ASR Device Control - Partner Readiness pt 2

0:00
Welcome everyone to our Fast Track Learn session.

0:04
I'm Josh Gingras from the Cxe Scale team and I'm joined by some colleagues today to talk to you about attack surface reduction and device control using Defender for endpoint.

0:16
We are bringing this new set of capabilities in the scope for fast track delivery model and we are hoping to lead a discussion on this topic today.

0:27
I will be joined later in the presentation by David and David, a couple of my fast track friends and let's get started agenda topics.

0:37
Here's what we plan to cover today.

0:39
We will go through attack surface reduction.

0:41
We'll run a refresher on the topic so you can remember what ASR means broadly.

0:48
We will also go through device control concepts and then talk about how those concepts relate to ASR.

0:53
Finally, we'll go deep into the things specifically that Fast Track will cover.

0:57
As part of this scope expansion.

1:00
We'll also cover problems and solutions that you'll encounter in the field.

1:04
We'll give scenarios and very specific examples of how to use these technologies.

1:09
And finally, we'll talk about some best practices and maybe most importantly, what can go wrong when covering this topic.

1:18
After this training, you will be able to describe how device control reduces the attack surface.

1:22
You'll be able to explain how USB device control can limit the attack surface and reduce your risk of data loss.

1:30
You will be able to help customers understand when to use device control versus other methods.

1:34
And finally, you'll be able to guide customers through implementation and validation of those device control policies.

1:42
Acronyms.

1:43
We, we may touch on some of these acronyms during the training.

1:45
I'm not going to read all of them, but you can refer back to the slide later if you do have questions, if you hear an acronym that you don't understand.

1:54
And that leads us to the meat of meat of the conversation.

1:57
Next, we'll talk about ASR device control products, features and capabilities, and I will introduce Mr.

2:05
David Spooner.

2:06
David, over to you.

2:09
Thanks, Josh.

2:10
Good morning, good afternoon.

2:12
Evening, everyone.

2:13
My name is David Spooner.

2:14
I'm a security Smee based out of Redmond, WA.

2:19
Over the next few slides, we're going to talk a little bit about what attack surface reduction are about the product, the features and the capabilities.

2:26
And with that, let's start with what is attack surface reduction and why is it important?

2:33
Attack surfaces are all the places where your organization is vulnerable to cyber, cyber threats and attacks.

2:40
Defender for Endpoint includes several capabilities to help reduce those attack surfaces.

2:48
It does this by hardening places where there a threat is likely.

2:53
Where there an attacker is likely to go after this hardening can mean creating policies or controls to prevent those certain behaviors from happening.

3:04
Closing these gaps, it's critical to ensure that we reduce the risk to the business.

3:10
Compromise devices are a significant risk to an organization and can lead to significant financial and reputational loss.

3:18
By proactively reducing the attack surface, we can prevent attacks from before they happen.

3:25
The best part about attack surface reduction with Defender is that we can increase security without impacting end users productivity.

3:36
It's customized, it's a customizable security approach that will fit your business so as not to reduce the the business, the productivity of your users.

3:49
And lastly, it also offers the audit mode capabilities.

3:55
This allows you, and this is the best part, it allows your organizations and your security teams to configure these attack surface reduction, whether it's rules and capabilities, features in an audit state so that you can see how they work.

4:09
You can enable them across a number of the different features so you can test them out and see without impacting your users.

4:18
And you'll see through the next few slides that these capabilities span many of the attack surface reduction capabilities.

4:31
So, So what features make up attack surface reduction and and Microsoft's attack surface reduction strategy?

4:39
You'll see here that there are a number of features that are listed.

4:45
We have areas that are covered and areas that are not covered.

4:49
Now today's presentation is going to be solely or mainly focused around device control, that new capability that is coming into to scope for fast track.

4:59
But there are other many other features that make up the attack surface reduction strategy.

5:06
I'm not going to go through every single one of them, but I'm just going to highlight there are a couple that that some that you already aware of and some that you may not be aware of.

5:15
When we think about a tax surface reduction rules, these are things we already do today.

5:21
These are areas that we implement policies to reduce and restrict some behaviors and within an organization for the within Defender, we have control for the access.

5:35
These are not new areas.

5:37
All of these should be familiar with today.

5:39
Web protection's another one, again helping customers secure against web threats.

5:45
For example, there are a number of other areas that are outside of scope for fast track.

5:52
So things like application control, exploit protection, hardware based isolations.

5:58
Now we won't talk about those today, but they are areas that make up that strategy towards the attack surface reduction capabilities for our Defender product.

6:09
Now as you'll see here on this slide, the the highlighted 1 is device control.

6:16
This is what we will be talking today and this is really around protecting against data loss by monitoring and controlling media on different on different types of devices.

6:28
And we'll talk a little bit more about that in the next couple of slides.

6:36
So now we're going to talk a little bit about what is device control and why we should use it.

6:42
So device control, as we, as we talked on the previous slide, is, is one of the features within our attack surface reduction strategy.

6:50
What attack device control allows us to do is is to really help protect organizations from and prevent data loss, prevent malware and other sort of cybersecurity threats.

7:04
And the way we do this is by allowing and preventing certain actions and certain devices from being able to be connected to device to a computer, for example.

7:17
Now these device is all device types can be things like removable media, whether that is Ausb device, whether that is other types of devices and printers and other types of devices can all be controlled through device control.

7:36
Where we will focus though is really around that USB type removable media.

7:42
And what you'll see later on in this presentation is there are different types of controls that we can apply to these devices.

7:51
But the key thing here is why?

7:53
Why should we do these types of controls and protections when we think about a USB device being inserted into a Windows computer?

8:05
This allows for data loss, prevent potentially a user being able to copy content from their corporate device onto this media to remove it and take it away.

8:18
So we want to look at device control as a way to prevent that type of data loss.

8:24
There is also things like malware prevention.

8:28
Very often we will see executables and malicious content hiding on, you know, removable storage media.

8:38
What device controls allows us to do is prevent execution, prevent copy from.

8:43
So not only copying to a USB, but also copying and preventing execution from that USB.

8:52
Additionally, granular controls, you'll see through some of the demonstrations, we have the ability not only to, to control what we can do on these, but which types of devices.

9:03
And when we talk about which, not what type as in Ausb versus a hard drive versus, but also particular manufacturers.

9:13
So for example, whether it's a SanDisk or another manufacturer or a model of that.

9:18
So the granular controls that we get allow us to be very specific to protect the organization.

9:29
When we think about the different types of policies and the different types of capabilities that Microsoft offers when it comes to protecting, as you very familiar, Microsoft offers many, many security controls with many different products offering different services.

9:46
You'll see here that we have different tools for different scenarios.

9:52
Now with device controls, we are going to primarily focus on a couple of key examples, block all and and copying to and from.

10:01
But what you'll notice here from this list, there are many different types of use cases and we have different tools for different use cases.

10:12
So if we take a look at the first example here, prevent copy of sensitive data to a thumb drive.

10:18
When we think about that type of behaviour, that type of action, copying data to and from device control can absolutely control copying of data to and from a a thumb drive.

10:32
But when we think about the actual detail here, the the key here is sensitive data.

10:38
From a device control standpoint, I can just control data to and from.

10:43
When I think about M point DLP, they have capabilities to not only control to and from, but also specifically with the the type sensitive.

10:54
So they can control that behavior based on additional information.

10:59
OK, now from this list you'll see here the same thing applies with BitLocker.

11:04
For example, we have BitLocker Dr.

11:07
encryption.

11:07
So controlling writing to removable media unless encrypted or from a lost thumb drive.

11:14
Using those scenarios would probably be better served using the BitLocker Dr.

11:19
encryption protections rather than a device control.

11:22
When we think about preventing of unapproved thumb drive, this is where we start looking at attack surface reduction device controls as well as controlling access to printer based on on the properties of the printer.

11:34
So just be mindful and and remember that just because you can do something within a device control doesn't mean it it is necessarily the best solution to apply that security control.

11:49
Make sure you look at the all up scenario that the customer is trying to achieve.

11:55
Make sure you think about what it protection is, is there, do we need to apply other controls, for example, like sensitivity labels of of content?

12:05
And then make sure that you point the customer towards the right method and the right and the best solution.

12:12
And it might be another person within Microsoft, it might be another SME, for example, on the Purview team that may need to provide guidance to a customer when it comes to, for example, endpoint DLP.

12:24
So just because we can do it doesn't mean necessarily that we should do it with device controls.

12:30
But just know that yes, you can do applied device controls in a lot of scenarios.

12:38
So always, always make sure that you talk to the customer, Ask the customer about the scenario that they're trying to protect.

12:44
Make sure that they are aware and make sure they're aware that there are other potential solutions that could also be layered on top of the device control capabilities.

13:00
So I want to talk just very briefly around common device control scenarios.

13:05
I, I mentioned on, on the previous slide, I, I hinted at a couple of these.

13:10
There are many capabilities within Defender for Endpoint that security controls that security teams can use to control access to those additional peripherals.

13:20
So we've mentioned some thumbprints, USB drives can be things like external CD drives, disk drives, printers, Bluetooth devices, etcetera.

13:29
There are many, many different types of devices that we can actually control and prevent prevent from connecting to to the device.

13:37
Now with that though comes many decisions, making the right decision as to what should be allowed to connect, what do we operate, what is used within the organization.

13:49
When you apply a device control, there is the potential to actually prevent any number of these type of devices from connecting.

13:59
And for that reason, it is super important that we don't just apply policies that are going to block a whole range of devices within a customer's infrastructure.

14:10
So be mindful and when you start looking at the policies in a moment, you'll see some of those capabilities.

14:16
Always, always make sure the customer understands that to that they need to document and understand the peripherals that they may have and the chance that they may block some of these peripherals, these devices inside their organization.

14:33
We will be focused mainly around USB devices, so you'll see here in a moment about preventing users

from installing and using certain device types specifically, and we'll have a couple of examples with, you know, particular brands of devices.

14:50
What we will not go through though in in within this training session though is around things like preventing users like Bluetooth devices for example, or allowing users on a BitLocker encrypted.

15:05
Those are outside of the scope of what we will be doing in this training and outside of the fast track scope initially.

15:14
So Please note that we will be focused on what is in scope, which is really around those control states for USB devices.

15:26
With that then we are going to I'm going to hand over, we're going to talk a little bit around scenarios and solutions.

15:33
And for that I'm going to pass over to my colleague David McQueen, who will talk a little about this.

15:40
Thank you, David.

15:42
Hello, everyone.

15:42
My name is David McQueen.

15:44
I am a fast track product specialist supporting our Defender products.

15:48
And I'm going to talk now about the scenarios and the solutions and how you all can actually go about implementing these for your customers.

15:58
So in preparing for this we have identified 3 general scenarios that most customers are going to fall into.

16:08
The first one being a block all scenario.

16:11

Block all means that a customer has basically decided they don't want any of these USB or removable devices to be available to their end users.

16:21
So we're going to demonstrate to you in a little bit how you can create this type of scenario and how you will leverage just the generic device identifiers to help you cover and address all of those items as opposed to having to worry about how do we find every possible manufacturer of USB's or other removable devices.

16:44
The second scenario is an allow some.

16:47
So this builds on top of our block all scenario and that we want to prevent most of the removable storage devices from being used.

16:57
But the organization has selected a limited set of devices that they will allow users to have.

17:04
These devices may be things that are controlled by their help desk.

17:08
So the organization has a specific vendor, potentially a specific product from a specific vendor that they want to make available.

17:17
So we'll see how we can take this block all concept and then add exclusions in place for the specific devices that the organization wants to allow.

17:28
And then still have the ability to control what those users are able to do with those specific devices, whether they want to say we want to allow read, read and write, read, write and execute, or various combinations of those.

17:45
The third scenario is similar to the last two, but it takes a slightly different angle.

17:50
In this scenario, the customer is aware of or concerned that there's particular manufacturers or particular devices that present an enhanced risk factor to the organization.

18:02
And so they want to ensure that those specific items are blocked.

18:07

They're still open to allowing other devices to be used, legitimate devices to be used by the organization, but they have concerns about some specific ones.

18:17
And so in a similar way that we allowed a certain set of devices to be used while blocking the vast majority of them, we're going to kind of pivot that scenario and instead say we're going to block specific devices and generally allow all of the other types.

18:35
What's really important as we think about these device control scenarios is that all of these are building on top of each other.

18:44
While we've come up with these three main scenarios to demonstrate for you today.

18:49
The take away from these items are capabilities that you all will be able to take and then Mish and Mash to come up to actually meet your actual customer scenarios.

19:01
So not all customers will fall into these exact 3, but as you start to take the various pieces that we demonstrate allow this block that audit these types of things, you'll find that you can scale these scenarios out to many, many, many, many more settings that are there.

19:21
One thing we do want to call out though as we kind of move into this is that as we do block scenarios, we really encourage organizations to also enable audit block with notification.

19:33
The reason we do this is it provides feedback to the end user who is plugged in a USB device into their computer.

19:42
Without this, users are left wondering why something isn't functioning the way that they are expecting to and they get 0 feedback from the organization.

19:52
This will often lead to difficult to troubleshoot help desk tickets being open for that organization and for them to have to deal with.

20:02
So we want to preempt those types of problems and challenges.

20:06
It will also ensure that your security teams gets alerts in the security portal so that if a device is being blocked and there's a legitimate business need, they can go back, look at those events and enhance or tweak their device control policies to later allow those to work.

20:26
So let's talk a little bit 1st about what the customer journey looks like as we go into the scenarios before we do our demonstrations.

20:35
So when we start having our conversations with the customers, we need to understand what their goals are.

20:42
Are they trying to be aggressive and block a lot of devices?

20:46
Or are they on the other end of that spectrum concerned about the specific set of devices?

20:51
Or do they find themselves somewhere in between?

20:55
This is important because it drives our next stage of finding the key attributes that we're going to need to help that customer build the policy.

21:03
If we need large quantities of items to be blocked, then we're going to be looking at Microsoft's documentation, finding those generic identifiers.

21:13
If there's specific devices that we're looking at blocking or allowing, we need to get the specific attributes from those devices about their vendors, their product IDs, and potentially something as unique as a serial number.

21:27
Once we have the information that we need, we will then move into creating reusable settings and we're going to set up a reusable settings into the groups that we're then going to use to apply policies to.

21:40
So we have our group of trusted devices, we have our group of devices that we want to not trust or prevent from having actions.

21:49
So we start to build those reusable settings, defining out what the device landscape looks like.

21:56
Following that, we then create our device control policies utilizing those reusable resources, reusable settings.

22:05
This is where we actually define can I allow something or will I block something for the user and specifically what is it that we are allowing or blocking?

22:17
Once we've created these policies, the next piece that we want to do is go forward with validation.

22:23
As was pointed out by David, there is a possibility that you can broadly impact a number of devices if we just create a policy and apply it out to the organization.

22:37
Likewise, we can leave gaps in our security policies here if we create a policy that doesn't actually close up all of the attributes that we want to block a user from while allowing other devices or other capabilities to still occur.

22:52
So it's very important here for us to go through a policy validation.

22:58
This is also a good place for us to be able to iterate.

23:01
So creating a deny all policy 1st and then creating, updating that policy to allow the specific devices that we want is also a great way for us to be able to work through the process and ensure that we've tuned the policy at appropriately for the customer.

23:19
Finally, if you find yourself in a scenario where the policies are not working, there's going to be a couple of examples in here how you can go and find where those policies were set and validate that the information that you configured in the portal was properly transferred to the machine and that the policy should apply in the way that we want it to.

23:42
We'll now move into a set of demo examples of our top three scenarios.

23:49
And in addition to this, we also have an example of how you can go and find the specific device properties and some potential gotchas as you're looking at some of the online documentation about those vendor IDs when we're bringing those into the policies.

24:08
Just to make sure that you don't have some of the trouble issues that we experienced when we were working through this, in this video we're going to talk about device control default enforcement.

24:24

Before we apply any device control policies to control access to USB type removable media, for example, it is important to understand what the default enforcement is set inside the customer's environment.

24:40
Now, default control.

24:42
Default enforcement for device control establishes what decisions are made during device control access checks when none of the policies or the policy rules match.

24:55
For example, if I have a device control policy that is inclusive of certain devices, and the rule is set to deny those, any devices that don't match that inclusion statement will fall back to the default behavior.

25:13
Now the two types of enforcement default enforcements that you can apply are either default allow or default deny.

25:23
The default configuration for any environment, if not configured is to have a default allow.

25:30
So again, if I look at a or if I configure a rule that says include these devices and deny them, any other device type not in the include statement would fall back to that default allow and would therefore be allowed to be used inside the environment.

25:53
Now that configuration can be changed, and it can be changed via group policy.

25:58
I will show you in a moment which group policy is required to make that change.

26:05
Please note that in my lab I had to update the ADML and the ADMX files to be able to get the Defender group policy that was needed in your customers environments.

26:16
That is outskart outside of fast track scope, but it is a requirement should those settings not be available within the group policy now?

26:29
How do I find out what is the default enforcement in a customer's environment?

26:35

Now you can certainly go and check Group Policy to see what is configured in there, but another way to check that would be to use PowerShell and to use the Get Dash MP computer status.

26:48
Now if you're looking at my screen, you'll see there are three properties.

26:51
A Device Control State policies last updated, but there is also a default enforcement value.

26:58
Now this.

26:59
The PowerShell you are looking at is from a machine that has no device control state policy assigned to it, and for that reason the state is disabled and the enforcement value is blank.

27:13
If I take a look at a different device that actually has a device control policy applied to it, you will see that the device control state is set to Enabled and it is now showing what the default enforcement policy is that is set on my device.

27:29
And in this case, I'm using the default allow because that is the default setting for all organizations unless you change it through Group policy.

27:40
I'm going to jump back briefly to my domain controller and I'm going to go into Group Policy.

27:47
I'm currently under the Computer Configuration, Administrative Templates, Windows Components, Microsoft Defender, Antivirus, and then Device Controls.

27:59
As you can see here I have a setting called Select Device Control Default Enforcement Policies.

28:05
If I open up this, there is a Not configured, enabled and disabled.

28:10
If the value of Not configured is set, then it's going to use the default by which is default allow.

28:18
If I want to change that behaviour inside the organization, I can set that to enabled and I can modify the setting to default deny.

28:28

Now the reason why this is important is when we get into our next videos and you see how we go about creating new device control policies and rules.

28:40
We are going to have the option to do a an allow or a deny based on inclusions and exclusions.

28:48
And it's super important to know what the default configuration inside the environment is.

28:53
Should my rule not target all devices and I have only certain devices targeted, anything outside of my rule would fall back to this default setting of either allow or deny.

29:09
In most cases.

29:10
Most organizations will not have changed this and so I expect it to be set to default, allow or not configured.

29:20
OK, we are going to walk through the scenario of creating a block policy for an example customer.

29:29
The idea here being that we have been asked by a customer to prevent their people, their employees from being able to use USB storage devices either for the purposes of reading, writing, executing off of those to reduce the exposure or risk factor that those can provide to them.

29:53
So we're going to begin here in the security portal.

29:58
We're going to go to our configuration management using our endpoint security policies.

30:05
And the first thing that we're going to create is a set of reusable settings.

30:10
So that button is available here in the upper right hand corner of our endpoint security policies.

30:18
The next piece that we're going to do is create a settings group.

30:22
This will be specifically for the attack surface reduction.

30:28
We're going to name this group log all removable.

30:42
Go to next and then under our device control, what we are going to do here is create a set of rules to help Windows identify what the devices are that are supposed to be blocked.

30:56
So now that we have opened our configurable reuse, our configure reusable settings blade here, we're going to create a new device control and we're going to select the removable storage.

31:09
From here, we are going to choose to configure our settings.

31:14
And we see that we have a number of options that are available to us that help us get pretty specific about which USB devices we may want to allow or block.

31:24
But because we're using a broad approach here to block all devices, the only one that we're really going to have to worry about is this primary ID.

31:35
And to help us with these unique categories of devices within our documentation, we have outlined some very specific strings that we can use to kind of cover those broad segments of devices.

31:53
So the first one is this removable media devices.

31:56
And what we're going to do is just simply copy that, bring it back over to here.

32:02
We will put that in as our primary ID.

32:05
We want it to look exactly as is, don't make any changes, no spaces, anything like that.

32:11
The other thing we need to do is provide a name.

32:14
So to keep this simple, I'm just going to use the exact same value that we pasted here into the primary ID, but I'm going to make it a little bit more human readable with a space organizations can choose.

32:25
This is a free text field for them to be able to use whatever makes sense to them.

32:30
So once we do that, then we'll go ahead and click Save, and then we're going to repeat this process again for our CD-ROM devices.

32:43
So we'll configure the settings here again, give it a human readable name, put that into the primary ID save, removable device.

32:59
Again, the WPD devices, OK, again a name and a primary ID save.

33:17
So now we have configured all of the various types of devices that this particular reusable setting is going to apply to.

33:26
Now an important piece here is you'll notice that there is this match type match any or match all.

33:32
Generally the match any is going to be probably the most effective for us because we a device would match into either a removable media device or a CD-ROM or a WPD device.

33:48
But if we had a scenario where we had a specific vendor specific products and maybe even specific cereal or bus I DS, that might be a situation where a match all could kind of do a combination or roll up of all of these items.

34:05
But in general, most of the time what we expect to see, we'll do this match any and that's going to hit or address all of our all the needs that we have here.

34:15
So we're at our review and create, we're going to go ahead and say save.

34:21
So we have now created a block all removable devices.

34:27
I can now close the reusable settings blade there.

34:31
And what we can now do is we will go ahead and create our attack surface reduction device control policy.

34:39
So in here, we're going to pick our operating system and then because we're using our security portal will notice device control is this very last option.

34:53
We'll go ahead and say create the policy, we'll give it a nice name.

35:09
OK, Now when we come in to configure our settings, you'll see that there's a number of different sections in here that provide configuration spaces.

35:22
The ones that we're really going to be concerned with is actually this device control section.

35:28
So this is where we're actually going to create the policy of what do we want to do with those reusable settings that we just created.

35:36
So here we're going to say, let's add and let's call this the block all setting.

35:49
And we want to include the use of all of our removable devices that were identified by those reusable settings.

36:01
So we're including this as who it's going to basically apply to.

36:08
We'll say save there.

36:10
We don't need to exclude anything at this point in time because we want this to be a very aggressive block everything policy with no exceptions.

36:20
So what we now need to do is actually configure the block portion.

36:23
And we do that by clicking on this configure under the entry column.

36:29
And when we configure the entry, we're going to add a policy rule here.

36:35

So when we expand this, you'll see that there are allow and deny rules here because our goal is to deny everything.

36:43
We're going to 1st choose deny under the options.

36:47
We can leave this as none and then access mask.

36:52
So our goal is to block everything in this particular scenario.

36:56
But you can see here that there is flexibility that you can block specific activities, should that be kind of your unique customer scenario and ours.

37:07
Because we want to block everything, we'll choose read, write and execute.

37:12
These other two columns, Sid and computer Sid allow us to target more specifically what users, what groups, and what devices these block events will happen on.

37:24
This is not going to be considered part of our standard fast track scope, but if you have customers that need these kinds of specialized, highly tailored scenarios, you can always reach out to your FPS team and we'll be happy to assist you with that.

37:42
The second thing that we're always going to recommend is that you also leverage this audit denied.

37:49
The reason that we're going to recommend this is we don't want an end user to plug in a USB device and have nothing happened and them wonder why things aren't working.

38:01
That will generate a lot of help desk tickets and concern and issues for our customers.

38:06
So instead, this audit denied allows us to give feedback to the user who is attempting to insert a USB device to see what is going on.

38:16
It also allows us to send an alert or send an event back to the security portal so that SoC team or anybody else can also see when these types of events when somebody's plugging in one of these devices is occurring.

38:31
So in this case, I'm going to choose, let's send the notification and the event.

38:37
And then again for the access mask, we want to replicate the same settings that we had chosen here from the deny.

38:45
We'll go ahead and say save to this and that's all that we need to do in order to create our deny policy.

38:54
The next thing is we need to assign our policy to devices or to groups so that they can be appropriately applied.

39:03
So we already have a group specific for our example user, this is Alex.

39:10
So we're going to apply that.

39:12
Like with all of our security policies, we're choosing whether we can include or exclude this user.

39:20
We'll go with next.

39:21
So now we have the option to review.

39:23
We're confident that it's good.

39:25
We can go ahead and say save, OK.

39:33
The device policy has now been created.

39:36
So what we will do next is we're actually going to shift over to our example user's machine.

39:53
OK, so we're now on Alex's machine.

39:58
And what we will do here is I'll go to our settings, we'll go to accounts, go to access work and school.

40:13
We see our work account associated here if we click that.

40:17
We can see our manage by Contoso if we click on that info now we can get to our synchronization point and we're going to click sync.

40:27
The reason that we're doing this in a demo and that you may do this with your customer is this should initiate the synchronization of the device policy to this device more quickly than it will naturally just communicate between the two.

40:43
So this will allow you during a single meeting with a customer to be able to create the policy, see it synchronized back to the device, and then help them with testing or validating that the policy has been applied.

40:59
The other thing that I'll call out here is as you are looking at these, the policy that we've created through the GUI is going to be pushed back to the machine and it will be applied and can be viewed from the registry editor.

41:15
So if we jump here to our registry editor, you can see it's in our HKLM registry key under Software Policies, Microsoft Windows Defender Policy Manager.

41:31
Currently, you'll notice that this is empty because this was open before we had tried to do the synchronization and before any policies were applied.

41:40
We'll go ahead and refresh now.

41:57
We haven't yet received the policy, so we're still waiting on sync to happen.

42:08
OK, our synchronization has now completed and now when we go back to our registry, you'll notice that we have a policy groups and a policy rules.

42:19
These are the translations of those reusable settings as well as the device policy to handle all of the appropriate security settings here on the device.

42:32
So what I'm going to do next is off screen we'll insert a USB device and immediately you can see we have a pop up down here that the device access has been restricted.

42:47
Your organization's policy block all settings doesn't allow read access to the device.

42:54
So this is the alert that pops up when we get that audit denied setting.

42:59
And this is what we expect users also if we come here into our Explorer, you'll notice that Ausb device does show up here.

43:10
But even if I click on it, I'm given device access is denied.

43:15
So I can't expand on it.

43:16
I don't get to see anything that is associated with it.

43:20
So our block all policy has been properly created and is now properly functioning on this endpoint.

43:31
The next scenario we are going to look at is how do we start to get specific about what devices we will want to be able to add controls to.

43:42
So for this example, we have a customer who is interested either in allowing or blocking SanDisk type of devices.

43:52
Before we used the primary ID to do our large categories of blocks.

43:58
This time, since we're looking at something like SanDisk, we want to leverage our product ID or our vendor ID or a combination of both.

44:08
And what we'll show you here is how you can find the vendor ID as well as product I DS over the next couple of steps.

44:16

So the first way if you're looking for Vendor I DS is you can go to theusb.org/developers site and under the valid USB Vendor I DS you can click on this which will open an Excel sheet of all of the known Vendor I DS.

44:34
So in here we can then do a search for SanDisk and we see that there is an entry here and their vendor ID is listed as 1921.

44:47
What is really important about this list however, is their vendor list is identified in a decimal based number and when we actually put it into the device control, we need to use a hexadecimal based number.

45:04
And we also need to make sure that we are always using a four digit hexadecimal number when we do that.

45:13
So in order to make that possible or in order for you to be able to do that more easily, you can leverage the calculator.

45:27
And what I'm going to do is switch to our other device where we'll show you in a minute the other way to do this.

45:34
But also here's our calculator on Windows.

45:39
And what we have done is we've gone into calculator, chosen the programmer mode, We've taken that 1921 number and we've typed it in here.

45:49
And now you can see here's the hexadecimal value 781.

45:55
What is really also important here is that if you get a number that is less than 4 digits, you actually need to add or prefix this with a 0.

46:07
All entries that go into our portal will need to use a four digit number.

46:13
The second way that you can also find this number is we can open up the device manager on a device where we already have the device inserted.

46:22

So you can see I have my USB mass storage device here under the under the Universal Serial Bus controls.

46:31
If I right click on this and I choose properties, then I go to details, then I choose my hardware IDs, you can see that we get a value that is similar to USB slash vid_0781 which again matches up to the value that we were able to calculate from the USB vendor list.

46:58
It also includes an ampersand PID of 558B and a revision number here.

47:07
So as we look at these hardware IDs, if there are more specific things like I want to allow SanDisk of a specific model, this is how we can start to also find some of those product IDs that we may want to be able to use in our portal.

47:27
Jumping back to our portal, now that we know that our vendor ID is 0781, I simply come back here to the vid and all I need to put in is just that identifier number.

47:45
I don't need to prefix this with the_vid or anything like that.

47:52
If I wanted to do just the product, Idi could populate that here, or I could do the combination of both the VID and the PID here.

48:03
And if we click or if you have questions, all that you need to do is click here.

48:08
Click on the Learn more.

48:10
This will give you some information about the specific formatting, but what you're looking for is something that is 0781_55A B WHICH, was captured from our hardware properties and, that's all that we would need to input into there since.

48:32
I'm Going to focus just on our vid associated with SanDisk.

48:36
We'll leave that field populated, our name populated, and now we click save and we have a SanDisk Reusable setting that we can now use in our next set of policies.

48:53

In this video, we are going to demonstrate how to create a device control policy that would allow certain USB device types to be used while blocking all other device types.

49:08
In the example, we will be using a SanDisk as the device types that we will allow, and then we have some generic other Usbs that will get blocked.

49:20
For the purpose of this demonstration we will also assume that you know how to acquire the VID or the PID to be able to configure the reusable settings.

49:30
If you are unsure how to do this, please see the earlier video generate created by David McQueen where we show you how to to to get those details.

49:42
We will also be using the Intune portal for this demonstration instead of the Security portal, but the same behaviour is applicable.

49:50
You can create these policies in either the Intune Portal or under security in the Defender Portal.

49:59
For the purpose of this demonstration, we will also assume that the Default Enforcement is set to Default Allow.

50:08
We have not changed that behaviour using Group Policy to a default deny.

50:14
If you would like to understand more about the default enforcement, please see the earlier video where we talk about default enforcement.

50:25
So in this demonstration, I'm going to go to intune.microsoft.com, I'm going to navigate to Endpoint Security, I'm going to go to Attack Surface Reduction, and I'm going to create a new policy.

50:38
From here.

50:38
I'm going to select Windows 1011 and Server.

50:41
I'm going to select the profile type of device control, and I'm going to hit Create.

50:46

Now this policy is configured is to allow SanDisk but block all other devices going to click next and now I can configure my policy.

51:07
From here I need to use or define my rules and use my reusable settings that have previously been configured.

51:17
If you're unfamiliar with how to configure reusable settings, please see the first the earlier video by David McQueen where he talks about how to configure reusable settings.

51:30
In my lab, I have two reusable settings that I will use for this demonstration.

51:36
Because my policy is I want to allow some and block everything else.

51:44
My policy is going to be set with an include of all removable Usbs.

51:52
OK, my exclude is going to be my SanDisk usable reusable settings and my entry is going to be a deny statement.

52:05
OK, so I'm going to name this one Allow SanDisk block all other.

52:16
So if I look at my type, it is set to a deny.

52:20
I'm going to set my option to none and my access mask because I want to configure this to all read, write and execute.

52:28
I'm going to select all three of these from my deny rule.

52:32
I'm also going to add an audit denied and I'm going to set my notification to notification and event.

52:41
Now this just means that my end user will get a notification on the device and also the events will be that's sent to the endpoint service.

52:48
I'm going to audit both the read write and an execute as well.

52:54
I'm going to click OK.

52:56
Now if I was to read back that policy I'm including or.

53:01
My policy is set to a deny and this policy will apply to all disks except my Sandisks.

53:15
So this should, assuming the policy works, allow me to use a SanDisk, but any other USB type will get a deny.

53:24
I'm going to click next.

53:28
I'm not going to set any scope tags in Intune, but I am going to assign a particular group of devices to receive this policy.

53:39
I have a group called Personal Computers.

53:41
This contains 2 devices from 2 test laptops that I have.

53:46
I'm going to assign that.

53:47
I'm going to click next and I'm going to hit create.

53:52
So now I have this new device control policy that has been created and it's this one here.

53:59
Allow SanDisk, but block all other devices and you'll see that I have a group and I have my configuration.

54:10
I have the include set, my exclude for my SanDisk, my include for all, and my type of denying.

54:22
Now, as with all Intune policies, it's going to take a couple of minutes for those policies to to get created and then I need to force those policies down onto the device.

54:33
While I'm waiting for those policies to replicate, I'm just going to jump into my reusable settings just to show you that I had previously configured these and my all USB is set to removable devices, cd-roms, and WPD, and my instance is set to primary ID.

54:53
This just means I'm not specifically targeting a particular type of USB.

54:59
For example, this is just generic all USB.

55:02
So this one is my all USB group.

55:06
If I jump back and I look at the SanDisk group that I created, you'll see that in this instance I've added a removable storage and I've targeted it to a specific VID, a specific manufacturer of USB, and in this case it is the SanDisk hexadecimal value.

55:30
Now that I've created the Intune policy and assign it to the devices, I'm going to jump over to my test laptop.

55:40
I'm going to share my screen over there and hopefully demonstrate the the the policy configuration actually working on a test device.

55:53
So I have in the interest of the pilot and demonstration, I have gone into the settings, Accounts, Access, Work or school, gone into information and I've hit the sync button so as to pull down the policy from Intune.

56:13
You can check in the registry as well under Windows Defender.

56:19
So it's under Local machine Software policies, Microsoft Windows Defender and Policy Manager and you should see the policy groups and rules if there is a policy applied to this device.

56:32
You can also use the PowerShell command Get Dash MP computer status and from here you should see that we have a device control status of enabled and an updated time on when the latest policy came down to this device.

56:48

So with this demonstration, we are hoping to achieve the scenario that will allow SanDisk device types but block every other device type.

57:02
So I'm going to start with my SanDisk type USB.

57:06
I'm going to plug this in and if everything is working, I should get a autoplay indicating that my USB is connected.

57:15
I should be able to click into my USB drive and I should be able to create files and folders, etcetera.

57:24
I should be able to modify files and content on this and it should allow me to save and it does.

57:34
So now I have a fully working USB stick from SanDisk as it because that is designated as an exclusion in my policy.

57:44
If I remove that USB stick and now insert any other USB stick that is not a SanDisk, you will see that I now get a notification indicating that the device access has been restricted.

58:03
So it indicates the all SAN in my organization policy.

58:07
All SanDisk block ALL others doesn't allow read access to this device.

58:13
OK, so it tells the end user that they have been blocked and we can prove that as well.

58:18
If we go into Explorer and I try to access this, I get an access denied.

58:25
I'm no longer able to write to this type of USB or any other USB that is not a SanDisk because the device control policy is now applying to this device type.

58:41
In my next demonstration I will be doing a an allow all but blocking some device types, so the reverse of what we just demonstrated.

58:56
In this video.

58:57
We are going to demonstrate how to use the Intune portal to create a device control policy that would allow all USB types to be connected to a laptop, but block a particular type of USB, and in this case it will be a SanDisk USB Removable Media device type.

59:20
I'm in the Intune portal and so I'll be leveraging this instead of the Security portal, but we can achieve everything that we do today in this portal exactly the same.

59:31
In the Security Defender portal, I'm not going to demonstrate how to acquire the VID and the PID information.

59:41
I will demonstrate in a moment just to show you that I have got the set so I can control my specific type of device.

59:50
Just so you know as well, the default enforcement for my test environment is set to default allow.

59:59
So if my policies are not targeted to a particular group or device types.

1:00:07
So if my device is not the rule doesn't apply to that device type, then the default will be for it to an allow, you know, so that device will be able to be used.

1:00:20
I'm going to go to endpoint security, I'm going to navigate to attack surface reduction, and I'm going to create or I'm going to show you the reusable settings.

1:00:30
To start with.

1:00:31
As you'll see here, I have a group for all devices.

1:00:35
I've got my generic primary ID of removable media devices.

1:00:40
This is the generic for all device types.

1:00:43
I'm not specifying a specific type or manufacturer particular type of device.

1:00:48
This is just all removable media devices.

1:00:53
And I also have another one for SanDisk.

1:00:55
And in here I have a specific VID that I have set indicating that this group is specifically for SanDisk.

1:01:05
Now you can use other things like VID and PID if you want to choose different not only manufacturers, but versions of the device as well.

1:01:16
But for the purpose of this, I will just be using the SanDisk VID of 0781.

1:01:24
So I'm going to go back to summary and I'm going to create a brand new policy.

1:01:28
I'm going to select Windows 1011 and Server Device Control and hit create.

1:01:34
Now for this one, I'm going to say Allow all lock SanDisk.

1:01:44
OK?

1:01:45
Now, a use case when maybe you want to block a specific vendor is maybe you know that there are some devices out there from a specific manufacturer that have been known or found to have malicious content embedded onto those USB sticks out of the gate and you want to prevent them from being used inside your environment.

1:02:07
This type of policy would meet that need.

1:02:10
So in this case, I'm going to allow all but block the SanDisk.

1:02:14
I'm going to say next I'm going to scroll all the way down to my device control and now I'm going to configure my particular rule that is going to block my SanDisk.

1:02:26
Because this is I'm going to use a deny rule.

1:02:30
I need to deny my SanDisk.

1:02:33
So I will target my include to be my SanDisk and I'm not going to target anything in my exclude.

1:02:43
And the reason why I'm not targeting anything in my exclude is because my default behaviour inside my environment is default allow.

1:02:54
So I'm targeting a deny to SanDisk, which means any other device type isn't applied is not affected by this policy and therefore would be affected by the default allow and could be used if I go to edit entry.

1:03:12
And now I call this one Allow all block SanDisk.

1:03:18
Just so it helps understand what this is for.

1:03:22
I'm going to set this as a deny because I want to deny my inclusion statement which is SanDisk.

1:03:28
I'm going to set my options to none, and I'm going to set my access mask to read, write, and execute.

1:03:35
So this will deny any access to the SanDisk types of devices.

1:03:40
I'm going to add another audit deny so that I can track these devices.

1:03:45
I'm going to notify the end users.

1:03:47
I'm going to set mine to a send notification for the end user and the events, and I'm going to target them for all of those same access mask permissions, read, write, and execute.

1:04:02
Now that I have a rule defined to deny SanDisk, I can hit next, go to the assignment section, and now I can add a particular group that I want to target these devices to.

1:04:19
And the purpose of this one, I could select A particular target group.

1:04:25
If I wanted to apply this to a specific set of devices, I'm going to select my desktops, I'm going to hit next, and then I'm going to create my policy.

1:04:40
Now I'm going to jump over to my test laptop, and hopefully once that policy replicates, I should now get an experience where I can actually allow any device except SanDisk in my environment.

1:05:13
Just as a reminder, if you need to sync your policies, you can do that on the Device Sync status.

1:05:19
You can check your registry keys if you want to see if the policy is in the policy manager or you can use the PowerShell Get Dash MP computer status to see whether the device control policy is enforced and when the last update for that policy occurred.

1:05:39
Because this is a an allow all blocks sum, I'm going to start with my generic non SanDisk key.

1:05:47
Because this is a non SanDisk, this should be allowed and I should be able to access this key.

1:05:54
As you can see from my demonstration here, the autoplay popped up.

1:05:58
I can access this key and I can in fact do anything I want to this device.

1:06:04
I can add new files, I can edit existing files on this key, I can write 2 files on this key, and I can save them all because this key is non SanDisk.

1:06:21
This is being affected by my default allow because my policy is only including SanDisk for a deny statement.

1:06:31
If I remove that key and I now plug in a SanDisk type key.

1:06:37
What should happen is hopefully I will get a block when I try to access now in this this demonstration, because I have inserted my key multiple times in my previous videos, I'm not getting that notification because it previously already I'd already dismissed that notification.

1:07:08
But I can still demonstrate and show that the key is not usable in Explorer.

1:07:16
I come to the USB drive that is showing as mounted here and I try to access it and I get an access denied.

1:07:25
Now this error, this deny is going to happen whether it's in Explorer, Word, Excel, wherever I'm trying to say from.

1:07:33
I am preventing or prevented from writing reading from executing anything on that USB through that device control policy because it is a type SanDisk and that was in my include policy.

1:07:54
As I mentioned, a good use case for this might be when you have a particular device that you do not want to be used inside your environment because it's been found.

1:08:06
Maybe it was given out at a convention and it's found to have malicious content on it.

1:08:10
You might want to stop that.

1:08:12
There are many, many use cases.

1:08:13
However, in my demonstration so far it's been a allow or a block on a specific device and we've blocked all read, execute and write.

1:08:26
But in in other rules you can get very granular where you allow specific actions or permissions.

1:08:37
Like for example you can read from one type of device but you can only write to a different type of device.

1:08:44
So in my next video, I will demonstrate a a variation whereby we can use multiple devices with different scenarios, different rights and reads to demonstrate that it is very a very scalable solution.

1:09:01
In this video, we are going to demonstrate device controls where we used multiple rules to control individual permissions across different device types.

1:09:13

In the previous videos, we've done demonstrations where we've just blocked all devices or blocked all of one particular manufacturer of a device.

1:09:24
Now in this case, we're going to get granular and allow us to control a read permission and a write permission and a block permission across different types.

1:09:35
I will be doing this demonstration from the Intune portal, but everything we do here can be done within the Defender security portal.

1:09:44
My default configuration is also configured that the default enforcement is set to allow.

1:09:51
So default allow in the Intune portal I am going to go to Endpoint Security, Attack Surface reduction and my Reuse and then the reusable settings.

1:10:04
I won't be demonstrating how to acquire the VID or the PID for specific devices that can be shown or can be seen in another video recorded by David McQueen.

1:10:15
Please view that if you need to understand how to acquire the the VID and PID information.

1:10:21
For the purpose of this demonstration, I have three different device groups.

1:10:26
I have my all removable USB devices where I'm just designating the primary ID, generic removable devices, media devices for my primary ID indicating all devices.

1:10:44
I have a second one which is PNY and I've designated an instance with a PID or sorry a VID of 154B.

1:10:54
This designates the manufacturer for PNY and I have a third and final sand group for SanDisk which is instance VID of 0781.

1:11:09
So now I have three different reusable settings.

1:11:13
One is all, one is for PNY and one is for SanDisk.

1:11:20
Now I'm going to go back to my summary page and I'm going to create a new policy.

1:11:30
Now in this case, I'm going to select Win 1011 and Server, select profile type of device control, and I'm going to hit create.

1:11:38
Now my device or my policy name in this case is I'm going to allow different devices with different permissions.

1:11:56
Obviously, you're going on to name this more appropriately so you understand what this policy is actually going to do.

1:12:01
I'm going to hit next and Scroll down into my device control.

1:12:07
Now, the first thing that I want to do is set and in this case, in or in the previous demonstrations, we've used a single rule.

1:12:14
Because we have multiple devices, we are going to need to add multiple rules to, you know, for multiple behaviors.

1:12:23
So the first one I'm going to set here is I am going to select A particular device type.

1:12:31
Now in this case, I'm going to select SanDisk as my first include and I'm going to set some entries in here.

1:12:41
Now in this case, I'm going to say I'm going to make this one a read only policy, aloud read only devices.

1:12:53
OK, so if we look at what I'm going to configure here, I am still going to do a deny.

1:13:02
I'm still going to set my options to none.

1:13:04
But in this case, I'm only going to select write and execute for my rule.

1:13:13
I'm also going to add the same audit denied that you've seen in previous videos.

1:13:18
I'm going to set my notification and event, and I'm going to set my access mask to write and execute.

1:13:26
If I was just to apply this rule as it is I would be including SanDisk and I would be denying write and execute but it will it would not block the read.

1:13:43
So if I was just using this policy I would be able to re write oh sorry read from SanDisk.

1:13:52
I would not be able to write or execute on SanDisk, but I would be able to do anything on any other device type because I am not doing an exclusion for this particular rule.

1:14:08
OK, now I'm going to add a second rule, however, and here is where I'm going to designate my other behavior that I also want to happen.

1:14:20
Now in this case, in my second rule, I'm going to designate my all.

1:14:28
All removable devices is in my include and in my exclude I'm going to designate PNY and SanDisk.

1:14:38
OK, And from a configuration in the entry section, I'm going to call this one deny all except PNY and SanDisk.

1:14:57
OK, now in this case, I'm going to use a deny statement.

1:15:01
I'm going to set none.

1:15:02
And I'm also going to do read, write, and execute.

1:15:08
I'm going to add another line for my audit, going to set notification and events, so end users no.

1:15:15
And I'm going to set my mask to read, write and execute.

1:15:20
So now I have two rules and when I combine these two rules together, the overall experience that I

will get is that on a disk of type SanDisk, I will not be able to write, I will not be able to execute, but I will be able to read OK of type PNY.

1:15:49
That is excluded from the second policy which means I can do anything on the device that is PNY.

1:15:59
For any other device type which is in my include statement in this one here it will get a deny for anything read, execute or write would get blocked.

1:16:14
So in this scenario I can only read, write and execute on PNYI can read on SanDisk and I'm blocked for every other device type.

1:16:29
OK, so as you can see you can get quite granular.

1:16:32
You can change the the different permissions based on different devices and you can mix and match.

1:16:42
Just remember, though, to use includes and excludes in the right grouping to ensure you meet the customer's needs.

1:16:52
I'm going to hit next and go to assignments here.

1:16:59
I'm going to assign a particular group.

1:17:02
I'm going to select, in this case, MDE attached desktop as my example, and I'm going to hit Next, and I'm going to hit Create.

1:17:15
Now that I have a policy, I'm going to flip over to my demo laptop and now demonstrate the experience based on the policy that we just created.

1:17:34
As with all demonstrations, if you need to get those policies down from Intune, you can use the Sync button in the Device sync status.

1:17:43
You can check PowerShell to make sure that MP get MP computer status is showing a policy and an updated policy time.

1:17:55
You can also use the registry to ensure the policy rules and groups are here.

1:18:02
So if I go back to my experience now, because we have 3 devices in play, I have a SanDisk, I have a PNY device and I have a generic.

1:18:20
So I'm going to start with the generic because that should be blocked because it is not PNY and it is not SanDisk.

1:18:31
So if I insert this disk, what should happen is I should not be able to use this this type and I I get the access denied just like in the other demonstrations.

1:18:49
As with this demonstration, I did not get a notification and that was just because I had recently received that notification and cleared it prior to this demonstration.

1:19:03
In most cases though, when a user, a new user inserts a disk, they should get that notification prompt saying this device is blocked.

1:19:14
So the key that I inserted was generic.

1:19:16
It is not SanDisk, it is not PNY and that in my policy was set to block all if I now insert a SanDisk.

1:19:27
If you remember in my policy, the first rule was SanDisk deny and deny write and deny execute.

1:19:38
It did not deny a read.

1:19:41
So what should happen is I should be able to use this disk and I should be able to read from it.

1:19:48
So I should be able to open up some files on this key and I can read the information in here.

1:19:56
I should be able to go into the word doc and be able to see information in here.

1:20:03
What you will notice though, if I right click, I do not have the options for new.

1:20:09
I cannot create.

1:20:11
I cannot add information to this.

1:20:14
There's no way to create a new file on here.

1:20:17
Save a file.

1:20:19
If I go into the test file and I try to write to it and I hit save, it pops up with a save window and if I try to hit save, you can't, it prevents me.

1:20:39
It says notepad.

1:20:39
You cannot save to this location and that is because my policy was configured where I prevent a write or an execute on that.

1:20:48
I can read however, so you can absolutely make my files readable on specific devices and writable on other devices.

1:20:59
So this was my SanDisk.

1:21:02
So my generic blocked all my SanDisk only allowed read.

1:21:08
And if I insert my PNY, you'll see that I get my autoplay.

1:21:18
If I click into here, I go into my PNY type device.

1:21:23
I can read files here.

1:21:25
I can create new files here, can update files on here and save.

1:21:42
So as you can see, you can get very granular and very specific with policies if you want to allow certain devices and not other devices.

1:22:00
I'm going to jump back onto my my policies to the policy that I just created.

1:22:09
Just to show you one last time the specific device information.

1:22:16
I realized that with three types, it gets quite complicated When to do and allow, when to do a deny, how to do an include and how to do an exclude.

1:22:25
So in the first rule I set an include of SanDisk and I did a deny but I denied only write and execute my audit.

1:22:39
I did the similar behaviour so Sandisks can read but they cannot write or execute.

1:22:46
So that was my include policy with a deny.

1:22:50
In my second rule I target this to all devices and I set this as a deny and I targeted this to everything.

1:23:04
So all removable devices are blocked with the exception of SanDisk and PNY.

1:23:14
So when you put those two together PNY has no policy being applied so you can do anything on it.

1:23:21
SanDisk is excluded from this deny but is included in this one and this one controls is allowed of read only.

1:23:32
So that's how I achieved my multi device type scenario.

1:23:36
Read only on one device, everything on another and block on other device types.

1:23:45
Be mindful when you create policies that multiple includes multiple excludes can get very complicated.

1:23:54
Always, always make sure you understand the default enforcement and make sure to use the right includes and excludes so as to achieve your customers requirements.

1:24:06
Always test, always validate that you meet those requirements with allows and blocks.

1:24:12
Otherwise you'll end up with a very complicated environment.

1:24:16
So be mindful and hopefully this was helpful.

1:24:22
In this final video we are going to briefly talk about reporting and how to look at events in advance hunting.

1:24:31
In the previous videos we demonstrated how to create device control policies to actually control access to devices.

1:24:39
USB removable type devices, how to allow, how to block and how to set permissions for different types, read, write, execute, etcetera.

1:24:52
Now in each of the rules you have the option to either notify and send the events if the If the events are being sent up to the service, we can use advanced hunting to actually go and query events that are going on.

1:25:12
Now in the public documentation we actually have under the Device Control Report section, we give you a couple of examples for advanced hunting queries that can be used to see information.

1:25:30
Now this first example shows removable storage policies that triggered by disk and file system level enforcement and there's a second one for removable storage file events.

1:25:40
Now in for the purpose of this demonstration, I'm going to copy this example for a policy triggering for disk and I'm going to review that and and use that in my advanced hunting.

1:25:55
To get to advanced hunting.

1:25:56
I'm in security.microsoft.com Investigation and response hunting and then advanced hunting.

1:26:04
From here I can create a new, create a new query and use that example in the public learned document.

1:26:11
I'm looking at events here over the last 24 hours and I can run that example query.

1:26:18
What this will do is it will go off and look at the advanced hunting tables to show me all instances where a device has hit this particular or triggered a device risk enforcement.

1:26:35
As you can see here, in my lab I've been demonstrating and recording some videos for this, so I have lots of blocks that are occurring.

1:26:43
If I take a look at one of these examples here and expand a particular line for example, you will be able to see in here that there is information around when this took place, the device ID that it took place with the name of the device, the user that this triggered from, what type of action fired.

1:27:05
In this case, it was a movable storage policy that triggered the access, was a read and it was a deny.

1:27:12
We have information about the media bus type, so in this case it was a removable USB device.

1:27:17
We can even see the device ID, the instance name, as well as the media vendor and the product ID.

1:27:25
So here's our vendor ID, our VID, and our PID.

1:27:29
Now if you remember from my previous videos, I demonstrated blocking the SanDisk vendor or VID of 0781.

1:27:38
So I can see from here information around what type of disk was inserted when and whether it was allowed or blocked.

1:27:47
All of this information is available through the advanced hunting and of course you can update and change.

1:27:53
Combine these queries to find more information.

1:27:56
You can change how long the queries go back for and how much information we are looking at.

1:28:02
Advanced Hunting though is not the only place that you can use to get reporting on this.

1:28:08
If we look on the left hand side and go all the way down to the report section, you will find that we have a specific report for device controls.

1:28:17
Under Endpoints we have device control.

1:28:21
Here we can actually go in and see a high level chart of the different types of media usage and actions taken in here.

1:28:35
Obviously this is just a very high level chart.

1:28:38
If we click on view details, we can actually see much more information about all of the different types of device controls, when and how they are applied and protected.

1:28:51
Now I can filter in here to the different types of policies or policy names.

1:28:57
And in this case, I'm going to look at a block all settings.

1:29:00
If I wanted to, I could look at specific media class names, for example, like USBCD ROMs if I was interested in those printers or Bluetooth devices, etcetera.

1:29:12
For the purpose of this, I'm just going to take a look at the last seven days of block all settings, and then we should be able to see some information.

1:29:19
And just like you were seeing in the advanced hunting queries, I can get information about this.

1:29:26
So on June the 3rd, I have a block all settings policy with a particular media.

1:29:31
And here's the the media name.

1:29:34
It is of the disk drive USB, the name of the device, the physical laptop that we're running this from the user that was doing this, as well as the device ID.

1:29:44
And if you look and click into this, we can actually see information around the action mode.

1:29:51
It was a deny.

1:29:52
We can see that was done on a read.

1:29:54
We can see the name of the media, we can see the grid, we can see the vendor ID, we can see the serial number, the type, etcetera.

1:30:04
And of course, if I wanted to dig deeper, I can go into the devices page, look at timelines and look at a lot more information.

1:30:11
But here you will see a long list of different types of devices, different types of actions, what blocks, etcetera when they occurred, as well as sort of high level charts and graphs to show that information.

1:30:24
I am filtered obviously on a particular policy type but if I reset that and clear the filter I can go back to seeing all device types and just need to re log in.

1:30:40
Bear me one second for the demonstration bank device controls view details, I should be able to see all types.

1:30:51
So any type of device connectivity that is being inserted into into the machines that we are leveraging, whether it be printers, devices, USB, etcetera can all be tracked from a from a reporting standpoint and through advanced hunting as well.

1:31:14
I recommend you leverage the public documentation under Device control, Device Control Reports.

1:31:22
There's some great examples for advanced hunting queries.

1:31:28
This will help you to get started to demonstrate how to pull information from advanced hunting to to see when something is denied or allowed or blocked based on your particular policies that you create.

1:31:44
Hopefully this was helpful.

1:31:46
Please make sure you leverage the public land documentation to keep up with the examples.

1:31:52
This is the best place to find those examples.

1:31:56
Now that you've seen the examples of how you can implement the top three scenarios, as well as finding information about the attributes on the devices, we want to re review that.

1:32:07
We go through defining our goals and our strategy with the customer.

1:32:12
Finding those device IDs that are relevant to the scenarios your customer is implementing.

1:32:18
Creating those reusable settings related to how we're going to define what our device landscape looks like.

1:32:27
Creating our device control policies, defining what we will allow and what we are going to prevent users from being able to do.

1:32:35
Validating the policies on test devices or on a limited set of devices and ensuring that the policies that we have created have successfully been transitioned to the devices.

1:32:49
On behalf of Josh, David and myself, we'd like to thank you for taking this time to do this training.