INGRAM MICRO CLOUD SERVICES

THOUGHT LEADERSHIP

4 Steps to MDM Success – Level Platforms

A 2013 Cisco Partner Network Study revealed that 90% of full-time American workers use their personal smartphones for work purposes, a finding that solidly confirms the reality of the BYOD (bring your own device) phenomena.

But, how does the fact that millions of personal smartphones, tablets, and laptops are being introduced into your customers' workplaces affect you, the IT solutions provider? Even though managed services providers (MSPs) may be adept at managing servers, routers, switches, desktop computers, and even laptops, many struggle to figure out where mobile devices fit into their business model. Some MSPs try to develop a different "per-device" monthly fee for managing smartphones and tablets, which often leads to a shock-inducing price tag as a customer tallies the number of mobile devices in the workplace. Faced with a difficult per-device pricing conversation, some MSPs may be tempted to throw up their arms and simply offer mobile device management (MDM) as a free value add. Even MSPs that are able to earn a little money managing mobile devices often shortchange themselves (and their customers) by addressing only a small portion of the management process.

The level of service you bring to your customers is far too valuable to merely give away or undersell. The good news is that MDM does not have to be a loss leader for your managed services business. By taking a different perspective on MDM and helping your customers do the same, you can start earning the profits your company deserves. Following are four steps that can help turnaround your floundering MDM sales.

Step 1: Don't Differentiate MDM Fees from Other IT Assets

Whether a mobile device costs less than a workstation or server or is used less or more is irrelevant. The fact is the device plays a key role in a worker's productivity, and if it's not managed properly, it can become a source of lost revenue, stolen intellectual property, or even hefty fines in the case of a HIPAA violation. Another important fact is that your customers often don't view mobile devices in a separate silo from their other IT assets. When an MSP calls special attention to mobile devices, it often creates objections and lengthens the sales cycle unnecessarily. Instead, MDM should be *part* of your entire RMM (remote monitoring and management) solution and mobile devices should be managed throughout their entire lifecycle.

Step 2: Start MDM Right With Automated Enrollment and Provisioning

One of the biggest challenges with MDM after the sale is the first step in the implementation process. How are you going to get all your customers' employees' mobile devices – many of which are personal devices – onto your managed services program? If you're managing more than a handful of devices, trying to manually enroll each device and provision it with your customer's policies will prove to be a daunting and unprofitable task. Instead, make sure your MDM solution includes automated enrollment and provisioning functionality that allows each employee to self-provision their device by opening an email, selecting a hyperlink, and following step-by-step instructions via a software wizard.

Step 3: Put Full Device Management in Your Customers' Hands

Mobile devices are often used to run mission-critical business applications and processes, and therefore require complete management — including software and firmware updates, security (user authentication, data encryption, remote lock and wipe capabilities), and automated notifications/alerting when problems occur. Unlike the standalone device management tools that come with consumer devices, a business-grade MDM solution integrated within an RMM platform enables you and/or your customer to monitor multiple devices, multiple operating systems, and multiple user names and passwords from a single dashboard, which is an absolute must for successfully implementing MDM as part of your complete IT services monitoring and management offering.

Step 4: Don't Make End of Life Management a Personal Issue

One of the trickiest and most frustrating MDM challenges your customers face is trying to keep each employee's personal data and applications separate from the company's applications and data. This gray area can come to an ugly head when employees leave the organization. MSPs can help their customers by using an MDM solution that addresses this issue from the beginning. One way this problem can be prevented is by setting up a "profile" for each mobile device, which defines the applications and business data storage areas for each mobile device enrolled in the MDM program. When an employee leaves, that business profile is then automatically remotely wiped off their device without affecting any of their personal applications or data in any way, making it a win for both parties and avoiding any unnecessary confrontation during what might already be an emotionally charged event.

By educating your customers on the value of a total RMM solution that includes MDM, you'll avoid devaluing this critical service offering. By selecting and deploying an MDM solution that addresses all key aspects of a customers' MDM needs as part of your end-to-end IT management — from enrollment and provisioning to ongoing monitoring and even end-of-life processes — you'll ensure your customers' mobile workers stay productive, your customers' data stays protected, and your role as the trusted business advisor stays intact.

Dave Sobel, Level Platforms

Dave Sobel is a former CEO of MSP Evolve Technologies. Sobel joined Level Platforms in January 2012 as the director of partner community, serving as the conduit between Level Platforms' partner base and its executive team.