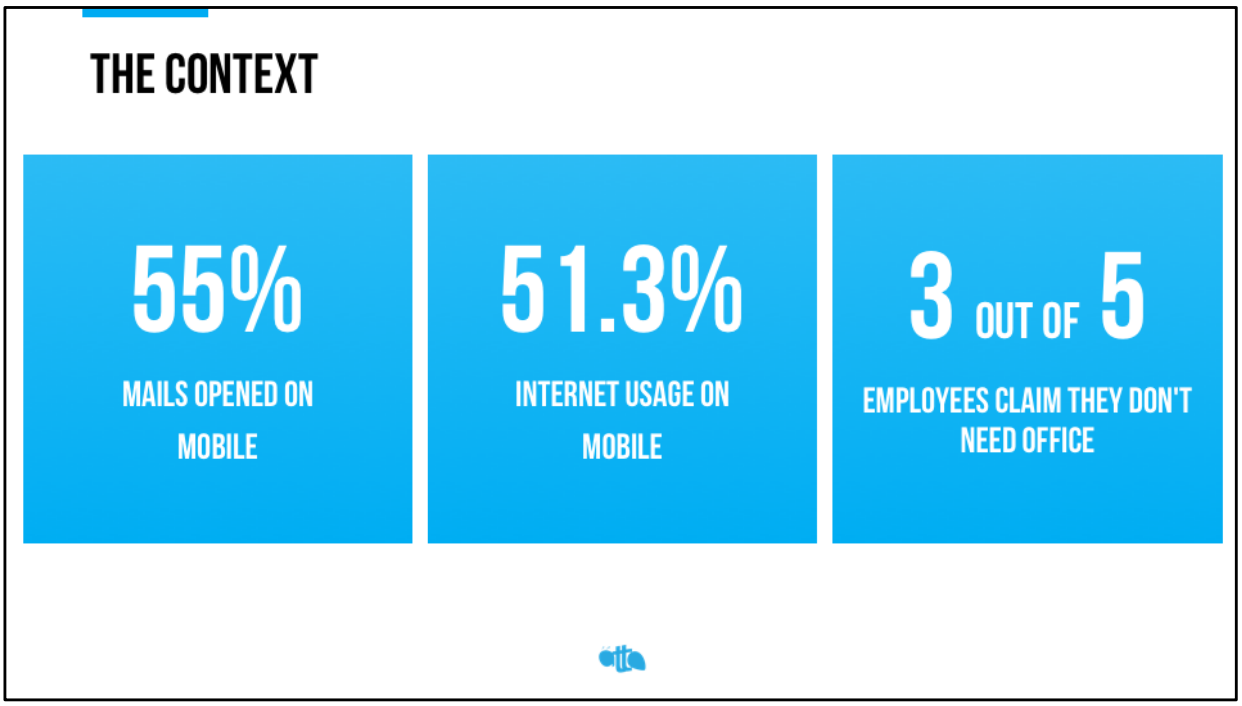
MICROSOFT INTUNE

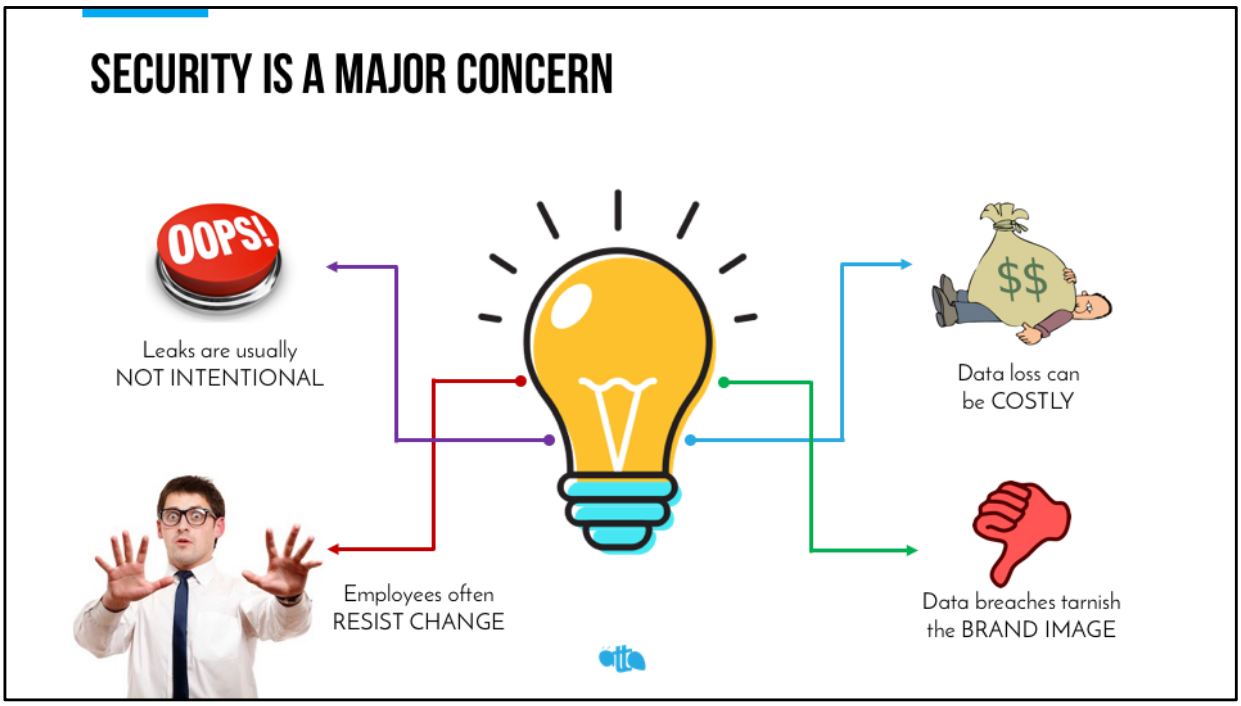
A QUICK INTRODUCTION

www.attosol.com



Let's start by setting the context of this discussion.

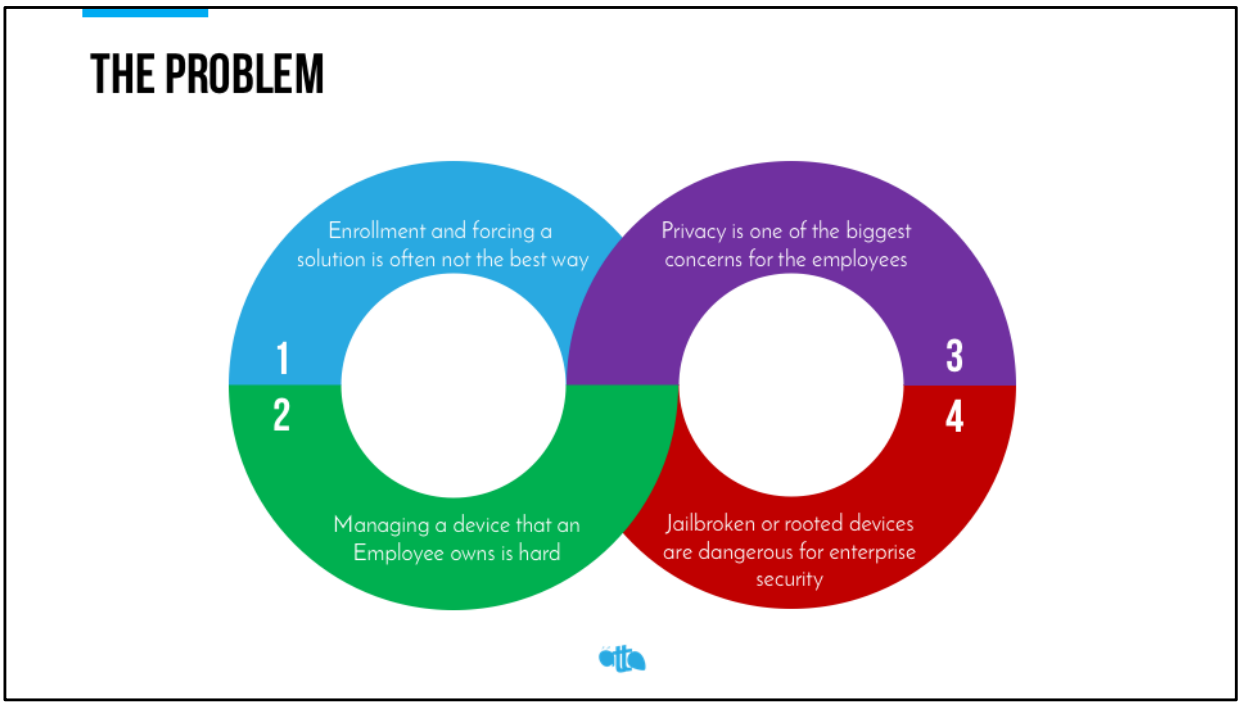
Mobile devices have the taken the world by storm as it is obvious in the staggering statistics shared here. Your workforce most likely has a device that you don't own, but they want to access your organizations data using it. Does it make you nervous?



Do you know that most data leaks are NOT intentional? Data leaks and loss are not only embarrassing, but also costly and sometimes devastating for the organization since it tarnishes the brand image.

Your employees are sometimes not aware of the complete functionality of the application and by mistake they (or their family member who accesses the phone casually) can hit a button that causes an unwanted data leak. How good would it be, if such non-intentional mistakes are avoided by using a corporate policy that you create and push?

You might say enrolling a device is easy, but pushing policies to devices and device enrolment are often resisted by the employees since they fear about their private data being accessed by the company. So much that they stop using an important Software that your organization needs them to use. There must be a solution that secures the organization data without jeopardizing the privacy concerns of the employees.

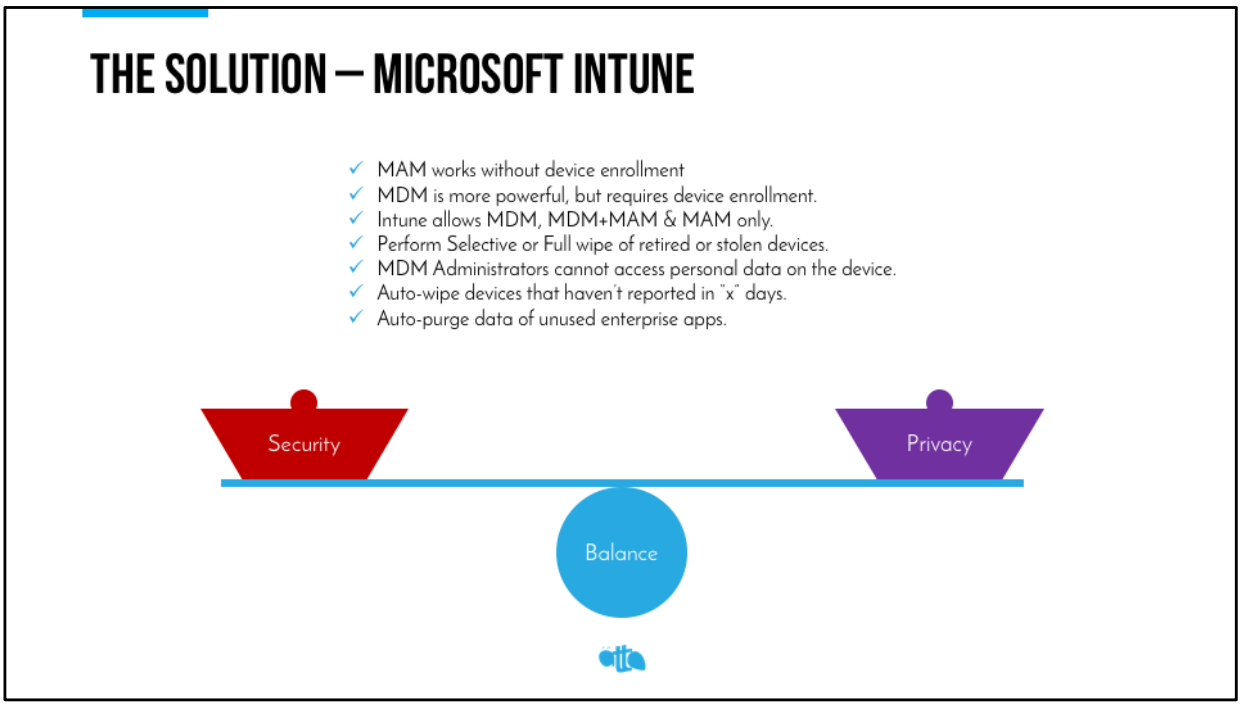


1. Forcing a device enrollment is sometimes necessary. However, force of any type attracts resistance and causes dissatisfaction. But how would you secure your resources in such a subtle way that employees accept the policies without resistance?

2. Managing a device that an employee owns is hard because you don't directly control it. They can format it any time they like and reconfigure as per their needs. How can you ensure that your data is always safe even when it is not a device that your organization manages?

3. It has been observed that the maximum resistance by the employees is due to their privacy concerns. They don't want their organization to peep into their private data. How can they be assured that they can use their devices without compromising on their privacy and yet being able to use the organization's data and documents?

4. Jailbroken or rooted devices are dangerous for the enterprises' security and many times the users are not fully aware of the implications. How can you ensure that no rooted device ever accesses your organization's data?



Microsoft Intune has an answer to all the problems stated earlier.

1. Enforce Application specific lock-down policies to devices connecting to/accessing corporate data.
2. Enforce Application policies to even devices managed by another MDM solution.
3. As Intune allows MDM, MDM + MAM & MAM only, you can have clearly defined corporate policies for corporate owned / employee owned devices.
4. Corporate owned devices may be forced to enrol into Intune, while employees still have the choice of not enrolling and being able to access corporate data.
5. Intune ensures Administrators do not have access to employee's personal data like call/message history, pictures etc. on the device, even when the device is fully managed.
6. Ability to full/selective wipe a device provides a great flexibility. Selective wipe ensures no personal data is touched while all corporate applications together with their data is cleanly wiped from the device.
7. Selective wipe an employee owned device when the employee leaves the organization, while Full wipe a device when it is stolen.
8. For scenarios where a thief may not turn on a stolen device for a few days fearing some remote action, pre-configure devices to auto-wipe themselves if they fail to connect to Intune service for "x" days.

Failing to plan, is planning to fail.

- Alan Lakein

CONTACT US

ATTOSOL TECHNOLOGIES

www.attosol.com
contact@attosol.com

THANK YOU