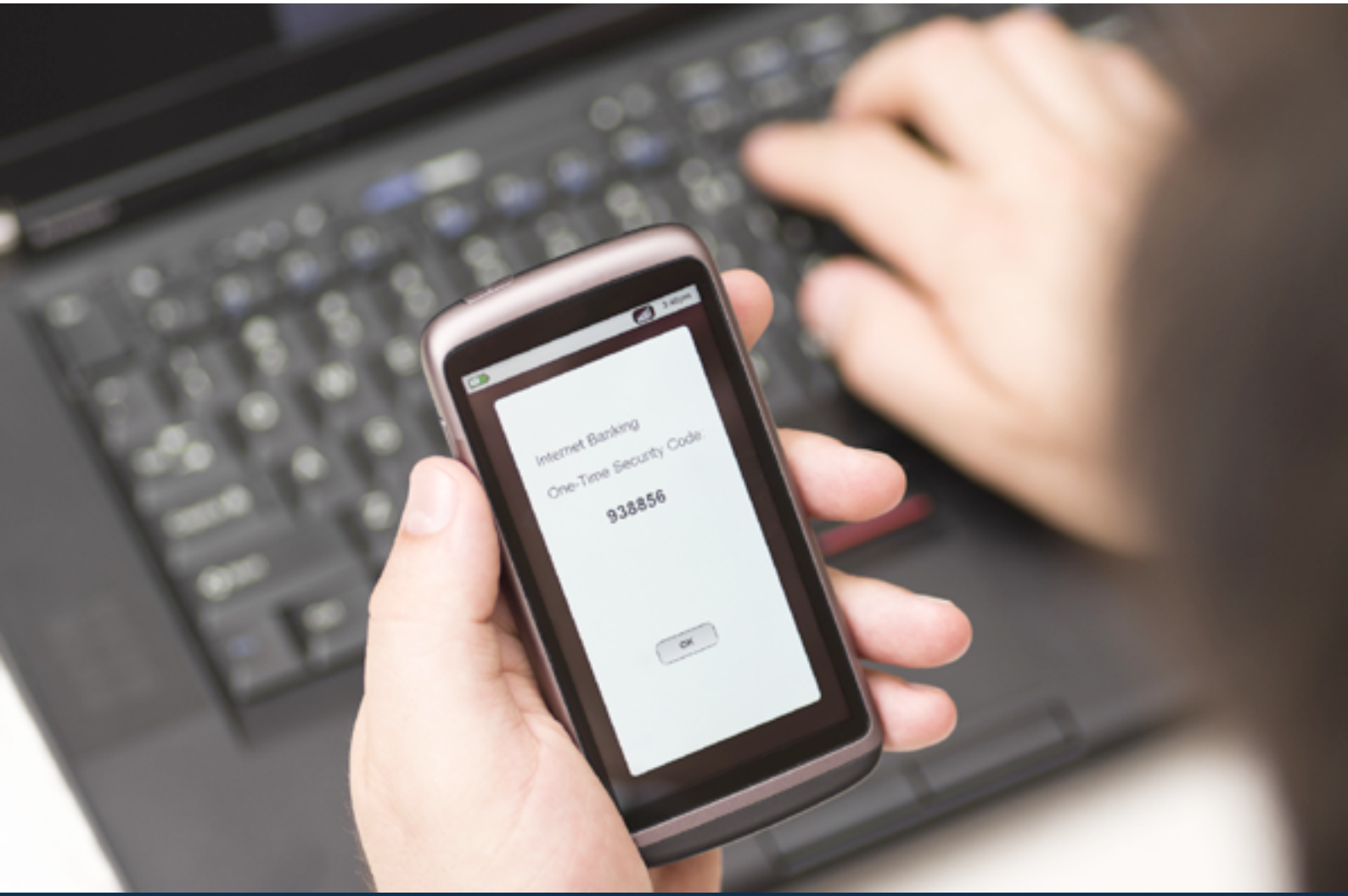
ZEROPIU
Difference as value

Mobile Security Suite



Con la diffusione e l'utilizzo di smartphone le aziende si sono trovate di fronte a uno scenario totalmente nuovo e in rapido mutamento:

l'utilizzo di smartphone e tablet offre infatti interessanti prospettive di business ma, causa l'impostazione di tipo consumer di questi device, può indebolire il perimetro di sicurezza aziendale.

E' importante sottolineare poi un'altra tendenza che si sta sempre più affermando, la così detta **BYOD (bring your own device)**, ovvero l'utilizzo del proprio smartphone e/o tablet personale anche in ambito professionale.

Tutto questo porta alla necessità non solo di assicurare la sicurezza dei dispositivi mobili ma, soprattutto, delle applicazioni e dei dati aziendali presenti su questi.

L'introduzione dei device mobili all'interno del processo di sicurezza aziendale (con l'utilizzo, ad esempio di sistemi di end-point-security) è sicuramente importante, ma non è risolutiva ed inoltre può non essere sempre possibile:

si pensi ad esempio all'utilizzo di device personali così come a scenari di tipo B2C.

SCENARIO

In Italia 20 milioni di smartphone
+52% dal 2010
+224% nell'utilizzo online
Il 77% lo usa in ufficio
17 le app installate
di cui 7 utilizzate quotidianamente

L'OBIETTIVO DI MSS È ESATTAMENTE QUESTO

garantire la sicurezza delle applicazioni aziendali presenti su smartphone e tablet, indipendentemente dal fatto che si tratti di un device aziendale o meno, che sia gestito e/o disponga di un prodotto di end-point-security o meno.

MSS consente inoltre di integrare i dispositivi mobili all'interno del sistema di Access Management dell'azienda, offrendo anche funzionalità di single-sign-on e strong authentication, ma soprattutto consentendo di salvaguardare gli investimenti effettuati sulle infrastrutture **IAM (Identity&Access Management).**

Queste caratteristiche rendono **MSS** un prodotto estremamente interessante sia in ambito **B2E** che **B2C** (si pensi ad esempio ad applicazioni mobile di home banking).

MSS IL FRAMEWORK

Il framework Mobile Security Suite (MSS) è in grado di proteggere la sicurezza delle applicazioni aziendali (app e webapp) fruite tramite smartphone e tablet.

MSS e' composto da una componente server che supporta nativamente le infrastrutture di controllo accessi più diffuse sul mercato (CA SiteMinder, OpenSSO, OpenAM ed Oracle Access Manager).

MSS dispone di diversi moduli in grado di offrire molteplici funzionalità di sicurezza: standard & strong authentication, single sign-on, autorizzazione app, profilazione, device management

CORE ENGINE

Mobile Authenticator
• Autenticazione dell'utente
•Self enrollment dell'utente ed associazione del device
• single sign-on authentication

Mobile App Launcher
• Menù delle app aziendali eseguibili dall'utente
• Firewall applicativo "Rule Based" integrato con la piattaforma di sicurezza aziendale (CA SiteMinder, Open SSO, Open AM, Oracle Access Manager, ecc.)

ENTERPRISE DEVICE MGR

Security Remediation
• Wipe e/o blocco remoto in caso di furto o smarrimento
• Localizzazione tramite le funzionalità GPS disponibili

Device Mgmt
• Piattaforma di gestione con funzionalità basate su policy definite (utente, call center, help desk)
• Self-enrollment del dispositivo da parte dell'utente

App Configurator
• Gestione del parco app disponibili per l'utente in base al ruolo (Role Based)
• Integrazione dei ruoli con la piattaforma di sicurezza aziendale (CA SiteMinder, Open SSO, Open AM, Oracle Access Manager, ecc.)

ADAPTIVE ACCESS CONTROL

Il modulo applica controlli legati al comportamento (behavioral) nell'utilizzo del device.
Alcune delle variabili di Adaptive Access Control previste sono:

• Coordinate geografiche rilevate tramite modulo GPS
• Orario di accesso
• Network di appartenenza

In base alle variabili d'accesso sono richiesti differenti meccanismi di autenticazione:
• Esplicito (username e password dell'account)
• Avanzato (password a consumo, codici, domanda segreta, email OTP, SMS OTP, etc)

STRONG AUTHENTICATION

Questo modulo sfrutta le funzionalità della Mobile Security Suite per costruire un sistema di One Time Password basata su Soft Token, integrato con la piattaforma di autenticazione aziendale.
Con il modulo di Strong Authentication un device offre le stesse funzionalità dei token fisici diffusi sul mercato, generando un codice time-based utilizzabile anche per autenticarsi su applicazioni aziendali fruibili da altre piattaforme

SANDBOX
(Cloud Disk con Sandbox)

Questo modulo offre la possibilità di accedere ad un disco cloud crittografato così da rendere sicuro l'accesso e la gestione degli allegati presenti nelle email e, più in generale, del File System utilizzato dal Mobile Security Suite e da tutte le App ad esso integrate.

In caso di furto del telefono è possibile impedire l'accesso ai dati riservati, anche nel caso questi fossero oggetto di un tentativo di accesso meccanico al terminale.

ZEROPIU
Difference as value

SUPPORT MATRIX

	iPhone	Android	BlackBerry	Windows Mobile
Modulo Core	√	√	Q3 2012	2013
Mobile Authenticator	√	√	-	-
App Launcher	√	√	-	-
Enterprise Manager	√	√	Q3 2012	2013
Device Manager	√	√	-	-
Security Remediation	√	√	(BES 5.0 SP3 required)	-
App Configurator	√	√	-	-
Adaptive Access Control	√	√	Q3 2012	2013
Strong Authentication	√	√	Q3 2012	2013
Sandbox	Q4 2012	Q4 2012	Q4 2012	2013
Local Sandbox	.	.	-	-
Cloud Sandbox	.	.	-	-

ROADMAP

Q3 2011

MSS Core

- Authentication
- Authorization
- Single Sign-On
- Device Enrollment
- App Launcher

Q4 2011

Strong Authentication

- Soft Token
- OTP

Q1 2012

Enterprise Manager

- Device Manager
- App Configurator

Q2 2012

Enterprise Manager

- Security Remediation
- Adaptive Access Control

Q4 2012

Sandbox

- Email
- File System

MILANO - Via Fra Luca Pacioli, 3 - 20144 Milano . **TORINO** Via Pavia, 11 - 10098 Rivoli (To) . **ROMA** - Via Ercolano Salvi, 18 - 00143 - Roma
OSLO - Nordregate 27 - NO 0551 Oslo - Norway . **TALLIN** - Roosikrantsi 2 - K209 K-209 11911 – Tallinn - Estonia
STOCCOLMA - Birger Jarlsgatan 2, 5 fl * -114 34 Stockholm - Sweden
ZEROPIU S.p.A. www.zeropiu.it info@zeropiu.it Tel.: +39 02 83102 300 / +39 02 83102 310