICINO ?
CON COSA SI INTERAGISCE ?
A CHE SCOPO CI SI TROVA QUI ?

CONTEXT,
PROFILE,
BEHAVIOURAL,
RISK BASED
RULE ENGINE

DYMORA AT A GLANCE

DyMoRA
Dynamic Mobile Resource Access

Innovative solution for <u>Business</u> and <u>Private</u> Security

Gestione dinamica dei **parametri di sicurezza** su **molteplici scenari di utilizzo** dei dispositivi mobili

Rilevazione immediata dei **cambiamenti** dello **scenario** e conseguente applicazione delle policy di sicurezza più opportune

Regole definite **centralmente da** una **Console** (anche in cloud)

Policy applicabili in funzione di criteri quali: **identità** dell'**utente** corrente, la **configurazione** del **dispositivo**, i **privilegi di accesso** associate al **profilo** dell'utilizzatore, il **tipo di connettività** usato, le **fasce orarie**, la **posizione**, etc..

COSA POSSIAMO OFFRIRE PER LE ESIGENZE DI SICUREZZA SUL MOBILE DELLE AZIENDE: OFFERTA ENTERPRISE

Consente uso dello **stesso device per scopi di lavoro e privati (BYOD/COPE)**

Utilizzo multi-users di un singolo device **regolato centralmente in base a policies di sicurezza e privilegi**

Autenticazione centrale su Enterprise directory (i.e Active Directory) e Single Sign-on

Garantisce **sicurezza e privacy dei dati** personali ed aziendali;

Agevola gli utenti a **rispettare le policy di sicurezza aziendale in ogni contesto di utilizzo**

COSA POSSIAMO OFFRIRE PER LA PROTEZIONE DEL CONSUMER: OFFERTA FAMILY

Da una semplice consolle di gestione …

… il controllo delle esigenze di tutta la famiglia

Protected, privacy proof environment for:

- Call/SMS
- Sharing Pictures and Videos
- Download Music, Games
- Using Instant messaging
- Going online, browsing
- Accessing Social Network, …

Controlled environment for:

- Games
- Entertainment
- Etc.

Cloud based services for:

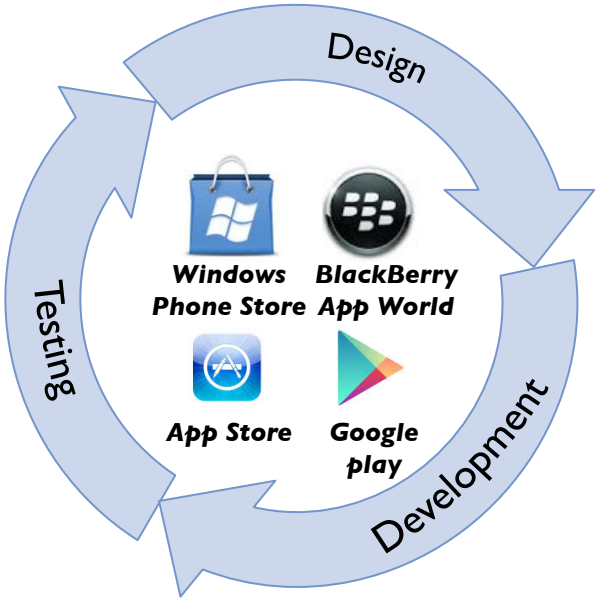
- Parental Control
- Secure and Private Call/SMS
- Secure and private Email
- Segregated environment for Entertainment, Music, games, social
- Secure Camera
- Secure Web browsing
- Security check-up for Mobile environment
- Etc.

Easy and protected environment for:

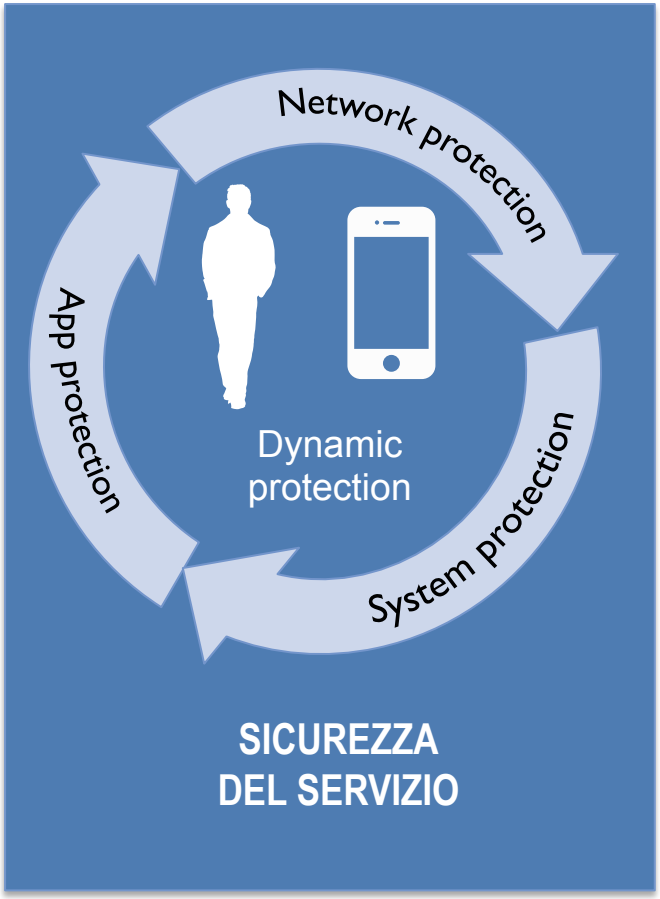
- Rapid call
- Entertainment
- Etc.

STRATEGIA DI SICUREZZA «MOBILE»

SICUREZZA SUL DEVICE



SICUREZZA NELL'APPLICAZIONE MOBILE



SICUREZZA DEL SERVIZIO

UN MODELLO DI PROTEZIONE EVOLUTO INTEGRA IL MOBILE APPLICATION SECURITY MONITORING CON IL DYNAMIC POLICY ENFORCEMENT

NTT DATA e Poste Italiane sono partner del Distretto Tecnologico **Cyber-Security**, iniziativa del MIUR relative al Programma Operativo Nazionale Ricerca e Competitività 2007-2013 per attività di Ricerca Industriale.

In questo contesto, si sta realizzando la **convergenza** della **soluzione MASM** di Poste Italiane per il **monitoraggio continuo** della **Sicurezza Mobile con** la soluzione **DYMORA** di NTT DATA per l'utilizzo sicuro e il controllo delle risorse mobile

Implementazione di un ***RISK-BASED POLICY ENGINE*** che permette di impostare le modalità di utilizzo delle risorse «Mobile» in funzione del **rischio stimato dinamicamente nel contesto**

Fattori di rischio considerati sono:

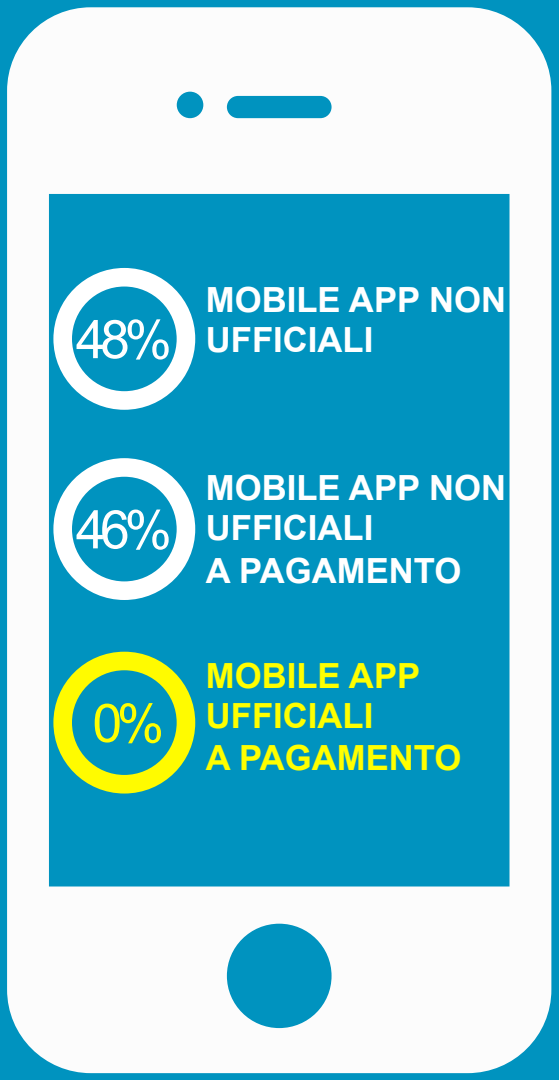
- **Caratteristiche** del **Device** e delle **APP istallate** (analisi statica e dinamica)
- **Condizioni** di **utilizzo** (dove, come)
- **Comportamento** dell'**utente** (finalità, sensibilità alla sicurezza, etica personale, ...)

Lo **score di rischio** determinato permetterà di:

- Fornire un **servizio di alert real-time**
- Effettuare l'**enforcement delle policy più opportunto**

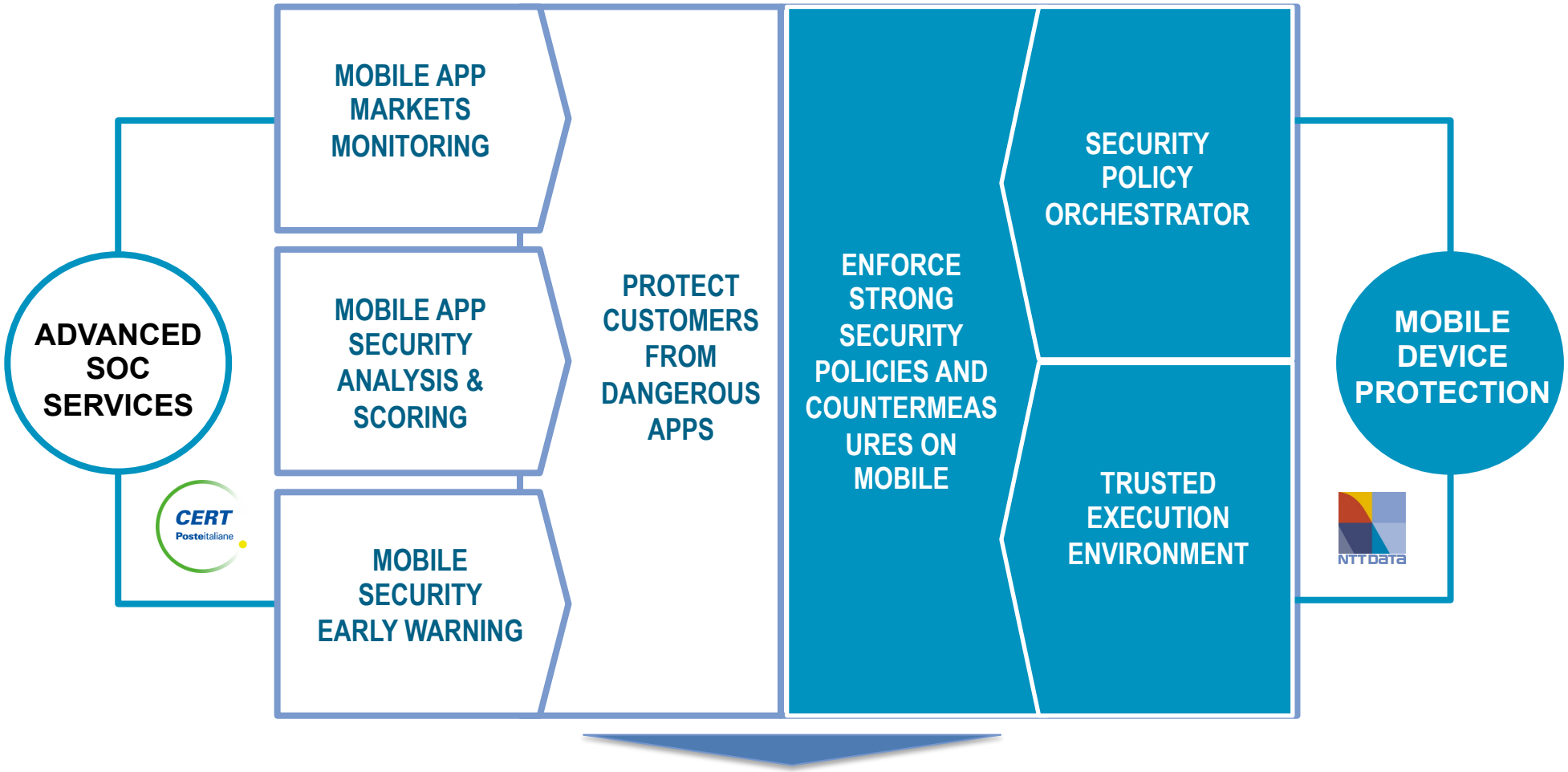
L'ESPERIENZA DI UN PRIMARIO SERVICE PROVIDER ITALIANO

MOBILE APPLICATION SECURITY MONITORING



NTT DATA

IL MODELLO DI CONTRASTO DELLE FRODI SUL MOBILE DATO DALL'INTEGRAZIONE DEI SERVIZI



STRENGHTEN MOBILE APPS, SECURE THEIR DISTRIBUTION AND CONTROL THEIR UTILIZATION BY REPORTING AND REMOVING DANGEROUS ONES

IL MODELLO DI CONTRASTO DELLE FRODI SUL MOBILE DATO DALL'INTEGRAZIONE DEI SERVIZI

CARATTERISTICHE

ADVANCED SOC SERVICES

CERT Posteitaliane

- **MOBILE APP MARKETS MONITORING**
- **MOBILE APP SECURITY ANALYSIS & SCORING**
- **MOBILE SECURITY EARLY WARNING**

AMBIENTE DI DISTRIBUZIONE/ ESECUZIONE **CONTROLLATO** DELLE APP FINANZIARIE

MONITORAGGIO ANTIFRODE VERSO UTENTI FINALI/ISTITUTI FINANZIARI

IDENTIFICAZIONE APP FAKE NEI (BLACK) MARKETS

PERMISSION DI ESECUZIONE/ ALERT IN BASE ALLO **SCORE DI RISCHIO** NEL CONTESTO DI UTILIZZO

RICONOSCIMENTO DELLE CONTROPARTI COINVOLTE NELLE TRANSAZIONI MOBILE DA UNA **TERZA PARTE «TRUSTED»**

- **SECURITY POLICY ORCHESTRATOR**
- **TRUSTED EXECUTION ENVIRONMENT**

MOBILE DEVICE PROTECTION

NTT DATA

STRENGHTEN MOBILE APPS, SECURE THEIR DISTRIBUTION AND CONTROL THEIR UTILIZATION BY REPORTING AND REMOVING DANGEROUS ONES

SICUREZZA E VALORE PER IL CLIENTE

MOBILE SECURITY: SO WHAT

TRAINING

AWARENESS