

Digital Workplace Deep Dive Podcast Series

Episode 41: Improving digital employee experience (DEX) through modern device management
<https://www.unisys.com/podcast/dws/41-improving-digital-employee-experience-through-modern-device-management>

Weston Morris:

Well, welcome to season four of the Digital Workplace Deep Dive Podcast. I'm your host, Weston Morris.

Weston Morris:

It's hard to believe four seasons. As I take a look back at the previous three seasons, we have all been through a lot together over the last couple of years, especially, and I know a lot of us, as we look ahead to 2023, we're wondering, what will 2023 bring and, uh, how will that impact the digital workplace? So I did a little research. One thing I looked at that got my attention was a study by Gartner they published just a couple months ago, back in November, on the evolution of the digital workplace. And one of their predictions really caught my attention. They said 85% of enterprises in the next three years will have implemented modern device management. They're saying it's here, it's real. It's finally gonna be everywhere <laugh>.

Weston Morris:

Now, I know you're probably familiar with modern device management. It's not exactly new technology- deploying Intune, Workspace ONE, something like that to manage your devices over the air, like you manage your mobiles. But it's still left me with some questions. Is this just another cost savings thing or does modern device management let me change the way my business operates, maybe on the security side or other areas? And even more importantly, does it change the experience that my employees get? Well, to answer those questions, I finally cornered someone I have been wanting to talk to for quite some time. Mr. Chad Arvay. Chad, welcome to the show.

Chad Arvay:

It's great to be here. Thanks for having me.

Weston Morris:

You know, Chad, five years ago, I think you and I were sitting on opposite sides of the table. You led digital workplace services for a life sciences company, and I was doing an innovation workshop for you on mobile device management. That was the topic at the time- personas, I think we chatted about. After you did some great work there, you went on to do the same thing at a large U.S. media entertainment firm. And then finally, we at Unisys nabbed you <laugh>. You're now the chief architect of experience management in our digital workplace business unit. So Chad, I am really looking forward to our chat today.

Chad Arvay:

Yeah, it's really great to be here and it's great to be on the same side of the table now, very fortunate to be able to take the customer side of the story and perspective and bring it into a living thing for managed services.

Weston Morris:

So, let's get into it. This topic about modern device management, it's something that you have lived and breathed for many years. I think our guests that are listening, they want to hear the real-world story. They don't want to hear the hype, they don't want to hear necessarily the bits and bites about technology. What they'd like to know is, when we have modern device management in place, what does that let me do for my business and my employees in real-world scenarios?

Chad Arvay:

So imagine that you're responsible for workplace security and ensuring that data is secured, and really preventing data loss for intellectual property. And you receive a phone call at 2:00 AM after hours, and you're told that there's some employees that have gone rogue to further

complicate things. This is all the way on the other side of the world, and they're taking intellectual property from the latest product, and there's worries that they're gonna give this or share it possibly to another competitor or, who knows what they're gonna do with it. And then to make it further challenging, it's on a mobile device, right? And with mobile device security, they don't really configure the devices per se or manage the devices the same way modern management will. So with traditional device management, you're typically gonna have two different consoles, two different teams of engineers and mostly are gonna be focused on the PC side of things, right?

Chad Arvay:

But with modern management, you start thinking about these things more unified, right? And you're starting to be able to go, okay, how can I help the security team with this? How can I lock down this device to ensure that the device remains intact for further investigation? So in this tricky situation with it being a mobile device, with it being all the way on the other side of the world, and not having any time to waste to, you know, contact different teams, or run different commands and wait, you know, 15, 30 minutes for the configuration to take place, you're able to use modern management, you're able to find that device and within about two to three minutes max of configuration, you're able to successfully reset the passcode on the device, work with the IT departments or security departments to recover the device and then successfully unlock it so they can continue their data forensics investigations. This could never have been done in traditional management. So I think this is a very important play on how we're able to immediately resolve these issues in the unified console and unified team structure with modern management.

Weston Morris:

So I think you're highlighting here, Chad, one of the reasons why modern device management is so important today is because devices are mobile. And we used to have them in the building, we could lock 'em down, we had control over them, but now they're not. And we need to be able to manage and support them while they're out, you know, in the wild. Now, the example you just gave here, I love because it's, you know, it's germane to the business, protecting the business and intellectual property of a company. But let's look at it from the end user side of things. Does modern device management do anything for the end user? Can you walk us through, maybe, a day in the life of- comparing that for us?

Chad Arvay:

Oh, yes, absolutely. I mean, we can start with sales, right? We've had scenarios where sales folks on the road need their laptop re-provisioned, and they don't have time for us to send them a new device while they're on the road, right? And they could be changing hotels in a 24- or 48-hour period. So how do they get that device? How do they know where to send that device to? But what we're able to do is actually walk them through some very simple instructions. I think it's about 10 steps actually, if I recall, and actually reprovision their whole device over the air from their hotel on the Wi-Fi. Typically, you know, on a Wi-Fi network at a hotel, it might take a little longer than being at your home. But the fact of the matter is, is within an hour and a half or less, they're not only up and running, but they're actually reining all their data back to their device and their files that they need for being on the road.

Weston Morris:

I've just gotta do my job, right? I've got this device, I'm swapping it out. I need to have my apps, I need to have my data, and it just needs to work. And in the past, I can think of times where prior to modern device management, I would have a hard drive shipped to me <laugh> and my instructions were how to swap out the hard drive for a failed device so that I could be made whole again, because there was this whole traditional imaging process where they would have a corporate image burned onto the hard drive and then sent over, and that's not needed anymore. Are there any other examples of where you see this making life easier for the end user if the company has implemented modern device management?

Chad Arvay:

Yes, absolutely. And I think before we jump into some of that, let's go back and talk about what you just mentioned, which is the traditional management being, you know, taking out a hard drive, right? I remember those days as well, you just gave me flashback central <laugh> on that, but how about not getting your data or putting it on a thumb drive yourself and then you forget, you know, did I transfer the right stuff over? And then you have these, you know, legacy thumb drives back in the day that would take forever, you know, gigs of data being transferred over <laugh> taking hours and hours to get back on your device, right? And then also, what about the files that you didn't have on your device, but they were stored on a map network drive, and now you have to use a VPN to reconnect onto the network to get those files?

Chad Arvay:

You know, so a lot of this traditional thinking originally was, expand your corporate perimeter, your network perimeter, and basically if you work from home, that's great, we're just gonna expand our perimeter and include you in that and use the corporate network, right? And there's a lot of limitations there. You can't get your group policy updates off of VPN the majority of the time. You also can't receive patches, and as you said, patching, you know, to the end user, it's not gonna be the most appealing thing. But also nobody wants to be the reason why a company got compromised, right? So it is our responsibility in it to maintain that. But back to the user experience is, you know, things like, I've been at companies where single sign-in was only working appropriately when you're on VPN, right?

Chad Arvay:

Because they were, they were sticking to being on-prem for their identity management. And that will come in a later topic about our forward thinking on how this is not only- traditional management was very focused around the device and supporting the device. This is now holistically enterprise architecture that we're looking at here. And that's what is really exciting about this, is we're not expanding the perimeter here for the network. We're actually saying, you know what? Let's utilize more of the internet and configure devices and secure them and have a great onboarding experience everywhere. And that's what a lot of modern management does, is it enables, from onboarding to the lifecycle of the device, integrity and a lot of precision when it comes to configuring and maintaining devices for a better experience.

Weston Morris:

And, and let's go back to the CIO's side of things or even the CFO. Does modern device management reduce the cost of managing my devices from a corporate side of things?

Chad Arvay:

I firmly believe so. And the reason why is because in, in my experience, I mean, I've seen companies when covid happened, they went remote every time they shipped a laptop, they had to call a service desk. That's a service desk ticket every single time. That's a resource, that's losing productivity. That's two resources, right? There's the service desk agent, there's the end user that's calling, and then you're paying sometimes, you know, for the ticket and the support depending on how you're set up or your billing is set up. So when you are able to make this seamless, everybody, if you really think about it, you're consumerizing enterprise onboarding and deployment. Most people have an iPhone or an Android device. What do they do when they get it out of the box? They turn it on, they go through a few, or couple steps. If they have an existing phone, it sets up and guess what it starts doing?

Chad Arvay:

Pulling from iCloud, right? Or pulling from Google's cloud and it pulls your files and your apps back from the Play store. So a lot of our users are actually already self-trained on this because they do it in the consumer market. So what ends up happening is you're gonna have less tickets. I mean, I've been in accounts where I've reduced tickets for onboarding 60, 70% from going to this method because it's something familiar. It may look different on a Windows device,

but the concept is familiar with the user and that concept of ROI- you're eliminating a lot of calls to the help desk.

Weston Morris:

And it's even worse than that. I think there's times when with traditional device management, you even have to have field services involved. Not just a service desk call, but somebody physically coming to your location and looking over your shoulder and banging on the keyboard or swapping out hard drives to make it all work. And that's all gone as well. Another big expense. So Chad, I think we've covered here the benefits to the organization, to the company in terms of security and cost, moving to modern device management. You've hit on some really good examples of how it benefits us as end users, especially working remotely, to have modern device management. Let's switch gears here a little bit and talk about what does it take to make it happen. I mean, when I think of modern device management, I think of, you know, Microsoft actually coining that term, I believe. And so I'm thinking, okay, I need a platform, so I'm gonna deploy Microsoft Intune. Or if I'm a warehouse, I'm gonna deploy Workspace ONE and that's it. I've got the platform, I'm good to go, but I feel like I might be missing something. <laugh> Is that right? What else is needed?

Chad Arvay:

That's a lot of times what companies think and they stop there. But really this is an enterprise architecture function. This is an enterprise strategy that has to go all the way to the top. And the reason why is because there's so many different functions in IT involved and there's so many benefits here. It was originally coined by Microsoft as Modern Device Management, and I see them using the term modern management now more than modern device. And I think the reason for that is because it's not just the device anymore. You know, for instance, the identity management, you have to have a good identity management platform. It needs to be cloud-based. If you go and do a ticket analysis on any account, I will say 80% of the number-one ticket drivers is password resets.

Weston Morris:

Mm-hmm, that's true.

Chad Arvay:

Yeah, absolutely. And some of that is, oh, we're gonna require a VPN to reset your password. My question is why? And the answer is because they expanded their network perimeter and their mindset is, use the corporate network. But we don't need to do that in 2022, right? We can securely reset the password using Azure or Okta or whatever IDP you want to use. So you know, there's a number of advantages there. Obviously, seamless single sign on across all your applications, handling your password resets. Also you start getting into your certificates, right? User certs, device certs. You want to be able to manage those securely, right? And not only securely, but you wanna have high availability, meaning that you're able to deploy and assign those over the internet, right? Not relying on a VPN connection to connect to some internal PKI on a domain. Those days are done. We don't do that with mobile devices.

Chad Arvay:

We also don't do that with Mac OS devices. So why would we do that with Windows devices? There's no reason to. You can eliminate and minimize a huge chunk of your PKI infrastructure to be internet-facing and still secure. And that's something that I see being a huge challenge, a lot of times. It's not that companies don't wanna do it, it's just they're not relaying it into an end-to-end modern management strategy. It's kind of all siloed off. You have identity management doing something, you have certificate team doing another, and then you have device management. And really all of those things need to be part of enterprise architecture. Some of the other items there, you get into asset management, and I think this is something that really evolves when you implement modern management and part of modern management is you're collecting a lot of data.

Chad Arvay:

And really any company with a healthy IT hygiene should be collecting that data, and part of modern management is incorporating that data into some type of data lake or data warehouse. And one of the benefits of that, and every enterprise you go to, you'll hear a joke of oh, asset management, yeah, my CMDB. Oh, if that's accurate. Well, why is it not accurate if you're plugging in multiple data sources, right? Azure AD can track what the device name is and map it to the user's identity that's actually using that device. SECM, Intune, AirWatch, they're all other sources of great data that can do similar things. So when you're able to combine this data and make accurate assumptions based on logic, you can start having an accurate CMDB. And I think that's huge because that's also a huge gap you see in a lot of companies.

Chad Arvay:

And this also goes for software, software usage as well, right? Is understanding what's installed, what versions installed, what has a license, and is that user using that software? And that's traditional software metering, but you're able to use additional sources to basically go, no, you're not using it. It's not just one source saying you're not using it. We have multiple sources saying you're not, so we're gonna reuse that license. And also being nimble enough to be able to go, you know what, maybe you only use it for six months out of the year, but we have someone else that does use it for another six months. So instead of having two licenses, we'll just, you know, split over to one. There's all types of benefits from really going to a modern mentality.

Weston Morris:

I saw a report from one enterprise where they actually started looking closely at that, what you're talking about, the asset management, specifically the software licenses, and found that they could save \$35 million in a year in licenses. Of course you have to have data knowing what's there and what's not. And you're telling me that's actually part of a good modern device management, or at least you better be thinking about it as you deploy your modern device management architecture. I love it. You kind of hinted at it a little bit, about some of the lessons learned. Cause you've done this with some pretty big companies and nothing goes perfectly. We don't want to paint, you know, oh, modern device management's the solution to everything. What are some of the challenges you've seen and what would you do differently? What can CIOs that are listening benefit from, you know, some tips that you'd like to share?

Chad Arvay:

I think a lot of the challenges, it really goes back to making sure to remove some of the internal friction in IT. Meaning you have to have a unified strategy for this to work appropriately. This is no longer just a device management technique. This is no longer just digital workplace. It incorporates a lot of different folks, especially in security and identity management. And it has to be seen as a priority. A lot of times some of this end-user facing technology is not, right, it's not seen as improving the user experience. Which at the end of the day, that's what this does. It improves the onboarding especially, it improves the overall user experience. It also improves security and prevents some configuration drift when you're able to saturate and deploy configuration to your environment holistically without requiring the VPN. So it's really, you know, embracing the modern techniques.

Chad Arvay:

And I think if you take shortcuts and you segment this, you will not get your maximum return of value. And you'll also see some of the pain points with this. A lot of what happens is this goes into a strategy and someone goes, yes, I want modern management, but what they're not doing is, they're not looking at all the steps that you have to take to get there. So you've gotta begin that journey. That's what I think is one of the biggest risks, is not lining those things up in a methodical approach and executing on them. And it's a multi-year strategy. It's not a, let's get this all wrapped up in one year. Luckily I've been at a company where we've done that successfully because the planning somewhat thoughtfully, but somewhat luckily <laugh> worked out in the end. But, you know, that would be my number one item I would discuss with CIOs is really make sure that this is an end-to-end strategy at the enterprise level. We have

buy-ins from the different teams, they're working together. They're not thinking of why we can't do this- because it can be done, and it can absolutely be done securely. And that's a big culture change and a big shift to a niche or functional technology to an enterprise architecture and strategy.

Weston Morris:

That last thing you said there, that it's also, it's not just technology, it's a culture shift. Now that is making me mentally here connect the dots between what we're talking about today and the last podcast we did on data-driven organizational change management, the importance of not just, you know, deploying the technology but educating and training people as to how this works, what their role is and how it would benefit them and how they can best take advantage of it. Cause if they don't, if they still do things the old way or have expectations of doing things the old way, having the field services person walk in and take care of everything for them, they're gonna say, oh, this is worse <laugh>. So, I'm gonna add that to the, to the list of recommendations: Think about your organizational change management. Well, we've talked about a lot of great tips here. Chad, I really appreciate you sharing your real-world experience with us here, but I'd like to come back to what you're doing now at Unisys. I mean, you've got this great career in making modern management a reality, but oddly enough we now have hired you to do something else. I'm gonna say it sounds completely different. I mean, can you remind us again what it is you're doing here?

Chad Arvay:

Yeah, I'm the chief architect for proactive experience management. So really the next step in device management, we're doing all these great things in device management and modern management, but it's not just the device, it's the experience, right? The employee experience. That's what we're concerned about. That's what we're improving. And there's a Vanson Bourne study that was done and it revealed that 34% of employees never call a service desk. Well, it is and it's not. I mean, if you walk around an office pre-COVID, oh gosh, I sound like a dinosaur saying that. But pre-COVID, you know, you hear people complaining and griping. I used to see blue screens happening, people plugging in, you know, next-gen workplace, they go from one desk to the other, plugging in with USB-C. You see blue screens. They don't have time to log a ticket, right?

Chad Arvay:

So they're suffering in silence and they shouldn't, they absolutely shouldn't. But it's really, it's not that much of a fault of IT. We really haven't had the tools to show the visibility or observability on the employee experience, right? And it's starting to happen in modern management, but also, experience management in general has come to the market in recent years. And this really allows the visibility of employee experience and how we can use that data to improve their experience and make them more productive. There's been plenty of studies that have shown increased talent retention, increased productivity when things just work, and we're really there to enable business outcomes. That's what technology's there for, right? Instead of typing on a typewriter 30 years ago, we're able to do things faster with all this technology, right? So we wanna keep up that pace and we wanna improve it for the end user.

Weston Morris:

And so for our audience, we're coming back to this topic of proactive experience or experience management, which has been the subject, this year alone, of at least six of my podcasts. I will say, "better together" at least once a week. And I will do that here. I know Chad, you can deliver proactive experience with XLA and all that with a customer that does not have modern device management. They're using traditional device management and you can greatly improve their experience and eliminate downtime and improve productivity. But how do you see things changing? If a customer has modern device management, they're managing devices over the air in Intune or Workspace ONE, something like that. They've got OneDrive and things like that.

How does your ability to deliver proactive experience change if they have modern device management employed as well?

Chad Arvay:

Significantly, because when we're able to use the various employee experience data, we're able to measure the issues in the environment, the impact. And then what we do is we use not only that experience data that, that we used prior to determine the issues or the targets. We use the proactive experience tool to actually put automation in place, meaning we're preventing configuration drift, we're preventing the issue from happening again. So we actually utilize event-based automation to complement the original configuration. An update happened and let's say, your VPN configuration got set back to default. Well, I can set that right back automatically to your company's VPN configuration. A setting got changed on the OS after a Windows update. Well, that's gonna get set right back. And that's not gonna be based on a 15-minute interval or 45 minute interval or being on a VPN. That's going to be real time based on the event happening, right? And that's where these tools really complement each other. It's a one-two punch. You configure the device, but then you enforce the configuration to stay in place even if an event takes place.

Weston Morris:

Well, these are great suggestions, Chad. I think probably the nagging question in the back of our listener's minds right now is, well, where do I start? What do I need to think about first if I'm really getting going on my modern device management journey?

Chad Arvay:

Yeah, absolutely. I mean, the first place that I would recommend starting at is really looking at what your IDP is, your identity provider, and understanding the identity management tool itself. Some of the tools work a little better natively with different device management tools. Also understanding where you're at with your PKI and certificate environment. Is it only internal facing? Are you able to issue certs over the internet? These are all things that a bit of due diligence is needed, as they're prerequisites for the journey of modern management.

Weston Morris:

That is a great suggestion. Not what I would've thought of, Chad, thinking about identity management first. Well, I tell you what, Chad Arvay, chief architect for proactive experience here at Unisys. Man, thanks for carving up some time to talk with me about your experience with modern device management.

Chad Arvay:

It's my pleasure. Always good talking to you, Weston.

Weston Morris:

You've been listening to the Digital Workplace Deep Dive. I'm your host, Weston Morris. Thanks for listening.