



The inside track
on how CIOs are
revolutionizing
device provisioning



In retrospect, it is obvious: Employees were typically bringing their own iPhones, iPads, Macs and other devices to replace enterprise-issued Blackberry devices and PCs at work. There were two reasons for this. First, Apple makes products that consumers find easier to use; and second, a typical enterprise does not provide employees with a choice of corporate-provisioned Apple devices. For many CIOs, Apple devices presented a daunting challenge to their traditional approach, refined over 30-plus years, of using traditional PCs. CIOs are risk averse—a trait that seems to come with the territory—and have naturally been resistant to the trend. However, things are changing. One recent industry study said 2016 showed a rise in Mac and iOS device adoption. It found that more than 40% of organizations included in the study offered employees a choice between a Mac and a PC, and over 65% offered a choice between different mobile devices that included Apple devices.

The fact that Macs and iOS have a ticket into the enterprise cannot be attributed *only* to pressure from employees looking for a better user experience. A key reason is that CIOs are being confronted with heightened security risks and stricter compliance requirements. They have figured out that Macs could bring a solution within grasp, without the need to increase funding.

To leverage the advantage presented by Macs, CIOs need to look at doing things a little differently from what they are accustomed to. This means looking at new processes to configure a machine, provide encryption and build a support desk. And once that is done, the astute CIOs will quickly realize that the upside goes beyond lower costs and better user experience. They will discover that they can take the lessons from a Mac environment and implement their experiences in a PC environment. In a single stroke they can enhance security, within budgets, and delight employees across devices.

Old way: High touch process

To appreciate how a Mac changes user experience, it is first necessary to understand the PC experience. Assume that Janie Doe¹ requisitions a new device. She places an order in the enterprise system and the device is shipped to an IT department warehouse. IT receives the package and unboxes the device. An IT specialist then proceeds to power up the device, checks for network connectivity, places a corporate image on the device, turns on system protection with passwords and a good dose of antivirus, loads it with data and corporate applications (such as accounting software if Janie is from the sales or finance function), configures email along with some collaboration tools, sets default printers and other hardware, then activates monitoring and encryption tools. This configuration takes hours, sometimes days. The IT specialist then provides the device to Janie. She receives the package and unboxes the device with some instructions. There is an obvious joy in doing this. But the joy is short lived. Once the device is handed over to her, she must complete the remaining configuration steps and personalize the device to her liking. She must call the helpdesk for support when the device needs attention. The act of calling helpdesk doesn't come easily to Janie. She lives in an age when self-service is the preferred model of support. And that means turning to Google for answers, not calling the helpdesk.

Notice the high touch, configuration intensive process this has been for Janie.

Apple has turned these traditional processes around by applying the Device Enrollment Program (DEP) to Mac—as well as iOS and tvOS devices—with a mobile device management (MDM) platform for enterprises. The program requires an enterprise to set up a DEP account. This account has devices linked to it.

¹A composite of several employees

New way: Zero touch

In our new Mac + DEP + MDM scenario, a linked device is shipped to Janie. She removes the shrink wrap and powers up the device. The device calls home to Apple and authenticates with the DEP server that the device is owned by Janie's organization. The DEP server then redirects the device activation to the organization's MDM platform. The MDM platform does its magic. For Janie, this is already starting to feel like a consumer experience. She is admiring the device in her personal space, while the device hums with activity and completes self-configuration.

The MDM prompts Janie for permissions and based on her role, job description and geography pushes over-the-air policies, applications, configuration and security packages. Mail, calendar, and contacts are synchronized and the device is ready for use! Janie is ready to be productive in minutes. No one from the IT department needs to touch the device. When she needs support, the MDM provides a self-service portal that can be loaded with a host of links and short videos that are user and context specific.

In the background, the enterprise has already paid for all the apps it needs and the app catalogue is available to employees to select their tools when required.

This is a zero-touch model that today's employees appreciate and one that CIOs want. They, however, have apprehensions because of the unfamiliar technological terrain the solution treads in.

About the author

Michael Vollmer
General Manager and Practice Head
for Wipro's Apple Practice,
Wipro Limited

Michael has a diverse global experience of over 17 years that includes Product Portfolio Management, Enterprise Risk Management,

This is a zero-touch model that today's employees appreciate and one that CIOs want.

Beyond the user: Better security and compliance

With the user taken care of, it helps to examine the Mac model from an enterprise perspective as well. Aside from the fact that the Mac model lowers the total cost of ownership, it also provides the enterprise with complete control over the device—something it cannot have in the BYOD model. Using DEP + MDM, the enterprise can turn on/off many features on the device at will. The user continues to have administration rights, but cannot overrule the policies on the device. This means the enterprise can turn off the camera, turn on encryption or take any such decision required for security and compliance without having to touch the device. This is a very powerful capability that CIOs do not have in a PC environment.

Enterprises—big and small—are realizing Apple has once again changed the game with new tools and methods to transform how devices are deployed, secured and managed by enterprises, with a focus on an amazing user experience. But, most of all, the use case provides improved security and compliance with lowered total cost of ownership.

Building Organizational Capability, Business Controls, Business Partner Compliance and Financial Risk Management. His expertise in digital transformation has helped enterprises empower their employees and customers alike with modern tools and capabilities.

He can be reached at michael.vollmer@wipro.com

● **Wipro Limited**

Doddakannelli, Sarjapur Road,
Bangalore-560 035,
India

Tel: +91 (80) 2844 0011

Fax: +91 (80) 2844 0256

wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 160,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information,
please write to us at
info@wipro.com

