Threat Protection focused on Attack Surface Reduction Device Control and Linux Deployment Office Hours [Americas_EMEA]-20250220_110109-Meeting Recording

February 20, 2025, 4:01PM

57m 54s

◉ **Amy Jarosky (AG Consulting Partners Inc)** started transcription

Amy Jarosky (AG Consulting Partners Inc) 0:15

Hi everyone.

Thank you so much for joining us today for the Threat Protection office hours.

We have lots of exciting information to present to you today and we also are here to answer any questions that you might have along the way, so feel free to post any questions in the chat and if we have time at the end, we will enable the M.

And you may ask your question in that way as well.

As always, we are recording this call and.

The event deck and the recording will be available on the FPC Portal blog within the next few days, so if you'd like to rewatch the session again, just head on over to the FPC blog and check it out there. If you'd like to turn on live captions, you.

May do so in your teams app by the more button.

Again, thank you so much for joining us and I will now turn it over to our first presenter, Matt Novitsch.

Matt Novitsch 1:15

Thank you, Amy.

Hello, good evening, good afternoon.

Whatever the location is that you're at.

So we'll start off with our first topic.

I will be presenting on device control and then I have Daniel backing me up for the deployment of Linux and the on Linux.

So that is what we're gonna be covering in the agenda. And then from the other part, we're gonna go over the advanced deployment.

Guides just to kinda make sure we get a refresher on those and then the SME request and then with if we have time the Q&A, we should have time for that. If not and we

don't get to any or any or all of your questions please.
Feel free to drop them in chat and we'll follow up with you afterwards.
Go ahead.
And next slide on this one, Amy.
All right, so this is just the presentation of me.
We'll go ahead and good for this one.
All right, so device control, main things that we're looking to focus on.
You know, what exactly are we trying to control here?
Main things are USB devices, cd-roms, printers, Bluetooth, anything that we can we're plugging into the device or into the endpoints. We want to be able to start controlling them.
While we're managing them on our corporate devices.
So a lot of things can come with that, with, you know, where do we start.
How do we, you know, determine what devices are?
There's a lot of ways to unpack this and how we generally start with this is.
What's your current policy like we we ask customers.
Hey, do you guys have a policy for if they already have one and they're migrating from a third party, that makes it significantly easier?
I do have some customers that are starting off with this as hey, we're going to start this from scratch.
We need to know, you know, where do we start from this. And that becomes trickier because your approaches on those are going to change depending on which, which way they tell you they're they're currently handling the situation so.
We're going to cover both of them.
If they're already using a device control or they're looking to like to call, throw the hammer down and basically block all the endpoints from being able to connect devices. There's a way we can do that where we do a, I'll call it a deny all first and then.
We start allowing devices going forward and some of those can be like USB sticks.
I have some customers that are like, hey, we want our our employees to be able to plug in their phones but not be able to mount their phones.
And there's ways we can control that as well.
So we'll go through all that and and I'll show you a demo of of what it looks like within Intune to get that going.
You can do this in Group policy as well, although we want to encourage people to

use Intune because it is significantly easier doing this through Intune.
Go ahead.
Next slide, Amy.
All right. So talking about, you know, benefits of it, really it's it's about, you know, what is the customer looking to do a lot of this is about controlling what people plug in, what they're accessing.
You know, this could start leading into like DLP technologies.
So depending on how your conversations are going, we could absolutely start off with device control and then it could turn into something like, hey, we wanna look at you know managing files and and what people are putting in those files.
Well, then we're we're jumping over to adlp discussion. And if you've seen deployments before or if you've actually experienced them yourselves or deploying them yourself, you'll know these conversations kind of bounce back and forth depending on every situation that you're in, which kind of highlights to the the.
Second point of ensuring corporate data is not printed outside.
So a prime example of that would be like, you know your you have employees that work at home, but you don't want them printing off their home printers, but you want to make sure they can still print off like corporate Wi-Fi.
Or their corporate printers, but not anything off any personal devices. So go ahead.
And next slide on this one, Amy.
All right. So we are going to be sharing the slide deck out.
There's a lot of links in here.
All this will be covering of what we're going to go over.
I did just want to make sure all the documentation we have is available out there.
The very bottom link is my own self plug.
Yes, I am not shameless at all to to go out there and plug that.
I do have an article about doing the device deployments that I've done previously, so feel free to use all of these links.
And then you can also always request to me at the end.
And we'll go through that process a little bit further down the road.
Go ahead.
And next slide.
And now we're going to jump right into demo.
So, Amy, I'm gonna grab this from you.
Alright, so let me get this bar out of my way.

Alright, so first thing I wanted to go over is when we're doing like an Intune deployment from it.
We were talking about that default deny all and what that does is it goes out there and says, hey, you plugging anything in the device, we're gonna flat out reject it and say we're not gonna allow this into the environment and that'll help keep it from the the.
The hammer approach I was talking about before, where we're just saying, hey, we're we're gonna flat out reject everything.
So we authorized the use of it and that could be like you have certain brands of USB sticks or you provide like iron keys that you're requiring.
But again, that's all the branding.
Of what you have, I will say one of the gotchas that I ran into with this was.
Have a couple of customers and I even have one myself where I've had.
Ausb stick from when you go to those like trade shows or conferences and you know they'll they'll hand out USB sticks going oh.
Here's some more material.
Those sometimes are really hard to block.
Without the default block, because they're not adhere to the same policies as like.
A reputable vendor I guess is is what I'm looking for, like SanDisk or Kingston or anything like that that use standardization when they're creating their products.
And that goes for like serial numbers. If you're blocking my serial numbers or anything along those lines.
So going into this, we do have default enforcement right now.
You can see I have set up the policy and we're doing it through the settings catalogue within Intune.
So I'm gonna act this up one bit.
Well, actually here before we do that.
So you can see within here the default enforcements. All we're looking for for this.
And it's set to deny right now, by default, every Windows device it is set to allow.
So that's why right now it's not an issue because people can plug it in all day long.
But what we're trying to do is lock these down and make it more secure.
We're gonna flip that over.
It's gonna be at denied state and all we got to do for that, I'm gonna back this out.
Gonna come down. We're gonna create a new policy, then do Windows Center later.
Do the settings catalog.

Copy and pasted it from the previous thing.

OK, add settings.

Let's search for that.

And it's right there and it goes right back to what we had the screen up before.

So I can close that and you can see it's just that simple. And then we can obviously deploy it to whatever our scope tags are and then assign it to whatever groups highly, highly encouraged customers to do.

Groups first do not recommend doing all devices unless you guys really want it like a whole bunch of support cases and tickets coming in going. Why is my stuff not working anymore?

You know, target the groups, do the deployment rings.

That'll save you guys a lot of stress and headache.

We're not just for you, but also for your customer, and it'll make the deployment much smoother. Sorry, smoother.

And it'll also allow you to get higher chance success with employment.

All right.

And then once we did, you know, deploy that we're good to go. The next piece of that is, hey, what are we going to do for the actual USB devices?

So we're going to come into endpoint security.

The tax surface reduction.

What we're gonna start with is you would think you would be creating a policy, but what we wanna do is look at the reusable settings and there's a lot of different options in here. So ignore what I have right now. A lot of this will make more sense. Here in a second.

We're gonna bring this up if it wants to cooperate with me. There we go.

We're gonna call this USB because I don't have anything else to call it right now.

So we come to the add, we have a printer device and then we will storage.

So if we go to removable storage.

If we can get the configuration on this.

And there's a lot of different options you can see within here.

So we can pull up from device ID serial number. This is actually something that I have a couple customers using.

Comes a little trickier because you'd have to literally know all the serial numbers for your corporate environment, which could be thousands. If you have a larger environment.

But I try to discourage 1 customer from doing it.
But they were really focused on doing serial numbers.
So that's the route they're going to go.
But I warned them that that's going to probably be like a management you know, issue.
For some longer term, putting in each serial number for each device.
But again, that's how they wanted to track it, so that's fine as well.
There's also like primary ID. You can look in here that there's different primary keys that we can put in here.
Some of them are like DVD drive or sorry CD-ROM drives and then others are printers themselves.
There's a list of those I can get those for you. I probably should have done ahead of time. I really would think about that.
The other pieces now are like hardware.
Where do you payment?
So where is the vendor ID, right?
Like every vendor has their own ID and some of those that I'm referring to is like if you don't know it, that's fine.
Like no one knows it.
No one keeps track of that.
But there's sites that have all that, so we can go like there's device time that has this location.
These are all the on the reference links that it was referring to earlier, so you can also come in here and look at like you know.
Let's see.
And disk.
The same disc is a common one. You can see here.
You know, hey, it's a flash drive.
It's Gen. 3.
Here's the render ID right there.
So you would still have to identify you know which one of these is the one that we're actually going to use. You can see here they have a couple of them.
But the majority of them look like they're gonna fall into the 1921.
So if that's how you wanna allow SanDisk, you can put in the vid.
That's fine.

Or you can do the VID and PID which is also something that you can look at by looking up which is the the device ID itself.

Or sorry the what is?

It's called product ID.

Sorry, but you can also look up the device ID and I know I'm throwing all these out here.

There's a lot of different ways of doing it.

There's no wrong way of doing it.

You just have to figure out what is easiest for your customer.

A lot of my customers will use the VID along with the primary IDs, and then I've had a couple use the device ID and then what we kind of pivot around depending on what they're looking for. The instance path is also beneficial to use 'cause we can act.

Use that with inside advanced hunting so and I'll show you that here in a in a minute.

So depending on what you pick, you can absolutely go through this whole list and we're good to go.

Let me scroll back down.

On a so I can cancel this.

I remove that one because I want to show you the printer one as well.

So the printer one comes up is it's pretty simple. We got USB corporate network, universal file, custom and local.

They're pretty self-explanatory on what they are.

A lot of customers just want to do corporate.

Some have a requirement for USB.

It really depends on what they're looking at from other organizations spread out. If you have people working from home, you can't necessarily say block USB. If they're required to print paperwork for you know whatever they're doing.

Further job function or if they have a field office that we have customers coming in, they might need to print something in the only way they have is a UNC prayer hooked up to their machine.

So we can't just come in and say this is the best way to do it because we have to ask those questions.

We gotta know what exactly are they are they doing to accomplish their job?

So we're not blocking them from doing that.

And then obviously come down here with like printers and we're good to go.

And also I did not mention this, but hopefully I think Phillip did earlier. If you have

any questions, please feel free to jump in chat, jump off, answer them whenever he gets a chance to answer all of them.
All right. So some of these things that we're looking to look at so.
I'm gonna bring up the one that I was talking about before, where we were talking about CD and CD-ROM drives, right?
So I have this reusable configuration just as simple as CD-ROM devices. We come over to the configuration settings.
I just popped in the name the CD-ROM devices. If you look at settings, that's the primary ID for this and it's gonna block any usbcd ROM that's plugging in the device. Hands down, it's not gonna end.
Discriminate. It's just gonna say everything you're gone.
So that's one setting that I have in here.
We're good there.
The other one I wanted to make sure that I call out was the WPD.
Same concept I described the the name for the primary ID and I put it as the name just so I could keep track of what it was.
It also makes it very simple for doing these demos.
So WPD would be like your cell phone trying to plug it in.
I'm not gonna bother mount that thing, but it'll still charge.
So that was actually one requirement I had from a customer where they're like, we don't want it to mount, but we wanna make sure they can still charge the phones that they need to.
This'll allow that to happen.
Alright.
The other one that we can add in here is removable devices.
Same concept for here we have removal devices, just pop it in there.
That would be anything in your thumb drives, right?
Like any USB stick you're plugging in, we can block it out, right? And it's gone.
There's there's real simple on that.
That's that goes back to more of the hammer approach of we're gonna block everything.
These settings here for like allowing these particular functionalities would be if you had the allow state and you're trying to slowly take back the environment and and secure it down.
You could also do it going the other way, where we're saying we're only gonna allow

certain ones of these after we have the denial.
So again, depending on how you're doing it, you gonna have to pivot the approach and kind of play with these settings.
All right. Let's see here.
I'll pull up the SanDisk one here.
All right, so for this.
I have in my lab.
I have two identical sandisks. I grab the serial number off one of them and you can pull up the serial number.
One or two ways.
One of them is pulling up through device manager. The other way is pulling it up through PowerShell.
I did not PowerShell for this, so I'm gonna pull this up as I'm talking, hopefully screening just go black for everyone. If they did, I am sorry.
And of course, PowerShell is taking a sweet time loading.
Alright, we're just gonna get rid of that one.
I probably have something else loading.
I don't need it to load.
All right.
So as simple as get disc.
And give it a second. I do have a couple of them that are plugged in, so it's no I don't have actually any plugged into my computer. My apologies.
Let me flip over my lab real quick.
Alright.
And it's taking it sweet time.
There we go.
All right, so you can see here we have the multiple drives plugged in.
The GPT is the my hard drive.
You can see I have two SanDisk ones in here and if you look back at the screen I have here it is the C25 which should be.
This guy right here.
See a 24.
So I copied that, popped it in there. We have it in here.
I just have it labeled as SanDisk.
We're good to go, all right.

So these are all of our reusable settings.
And you can see we haven't even touched policy yet.
But we have all these different options.
We have.
We could already have set up and ready to go now going forward into it. Let's say now we need to create a policy to go with it.
So we go in here, we're going to open one up.
I'm going to use this one I already have because I know it's working and it's already applied to my device.
So you would open up the device control, you give it a name, you would apply one reasonable setting, so it pulls up the list of everything that you would have pre configured ahead of time.
In this case, we're going to do a allow by serial number and we already put that one serial number in there.
We're good to go.
And then we don't have anything under the exclusion list.
So we're good there, but we also want to make sure we edit the instance of it. And the reason for it is we want to actually give it functionality of allow.
Now, if we were doing a deny, we would flip this over to a deny state and we can see here we can deny specifically read, write, execute.
This is all really going to depend on what your customer's looking for.
So you're going to have to kind of go through and walk through.
What specifically are you looking to block?
Are you looking for them to block full USB just outright.
Then we check everything off. If they're looking for just, you know, blocking, say write access.
But they want to allow read. Then you know we would just accordingly.
Something to that effect. If they didn't want anything execute on there, we would obviously remove execute again. A lot of this would it really depend on what your customer wants on it.
So you'd have to kind of play with it and I'd really encourage you to play with it in your labs just to make sure you can understand how all this works.
The second important piece is we wanna do an audit deny and then for this one we wanna show notification and event.
And then again set a saying I would match it to the same one that you have for the

deny role up here so.
In this case, it was just we want to allow file read.
So what happens with that is if they plug in and they try to write something, they're gonna get a little pop up message in the bottom right corner that says your corporate, you know, policy does not allow you to write, you know, files to this device but it.
Still allow you to read the the device and you're good to go from there.
All right.
And then you know, again, depending on what your policies are, we would add more, subtract more.
But I do wanna make sure we get enough time for the other contents, so I'm gonna kind of zip these along here.
I'm gonna come back to here.
This will be the same thing if we wanted to block cd-roms and phones. I'm gonna come back into those policies.
So all we're doing here is blocking that one that I created that was cd-roms. It's good.
And then for here it should be the WPD devices.
We're good there, but since I have the default deny policy out there, it's not gonna work except for anything that I have for this.
But these will work anyways, but this is kind of the I wanna make sure you guys are aware this is everything that we would we could plug in if we wanted to deny certain ones.
Alright, now I'm gonna flip back over.
Demo.
Should say my lab alright so.
We saw the two USB devices for their these two are identical.
You can see they're different though, right?
You can see one has the on the F drive that has, you know, actually looks like their disk space on it and the other one just looks like it's a generic drive.
That's because the policy doesn't deny them power.
It's just denying them access. Depending on what your policy states.
So that one that wasn't the correct serial number, I try to access it and it comes up with absolutely nothing.
It says this drives unaccessible, so policy did its job.

We're good there. Then if we go over to the one that we allowed, you can see it's fully functional.
I can access it.
It's good all day long.
Now the other part of this is I do have a USBC ROM plugged in.
It does have a disk in it.
But it can't access the drive because we have that policy set out there for tonight.
I did not have an extra room for my phone on there, but I would show you, but it would be the same policy where it would show up as the phone mounted, but you wouldn't be able to do anything with that phone going forward.
And hopefully we don't have any questions going into this.
But at this point, that covers everything from a device control.
I know it's a lot of data to to absorb in the in the 20th ish minutes that we were talking about it, but feel free to play with it.
Watch the video again.
Go to all those reference links and if you always need to put this in your request in.
But now I'm going to turn it over for Daniel to go over the deployment for Linux.

Daniel Selleri 24:07
Thank you, Matt, and good morning.
Good afternoon, everyone.
It depends on where you are.
I'm Daniel solari.
A defender is me and today I'll be covering a few slides to get started with the customer and also some tips and tricks on Linux deployment.
Can you go to the first slide, OK.
So yeah, let's get started with the service description.
That'll be what would be covered by fast track or not, right?
And it's similar to what we have for Windows, but on Linux there'll be only servers, so chip Co engagement.
We can help the customer to check the network connectivity if they have any firewall proxy blocking the communication for. Of course the custom needs you have the license.
And the other point will be the OS version.
We have a documentation that says which version of Linux and distribution will be

supported. So we need to check out those and help them to understand their onboarding process and the key point here.

Be we help them to do the manual process to allow them to understand how to to do that and then they can automate using some third party tool right. In addition, we'll help them to create MDE policies, apply to the device we have different ways to apply those.

Policies it can be through a Jason file or through the defender portal.

That would be our recommendation. So in some case the customer is already using defender.

They are already have those servers onboarded, but they are pushing Jason files and OK.

It's supported, but our recommendation be to use the portal.

That'll be a centralized way to make sure all of the policies that were push it to those servers and they can see everything from from the portal, right? What is not covered if the customer is using a custom.

Or customized kernel of Linux again.

Needs should be listed on the supported device or I'm sorry. Supported distributions and versions.

That is not part of the benefit to help them to use thirty party tools to go in at scale, like Chief Puppet. Of course, if you will have, if things me have some more background on some of those tools, they can share some information, but that'll be as.

Best effort, not part of the benefit. We do have a lot of great documentation.

On how to configure and onboard those servers, push the client the the agent, the the vendor agent and onboard that to defender.

But it is not part of the benefit.

We can share that documentation with them and they can move forward with it.

Windows subsystem for Linux. It's not part of the benefit.

Excuse me.

And like any other workload, troubleshooting is not part of the benefits as well, right?

We need to ask them to get the support engaged with that. Of course, if we have the background, we can share our experience with them.

But the support team will need to lead it on the left bottom corner of the slide.

Actually, all of the slides will have the reference.

So you can check all of that information on there, for example, how to deploy defender using 35 tools that be the bottom link. There you can click it on it and see all of the instruments and those documentations are.

Very detailed, so I really recommend you share that with the customer.

OK.

Next slide.

Thank you.

Chip Co engagement.

I'd like to share that as an initial timeline some time to some. Sometimes the customer doesn't have the full visibility of what kind of activity they you need to do or how long that will take.

It is just a suggestion here.

Again, typical engagement and the key activities that you're gonna go through with them.

Those have the links as well. So let's say the customer wants to review.

Overview of security posture.

They can just click on it and see the documentation, and of course we'll cover all of that with them, right?

And again, the timeline, it's a one week two to three weeks.

It's just the baseline that if they need more time, we can extend that. While that is covered by fast track, we are good with it.

Next slide please.

Kick off discovery questions. So for the kickoff meeting, show the initial timeline so that you have an idea of how long that will take and activities.

But we need to discover the customer environment, right?

So ask them the number of servers distribution that they have and versions and another great example here would be if they are already using MD for any other OS. For example, Windows 1011 or Windows servers.

If they do, they are already familiar with the the portal and the onboarding process, right?

It's similar with when we talk about Windows, we need to install depending of the version of the windows we need to install the agent, the the defender itself.

Or for newer version it is already there, but we need to run the onboarding process and apply the policies.

So if they are familiar with Windows.

They are a step ahead for Linux as well.

Right. It is just initial questions. So of course you can.

Change those questions or add more questions as the answer and get more details about their environment.

OK.

Next slide please.

OK, once that you have the the the Kickoff discovery meeting and know their environment, we need to start explaining them to how to onboard.

Defender.

On Linux, to to the portal, we have the more.

Native way that'll be on the right part of that slide.

Up there we have Azure, so that'll be servers that are hosted on Azure. You can onboard that to defender in a automated fashion.

Same thing if they are using any other cloud solution to host their servers like AWS or Google.

They can configure.

The cloud connector plus Azure Arc and Azure Arc we will manage to push the the client to all of the device servers and.

And apply updates as needed.

Same thing for on premises.

Let's say your customers.

You having some on Prem servers they can onboard that to arc and arc we will handle to onboard that to defender as well right. And the the the last item that I want to highlight.

Uh, if you hit next, uh, it should highlight there is an animation on that.

Just click on it.

Yeah. Thank you.

Uh, that would be the direct onboarding. So let's say that the customer doesn't have arc and they want to use defender for cloud portal to apply the license for that server, right? How to do it?

Follow the the onboarding process doesn't matter the way that it did.

It can be a manual process.

Or.

An automated process just onboard that to the defender portal and enable the director onboarding.

The director onboarding will get the service that you have onboarded to the defender portal and also onboard to the defender for cloud and you'll see the server there.
With that said, you can apply the license or any other policies that you want.
Right on next slide, please.
OK.
So we had a kick off meeting with the customer.
We understand their environment.
We are suggesting the ways that it would do the onboarding process right and now once that you have the agent, the agent will be the defender client itself.
So once that you have the agent, install it and onboard it. Now we need to manage the update process.
Right. Like we have the I will say any version here, the agent version one.
And Microsoft released a new version. We need to push that new software to the to the server, right?
We have different ways to do it.
The first one, of course.
That'll be our recommended way manage with defender for cloud for that one. Once the device is onboarded and managed by a defender for cloud, the updates will be applied automatically.
Every time.
That Microsoft release.
It will receive the update.
Important point here that we require the P2 license if the customer just have the P1, they would need to manage the agent update in another way like manual process or automating with a third party tool.
But if they had P2, they can integrate with Ark.
That would be include arc as well.
And that that'll be handled by Microsoft.
OK, going to the centre of that slide, a manual or automating using a third party or Chrome tab Chrome tab.
It's like comparing to Windows.
It's like a task scheduler, so you can create some tasks there on your Linux and run a command line to update.
That.

In here we are seeing some option on how to start using or editing the Chrome tab.
A task via via Ansible G for Puppet.
Again, the documentation should be on the right left corner.
Of those links will go in deep with the information that I'm sharing here.
So yes, you can push the automation to create a task on on Chrome tab using any of those tools.
And for example every.
Month.
Day one. At that time the command line will run and you're gonna get the. The agent updated right on the right side of this slide, we have a command line at the syntax of the the Chrome tab and explaining what that means. For example, star five, that'll be. Zero minute 50 clock.
And some specific day.
So it is just explaining the command line.
So be helpful if the customer is not experienced with that you can explain and we do have some other third party tools. For example I just added the link in the Chrome expression examples there.
That link will open like a wizard.
You can type what you want to do like I want to apply every Monday at 3:00. Just put that information there.
And that too will create the command line for you.
And then yeah, you can configure on Chrome tab right?
If you reveal the command line, it is just saying the timing pseudo to run with privileged and then the command line should get the the the patient updated right in that case that'll be app get install Dash, only upgrade and mdatp.
You can run it manually and see how that works fine. OK so.
I already have the device onboarded.
Managed by the defender portal and now I need to keep that updated.
What would be the life cycle for that?
For the Asian, there'll be nine months, so the customer needs to to update prior to that time, otherwise they will be out of support and a common request that I'm seeing from my customer is OK, what would be the recommended time for for that?
Again, the support will be nine months and for each new version we will have some new capabilities.
So the customer needs to balance if they are looking for some new capability.

And their process is every six month they need to wait for that schedule to start using that new capability or they can update in advance. So that'll be up to them, right?

Three months.

Four months doesn't matter.

The time it cannot exceed the nine months.

OK.

Let's go to the next slide.

Audit and ebpf support.

So those tools are secured tools. Microsoft is not supporting odd anymore.

The key reason for that is because we need to make some change on the kernel to use those tools.

Right. And it can bring some stability.

So Microsoft is migrating from audit to ebpf. If for some reason the customer needs to keep using odd because they had some other process or the other tools are still using that.

We need to make sure that defender agent will be on on the version 24, zero 72 or lower and they can keep using that.

If they are good and I read migrated to EBPF 248082 or nearer.

They're good to go, right?

I'm not sure how bad configuration on the customer is using.

We can double check.

And even disable E BPF if you want to do some tests or something like that. I just had at the command line to enable or disable that and also the screenshot that that we have on the right.

It's showing how to check which one of defender is using right just type MDA TP health and the line with their saying in that case.

Ebpf.

OK. Again, all of that documentation and recommendations will be placed on the the right corner that left bottom corner of the the slide and if you want to go deep dive. I recommend you reveal that OK next slide please.

Network protection. That is a a great.

Feedback or a very common request that I have from from my customers.

Usually, let's say the customer wants to use network protection and we do have some prior exits here, like needs should be on version 101-7813 or later. Needs

should be on insider slow insider fast. That means chewing preview.
But the customer wants to start testing that and OK.
Yeah, I did that change and I still seeing that it's not supported. If you see that the screenshot from the command line down there, it's saying insider fast, but network protection cannot start due to the supported release.
The reason for that is because the customer needs to send an e-mail to Microsoft with the org ID.
Asking them.
Asking Microsoft to enable.
The network protection for their tenant. So I I I just wanted to add that slide here because again most parts of my customers wants to try that and do off the configurations that just forgot to send the the the e-mail to Microsoft. And yeah, we're gonna need to.
Start troubleshooting and understanding that and at the end that'll be just send an e-mail to Microsoft.
So good tip here.
All the times the customer will ask for that.
Next slide please.
Security management. That is a great and important point.
Security management will be the ability to push defender policies to.
To the server.
Without Intune, right?
Mainly in that scenario will be Linux server.
We do not support servers on Intune, so how to push that?
Microsoft have the security management that we will allow you to push those policies.
Without having to.
So how to do it?
The recommended approach that we have will be if the customers new on that do a pilot, apply those policy for a small set of servers and once that they are comfortable, go at scale and what that means. You can enable enforcement scope and set your target device and.
All of the device that you have MD management.
Will have that configuration.
And what will happens if you do it?

Adding the tag.
1st we need to enable the enforcement scope and tag it device.
And doing that.
The defender will create a computer object on intra and on that way you can create a secured group, add that server as a member of that security group and apply the policy.
From the portal, it is a common request here because sometimes the customer did their own boarding process.
They can see the server they manage. All of the incidents from the portal, but they are still pushing for example.
The settings of the off through a Jason file.
OK, they can do it.
It's supported, but our recommendation again will be to do it through the portal right centralized. That way you can make sure of the policies were receive it there and.
You can do it.
So OK.
So I need to enable the enforcement scope and add the the, the the MD management tag.
So how can I do that?
You have different ways you can manually add the tag from the portal.
You have the computer there.
Just add the tag, it's fine.
You can do it through a Jason file.
It's fine as well, but my suggestion would be to run through a command line.
So thinking on the the onboarding process, the customer will need to install the agent, run the onboarding script and then add that line.
With the process so the the server will have the tag and all of the secured management process will be started.
Creating the computer account and all the stuff so you can start applying the policy.
Another request that I had that from a few customers was OK Danielle.
I am on a pilot and for some reason someone or something has removed the tag.
What will happen, defender?
The portal will stop managing. That server will stop pushing those policy just because the device doesn't have the tag anymore. In addition to manually add the tag, you

can create a EDR policy.

So that will remove the ability to someone or something. Remove the tag and the screenshot that I have here is just showing that I'm trying to run the mdatp EDR tag and set some tag and I'm getting the message saying the settings managed by your organization so that.

During the pilot that we avoid someone or something, removing the tag and stop managing and we need to troubleshoot and understand what's happening right.

Right, OK. And it's not required if just if you want you to avoid that behavior?

So another important point dynamic device tagging are not supported.

The only way will be manual tag or EDR policy, right?

So like creating that denim tagging and trying to see wait 24 hours to see if the computer account was created and it wasn't.

The reason will be then I'm tagging is not supported.

OK.

So once that it will have our parallot everything up and running, the customer is confident with all the policies that they want to apply.

They can just move.

And go at scale.

Move from Ontogen device to all device.

So all of those steps creating the text through a common line and adding the EDR policy will not be required anymore.

So going at scale, move the the toggle to our device and remove those manual configurations from your process from the onboarding process and also the EDR policy.

You don't.

You won't need that anymore.

OK.

Next slide please.

Another common request from my customers network connectivity so.

Let's say that the customer is trying to configure the security management and never seen the the computer object created and they will start troubleshooting and reviewing the configuration and then they figure out that it's all configured, but still not seeing that.

A very common reason for that is SSL inspection.

It is not supported and when you run the MDATP connectivity test to see if there is something that is being blocked by firewalls or proxy that will pass and the reason for that is because.

The Mdatp can connect to those destinations, but cannot exchange out information because something in between the the inspection is changing the package and it is not supported.

Komoj here will be OK.

Yeah, we need to do to start doing an advanced troubleshooting.

But before that, if you go and open the portal, go to the device that you want to troubleshoot, settings properties of the device, you'll see a attribute under device management like MD managed by MDE and MDE enrollment status.

The MDE enrollment status should say limited connectivity, so the 1st 2 the connectivity test.

Couldn't detect that because the device can reach the destination.

Not exchange information because you have something that's filtering the user way or the first step. I'll say to check will be.

Mde roaming status.

If it is limited connectivity.

Probably there will be assl inspection and if it is showing as OK, yeah, we will need to have advanced troubleshooting, OK.

Next slide please.

Recommended AV policies.

That is another great point that I always hear from my customers.

OK. Do you Microsoft have any recommendations?

Should get started applying policies.

The first for for the pilot, for the first configuration, we do have some sample profiles that you can point to your customers.

Again, that will be down left corner the slide.

That'll be the links that we point to that.

We do have some samples so they can start from it.

That is another article that I really like that is common mistakes to avoid is down there as well, like in that article will not be only for Linux but for Windows and Mac OS as well.

So it's a really great slide. The documentation so share with your customer.

And apply the vendor recommendation.

Let's say the customer is using SAP solution or a database.

OK.

Talk to the 30 power solution and ask for the recommended configurations like avoiding or not scanning some specific files, process or.

Folders so yeah, following that and even with the customers don't falling out of those recommendations, there will be some other items that I recommend to check.

For example, I highlighted the enforcement level for the off by default.

It's passive, just like the way that you have on Microsoft on Windows.

Passive will not take any action just.

Will be reporting the incidents, of course.

Our recommendation will be to set you on demand, so that'll be one configuration after applying all the recommendations, that'll be one of the configuration that we need to change and make sure that we are following the best practice, right?

And yeah, I think that's all I have.

I'll check the chat if you have any questions, but other than that I will handing over back to you, Matt.

Matt Novitsch 50:17

And I'm struggling with me button all right.

Advanced deployment guides.

I'm covered for Phillip here, so bear with me as we go through these so advanced deployment guides.

Hopefully everyone knows what they are.

If not, they are the walk through to help customers get on boarded for a lot of various situations. We have developed these probably over the last few years. We keep adding to them.

And trying to get them to be more reliable and successful.

For customers to follow them so they can do like their self deployment piece of it.

I did did add in the chat here and Darrell was able to kindly help me with my follow up. We are looking for any kind of self-service experiences that people have had with the advanced deployment guides.

Please feel free to reach out to me on e-mail.

It is also in chat to go in there and we don't wanna in chat just because it does have.

We're asking for like tenant IDs.

And any other customer information that can be sensitive.

So so please don't share them in in chat directly.

Go ahead.

And next slide on this.

All right. So going further on on the advanced deployment guides, you know looking at it, we have about 62 of the guides right now. Like I said, we keep looking at you know ways to improve on those, adding to them to the ones that we have and.

Going forward and a lot of questions that.

I have or we have internally not just myself, but you know, are these useful, are they?

Do they need clarity?

These are the kind of feedback items that we're always looking for.

So if you if you don't, you don't find them helpful or you find any people are struggling with them, please let us know.

Reach out to your partner leads partner managers.

Reach out to the communities.

You know, whatever it is you feel comfortable doing even on these calls, we're here to get that feedback.

We're trying to help make this so it's a seamless process for everyone.

Go ahead.

And next slide on this one.

Alright, so how to deliver on them?

This goes back to you like when I was talking about before.

We can either do a self-service, you know, tell the customer where they're at, or we can kinda expand on as we're walking through them.

It really depends on on your customer and your engagement for it.

Everyone kind of handles these differently, like example of I follow a good chunk of these advanced deployment guides, but I don't actually pull them up just because I've done enough of these deliveries.

But I do let customers know, hey, they're here.

You can actually assign you know customer.

Or not customers, your engineers within your your tenant. You know, tasks that they need to do, like if they need to worry about, you know, deploying a defender for endpoint.

You know they can.

They can set up groups that way and start signing roles so that they can kinda use it.

I'll call it like a student project plan.

So that does help.

Moving forward with all these different capabilities within the advanced deployment guides, along with helping the customer move forward.

With their project and hopefully keep everything on a a timely manner, go ahead and the next slide on this one.

All right, so this goes back to what I was talking about before with the, you know, how do you we get this information?

You can get them from the FPC Academy.

You can also get them from the the admin section within your your tenant.

Sorry I didn't say defender portal and like my brain is so far on that one.

So just wanna make sure you guys are aware of that.

And I know we're coming up on time.

Go ahead. The next slide on this one, Amy.

Hopefully I think we're about done with these oh smear requests.

Totally forgot about that.

All right, so Smee, process if you guys have questions and you get stuck, you need help like with it like anything with Linux or device control and you guys are like look, we're we're trying to get it.

We just need the extra help.

Please put the smear requests in someone like myself will be able to hop on the calls with you and we will go over it.

Any road blockers you have, we're here to assist you, to make sure you guys are successful going forward with all these things.

So let's work together and figure out what when you get some clarity done on that work, like I said, we're all here.

We have a huge partner community within Microsoft to help partners expand your guys horizon.

So let's keep this information flowing.

Get those requests in if you need them. You know you can always just ping us directly to, but you know we're actually going to say, hey, we need some requests for for when it is.

You know, go through, ask the questions.

Let's get those Rd. blockers off the the table.

And move forward with it.

Amy also has feedback form in there. If you guys have the time, please go out there. Fill it out.

It helps us to figure out numerous things of was this helpful?
Was it not helpful?
There's also a section near the bottom that's called a blank text area. If you guys have other topics that you're interested in seeing us cover, please put those in as suggestions.
We'll absolutely start doing more of these if we get enough people saying, hey, we, we need these topics covered.
Or we want to know more about, you know, X and it's not necessarily just for defender for endpoint. You know, pick your topic for anything security related we're here.
Let's you know, figure out how we can help each other move forward with that.
I don't think I'm forgetting anything but Daniel. Phillip, there's anything else? Please let me know.
I'm gonna give it for quick three minute QA.
If anybody has any questions, I don't see any pop in chat.
At least none that were weren't already answered.

Amy Jarosky (AG Consulting Partners Inc) 56:38
Feel free to come off mute if anyone has any questions they'd like to ask.
In that way, I've enabled all the mics as well.
We have 3 minutes.
If not.
Any last?

Matt Novitsch 57:10
I don't have any.

Amy Jarosky (AG Consulting Partners Inc) 57:10
Comments.

Matt Novitsch 57:11
Yeah, I don't have anything else.
I thanks everyone for your time. Again, if you have any feedback on the advanced deployment guides, please feel free about in my e-mail and we'll go from there.
And then Please remember also that fill out the feedback.

Feedback's always important to us.

Goodbye. And we will take it and and go with it from there.

But thank you everyone for your time.

Amy Jarosky (AG Consulting Partners Inc) 57:39

Thanks everyone.

Thanks all.

We'll see you very soon.

Hopefully have a great rest of your day.

Lucian Popa 57:47

Yeah, bye.

Amanda Lima 57:49

Thank you.

Bye bye.

Amy Jarosky (AG Consulting Partners Inc) stopped transcription