IBM CIO Office

IBM on-boards 15,000 devices the first day after deploying mobile device management software

Overview

The need

The IBM CIO Office sought to rapidly deploy advanced mobile device management and security to its worldwide population of smartphones and tablets.

The solution

The office deployed MaaS360 by Fiberlink®, an IBM company, mobile device management software with advanced device and application security and a cloud-based delivery strategy.

The benefit

Using the MaaS360 software the office began on-boarding 200 devices per minute at peak—15,000 users on the first day—providing them with mobile flexibility and helping IBM tightly manage access.

The IBM CIO Office drives change, innovation and efficiency within the enterprise by helping ensure that the company's IT operations are responsive, resilient and secure enough to keep pace with ongoing changes in technology and business requirements.

Advancing mobile device security

The CIO Office manages about one hundred-thousand IBM employees' smartphones and tablets. Not only must it provide these employees with mobile flexibility, it also needs to ensure that these mobile device assets are adequately protected. Achieving these objectives required the office to deliver more than basic mobile device management; it needed to provide advanced mobile application and access security as well as expanded levels of mobile capabilities. Moreover, the CIO Office wanted to deploy these capabilities to 90,000 devices within one month, at a low cost.

The Fiberlink MaaS360 solution's cloud-based capabilities help the IBM CIO Office team rapidly deploy advanced mobile management and security solutions throughout the global IBM mobile community. "We were boarding devices on MaaS360 five days after the close of acquisition—15,000 on the first day, and over 30,000 in the first week," says Bill Tworek, executive IT architect for the IBM CIO Office.

Cloud-based mobile management and security

The CIO Office deployed the cloud-based MaaS360 by Fiberlink, an IBM company, mobile device management solution to speed adoption among the over one hundred-thousand IBM mobile users and reduce risk for IBM. Plans include deploying a MaaS360 built-in application security layer, which will allow the software to encrypt and authenticate each user and each application as it is deployed. The device management capabilities of MaaS360, Gartner Magic Quadrant leader, will help IBM easily distribute, update and manage these applications throughout their lifecycle.

Speeding deployment and reducing risk

By using MaaS360 software on the cloud, the CIO organization rapidly extends unprecedented security and mobile device management capabilities to IBM and its mobile users. "We were on-boarding devices on MaaS360 five days after the close of acquisition—15,000 on the first day and over 30,000 in the first week," says Bill Tworek, executive IT architect for CIO Office. He notes that, to-date, nearly 70,000 IBMers have self-enabled their smartphones and tablets with MaaS360. "It took us less than 3 days to integrate MaaS360 into the IBM architecture and by moving from an on-premises model to a cloud model we'll save USD 500,000."

Solution components

Software

- Fiberlink® MaaS360, an IBM company

For more information

To learn more about the Fiberlink MaaS360 mobile device management solution, please contact your IBM marketing representative or IBM Business Partner, or visit the following website: **ibm.com**/mobilefirst

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
March 2014

GMC14035-USEN-00