

The Beginners Guide to Microsoft Purview

40 MIN · YOUTUBE · [HTTPS://WWW.YOUTUBE.COM/WATCH?V=YAJTWKAPN6Q](https://www.youtube.com/watch?v=YAJTWKAPN6Q)

<https://www.youtube.com/watch?v=yajTwkAPN6Q>

SUMMARY

Microsoft Purview is a comprehensive compliance solution for Microsoft 365 that centralizes data management and compliance tasks. This video serves as a beginner's guide, highlighting key features and functionalities that IT professionals need to know to effectively use Purview for data protection and compliance management.

- Microsoft Purview replaces the old compliance portal, providing a unified experience for compliance management across Microsoft 365 and Azure.*
- Key functionalities include data loss prevention (DLP) policies, information protection through sensitivity labels, and data lifecycle management.*
- Users can create DLP policies to monitor and prevent the sharing of sensitive information, with options for customizing alerts and restrictions.*
- Sensitivity labels allow for the classification of data, helping organizations manage access and compliance requirements effectively.*
- Data lifecycle management enables organizations to retain or archive data based on compliance needs, with options for automated retention policies.*
- The portal offers insights into data compliance posture, helping organizations identify and manage sensitive data effectively.*
- Integration with various data connectors enhances the compliance capabilities of Purview, allowing for a single pane of glass for compliance management.*
- The video encourages viewers to engage with the content by subscribing and asking questions for further clarification.*

today's video is sponsored by sprocket 365 finally create a robust knowledge base in SharePoint for more details visit them today at Sprocket 365.com in today's video I'm checking out Microsoft perview for beginners this is the ultimate getting started guide for it Pros so if you're ready to learn let's go

you know compliance the world res revolves around it especially life in the cloud and compliance is such an important topic especially for Microsoft 365 admins so in this episode I'm going to take you through everything that you need to know about the newly updated Microsoft perview we're going to look at some of its cool features as well as a few of its secrets that lie within now if you've not subscribed to the channel as always bump that subscribe button up

there and ring that Bell come and join my ever growing learning community and if you've got questions as always you know what to do get those down below and if you'd like more then why not consider signing up to my patreon site here you'll get access to full Microsoft courses and an Ever growing Library actually of courses

so again details below just there so I think without any further ado I think it's about time we dive in and check out some of

the secrets that lie beneath Microsoft Purview let's check it out okay so starting right at the very beginning to get into Microsoft Purview you can do this in one of two ways from the Microsoft 365 admin Center you need to come down into the various different admin centers here on the left hand side and if you click on compliance now you will get a little note and it will tell you that the old compliance portal has

now been retired and in fact it will then as you can see so the compliance portal is retired but the new portal you can go there directly by going to perview.microsoft.com but you can also see you can easily just switch to it almost instantly and it takes you into the new portal so perview.microsoft.com is the new dedicated portal that we now have now as the portal opens up here

let's just have a quick look at around around the various elements of the portal why did we need a new portal anyway well there's always been a compliance Center in Microsoft 365 and it's had some pretty good features but we've also had a compliance Center in Azure as well so in the Microsoft Defender for cloud portal we've always had that Defender or the Purview portal in there as well so what Microsoft had decided to do is really

kind of unify this experience so we now have one portal if you will to run them all now like all of the Microsoft products at the moment we can see that we have got a co-pilot button here and again this can be very useful however you'll notice here that you do need to subscribe so it is an extra subscription and I'm not going to cover that in this session so you can see here I'm just going to scroll down and

you get an idea of just some of the various solutions that we have in Purview and again one of the nice things I like about this is that you can scroll right down and you get this insights page and one of the most important things is knowing your data so compliance is super important so if you're in aviation oil and gas Pharmaceuticals Finance for example There are rules about how and where data

is stored who has access to it and so on so knowing that the fact that you have sensitive data can be super useful what is sensitive data pii personally identifiable information names addresses phone numbers it might be credit card numbers Financial details medical details and so on I can scroll down we have something called the compliance posture

and basically all the Microsoft Technologies are basically Microsoft do their part to give you the tools but it's up to you at the end of the day to actually go ahead and configure them so for example here you can see your data protection again so if you've got data in for example in Microsoft 365 and so on you can also if you scroll down further there are a number of Trials of

course there's always the add on sale from Microsoft of course you can add in and you can enhance your experience what I'm looking at here by the way this is an E5 subscription so I've got kind of most of the kind of

cool features here so on the left hand side you can see that we have the left hand navigation bar so we have a number of as I said shortcuts to the most popular Solutions here on the main

page but we also have the left hand side navigation bar so the first place that you're going to want to go really is the settings page here so the settings page basically is the settings for all the various Solutions and you can see that here one of the first things that you get is called roles and Scopes now we have what is a role and admin role of course is basically a collection of permissions so

for example if you are a super user in Microsoft entra you would typically have a global admin role and these can be found in the Microsoft entra admin rules however you should know that for compliance reasons you typically get what we call role groups for both security and compliance and this is really important because you need these additional roles in order to

perform certain compliance features for example carrying out a data investigation or if you're doing an audit or you're working with Microsoft's Insider risk management tool and again it's a super important very very flexible way of giving users just the permissions that they need at any one time so roles and Scopes super important so for example if I wanted to Grant a

purview administrator role so by simply going into edit I can then say okay which users do I want to have access to this role now in this case I'm going to select my own demo user account here so I'll just bring this guy in and I've got a user here called CDX so I'm just going to bring that user in so I'm a global admin and I'm now also a purview administrator as well and you

can see the roles that are included with this role group so I'm going to click on done there so that's the one of the first things that you probably want to do is have a look at the role groups okay now other things that we've got here are just kind of optional so data connectors so Microsoft have basically connections that Connect into Microsoft purview so if you've got things like HR tools HR connectors salesforce.com if you've got Citrix in

fact there's a whole list of different connectors here because ultimately you want that single pane of glass solution for compliance okay so we literally have tons and tons of different connectors here now please note that some of these may entail additional costs so again make sure that you want to research that before you get started now any connectors that you do have will be listed obviously here in the my connectors

tab there as well now in terms of device onboarding so device onboarding we have what do we mean by that this is particularly useful for the information protection so if you want to extend information protection I.E. labeling and classification features to your on premises environment there is an onboarding agent that you can install and in fact this is also available with

the likes of Defender for endpoint as well okay so that's one of the first things you would go in I'm not going to go into all of these different settings I'm sure you can have a look through those in your own time but

needless to say one of the first places you'll come is you'll want to come into those settings page there and now in addition you also get the settings for the various Solutions as well so that's

important that you know that it's here in the settings page okay now on the subject of the different solutions or the different tools you can see that we have a bit of a catalog of the various tools and again I'm going to go through most of these in this session with you all right now what else have we got again anything that you open up for example any recent tools that you open up will actually appear here in the

left hand side so this is a dynamic menu and it will change accordingly so looking at Microsoft perview then what can you do with it well we're in the business of compliance and we all have to have compliance to our industry so for example if you're as I said Finance oil and gas you're banking maybe you're an electricity provider maybe you're a Medical Center Medical Professional we all have

to keep records likewise we have to protect our user or customer or patient data and we can do that in a number of ways so over here on the left hand side as I've mentioned we have a number of various tools and we call these Solutions in Microsoft perview and generally they break down into a set of tasks so whether those tasks are for archiving data for compliance reasons so you need to back up your data or store your data for x

amount of time so a number of years perhaps like tax records for example so we have storage solutions for that in addition we also have protection Solutions so things like information protection that's labeling and classification we have data loss prevention policies or as I call it data leakage prevention and we also have compliance tools as well such as compliance manager so for example if you

you're taking your company through ISO 2701 or if you're currently going through gdpr registration this can be quite useful for that there we also have communication tools and we have Insider risk management and also something called Communications compliance and these can be really powerful Tools in defending against for example malicious insiders within your organization or perhaps malicious use

within your organization as well and again as we go on I'll talk more about that recent additions as well we also have data security posture management and also posture management for AI so before you start hitting that co-pilot button and bringing Microsoft co-pilot in it's super important that you get your data protected more than anything else and in fact this is one of the first places that we're going to

look at so first up then I want to talk about data protection so coming back then to do I have any sensitive data this explorers feature here can be really useful you can simply click on the drop-down arrow and we have the data Explorer and its previous version so there's a couple of versions in there just now to be honest they're very similar so if I go into Data Explorer what this does is it takes a snapshot of

all of my data at the moment and you can see it looks to see if there is any sensitiv sensitive information so things like credit card numbers full names and addresses and again you can see there's quite a few of these so I

can say right okay what about credit card numbers that could be very serious and obviously there are regulations within the finance industry to protect that so you can see I've got 49 occurrences of

debit and credit card numbers and you can see it's dispersed throughout the various Microsoft products here so for example if I click into Microsoft Exchange it goes in even deeper and it shows me first of all it shows me what the sensitive information types are and more importantly it shows me the ACT actual mailboxes that they're in as well and as you can see I'll just come back into that you

can see that I can then click into that specific mailbox to find out more details so I can see hey you know this Alex has actually got a user he's got an email that's actually got this sensitive information in here here as a compliance manager you will have the rights to see this but again everything is logged everything is audited for compliance reasons so right away now I

can see that we do in fact have sensitive information so that's the first thing we now know where our data is you can also come into activity Explorer here now in this example I don't have much to show but you can see you can get a complete graph of your data over a period of time and again you can choose what kind of sensitivity so if you've assigned for example a sensitivity label that can be really

quite useful so we determined how to find sensitive information within our business so the next thing is we might want to prevent data from leaking outside of our organization so what I want to do is I want to come in here and create what we call a data loss prevention policy so again I can click on create policy and it now offers us a series of

templates so these templates can be based on financial medical and health privacy and of course you can even create a custom one as well so for this demo I'm going to come into privacy and I'm just going to scroll right down and you can see we have depending on where you are in the world you'll have a selection so I'm going to come in here let's say the US state social security number confidentiality law or you might

come in you have to work with the US Patriot Act for example so and I can scroll up and you can see it gives me a list of the pii categories that are included in this option here so I'm quite happy with that I'm going to go ahead I'm going to click on next and it then creates the policy for me so simply just clicking on next I get the description and it says okay do you want

to assign it to all users or just specific admin units so admin units are a scope of administration so you can manage your users for example in Washington DC C or in Chicago or in Cape Town South Africa or San Paulo depending on where they're located for the purpose of this demo I'm going to keep it simple I'm just going to click next so now it says okay exactly what would you like to

monitor so you can see I'm monitoring all of these now if I in this particular tenant I've not deployed in tune but if you have it will also look at those devices for potential violations as well you can also Link in with on premises

repositories as well okay so now it's saying okay do you want to detect the content from Microsoft 365

with people outside of your organization or only with people in my organization so obviously we're more concentrated here on people outside of your organization so again I'm going to click on the edit button here and with the edit button this is where you can go in and you can add in additional categories if you want to so again you can add in those additional sensitive information

types there if you want to so now coming in we're talking about potential actions so what do you want me to do if it finds sensitive information like this so you've basically got the option it will send an incident email and it will fire up an alert as well you can also restrict access or encrypt the content in Microsoft 365 locations as well which is something you probably

want to do now the way that this is in force is it's either enforced as I'm sorry you can't send that out period okay full stop or alternatively you can let people override it so you might get an email that says hang on you're trying to send out a credit card number I'm sorry we don't permit that or in this case let people who see the tip override

the policy so this gives you a little tool tip in Outlook and it says you know hang on a minute there's some personally identifiable information here are you sure and you can basically say yes I'm going to let that go so this is really on the user so the user would come in here and they would go yeah I'm happy with that I'm going to send it out now the one thing that you might want to

do is you might want to say I want to require a business justification to override that so that can be used full we also have some auditing features here I've not enabled that at the moment but you probably would in reality okay and you can also do file activities for apps and you can restrict them if you want so in other words you're restricting certain

applications okay so again scrolling down here you can also I don't want my data talking into any thirdparty apps now these would light up if we had those connectors in that I mentioned earlier so in this example I'm not using that now a good idea is always to run the policy in simulation mode first all right because if you don't get it right it can be an absolute nightmare so always run it first okay in simulation

mode typically this lasts 90 days and then it will be switched on and it just gives you a chance to kind of iron out any issues so I'm just going to Simply click on next I'm going to click on finish and that my friends is how you create a data loss prevention policy so for the second solution I'm going to come back into Solutions here and on the subject of privacy a super important one especially now that everybody's talking

about co-pilot is information protection and information protection essentially is labeling and classification I'm just going to close these little options down here so here in the information protection page we have the we can do some reports you can make some recommendations this is where you can create your sensitivity labels

and you essentially assign a sensitivity label in one of three ways label publishing policies is manually though this is

typically where the users it would choose or select a particular label that meets their requirements auto labeling policies combine with data loss prevention policies that I've just shown you so essentially if it detects for example a credit card then it will automatically apply the corresponding label that's the idea behind it and we all also can create protection policies which are currently in public preview and I'm not going to

cover in this session but I'm going to cover that in a dedicated session in the future we also have the classifiers as well so you can create your own for example sensitive information types now you also have the same explorers window that I just showed you and we also have Diagnostics here so the first place that we're going to go is we're going to come up into sensitivity labels so again sensitivity labels are really

nothing new new they've been around since the 60s and essentially it's a way that the military for example can classify a piece of data as being secret top secret classified unclassified but we can also use these in a commercial environment as well and you can see that we have a number of kind of pre-created ones here so I'm going to go ahead I'm going to create a sensitivity label and what we're going to do is we're going to

call this we'll call it Finance confidential okay so Finance confidential and I can take this and I can then copy that into for example the display name and put it into a little description for my users as well now you can also use a color as well so you can select any color of your choice so I'm going to choose that one now one of the nice things about sensitivity labels

is that you can classify different types of data so this might include for example files and other data assets so if you're using things like powerbi Microsoft as your data data storage and also Microsoft fabric then you can use the classification labels here emails of course meetings if you're using Microsoft teams now the key thing about this by the way is you do need a premium license for this and this

particular tenant doesn't have that so I'm going to deselect that at the moment we also have groups and sites please note a Microsoft 365 group can also be a Microsoft team so again yes you can follow through that labeling with that option there now once you've chosen those I'm simply going to click on next and we have three options so do we want to use labeling and classification to control access do we

want to apply content marking for example headers or Footers and do you want to protect teams meetings and chats again for this you'll notice it's grayed out it's because I don't have the team's premium license within this particular tenant so the next thing that you want to do is I'm going to click into next and this is where I can add in a header so I can put my text in here so I'm just going to paste that in you can choose

the font size so for example if I set a size 12 and you can also choose the color scheme as well in this case I'm going to choose red I'm going to say next and again it now says okay do you want to do auto labeling so Auto

labeling is basically where you use data loss prevention policies so by clicking this I now add the conditions for data loss prevention policies So based on the condition it will you can then assign a

label automatically for the purpose of this demo I'm going to keep it nice and simple now it says okay do you want to define the protection settings for groups and sites so again you can select these option here based on your design of your infrastructure so I'm going to choose privacy and external user access and as you click next you can now refine your privacy options so for example

anything that's labeled with this particular label you might say you know I want it to be private I don't want anybody to be able to make it public and likewise external user access this is disabled here because of the private option but again you might want something a little bit different so Define external sharing settings for conditional access so again you can control external sharing from for

example Microsoft SharePoint and you can also protect the data within SharePoint here as well again privacy what very important when it comes to teams because a public team is discoverable by anyone and anyone can join it where as a private team it's By Invitation Only so what this does is it a private teams and shared Channel controls so in other words if you had a document that you had

in a Channel or in a particular team you might say well you know I only want for example private teams to be able to view this only okay so clicking next you'll notice that we can now Define the privacy and Grant external user access so in this case it's a private team I don't want my users being able to invite external users to access this very private sensitive data you can also

control the sharing from labeled SharePoint sites and you can also use conditional access to further granularize here and again for the purpose of this demo I'm just going to click next in terms of do you want the team to be discoverable I.E if it's public anybody can view it or if it's private again you might not want it discoverable you might want it private so in this example allow users to discover private

teams that this label is applied and I'm saying here for example internal use only I don't want this to go public so now that I've created my label I simply click on next and one of the first things it will ask you is you want to publish this label so you can publish it now or it says don't create a policy yet and that's the other quick gotcha with information protection is that so you

create a sensitivity label it ask you do you want to publish it and you go yes and you end up with a situation where you've got 50 labels and 50 label policies so in this case I'm going to say no I don't want you to publish that label yet so what you can do rather than publishing the label to a new policy I can simply come down here to policies and I'm going to choose label publishing

policies here I can select the label public policy so in this case I have two options here so I'm going to select this policy and I'm going to edit the policy so by coming into edit here I can now select one of my custom label

policies that I kind of pre-created so here's my finance confidential I'm simply going to click on ADD and this

will add it to that confidential category here now just a quick mention by the way that this can potentially take up to 24 hours so you might need to be a little patient here do I want to push this out to particular admin unit or the entire organization I'm just going to say the entire organization so the policy settings here you've got a few selections again I'm just going to keep it simple I'm going

to click on next do I want to add a default label or do I'm do I just want to trust my users that they assign an appropriate one so in this case I'm not going to assign any default labels I want my users to be able to create something so now that I've clicked on next I can simply submit that and again that is my data loss prevention policy so how is this policy applied so for

this I simply come back into Microsoft 365 let's say I've got a document here that says quarter 1 product strategy so I can simply come into this document as a user now and you'll notice up here on the right hand corner that we have this paintbrush and this my friends is the sensitivity labels so you can see here I've got a selection of sensitivity labels now you'll notice that my new

label is not yet available because it can take a little time to propagate so for the purpose of this demo I'm just going to say Hey you know this is confidential and I'm going to say recipient only now if you choose this the administrator in this case says hey okay if you want to assign this label you need to provide justification so I can say yeah either the previous La

label no longer applies it was incorrect or you can put in your own decision in there if you want to so I'm going to just say this is my own Choice once you finished I'm just going to click next and now you can see that this document has been classified and that my friends is labeling and classification okay so so far we've talked about data loss prevention policies we've talked about information protection I suppose the final piece of

the puzzle in protecting your data is ensuring that it's available in case you lose it so for compliance Reasons I'm going to come in here into Solutions and in here I'm going to talk about something called Data life cycle management now I although I you must appreciate I can't cover every topic in this kind of getting started guide there are some core topics that you definitely need to know so data loss prevention policies information protection and this

data life cycle management so data of course has a life cycle throughout your organization somebody will create data it'll be used it'll be managed you might get different versions of it and then ultimately at the end of the day it'll be archived and then finally removed or replaced so we need to know how to do that and to do that what we do is create something called retention labels so I'm going to click on here and I'm going to

come into a retention label and I'm going to say you know I want to retain my data let's say for example I'm in Oslo this week so I'll call this my Oslo marketing and I'll say once retain or once retention okay so again I can

copy this and I'm going to copy this into the information tab just down below and also as a description as well I'm going to

click next and it then says okay how long do you want to retain the data for do you want to retain it forever in other words your placing the item on hold or just for a specific period of time or alternatively do you want to enforce actions after a specified period or simply just label the items so for example personal you don't need to keep it you don't need to store it for compliance

reasons so that's another question archiving why do we archive data typically it's because because of compliance reasons so for example you may need to retain your tax information for 7 years and so on so how does that work then in data life cycle management so I'm just going to say retain forever or for a specified period and for the purpose of this demo I'm going to choose a custom option and I'm

going to let's say just save it for 12 months so how it reten Works in Microsoft 365 and in aure is that there are two recycle bins when you delete something it goes into the first recycle bin for 30 days and then a second recycle bin for up to 63 days so for a total of 93 days so at the end of that 93 day period it's finally removed unless you have a a

retention quity here so I'm going to say I want this to be retained for items when it's created up to a year beyond that year it then goes into that recycle bin system the other option here that I like is when the item was last modified so for example I create a document today let's say it's the first of February 2025 and that is then retain till the

1st of February 2026 and then if you choose to delete it after that retention period it would then go into that recycle bin period beyond that it just removes the retention label and you can then delete it now here with this option is if you went in and changed that document on the 1st of March 2025 then it would retain the item till the 1st of March 2026 and subsequently

get the idea so for the purpose of this demo I'm going to choose when the item was created there are other options here as well typically based on employee actions so if you're using a HR package that's integrated and the employee leaves the company for example it would then go into a recycle bin system let's keep it simple and just choose when the items will last modified 12 months okay so at this stage it's saying what

do you want me to do do you want me to publish the label to various Microsoft 365 locations or to apply the label and this really depends if you're using data loss prevention policies so if you've just created a DLP policy that looking for credit cards for example then it would Auto apply this label please note this is dependent on license so if you've got a small business license you may not get this option here or do

nothing so just leave it that's if you've already got policies so I don't have any policies at the moment so I'm going to say let's publish this label and I'm going to say you know I want to I'm publishing this label to this

policy I'm just going to publish this to everyone rather than what we call an admin unit or you know let's say I'm I want to deploy this to New York or London or Chicago I'm just going to say

to all of my users and I'm going to choose a static option rather than adaptive adaptive is basically rule based so any users in Oslo for example it will automatically pick up the Oslo field from the user's properties I'm just going to say next and I'm going to say all locations or you can choose specific locations so I'm just going to say one drive exchange

teams I'm going to say everything so I'm in Oslo this week and I'll just call this my Oslo policy and I'll say next and then finish and there we have it I've now create a l and there you have it I've now created a policy and I've published it as a label policy so that will now be available for my users how cool so there you have it my ultimate getting started guide with Microsoft perview Hey

listen I really hope you found that useful and if you did give me a big thumbs up and let me know that you enjoyed it and if you've got questions and comments you know the drill get those down below and I'll do my best for you okay that's it for this time I really appreciate you dropping by you stay safe I'll see you soon hey thanks so much for dropping by today here's a couple of videos that you

may enjoy and while you're here here go ahead click on the Subscribe button and you won't miss out