nomasis
secures your mobility

MDM de MobileIron dans le contexte du BYOD

BYOD? Quoi faire…

On veut…
…plus de flexibilité
…communication moderne
…un seul appareil mobile
…Smartphones & tablettes
-> **B Y O D !**


Collaborateur type: 2013

…risque sécurité?

…situation juridique?

…coûts / avantages?

…complexité?

…gouvernance?


Responsable IT

Utilisateur vs. IT

nomasis
secures your mobility

Désir utilisateur

- Expérience native
- Accès ressources interne (Mail, Intranet etc.)
- Utilisation 1 smartphone (corp. et privée)
- NON ‘big brother is watching you’

Exigence IT

- Sécurité
- Gouvernance
- Minimal tâches opérationnel
- Inventaire
- Eco system apps métier
- Communication entre apps métier

Avant l'implementation d'une solution MDM…

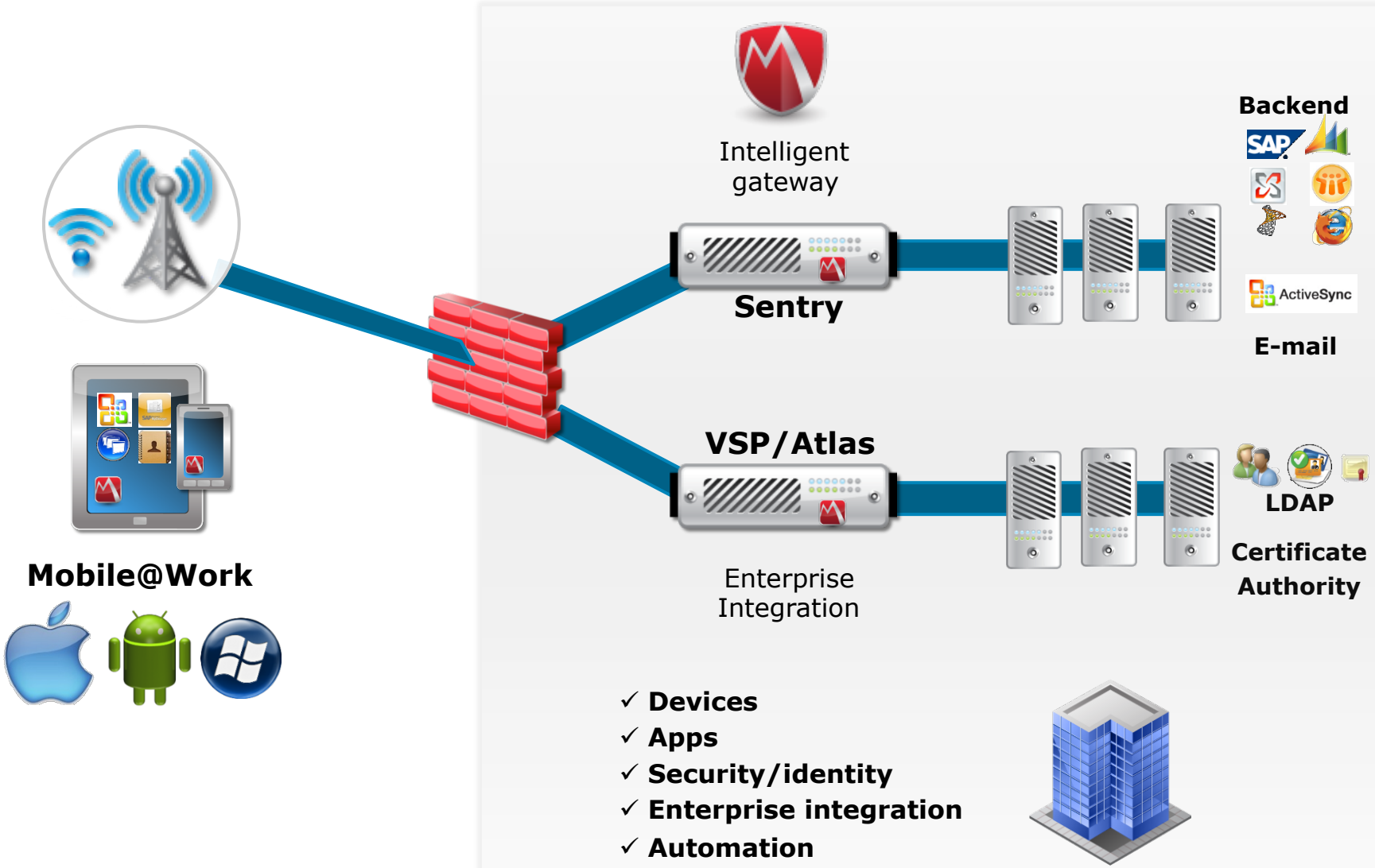
nomasis
secures your mobility

- Développement stratégie BYOD avant l'intégration d'une solution MDM:
  - Définitions des règles de privacy (aspect légal, localisations, apps etc.)
  - Définitions des règles de sécurité
  - Création de la documentation complet et des outils pour utilisateur
  - Formation du Helpdesk
  - Communication utilisateur et accompagnement
  - Etc.

Stratégie d'intégration…

- MDM comme solution indépendant
- MDM intégrer dans les processus d'entreprise
  - Procédure d'enregistrement
  - Processus ressources humaine
  - Gestion cycle de vie
  - Accès systèmes
  - etc.

MobileIron solution MDM on-premise



Mobile Device Management

nomasis
secures your mobility

Device Management

- Inventaire de l'appareil avec reconnaissance de Jailbreak/Root, version OS, IMEI, IMSI, utilisateur
- Réglage de la protection par un mot de passe et d'autres paramètres de sécurité
- Configuration des points d'accès (APN), VPN (Server, Account, Proxy, Certificats, Token, des groupes, ...), point d'accès WLAN
- Inventaire des applications installées

Identité

- Las gestion des certificats, y compris la détection de l'expiration et renouvellement
- Distribution des certificats (PKCS1 et PKCS12) et SCEP
- Signez et lier les profiles aux appareils
- Identification de VPN, WLAN et Exchange

Device Control

- Installation des applications in-house, Blacklisting / Whitelisting
- Définition restrictions: YouTube, Safari, appareil photo, copy d'écran etc.
- Quarantaine, exclusion des appareils non conformes
- Blocage / mise à zéro du mots de passe / Business-WIPE

Cryptage de contenu

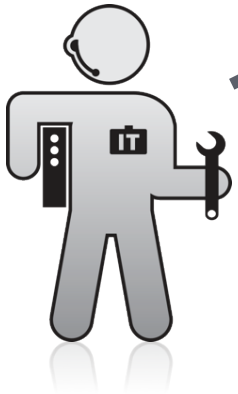
- Cryptage des données
- Cryptage des applications
- Cryptage de communication
- Backup crypté

Défis: applications de métier?

"Comment distribuer les Apps et supporter BYOD?"

"Comment contrôler l'explosion des apps et les différents OS?"

"Comment garantir la sécurité, l'accès aux données et l'identité?"



"Comment rendre les donné mobile?"

"Je suis obligé d'agir dans la **vitesse des consommateurs**, toute en garantissant la **sécurité et gouvernance** de l'entreprise"

Enterprise App Store

nomasis
secures your mobility

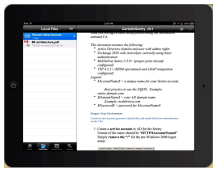
- Enterprise App Store
  - Rendre des In-House Apps dispo.
  - Rendre des Apps du public App Store dispo.
  - Sécurisé!
    - Authentification automatique de l'utilisateur
    - Disponible uniquement pour des appareils mobiles enregistré et intègre
- Retirer des apps (avec donnée):
  - Activation du mode quarantaine -> Désaffecter un appareil
- Gestion de la fonctionnalité iCloud/ Backup par app (iOS)

Containeriser App de métier

nomasis
secures your mobility

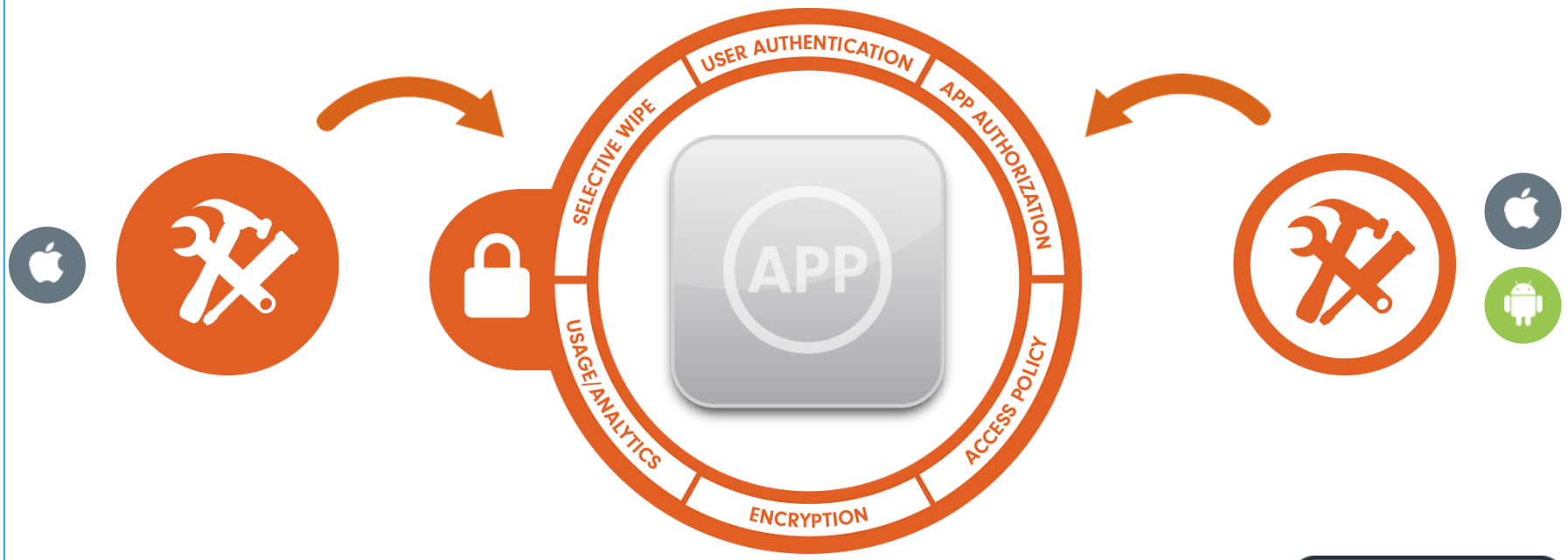
Distribuer les app de métier adapter a l'utilisateur

Sécuriser uniquement les apps de métier et ces donnés sur les appareils BYOD



AppConnect & AppTunnel

nomasis
secures your mobility



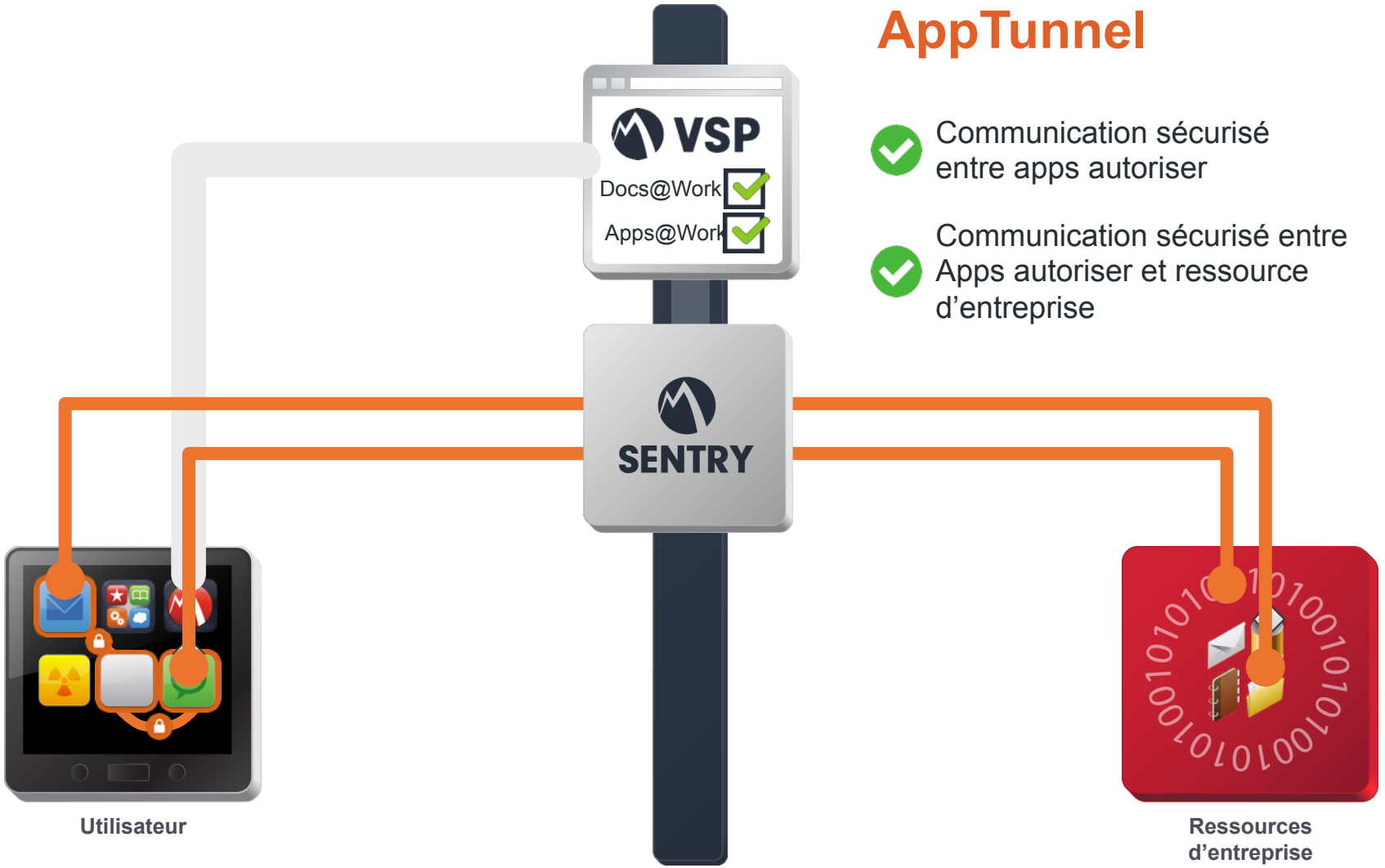
AppConnect-enabled

GSMA GLOBAL MOBILE AWARDS 2013
WINNER
"Best Enterprise Mobile Service"

Containeriser Application fonctionnalité de sécurité

- Enterprise Container App Passcode
  - Dual Persona Capability
- DLP Controls
  - Open In Control
  - Copy / Paste Control
  - Block Screen Capture (Android)

AppConnect & AppTunnel



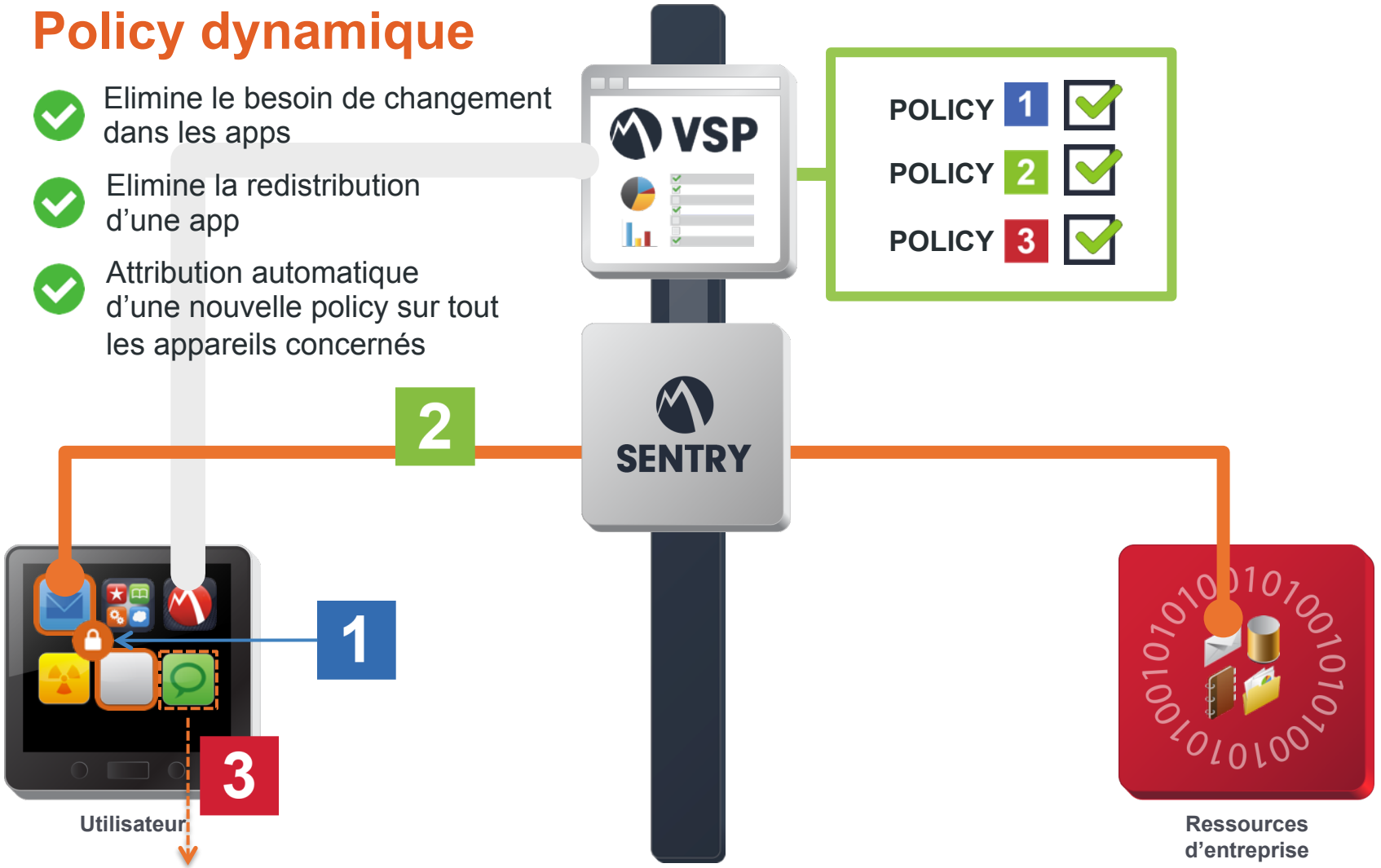
AppTunnel

- Communication sécurisé entre apps autoriser
- Communication sécurisé entre Apps autoriser et ressource d'entreprise

AppConnect & AppTunnel

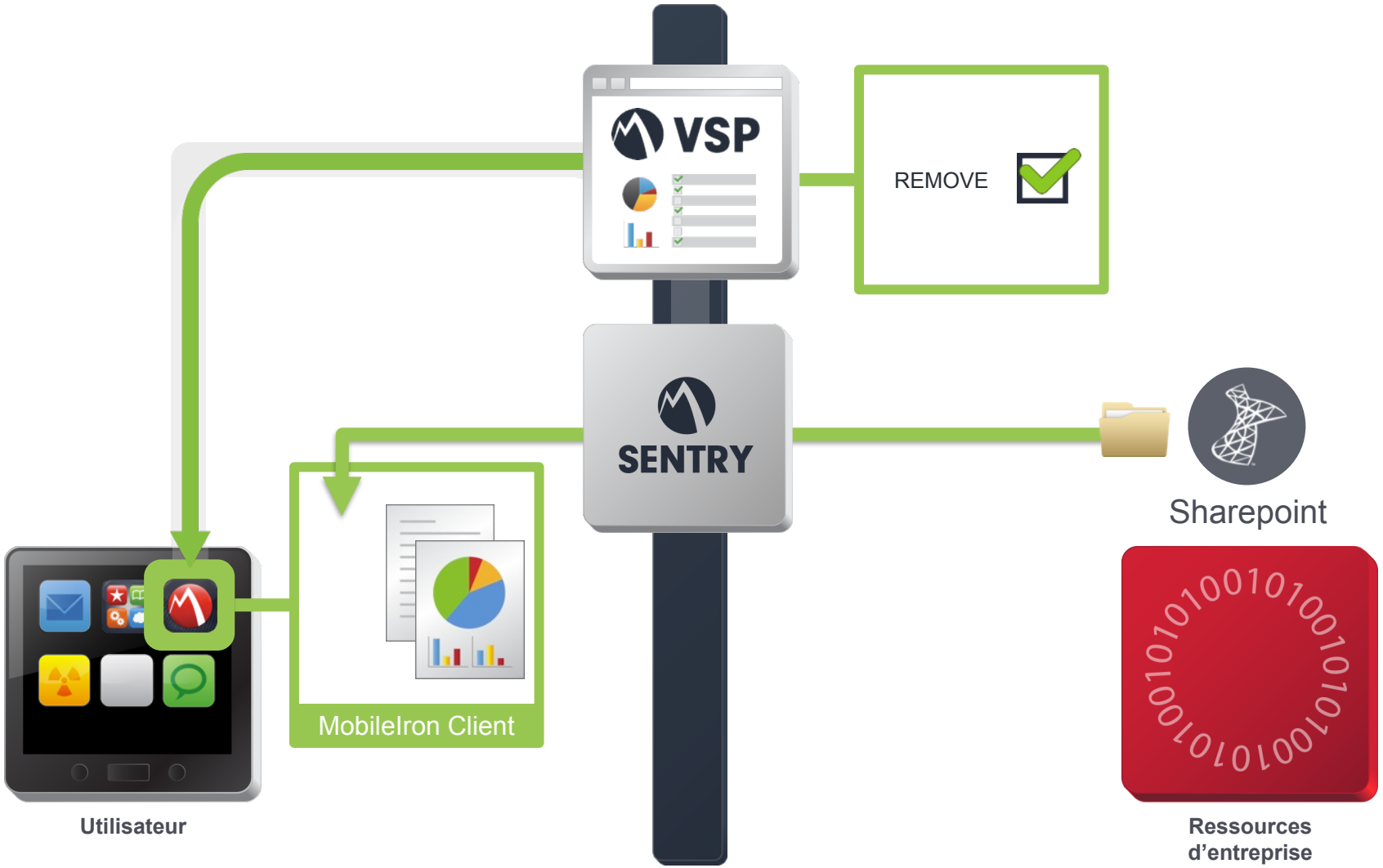
Policy dynamique

- Elimine le besoin de changement dans les apps
- Elimine la redistribution d'une app
- Attribution automatique d'une nouvelle policy sur tout les appareils concernés



Annexe mail sécurisé
MobileIron Docs@Work

Sharepoint/CIFS sécurisé
MobileIron Docs@Work



Accès intranet
MobileIron Web@Work

nomasis
secures your mobility

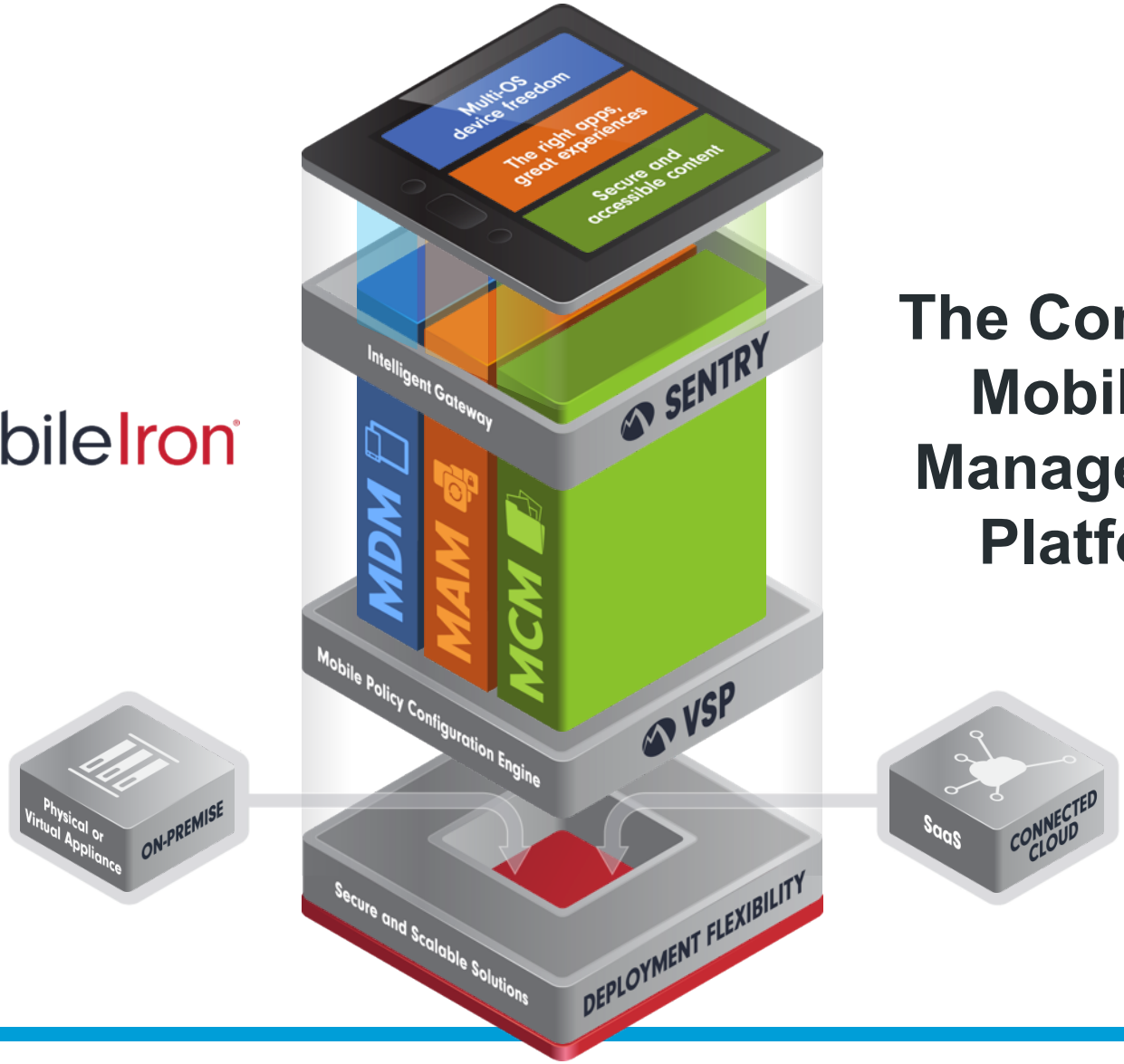
Secure Browser

- Accès sécurisé sur l'intranet sans VPN
- Sécurise les donnés restent

La solution complète de gestion des appareils mobiles

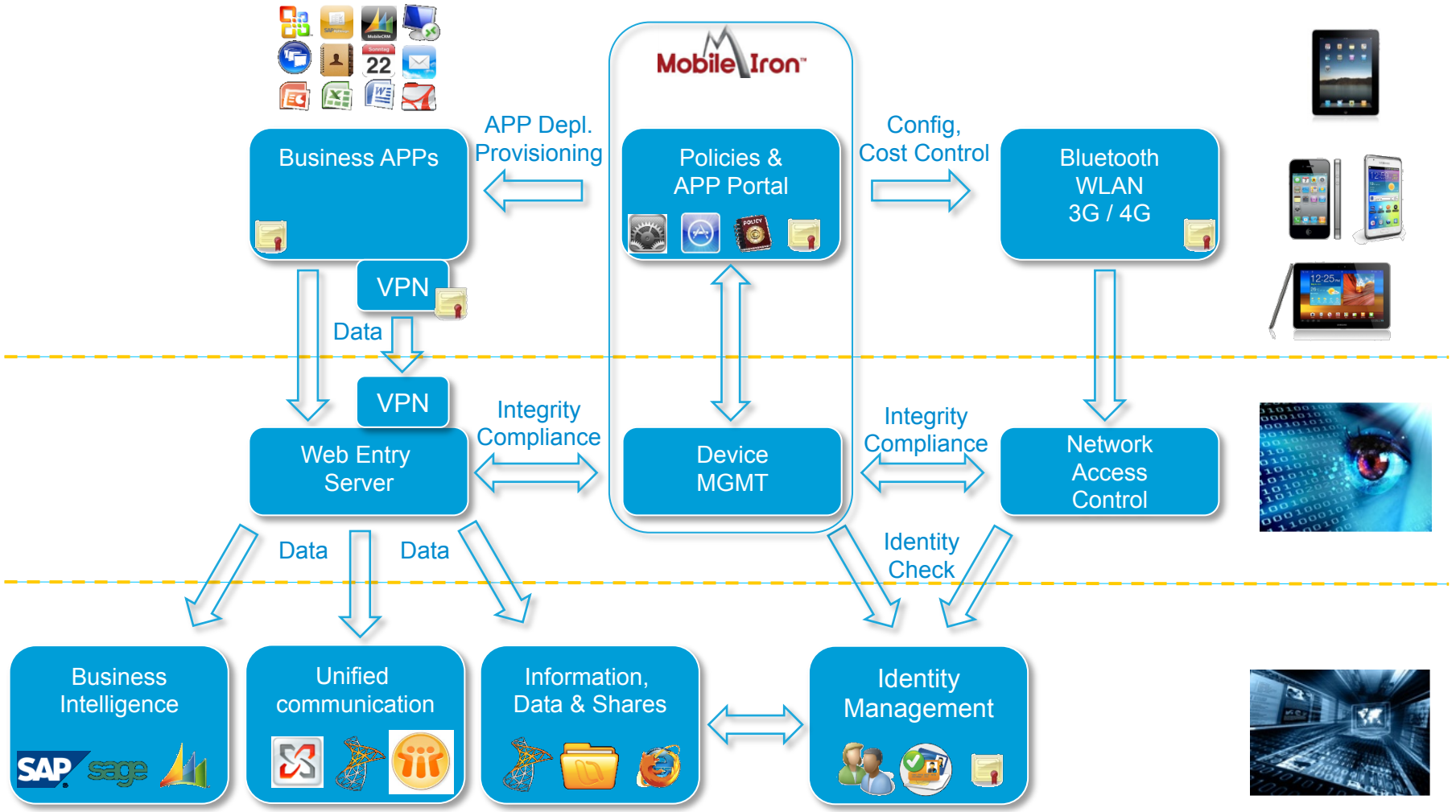
nomasis
secures your mobility

MobileIron



The Complete Mobile IT Management Platform

Intégration MobileIT



Avec le concept BYOD de MobileIron vous avez…

- Règles/configurations séparer entre appareil d'entreprise et BYOD
- Une solution simple qui propose un niveau élevé de sécurité
- Une solution clef en main
- MobileIron 'leading in innovation'
  - Quarantaine, Enterprise app store, distinction BYOD vs. Corp, AppConnect etc.

Nomasis – Best EMEA Partner of the Year 2010 & 2011 & 2012

Christof Baumgärtner, Director and Country Manager MobileIron DACH
Kees van Veenendaal, VP MobileIron EMEA
Philipp Klomp, CEO Nomasis AG

BYOD comme ça…

nomasis
secures your mobility

…ou comme ça?

Contact

Nomasis AG
Ave. Beauregard 12
CH-1700 Fribourg
Tel: +41 43 377 66 55
Fax: +41 43 377 86 49
Mail: sales@nomasis.ch