How modern device management is helping Microsoft employees and IT managers work better

Microsoft is now reaping the benefits of fully embracing modern management, says Senthil Selvaraj, a principal program manager in Microsoft Digital. (Photo by Senthil Selvaraj)

Microsoft Digital technical stories

Microsoft lights up around 40,000 new devices each year. To efficiently manage all these devices, the company has been on a mission to move a modern device management system to the cloud on Microsoft Azure.

For better or worse, that has meant two years of working in a rather complex co-managed state between the legacy and modern device management systems. Now, thanks to the final roadblocks being cleared, the new management platform, Microsoft Endpoint Manager, has achieved the full functionality needed to bid goodbye to the old legacy system and fully embrace modern device management.

“For us, the biggest need was to enable device mobility for our users, so you can use any type of device you want to access corporate resources,” says Senthil Selvaraj, a principal program manager who leads the project for Microsoft Digital, the organization that powers, protects, and transforms Microsoft. “We’re contributing to our digital transformation.”

The legacy System Center Configuration Manager (SCCM) required that any new device being added to the network had to be joined on-premises through a hardwired ethernet connection. That kind of requirement is increasingly unviable in the current and future remote work world.

Secondly, cloud-based modern device management breaks free from the legacy device imaging process. That process involved building and maintaining images—the files that enterprise companies send to manufacturers containing the

operating system, apps, and certifications that should be included on specific devices—on a monthly basis.

> *With this move we're now able to eliminate all of those costs associated with imaging, the cost of lost productivity of users having to set up their devices, and potential security risks and threats.*
>
> *—Senthil Selvaraj, principal program manager, Microsoft Digital*

These enormous files of 30GB or more had to be shipped overseas by enterprises to manufacturers, tested, and then shipped to users. "That was kind of a problem because by the time those devices would be sent to our users, they would already be out of compliance, in terms of policies, security, and updates," Selvaraj says.

The final destination of the device's journey also had opportunities for improvement. Once a user received the device and turned it on, it could be hours before they were able to actually use it, waiting for the machine to download those 30 GB of images, rebooting, and rebooting again.

"With this move we're now able to eliminate all of those costs associated with imaging, the cost of lost productivity of users having to set up their devices, and potential security risks and threats," Selvaraj says.

[*Find out how Microsoft is managing Windows 10 devices with Microsoft Intune*. *Learn more about reducing friction throughout the device lifecycle at Microsoft*.]

A phased approach

Moving from the on-premises environment to the cloud couldn't just be done by flipping a switch. Selvaraj and his team wanted to make sure it was done with minimal disruption to employees.

"When we went to make that move, we realized that Microsoft Intune was not as mature as SCCM as a solution that's been in place for decades," Selvaraj says. "We partnered with the product teams to make sure that all the capabilities were there – provisioning policies as well as apps, and accounting for Microsoft devices as well as personal 'BYODs' (bring-your-own-devices) that would need to be supported by the new platform."

Working closely with the product teams, they started small with early adopters to move into the pilot phase.

During that time, they worked to identify gaps and further develop various integrated systems—this included adding layers of authentication security with Azure Active Directory and Microsoft Intune, the company's cloud-based service focused on mobile devices and application management.

The team also leveraged Windows Autopilot, the technology that provides setup and pre-configuration services for new devices so they're ready to use right out of the box. That would allow users to start working on their new devices within minutes of turning them on and become a zero-touch solution for IT managers, something that has since turned into reality—the only thing the team must do now is test original equipment manufacturer (OEM) Autopilot images to make sure they meet Microsoft's requirements. "This is a best practice that we share with our customers," Senthil says.

> *One of the beautiful things about it is that it doesn't have all these massive churning pieces. It can update itself dynamically, and it's pretty much seamless to the user.*
>
> *—Daniel Manalo, senior service engineer, Employee Experience team*

Daniel Manalo, a senior service engineer for the Employee Experience team at Microsoft, remembers the pre-cloud days with a shudder.

“There was this churning update process we’d have to do several times a year,” Manalo says. “If we had security updates for software, feature updates, etc., being dependent on physical on-prem infrastructure, basically we had to do our day job while taking infrastructure down and allowing this backlog to churn through. Meanwhile, people are frustrated, and the global help desk is getting a lot of calls. It was not fun.”

Modern device management, by default, doesn’t have the physical infrastructure where services must go offline.

“One of the beautiful things about it is that it doesn’t have all these massive churning pieces,” Manalo says. “It can update itself dynamically, and it’s pretty much seamless to the user.”

A phased and gradual approach to introducing new cloud-managed devices, the team realized, would dovetail well with Microsoft’s existing device refresh cycle, with employees receiving new devices every three years.

“The biggest learning was for us was how important it is to allow time for the piloting and testing so the solution is ready for primetime external users,” Selvaraj says. “Don’t rush into it. Take your time, and if it takes you a couple of years, so be it. Ultimately you’ll get to the end goal.”

Co-management becomes modern device management

By the end of 2020, primetime was just within reach—but there was one final hurdle.

With SCCM, the management team had the ability to use Group Policy Objects (GPOs) to target policies. That meant that for any given device, they could assign a rules-based value that would communicate the desired Windows settings for particular categories of builds.

But that didn’t yet work with Microsoft Intune. Manalo says that while Intune was certainly more modern, it wasn’t originally designed for enterprise scale.

Plus, for mobile devices managed by Intune, the team needed to ensure that they could push expedited patching in the event of a security threat. “We needed a break-glass solution,” Selvaraj says.

It took close coordination with the product team to bring Intune to the ideal state of parity. Meanwhile, some devices were enrolling directly in Microsoft Endpoint Manager while others were still enrolling in the legacy environment.

In late 2020, that all changed.

“Now we have that parity,” Selvaraj says. “We’re able to push all the policies, we’re able to provision the apps, we have the security, the automation and the flexibility we need, and now we can officially say: Let’s move forward.”

A refreshing future

The use of SCCM co-management agent has been largely deprioritized. Through the device refresh cycle, the remaining 40 percent population of on-prem client devices will naturally dwindle to zero. Microsoft expects to be down to the last 10 percent by July 2023.

“We’re trying to expedite our migration of on-premises devices to modern ADD at any opportunity we can,” Selvaraj says. “Considering how we’re working to help our employees go back to working in their offices at some point in the near future, we’re recommending that when our employees start bringing these devices back online, that they do so using our modern ADD process.”

Within three years, every employee device will be in the cloud with full modern device management.

Employees likely won’t notice much of a change, other than being able to get to work right away on a new machine without fiddling with temporary loaner devices and endless reboots. They probably won’t have to call the help desk.