Insurance Company with a High Attrition of Sales Force Took Control of Sensitive Mobile Data

Client Profile

Industry: BFSI
Business: Insurance

Need

Delete corporate data from mobile devices (remotely) when employee or agent leaves the organization

Solution


Mobile Device Management


Mobile Application Management


Mobile Email Management


Data Loss Prevention

1Mobility Offerings

- Enterprise Mobility Management (EMM) through consulting, development and managed services
- Data Loss Prevention (DLP) of Mobile Data
- Compliance enforcement and monitoring
- Containerization
- BYOD Management

With 50 -80% attrition in the insurance industry, it is critical to be in control of sensitive corporate information as well as customer data and wipe the corporate data from mobile devices when an employee or agent leaves the organization

Challenge

One of the India's highly trusted insurance companies was concerned about the visibility into the devices which carry the corporate data and exit process for the sales force, both employees and consultants. For ease of doing the business and for increasing productivity and efficiency of the employees on field, the company embraced mobility. They deployed use of mobile devices, few of which are corporate-owned along with some productivity applications and Sales Force Automation (SFA) Apps.

"The devices on field have access to an enormous sensitive data, mainly of the customers", quotes the insurance company's IT administrator. However, the IT had no procedure of managing and wiping the selective data when the employee leaves.

Solution

1Mobility provided with affordable solutions which was privately installed for the company, enabling **over-the-air distribution** of mobile applications, configuration settings and security policies to corporate-owned or employee-owned devices through a central web console.

Meeting all the requirements of the insurance company, firstly, **1Mobility MDM** helped them in keeping the inventory of the devices, publishing the security policies and compliance requirements and the most important one was remote access to the devices to enable and delete the corporate data. IT administrators could over-the-air de-enroll the devices from the environment instantly when an employee leaves.

"We could selectively wipe the corporate data which is stored in a

About 1Mobility

1Mobility, a global company, offers a cloud based, internationalized and scalable Enterprise Mobility Management (EMM) solution that secures, monitors, manages and supports mobile devices across platforms, service providers and manufacturers.

1Mobility provides an affordable solution, enables over-the-air distribution of mobile applications, configuration settings and security policies to corporate owned or employee owned (BYOD) devices through a central web console.

Contact 1Mobility at

info@1Mobility.com

separate container on the employee's personal device. Thanks to the 1Mobitlity Containerization!" says the IT Administrator.
IT Administrator was able to remotely disable access to the corporate apps though **1Mobility MAM** whenever an employee leaves or loses the mobile device.
In addition, 1Mobility's **Mobile Email Management** enabled the company to protect the email data and attachments on the mobile device.
1Mobility also provided company with many **Data Loss Prevention** (DLP) restrictions and policies on the mobile devices.

Results

1. Increased efficiency without compromising security

The insurance company was able to keep the vision of increased efficiency and productivity through mobility and also take control of the corporate data. The sensitive data and information about the customers on the mobile devices of employees could be easily wiped once they leave.

2. Streamlined Process

Earlier, procedure was to confiscate the mobile device and manually delete all the data relevant to organization if the administrators ever got physical access to the device, now this could be achieved with a click of a button through a central web console. Also, IT has complete control and insight into the inventory of devices that has access to corporate data as well as was proactively manage Apps and compliances.

3. Escalated concentration on core areas

Though dealing with high attrition with field force resources, rehiring and training them remains a challenge, the Company doesn't need to worry about the potential loss of sensitive data anymore.