

# Sécurisation des données et la gestion des utilisateurs

---

Présenté par Saïd AGHZOU - Samir BERKANI - Charlys RETITA

# INTRODUCTION

**Plus de 70 % des salariés font usage d'équipements mobiles mis à leur disposition dans les entreprises.** Cette profusion d'appareils entraîne des risques pour les entreprises comme le *vol de données* faute de protection suffisante, la *perte d'un terminal* ou encore la *diffusion de programmes malveillants dans les terminaux et dans le système d'information via des applications douteuses*.

Partant de ces constats alarmants, **de plus en plus d'entreprises déploient des solutions EMM.**

les données  
informatiques :  
quels risques ?

l'erreur de manipulation

les virus et programmes malveillants

l'espionnage industriel

le piratage

les emails frauduleux

la malversation

# Précautions :

---

Anticiper les incidents et minimiser leurs impacts,

---

Sauvegarder vos données informatiques, qui sont à la fois votre base de travail et l'historique de votre entreprise,

---

Protéger le réseau informatique,

---

Filtrer les courriers électroniques,

---

Sensibiliser les utilisateurs,

---

Protéger l'accès à internet,

---

Auditer le contenu de votre site web, vitrine sur internet de votre entreprise

# Problématique :

01

Une entreprise possède deux locaux, un situé à Saint Denis et l'autre à Puteaux. Ce dernier contient un serveur interne qui stocke toutes les données confidentielles comme les coordonnées bancaires des salariés.

02

90% des employés se trouvent à Saint Denis et ce serveur n'a pas l'accès depuis l'extérieur du local et à distance.

03

Le personnel travaillant sur le site de Puteaux peut également accéder au serveur une fois qu'ils sont connecté au réseaux, ce qui provoque un manque de conditions d'accès.

# Nous avons choisi AirWatch !

Selon le cabinet IDC, **le marché mondial de l'EMM va considérablement augmenter d'ici à trois ans pour atteindre les 2,9 Mds de dollars en 2019, soit une croissance de 10 % par rapport à 2016.**

Parmi les leaders incontestés de ce marché figure l'entreprise américaine **Airwatch by VMware qui dispose d'un catalogue de solutions complètes d'EMM** répondant aux besoins des entreprises pour la gestion de terminaux mobiles, des e-mails, des applications et des données mobiles, associées à des technologies de sécurité



# Solution :

---

AirWatch



# Pourquoi ?

- Il permet de créer des comptes utilisateurs personnelles et sécurisées avec accès à distance.





# Comment?

1. Installer l'application AirWatch sur le device de l'administrateur.
2. Installer l'application VMware Content Locker et créer un tunnel vers le serveur interne.
3. Définir les utilisateurs qui peuvent accéder à ce serveur.
4. Installer les applications sur les smartphones des employés.

# Plan d'action

Mise en place des comptes utilisateurs,

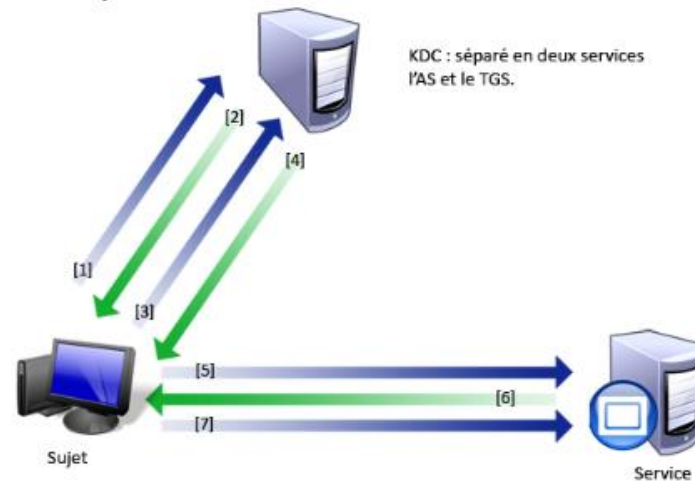
Création des politiques de sécurité avec les paramètres souhaités,

Test de l'enregistrement des terminaux

Observation du comportement des utilisateurs et prendre des mesures sur les terminaux.

La validation de toutes ces étapes nous permettra d'effectuer un déploiement en masse en passant notamment par une formation pour les administrateurs et les utilisateurs.

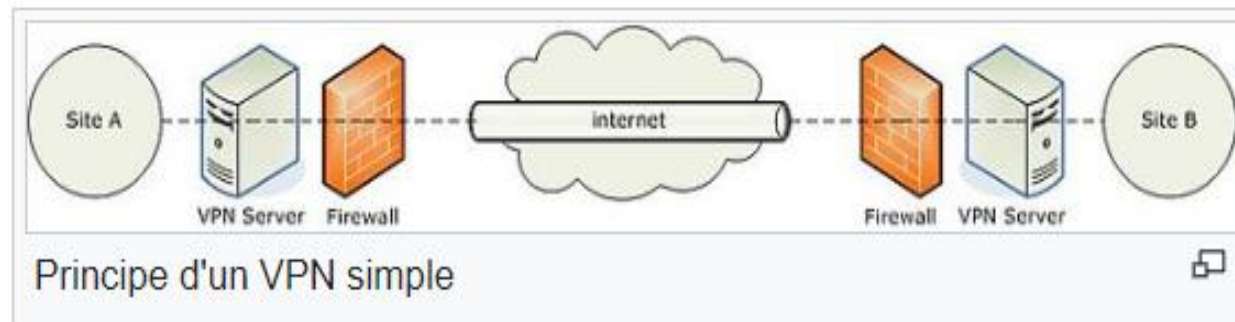
La connexion  
de chaque  
utilisateur doit  
respecter le  
principe  
“Kerberos”:



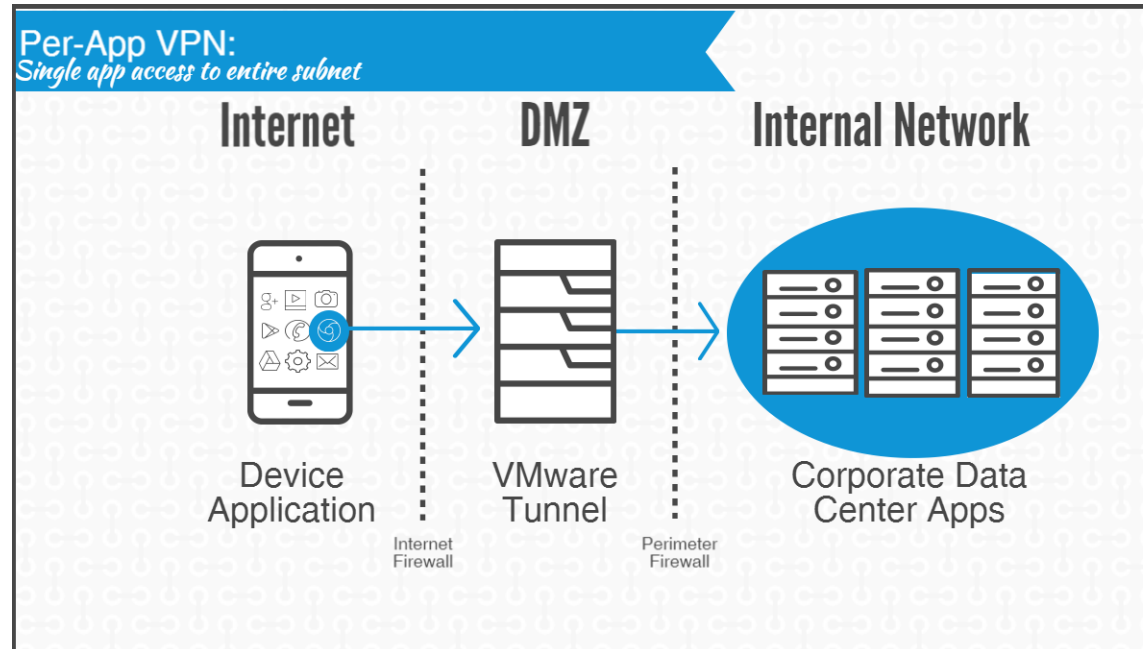
**kerberos** introduit le principe de Single Sign-On (SSO). Ainsi avec une authentification unique, l'utilisateur aura accès à tous les services du réseau.

# Type de réseau utilisé : VPN ( Virtual Private Network)

C'est un système qui permet de créer des liens entre des ordinateurs distants, accès au cloud computing et les services MPLS ( MultiProtocol Label Switching). Ce dernier se base sur la commutation d'étiquettes ( Labels ou identifiants ), qui sont insérés à l'entrée du réseau MPLS et retirés à sa sortie.



Pourquoi  
dans notre  
cas ?



Avec AirWatch, activer le composant tunnel par application (VPN per App) permet aux applications internes et publiques d'accéder aux ressources de l'entreprise application par application.

# Sécuriser les échanges des mails:

Pourquoi ?

- les employés accèdent au courrier électronique sur des réseaux non sécurisés.
- Existence des mails confidentielles sur les appareils personnelles des employés.
- Les utilisateurs qui ont quitté l'entreprise ont toujours accès au courrier électronique.
- Dispositifs non autorisés, perdus ou volés permettant d'accéder au courrier électronique.



# Tableau de bord pour la gestion des mails:

- Il permet à l'administrateur d'autoriser aux employées l'accès aux mails de l'entreprise avec toute sécurité.
- Effectuer les actions en bloc "Bulk Actions" en sélectionnant un périphérique et gérer les mails.



- Contrôler les appareils connectés en ayant la possibilité de leur envoyer un courriel ou une notification push.

# Modèles d'intégration des mails :

---

Deployment Model	Configuration Mode	Mail Infrastructure
Proxy Model	Secure Email Gateway - Classic Platform	Microsoft Exchange 2003/2007/2010/2013/2016 Exchange Office 365 IBM Domino w/ Lotus Notes Novell GroupWise (with EAS) Gmail
	Secure Email Gateway - V2 Platform	Microsoft Exchange 2010/2013/2016 Exchange Office 365
Direct Model	PowerShell Model	Microsoft Exchange 2010/2013/2016 Microsoft Office 365
	Gmail Model	Gmail



# Proxy Model



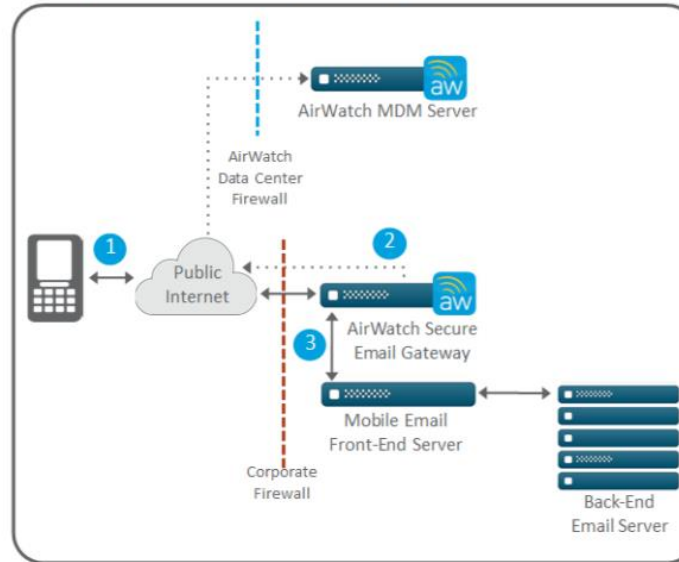
Pourquoi ?

The diagram consists of two light blue circles connected by a light blue arrow pointing from left to right. The left circle contains the text 'Pourquoi ?' and the right circle contains a multi-line text block.

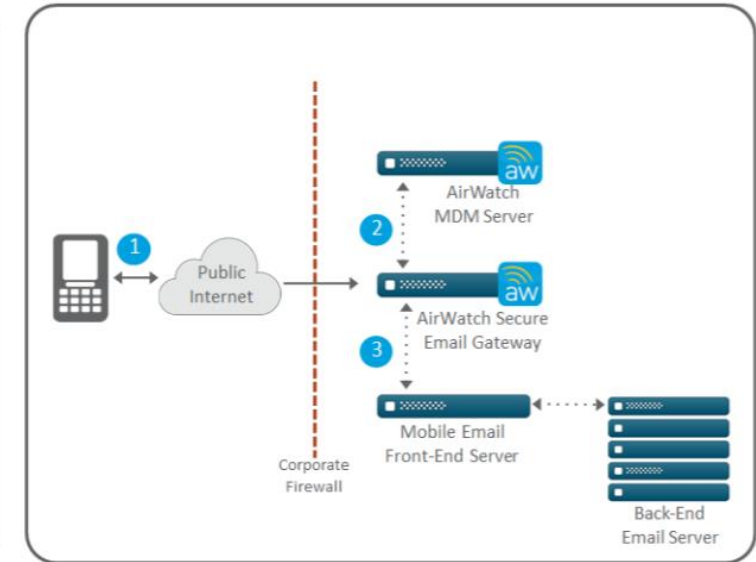
Nous pouvons  
alterner l'intégration  
des infrastructures  
de mail avec la  
configuration en  
mode basic, ce qui  
n'existe pas pour les  
autres modes.

# Proxy Model - Secure Email Gateway

## Proxy Model Topology



Cloud/SaaS Architecture



On-Premises Architecture

# Comment il fonctionne ?

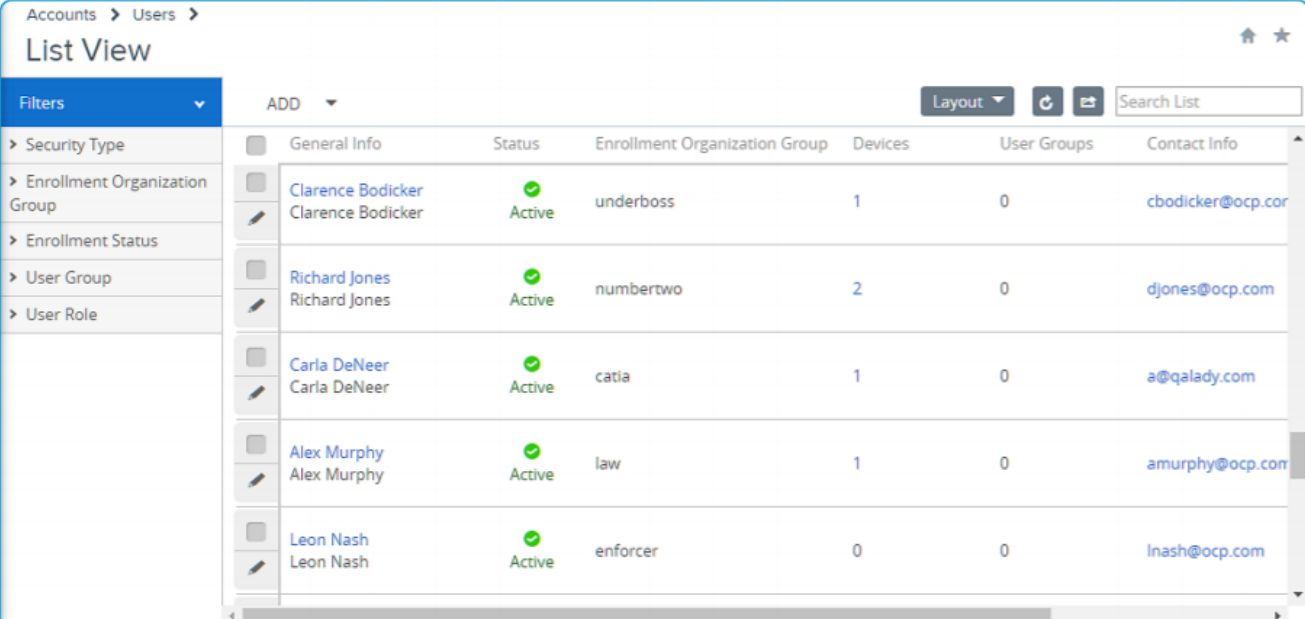
## Architecture avec le Cloud :

- Demande d'actualisation de politique.
- Recevoir les politiques de la base de données.
- Mettre à jour les politiques.
- Le périphérique envoie la synchronisation du courrier électronique demandé.
- Si le périphérique est conforme, AirWatch Secure Email Gateway transmet la demande par procuration.



# Gestion des utilisateurs via console AirWatch

La page d'affichage liste des utilisateurs, à laquelle l'administrateur peut accéder et utiliser des outils utiles pour la maintenance et la gestion des comptes.



Accounts > Users > List View

Filters ADD Layout Search List

General Info	Status	Enrollment Organization Group	Devices	User Groups	Contact Info
<input type="checkbox"/> Clarence Bodicker Clarence Bodicker	Active	underboss	1	0	cbodicker@ocp.cor
<input type="checkbox"/> Richard Jones Richard Jones	Active	numbertwo	2	0	djones@ocp.com
<input type="checkbox"/> Carla DeNeer Carla DeNeer	Active	catla	1	0	a@qalady.com
<input type="checkbox"/> Alex Murphy Alex Murphy	Active	law	1	0	amurphy@ocp.com
<input type="checkbox"/> Leon Nash Leon Nash	Active	enforcer	0	0	lnash@ocp.com

# Avantages de la solution AirWatch



## Performance

Une gestion performante des terminaux mobiles et de leurs contenus



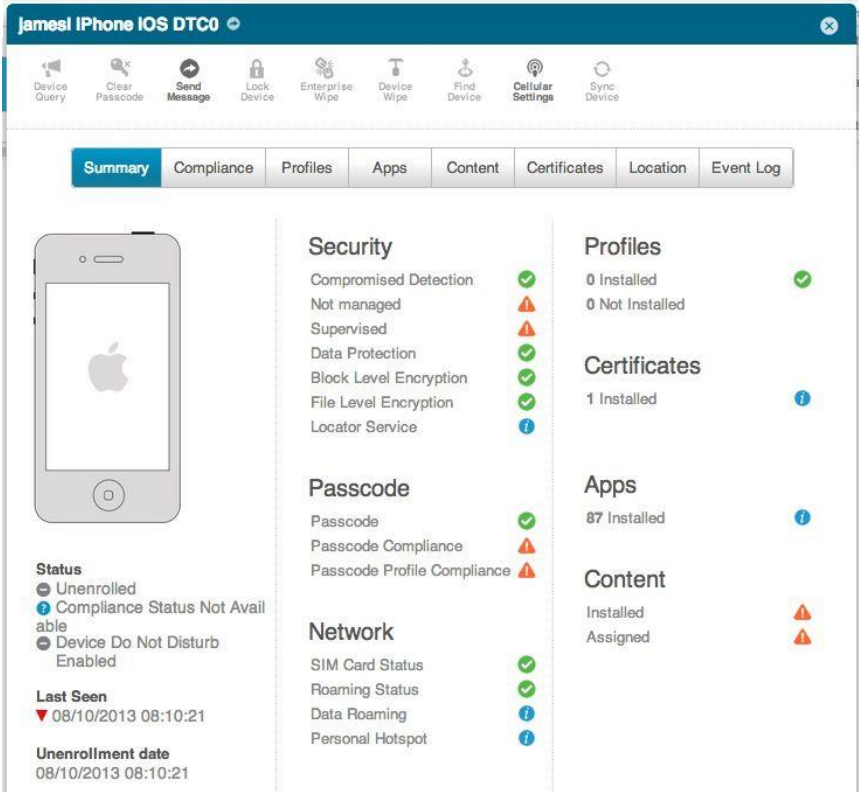
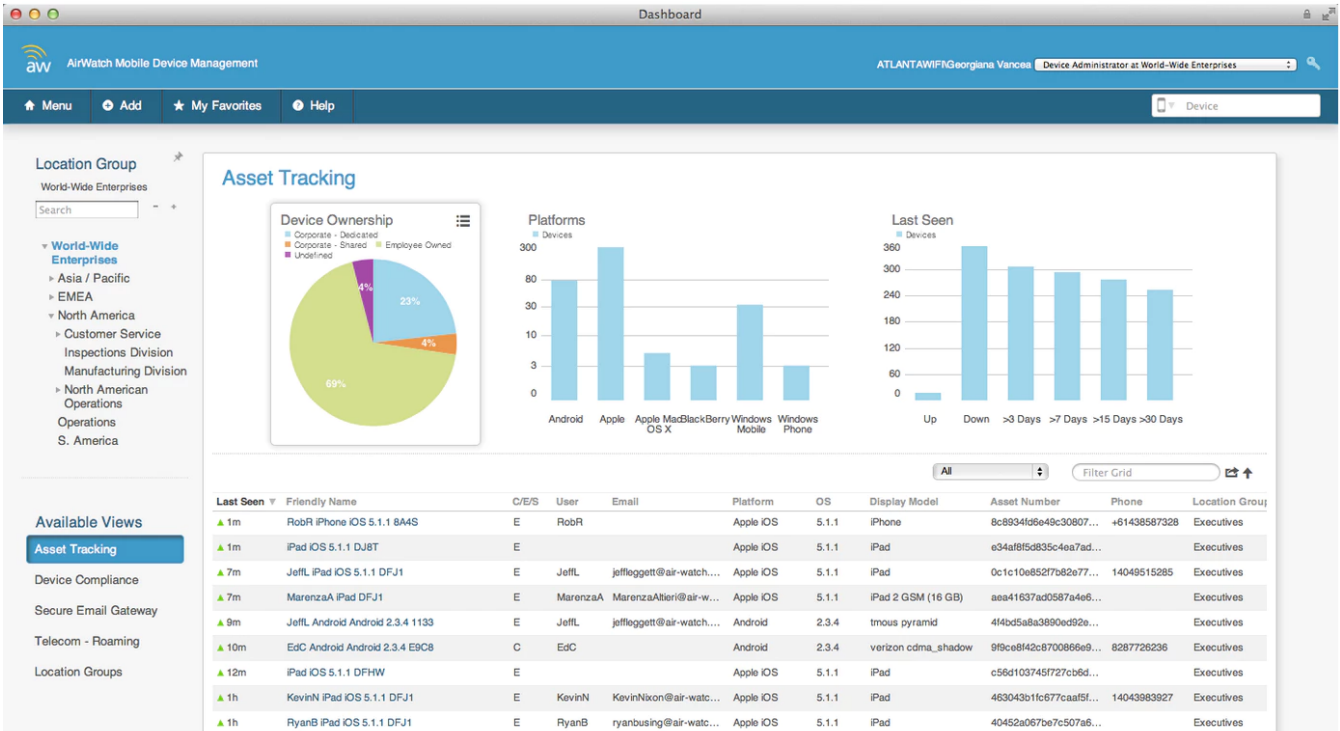
## Flexibilité

Un ensemble de solutions de gestion de la mobilité



## Rapidité

AirWatch permet d' enrôler rapidement les terminaux dans les environnements d'entreprise



# Conclusion :

---

AirWatch reste la solution de gestion de flotte mobile la plus appropriée face aux problèmes de gestion des utilisateurs et de sécurité que rencontre mon entreprise.