ANDROID VIRTUAL DEVICES TO MEET BOTH IT AND EMPLOYEES NEEDS IN TERM OF ENTERPRISE MOBILITY

Enterprise mobility is a new trend.

More and more workers work out of office : **worldwide mobile workers is estimated to grow to 1,75 billion in 2020 (IDC).** They need to stay productive and be able to access their corporate data anywhere and anytime they want. Applications tend to be more and more connected for multi platform business tasks : a document started on a computer can be finished on a mobile device.
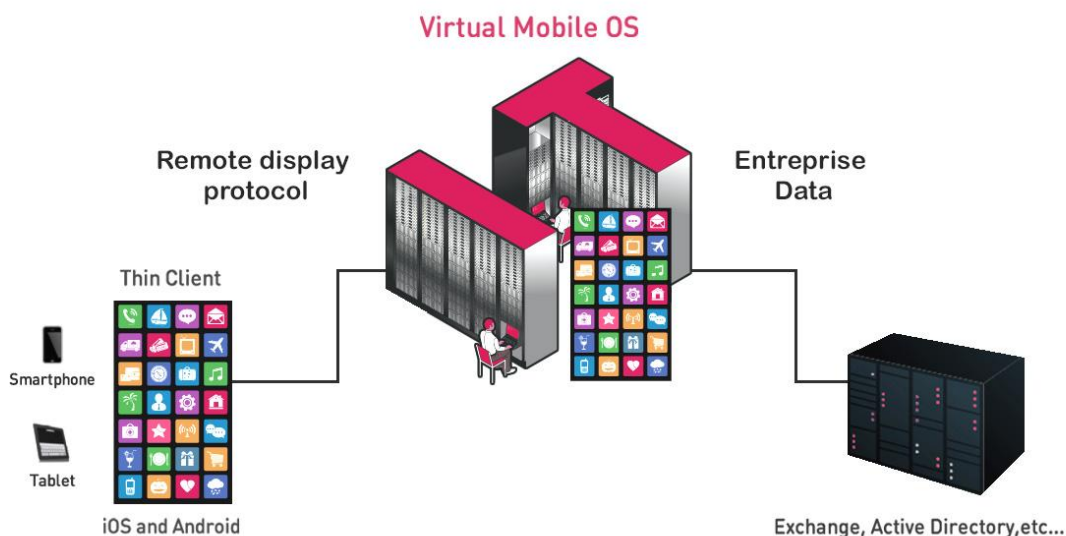
But this creates **security risks** especially in some domains with high security constraints (government, healthcare...) resulting for the IT department to **make sure that there is no data leakage**. **IT department** already uses Enterprise Mobility Management products to prevent this risk but they face the **complexity of maintaining a fleet of heterogeneous devices up to date** (device OS and mobile applications).

Employees on the other side need to abide by their IT department security policies whether they use their own device (BYOD) or corporate one (COPE).

Especially for BYOD devices, employees can be reluctant in using their personal device also for corporate purposes because **they fear of their personal data being monitored by the enterprise**. Moreover, having a device enrolled on the enterprise can be a complex process for some users (downloading and registering on the mobile application agent).
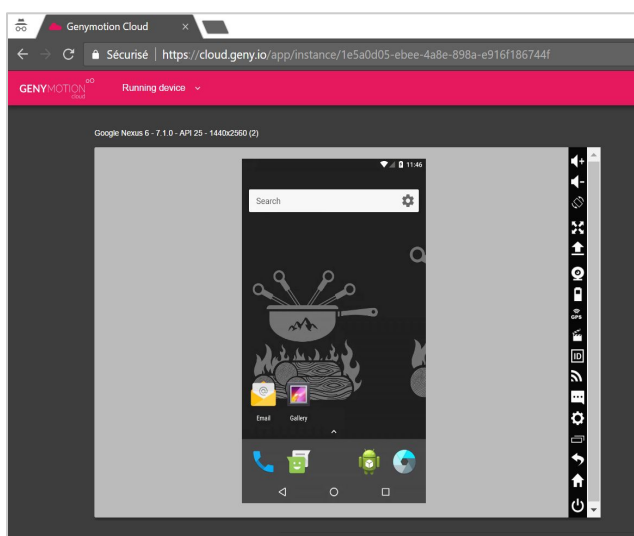
A Virtual Mobile Infrastructure (VMI) **addresses the needs of both IT and employees** to meet optimal security, manageability and usability requirements.

VMI is **a service that hosts mobile apps or full operating systems on remote servers**, providing mobile users access to apps and data seamlessly, without the need to download a mobile app, or to store corporate or sensitive data, on the user's mobile device itself.

Virtual Mobile OS — Remote display protocol — Thin Client — Smartphone — Tablet — iOS and Android — Entreprise Data — Exchange, Active Directory, etc...

Genymotion allows you to access and use **virtualized Android devices via a web browser.**

You can pre-configure an environment (apps installed, securities parameters, branding, etc.) and deploy it over a chosen amount of virtual Android devices that would be accessible from anywhere by your employees.

Genymotion meets VMI requirements into 3 main benefits :

Manageability

A single app version is developed and maintained centrally, widely reducing development and maintenance costs, and making deployment of new releases immediate and comprehensive.

A centralized web management console where the IT can update applications and user access to the Genymotion virtual devices. IT can easily scale the number of Genymotion virtual devices to create.

Security

Because **no corporate or otherwise sensitive data is stored locally on the users' device**, it eliminates the risk of data leakage and meets data privacy regulations (such as HIPAA for healthcare). Watermarking can be easily incorporated to prevent screenshots. A lost phone doesn't have to be wiped.

Since Genymotion devices are Android virtual machines, implementing **strong authentication methods** is easier, especially in BYOD deployments.

Usability

Direct access to the work environment on Genymotion virtual devices **from the mobile web browser,** no agent needs to be installed. It is compatible with different mobile platforms.

Thanks to the performance level brought by Genymotion, with its **market-leading low latency even over slow cellular networks**, removes one of the main user experience obstacles of other Android virtualization solutions. Using apps, even graphics-intensive apps, on Genymotion is indistinguishable, from a UX standpoint, from using native apps running on the device itself.