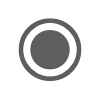
**Teams Meeting Entra Suite The Good, The Bad, and The Ugly-20251029\_120600-Meeting Recording**

October 29, 2025, 10:06AM

59m 21s

 **Nicolas Blank** started transcription

 **Nicolas Blank** 0:03  
And we have started. So with that, let me say welcome to everyone to today's lunch and learn. And the picture that you can see is actually where we're at since Monday on the South African Azure User Group where we have grown from 2009 to.  
Actually that that picture is wrong. It's I pasted the wrong one. Anyway, there's more and I'll fix that for tomorrow. But we are growing every day and this week in leaps and bounds and this is a lunch and learn session for the South African Azure User Group.  
We are in week 44 of 2025 and if you don't know what that means, it means that there are less than 10 shopping weeks left for Christmas. You are here because you are finding the session on meetup.com on the Azure User Group South Africa and today we are doing.  
The third of this week, which is Entra Suite, The Good, the Bad, and the Ugly, presented by Shaun Hardneck. If you are with us tomorrow, you'll see that we're doing Azure Networking, choosing the right connectivity architecture for your cloud with Warren Detoy.  
If you missed today's session or if there's something that you want to go back to, have no fear because the session is recorded and it is available for free like beer and fresh air on the following GitHub and I will communicate this to everyone via mail after this session. We do have a code of conduct and it's.  
That we talk about the code of conduct as a user group that is subordinated to the global set of Azure user groups. The code of conduct says that we accept everyone and we will not tolerate any form of discrimination of any sort.  
And if any of that is reported to us, we will evict you from the group.  
With that, with no discrimination, we talk about Shaun, and Shaun has a lot of history in the industry. I've known Shaun in several guises, and in his current role as a cloud architect, he actually is a little bit of a generalist in the M365 space.  
So with that, there's not a lot of things he hasn't done, but he does spend a lot of time in the M365 and intra space, which is why he is doing today's session. And today's session, as I mentioned, is intra suite, the good.  
The bad and the ugly. And with that, I'm going to hand over to you, Shaun.

 **Shaun Hardneck** 2:42  
First things first, I I like the animation. That was brilliant.

 **Nicolas Blank** 2:48  
You are annoyingly good looking in a suit. That's all I'll say.

 **Shaun Hardneck** 2:53  
I've picked up weights since then.

 **Nicolas Blank** 2:56  
We all have. I have a suit I don't fit to anymore.

 **Shaun Hardneck** 2:59  
And thanks for the introduction, Nick. So I'm gonna dive in. I'm not gonna.  
Around too much on myself, but I from time to time I do blog on blog is called thatlazyadmin.com like Nick mentioned, bit of a generalist and I share a bit of everything that is Microsoft cloud related or issues that I pick up or challenges that we face from time to time.  
Good. Let me minimize Skype. All right. So the presentation for today or topic for today, enter the good, the bad, the ugly. It's not a sales pitch. So we will dive in some of the real world scenarios or things that.  
I've seen from time to time things that customers have picked up from time to time and we will just have a chat about it. And like the sessions suggest, it's a lunchtime learn session. So if you have any questions, please feel free to ask.

 **Michael Engelbrecht** 4:03  
Mhm.

 **Shaun Hardneck** 4:07  
So the first slide that we've got why identity matches.

 **Michael Engelbrecht** 4:10  
2.

 **Shaun Hardneck** 4:14  
And one of them is traditionally identity has changed quite a lot. So we used to rely on our firewall, our network parameters to control everything. But because in nowadays traditional network parameters have gone, people are working from a.  
From coffee shops, they're working from some hotels and that makes it difficult for the perimeter or the traditional perimeters to kick in. We are now flooded with SAS applications. People have AWS, they've got Azure and.  
Incorporating our traditional approach for perimeter security has become a bit of a challenge. So that's why we start looking at or hence Microsoft started looking at Intra ID. How can we secure our identity or how does identity become the center of our zero trust as we.  
As we call it, so Microsoft Entra ID sits at the center of the model, controlling anything from conditional access, enforcing MFA and monitoring our sign insurance for our users across the board.  
So what is Intra Suite? So Intra Suite as it as the name suggests, Microsoft has moved away or has enhanced Azure Active Directory as Nick gave us a nice introduction of the name Intra where it comes from.  
So Microsoft has continuously evolved Microsoft Entra into a suite of products as what we know it as today. So it started off with Azure Active Directory, now evolved into Microsoft Entra.  
And if we think of it, think of Microsoft's end to end identity ecosystem covering anything from users, devices to workload management and controlling permissions for other third party products as well.

 **Michael Engelbrecht** 6:10  
Hello.

 **Shaun Hardneck** 6:13  
It also brings in identity governance. So identity governance brings us user automation, lever, joiner, mover. We think of users moving from different departments. Users HR creates a new user in a payroll system or HR system that filters.

 **Michael Engelbrecht** 6:14  
OK, why don't you meet?

 **Shaun Hardneck** 6:33  
Through Entra ID creates the user objects, et cetera. Entra Identity Governance ID governance allows us now to have all of that control within Entra suite, so we don't have to have all these a lot of third party products orchestrating and creating workflows and automation.  
Some of those functionalities now we can get directly from intra ID identity governance. Then one of the big products and I think there isn't enough talk about it, which is permission management which extends the principle into cloud applying least privilege across Azure, AWS and GCP cloud.  
So instead of having split identities across these different clouds, now we can have permission management where we can control those sets of permissions across the different cloud providers. So we have enterer ID as our source of truth for our identity and we leverage that to sign into.  
AWS and GCP so we can still maintain control over that.  
And then we also have what is called verified and workload ID. Workload ID ensures that not only people, but apps and services themselves can become trusted identities as well.  
Although the suites form the backbone altogether, this is the suite forms the backbone of zero trust strategy. How we implement the products just helps us to make sure that our it enhance the way that we implement and control and govern that zero trust environment.  
So now let's look at the first part, the good of entra ID, and that is the unified governance. So I was telling Nick earlier it is.  
Such an amazing product that Microsoft has created. So with lifecycle workflows, as I've mentioned earlier, you've got users starting in an organization. No more do we have to wait for it to create a user account or.  
Enable that user object when the user joins the environment. Now with workflows we can have that user on the day the user starts send a notification. These are your login credentials. Send the information to the hiring manager or the reporting manager. This is the new user's information.  
So workflows have become an amazing piece of technology in Entra where we can automate a lot of the tedious tasks that used to sit with helpdesk. And then additionally we look at access packages. How do we bundle easy access management across?  
The M365, the Azure space, we sit in large organizations where we've got hundreds or even thousands of employees, but they all need access to either some form of applications. Department has got a structure where they need to access SAP.  
SAP access or they need HR access or they need a development tool access. With Entra ID and Entra governance, we can now leverage those access packages to predefine the access that a specific department requires and then let the user request access to those packages.  
Via an approval process. So if we look at it, most breaches start with forgotten access. So we need to now be able to control. What do we do with access that has been forgotten? User left the organization. IT forgot to do cleanup.  
So that is where ID governance fixes by automating, provisioning and forcing reviews. We have HR triggers review and confirm if the user is still there. One of the biggest risk organizations is still facing today. It's just simply objects that have got access to.  
Environments, but the user is no longer there or the user has been moved to a different department, but that user still has access to either a development system or a critical business system with access rights into it. So we need to be able to make sure that we can control those permissions and that's where access rights and identity governance.  
Solves those problems with automation. As much as we can automate the access reviews, the granting of accesses, then we have more control of when users are starting to shift different departments or organization or user leaves the.  
Organization. So we don't want to sit with the risk of forgotten identities or forgotten access in the environment.  
One of the additional good is the Microsoft Permission Management. It's a proper SIM across three major clouds. The permission creep index is brilliant. It will show you where you've got permissions that is either too high or there's a gap between.  
How much permissions that this user has been assigned to? Do they actually leverage those permissions? Do they still require that permissions? So it's quite a brilliant and intuitive product. It shows you exactly how much damage each identity could cause.  
Across unused across the clouds based on unused permissions. So if you've got user X setting with let's say global admin permissions, but that same user has the same equivalent permission sitting on GCP but they don't log in.  
So permission management will then be able to show you those critical gaps that you have. So we can reduce that user's permissions or we take away it completely because the user hasn't signed in for X number of months or hasn't managed anything. So we need to take control back into our identities or permissions that we have set.  
So this is where Interoper Mission Management really shines as a product because it caters across or it covers across Azure and AWS and GCP. The challenges isn't granting access, it's that we grant.  
Too much access and that's where we rally and we really need to start taking back. It's the same as when we started with M365, everyone was in IT started having global admin permissions and we started over.  
Provisioning people with access that didn't really need to have access. So what was discovered, it gives a complete visibility. Permission management gives us a complete visibility into who has access across which cloud.  
And it gives us the ability to help right size the permissions automatically by auto removing users. After a set number of days, like 90 days, we start remediating those permissions and it gives us the ability to monitor. It continuously watches for anomalies leveraging the machine.  
Machine learning capabilities in it detect if there's over privileged identities because before they become a breach, the insight is eye opening. Most organizations find they can safely remove up to 80% of permissions without breaking anything, and that is purely because we assume.  
That our service account needs to be global admin. Our service account needs to be Exchange admin, where in fact a service account is pretty much just happy with having read only permissions and that's it. And that is why we need to have a look at permission management.  
The tools that forms part of the intrasuite and leveraging those caabilities.  
Then as we continue on on the good, so we look at zero trust in action. So we all have heard what zero trust is trust, trust, no one verify everything. So this is if we look at zero trust trust in action, this is where everything comes together.  
Together zero trust in motion in Microsoft Entra we start looking at conditional access policies, the brain behind policy enforcement. It makes decisions dynamically based on factors like what is the user's risk? Where is the location the user is coming from? What is the device health?  
So conditional access is one of the great features of Inter that keeps evolving. We continuously see features being involved like the sign in sign in factors where users are signing from so we can.  
Set quite strict controls based on what is required in the environment. Then we're looking at Progress Identity Management, or PIM for short. This limits exposure by giving admins just the right access.  
At the time that they required nothing longer, nothing less. So with EM we can control global admins to only have access for four hours to erform the function that they need to erform. With that we include.  
We'll include a completional controls before the user gets elevated to a global admin or specific admin role that they have to get approval from line manager. So get a e-mail notification. Line manager proves so and so needs access to global admin role.  
Elevate the user and the user starts getting gets added to the role based role based group to perform at their function and then we look at last but not least we look at the defender signals feed real time intelligence into Entra.  
If defender detects risky activity, conditional access response instantly, forcing MLO or even block access. So when we look at those defender signals, we will see signals like.  
User signing in from abnormal sign in identified where user is coming from sign in detected out of South Africa but the users based in South Africa Defender signals will will pick those up. Enter ID will flag those.  
As abnormal traveling or signing activity being detected. So with even with those few controls put in place, we already we can already see major differences in in identity security by just making small changes in the environment.  
Together these these create loving, breathing zero trust systems, one that continuously verifies every logging, every session, and every privilege.  
It's not about trusting ones, it's about verifying always.  
Then we look at the bad in enterprise complexity. So one of the the ones that is a real challenge is if we look at from a bad point of view is Microsoft always has this carrot dangled in front of us of.  
What is, what is possible in Entra? What is the nice to haves, what you can can do, what you can block and what enhancements you can do. But then we come to the licensing part and we start seeing the complexities across the P1P2, the skews that's been broken up between governance and then the same tiers.  
It just becomes a nightmare for IT departments to start and manage what works for me, where do I, what SKUs do I add and what SKUs don't I add.  
And then we also have the challenge of the portal fragmentation where we see admins have to navigate between the Azure portal, the Entra portal and the Defender portal. So we need to start doing investigations, compromised user account or.  
We need to make settings changes, then we get redirected to a defender portal or Entra redirects us to a portal in Azure for related to PUM that we need to configure. So there is these little fragmentations that we need to be aware of or that can become a.  
A daily frustration, depending on how often we live and breathe in that portal, and then visibility becomes a bit of a challenge if we need to, because the portal, the information that we always see within the portal might not necessarily be.  
All of the information. So that's where we start relying on reporting tools like Microsoft Graph API. Now we need to start harnessing and updating our skills related to Microsoft Graph scripting. How do we use Graph API and then script the information that I require?  
Require pull out that necessary information. So then those are the part of the complexities that we have to realize is the real world. Not all departments or organizations will have the budget to say I'll purchase this tool out-of-the-box.  
It can give me this report or it can do that. We have to be mindful of the departmental financial challenges and constraints that we are facing. Hence the Microsoft Graph API and how we can query the results that we pick up from it. It's amazing. We just need to think what it is.  
That I want to see and then use the Graph API to try and pull out that information that's not natively visible into the portal. So one scenario I can think of we in order for you to have longer.  
Logs in of intro logs. So by natively that we see 90 days worth of logs. So if you have not incorporated Microsoft Sentinel and shipped off those logs to a Sentinel workspace, you need to find other mechanisms of pulling out those logs, storing it somewhere for your own use or.  
Do a regular month end report extracting that information. The graph becomes your perfect tool of choice to perform that kind of functions and just saving those information somewhere. And for enterprises managing multiple tenants, there's a real operational overhead coordinating different policies.  
Reviews identity governance across environments. That doesn't become easy because now I need to control what access packages we've configured for tenant A, what is happening in tenant B, so keeping.  
Keeping all of that In Sync does become a challenge and as we look on later on.  
How do we what? What ways can we put in place to manage the these multi tenant organizations?  
The key is to centralize and streamline, consolidate logging into Sentinel, define clear admin workflows and invest in graph automation. So Microsoft still pushes us with all the greatness and the.  
And the beautiful things that we see in Entra, a lot of the information we still pull out and we still use the Graph API on an almost daily basis to surface the information that we really want to see.  
So while Intra provides incredible capabilities, it still requires careful design and governance to keep things manageable. So adding more tenants because we want to.  
Separate a business unit or we we want to add another business, but it's going to be there for six months only and then we need to tear it apart. So those are where we have to carefully design different type of scenarios.  
The organization goes through because managing all of this does become a bit of a challenge.  
And then the ugly that we have to look at and and talk about is service principles. So often we get a vendor requesting, look, just spin up a service principle, give it owner rights for now, we'll get back to it.  
But the problem with that is that those service principles sometimes have more access than what the administrator accounts have. So we forget about them totally because they're running at the back. Service principles are configured with never expired secrets.  
So they are a.  
They are a compromise entity waiting to happen if they are that aggressively assigned permissions and secrets that doesn't rotate or that doesn't expire. And then we've got legacy authentication which bypasses conditional access policies. It still hangs around through old exchange.  
Connectors, SMTP relays and the Power BI connector. All of these bypass conditional access and MFA, making them an easy entry point for attackers to get into. And then we've got the audit blind spot.  
Another concern, workload identities often don't show up properly in sign in logs, meaning you could have activity happening without visibility or alerts, so we need to be careful with.  
What we have and that is where if we look at the ordered blind spots, that's where we have our day-to-day of Microsoft Graph API comes into place. OK, what application do we have that is? What workload do we have that is configured for in intra ID as a signing? Do we have those logs? Nope, we don't have them.  
OK, how can we get those logs? Let's use Graph API. Let's pull out those logging information to see what is happening. Or just make it a conscious habit to say we need to start reviewing the applications that we've got integrated into Entra ID.  
And start going through those logs and the alerts that being or the failed logins that's been triggered within Intra ID for those specific applications. And then finally we're looking at privileged access workstations.  
Or the lack of them. Too often we've got we still have admins performing domain admin, enterprise admin level functions from their laptop where they are the local admin on their laptop.  
Organizations is not having the conversation enough about privilege access workstations. Why do we need to have that privilege access workstation? Why does the workstation needs to be isolated and separated and only perform certain functions from that laptop if I'm a global admin?  
I shouldn't be able to just go into a coffee shop. I take my laptop and I access the my organization's environment. That's a that's a major security risk. So what happens if someone managed to steal my laptop and there is keys and stuff stored on onto my laptop or access tokens? So those are.  
Critical things that organizations are not having enough conversations about, which should be talked about more and should be implemented. So these are the gaps that attackers can exploit. But the good news is they're all flexible through strong governance, monitoring and proper lifestyle management.  
So if we're looking at our Privileged Access workstation, yes, we've got a workstations, we've got the CIS package deployed to a AVD machine or Windows 365 machine locked down completely with CIS controls, and only from that machine I'm allowed to use conditional access to access the.  
M365 or the Azure portals to perform my admin functions. So those are the type of scenarios or the thinking that organizations should start having to make sure that they safeguard the most critical assets, which is data that they have that they've built up.  
The access to the critical systems, finance and the SEP systems so.  
Yeah, so the ugly of the is real world pitfalls that can damage an organization pretty quickly.  
And then we look at designing for control.  
So one of the one of the things that we look at is.  
I think we all are fairly familiar with the tiered admin model based on when Active Directory started rolling out. All organizations start having AD and then we had this tiering model, Tier 0, tier one accounts.  
And those are the same thinking that we should start applying in intra ID. Let's not take it away. How do we incorporate that some type of tearing structure into our environment at the moment? Because we need to say not everyone should be able to see to have access to tear.  
Tier 0 role based groups that should be strictly locked away with with privileged identity management hidden behind an access package where only certain people in the organization can approve access to that. Then we're looking at DevOps integration. How do we make sure that the changes we apply in our organization?  
Has is approved changes the code that we are kicking off against our environment that we are not executing malicious code because we cloned A GitHub repo from the Internet and it says you can automate your environment, just clone this GitHub repo. So by integrating that in that.  
Security checks with Defender for Defender for Cloud scanning the code that is being being pushed inside our environment via Azure DevOps. We get to scan those codes. Defender for for Cloud be able to give us and tell us look, this code is got secrets in it.  
Are you sure you want to publish it or you block that code from being published because you're sharing a secret over plain text that should be hidden either in a key vault and then reference the key vault and then do the deployment. So those DevOps integration is becoming a.  
Massive critical function of our of how we move forward because we want to make sure that we've got controls implemented that is standardized. Business has signed off and agreed on it. We've got security checks. Every time we push a new script, we push a new deployment of a piece of code.  
It gets controlled. It's validated by at least two members for approval, so everyone. So there's views on the code, not just Defender for Cloud saying where's the security flaws in it, but there's actual people validating what we are deploying into production into our environment.  
So and then we've got automated reviews and reporting. So we need to start automating our reviews. So if there is controls that we need to pull out on a database, if we look at intra ID, the reports that we are getting, we get set up reports.  
For risky users on a weekly basis, send the e-mail notification, say these are the users that has been found. Let's review them. We organizations or InfoSec should start taking ownership of those notifications or those.  
Those reportings that comes in and then actively work through them to make changes in the environment. And then finally brilliant tool that I think most all of us have seen, which is the Meister tool. So Meister with Azure DevOps allows us to monitor control.  
Drift and compliance in the real time. So with DevOps integration and Maesto running continuously, we can say OK, conditional access policies have changed. There is change that happened on our global admin groups that has been modified. Our critical groups have been modified.  
Like fire or for e-mail notification to this department say why do we have drift? But we need to start making conscious decisions that we need to actively start assessing our environment on a monthly or regular basis so that we know what is happening in our environment and if we take ownership and control of it.  
O.  
On the next session, I just want to quickly show you guys a functionality in inter ID part of conditional access that we all should use quite actively and I hope everyone else is also using it, which is the what if function.  
So I'm just going to quickly while I switch screens, do you have any questions yet?  
Yep.  
OK.

 **Nicolas Blank** 32:21  
No one's coming of meat, so I'm going to assume there's no questions.

 **Schalk van Wyk** 32:25  
I'll ask questions later. Too many.

 **Shaun Hardneck** 32:30  
Good.

 **Nicolas Blank** 32:30  
Actually, if if we were on in the same room, we would, we would just stop the bus and ask questions. So you're welcome to ask questions, Skulk.

 **Schalk van Wyk** 32:41  
So my question is more related to to um Microsoft Intra external ID, so.  
And using it together with Entra. So there's a scenario that I'm thinking about that I needed for a client where we're building applications that's going to be available external to your organization.  
So hence the use of Microsoft intro external ID.

 **Shaun Hardneck** 33:13  
Mm.

 **Schalk van Wyk** 33:14  
But those applications will need to allow people within the organization also to authenticate on them.  
So would one use the entitlements and stuff like that in the main tenant to sort of keep them In Sync or?  
I don't know if it entitlements really fit in with external ID or or is more specific to.

 **Nicolas Blank** 33:43  
I see Matthew swooping in on that one. So Shaun, if you want to, you can hand the one over.

 **Shaun Hardneck** 33:46  
Yeah.  
Yeah, Matthew, you can go.

 **Matthew Levy** 33:52  
Thanks, Nick. It's sorry, Shaun. It's so in that scenario, Skulk, you're going to have two separate tenants. You're going to have a workforce tenant and an external ID tenant where the app is published.  
And they're they're they might be associated with the same company, but they're separate tenants. So your workforce identities, you know, bob@contoso.com is gonna need to be granted access to the applications in.  
Uh, you know, whatever app. Um.  
Woodgrovewoodgrovebank.com external ID tenant as a guest. So you'd have to add that identity as a guest and there's ways you can do that through cross tenant sync so you can do synchronize identities from the workforce.  
Tenant into the external ID tenant so that they can then be granted access or you just let them sign up and sign in like the users of Woodgrove Bank would do anyway and grant them access.  
Does that answer your question, Skog?

 **Schalk van Wyk** 35:07  
So I mean, so yes, you have your main tenants. Are you gonna have another one which is your workforce tenant or is that part of your main tenant?

 **Matthew Levy** 35:15  
Hmm.

 **Nicolas Blank** 35:17  
Sorry, Scout, something that Matthew didn't mention is that B to C is also depreciated in favour of another mechanism.

 **Matthew Levy** 35:18  
Mm.

 **Schalk van Wyk** 35:23  
Yeah, yeah, I know. I know that one.

 **Matthew Levy** 35:24  
Hmm.  
It's called you and I have. We've spoken. We before we spoke about some of the customization that wasn't there in the the external ID stuff. I actually asked about that. I think I owe you a.

 **Schalk van Wyk** 35:27  
Um.  
Yeah.

 **Shaun Hardneck** 35:36  
Mm.

 **Schalk van Wyk** 35:37  
So this scenario is a bit different to the previous one. So there's there's a third scenario which is for customers. OK, so this scenario is like there's branches or whatever that might need access as well to these applications.

 **Nicolas Blank** 35:55  
Scott, just for the the sake of the where where Shaun is in his current flow, I'm going to ask if if we just to respect where where Shaun is, if we're not on on the the current feature, let's take this one to the end of the session from a Q&A point of view and then we'll pick it up gladly.

 **Schalk van Wyk** 35:55  
So I need to be able to sign in.

 **Matthew Levy** 36:01  
Mm.

 **Schalk van Wyk** 36:05  
Sure, mhm, yeah.  
Cool.

 **Shaun Hardneck** 36:15  
So happy.  
Good. So one of the.  
Great features of conditional access policy of how we restrict access into our environment or intra ID. So I've just created two basic conditional access policies. One of them is restricting access.  
To everyone else apart from a location that I have defined and that is South Africa as a as a country, everything else we have blocked access so now.  
And the second one is just risk based sign in. So we define conditions, sign in risk. Any user with medium or high end risk will be prompted for MFA sign in. So note that this is an empty.  
Empty tenant and no other policies configured, but what I wanted to show was.

 **Matthew Levy** 37:16  
Shaun, could you could you maybe zoom in a bit? It's small for me and I'm sure it's small for others too.

 **Shaun Hardneck** 37:19  
Yeah, yeah.  
Hang up. How's that better?

 **Nicolas Blank** 37:26  
And you still have young eyes.

 **Matthew Levy** 37:28  
Yeah.

 **Shaun Hardneck** 37:28  
OK, so we're going to use the what if function. So every time that we deploy a new conditional access policy in the environment, we always have the risk of what if.  
If I deploy this policy, am I going to break access to my application? Am I going to prevent my users from signing into specific applications? So that way we can define and test workload identities. We can check guest and external users.  
Test what the flow or the experience will be for those users. O if I just select a user, I'm going to use a demo user.  
And I'm going to select the the target type. What are we going to authenticate again or what are we going to test? I'm going to test the cloud app. I'm going to select the cloud app which is visible within the MTRA within conditional access. So we're going to say.  
M365.  
And then here we can start defining the specific countries where we want to come from. So I'm going to say let's do a test flow. Let's validate if we are allowing people from Brazil.  
And I should have an IP for Brazil. Sorry about that.  
So because I set the policy.  
The changes that I've made in the policy, so location state which is on and I've not configured anything for it. We can see that the reason the policy will not apply is because of the location, which is interesting because they're coming from Brazil.  
So this is how we can validate what our policy will do. If we look at the policies that will apply, all the policies that will apply will be listed here and we can exactly see what the impact on the user will be. So will the user receive MFA? Will the user be blocked out or locked out from the tenant?  
If so, this policy will show you here what the configuration is. Then we can also continuously filter with what you want to do. What is the authentication flow going to be? So the what if tool has grown so much that Microsoft started adding.  
Adding.  
Adding all the additional conditions, sign in conditions. Previously we could just specify the application, your source IP address or the country that you're coming from and it will tell you which policies will apply and what will not apply. Now we have a sign in risk. We can define the risk level that we are signing in from.  
User risk level, what does that look like? And we can specify more and more type of platforms where we are logging in from to start understanding what conditional access policy will do. How would it have an effect on our end users at the end of the day?  
Then we one of the things I want to showcase is sign in events. So we in order for us to do start with troubleshooting within intra of why specific users are not able to sign in.  
Or why is the conditional access blocking them? What is what specific control? So yeah, we've got a user that has got an interrupted session. So if we look at this and we expand, then we can see the user's password is expired and therefore the login or session was ended.  
So now we can with enter a sign in logs. Now we've got all of this information that's readily available to us that we can start understanding what is happening with our user sign insurance. What will the effect be of certain policies if we are rolling it out? Is there any conditional policies that's been applied?  
To the users. So here we can see conditional access policy applied for unrestricted countries. Success policy not applied for risky sign insurance for the risk score.  
And then we can look at additional information. Was the user prompted for MFA? Was that completed? MFA was completed within Azure AD. So we have all this information that becomes.  
More and more available, the more Microsoft enhance the the product and the functionality.  
Hey.  
And then I'm going to just quickly switch back. Almost time to Q&A.  
So.  
Just to wrap up the quick quick demo, I didn't want to steal too much time, too much of everyone's time, but it's to utilize design with visibility. That's where the what if tool comes in when we design the security measures around our environment, how we allow access into our environment.  
We need to leverage tools like the what if tool to simulate what the policy effects going to be. We need to use runtime protection to implement the risk based policies, the user risk, the sign in risk. Do they have any risk applied to them? What do we apply if user?  
Is medium. Do we just request MFA? Do we sign the lock the account and get them to contact help desk? What is that flow and what does our organization require us to do in those type of scenarios? So we need to always make sure that when we design.  
In our intra ID solution or the intra ID environment that we take these type of measures into account because a lot of the time we just go to conditional access policy and you're like you know there's a template, click, click, click. Not sure if that template is fit for purpose or fit for the organization, we just go ahead and apply.  
But we should apply some thinking process as to why specific conditional access policies have been implemented and what the consequence of that policy will be if we implement it in a certain way.  
Then as we as we wrap up, just to build your identity playbook, conduct tenant audits. So the Meister tool brilliant on allowing us to do regular assessments with the use of a DevOps integration perform.  
Monthly or quarterly assessments across the tenant, see what the the control drift was like from the from the quarter before, what is our changes in in our admin roles etcetera. So we need to be able to.  
To audit our own environment instead of waiting for third parties to do that for us at a hefty fee. And then we need to transition our admin roles to a PIM solution or PIM equivalent Private Identity Management equivalent type of solution.  
To make sure that we have control over critical roles that not everyone can just jump on and leverage that that critical roles, then we need to automate tedious task users being new users joining the environment, users moving departments.  
What is required? I am moving now from IT and I'm moving into HR, new set of groups, new set of access that I require into applications and that is where we have workflows, automations that kicks in. HR changes me in the SAP system to from IT to HR based on that job.  
Or the department change my access on my user identity starts changing because now I am in a completely different department. So we need to automate those things. It's not. These are not.  
Functionality that is of the future. Those are functionalities that we can leverage right now and we should be able to use them if we especially if we're sitting with the licenses, we can automate joiner, mover, lever with logic apps those.  
So we don't have excuses why we shouldn't be able to do it. If we've got an Azure environment, Azure subscription, we can create logic apps and we start automating some of those basic functions to make sure that every approach still stays the same and we don't rely on helpdesk to do those things for us.  
And then we need to monitor service principles in Sentinel. One of the things that many organizations forget to do. I start a new application or I'm building an application, but I need a service principle. So I'm going to start off with the highest permissions. Instead of starting with least privilege, I'm starting the highest because I don't want to struggle.  
So I'm going to give it all the ermissions it needs. We need to set U monitoring alerts within Sentinel for those service principles so that we can get alerted if anything happens to those service principles. Are signins being conducted from?  
From different countries where we don't operate, why is that service principle allowing a sign in connection? With Sentinel we can monitor those type of events and then act upon them and then regularly test conditional access policies. Use the what if tool we dive into.  
The different policies, OK, I'm a user coming in from so and so country. What will apply? What will happen to me if I leverage this, if this conditional access policy gets rolled out? So we need to be able to make sure that what we rolled out, that we've tested it, we've validated it before we start putting it.  
Into production.  
And then some takeaways the good intra the.  
Provides us a unified identity and access governance, access governance, delivery, comprehensive zero trust capabilities in our environment. One of the bad licensing, it's starting to feel like Microsoft's one of the best things that they ever invent is how to.  
Make licensing complicated for things that we do need to make enhancements into our environment and then the ugly. We've got uncontrolled configuration drift. How can we manage that? We can leverage tools like Meister or put it in place with.  
With a DevOps process, monitor what our service principles look like with Microsoft Sentinel, and then not just to have monitoring or viewing or know that we've got a problem, but we need to actually fix those problems that we do have.  
So as much as we organizations conduct pen test, now I need to tick a box. I'm going to do a pen test. A pen test say I've got 50 issues, but I'm going to pick the first two because that's going to make the auditor happy. So I'm going to do only those. We should fix the issues that gets.  
Picked up. If there is configuration drift, resolve the configuration drift. If there's a conditional access policy that is allowing or that's been configured incorrectly and now it is a set of users is excluded from MFA policies.  
That should be fixed and resolved and either have a a separate controlled group that is excluded, but for known reasons or specific reasons. So yeah, those are some of the key takeaways.  
Um.  
Do we have any questions?  
I know, I know Matthew is probably eager to feedback to.

 **Schalk van Wyk** 50:13  
Oh, before you go for the the external ID like you mentioned that them is that specific with just in time admin rights is specific to intro when admin uses what you're talking about. OK, cool.

 **Shaun Hardneck** 50:13  
To Schalk.  
Correct, correct, yes.

 **Schalk van Wyk** 50:28  
I mean like you mentioned the the licenses, so like governance, you need to separate governance licensing for the lifecycle work flows and stuff it seems. Oh edit.

 **Shaun Hardneck** 50:42  
You can achieve with by using logic apps and integrate into whatever your HR system is, right? But if we're gonna want to use the lifecycle management from Android itself, there's a license attached to that. So we can if we've got.

 **Schalk van Wyk** 50:50  
Yes.

 **Shaun Hardneck** 50:57  
E5 might be right, but I'm going to lean to Matthew for that. But if we have a E5 license, you can still have your access packages, your access reviews, review your your, your critical groups that's associated to PUM for global access. Set set up those.

 **Schalk van Wyk** 51:00  
OK, OK.  
M.

 **Shaun Hardneck** 51:17  
Reviews, access reviews on a weekly basis or monthly to say Matthew and Shaun and Matt is still part of this global admins. Do they need to be in that group? Yes or no? That owner of the environment will then reject or either approve. So we need to start thinking of.  
How we can automate a lot of those things to safeguard ourselves going forward?

 **Schalk van Wyk** 51:38  
So that sort of ties in what I was wanting to ask about the the additional tenants.  
If they if a user is linked in that tenant, it'll also sort of give a lifecycle management in that tenant or is it? I don't know, that's what I'm trying to figure out.  
Mm.

 **Shaun Hardneck** 52:07  
Environment in in Microsoft that you have to manage, but you do have the you can integrate some of those accounts to synchronize or be.

 **Schalk van Wyk** 52:19  
Specifically like the admin accounts, I mean on the tenants. Yeah, yes, yes, yeah.

 **Shaun Hardneck** 52:21  
That you can synchronize between the two environments, but you don't want to do that for everyone because then you're going to sit with junk that you don't want in your tenants. So you have to be careful with that type of design.

 **Matthew Levy** 52:22  
Hmm. Yeah.

 **Nicolas Blank** 52:22  
Yeah.

 **Matthew Levy** 52:26  
So.

 **Schalk van Wyk** 52:28  
No, exactly.

 **Nicolas Blank** 52:29  
Hmm.

 **Matthew Levy** 52:29  
U.  
By default, the person that creates the external ID tenant that was started off in the the workforce tenant becomes the administrator of the external ID tenant by default and then you can add additional.

 **Nicolas Blank** 52:33  
Oh.

 **Schalk van Wyk** 52:33  
Yeah.  
But.  
Yes, yes.

 **Shaun Hardneck** 52:47  
Yeah.

 **Matthew Levy** 52:50  
Admins. So there is that kind of link, but there's also cross-tenant sync capabilities where you can, you know, create users in both.

 **Schalk van Wyk** 52:53  
Oh.  
Yes, yes, yes.

 **Shaun Hardneck** 53:00  
Mm.

 **Nicolas Blank** 53:01  
Um.

 **Schalk van Wyk** 53:01  
It gets a bit tricky with XMID. So I think it's like federated, but it's not federated. So like, I mean you can also do federated identity then, which is not quite the same I think.

 **Matthew Levy** 53:04  
Yeah.

 **Nicolas Blank** 53:04  
Oh.

 **Matthew Levy** 53:13  
Yeah, yeah.  
Just with regards to the licensing the the, so the PIM stuff that you asked about, you can do PIM stuff on an external IDE tenant, but you have to purchase into a premium P2 for that tenant. So you can buy the premium P2 capability.

 **Schalk van Wyk** 53:18  
Um.  
Yes, OK.  
And then licensing changed completely.

 **Matthew Levy** 53:37  
Is.  
Yeah, so the the whole point of external ID is it's the same code base as external ID as intro ID. So yeah, so you can do a lot of the stuff that you can do in intro already.

 **Schalk van Wyk** 53:40  
Mhm.

 **Nicolas Blank** 53:46  
And.

 **Schalk van Wyk** 53:48  
That's intro, yeah.

 **Matthew Levy** 53:54  
On external ID.

 **Shaun Hardneck** 53:54  
Yeah.

 **Nicolas Blank** 53:55  
Oh.

 **Schalk van Wyk** 53:56  
And then you also, sorry Shaun, you you didn't mention entitlements. I don't know if you actually work with or if you've done anything with entitlements. I don't actually know, you know.

 **Shaun Hardneck** 54:05  
I I I skipped entitlements for a reason because it becomes a big topic on its own and especially when you start configuring entitlements and within entitlements you can have a a a form of.

 **Matthew Levy** 54:07  
Hmm.

 **Schalk van Wyk** 54:12  
OK.

 **Shaun Hardneck** 54:22  
External identities in your entitlement, but I would I would think for your scenario we would have to kind of whiteboard exactly what it is that you want to achieve to see which functionality fits and tick that box off.

 **Schalk van Wyk** 54:33  
Yes.  
Yeah, see, I'm not an expert in this area, so I'm asking these questions because your questions are sort of it's floating me. Yeah, yeah, I would like to have an expert in the knows this stuff.

 **Nicolas Blank** 54:36  
Hmm.

 **Shaun Hardneck** 54:43  
No, but it seems like a fun project you're working on.

 **Schalk van Wyk** 54:53  
Um, secret rotation? Is it any recommendation that you have for like um?

 **Shaun Hardneck** 55:01  
Secret.

 **Schalk van Wyk** 55:01  
How to manage the like dependence on that? Or is it a way to find what apps or something that uses a secret?

 **Nicolas Blank** 55:14  
So remember that secrets are basically like a password and that when the secret expires effectively you've got an expired non valid password on that and there actually is both intra as well as graph instrumentation for that. So in intra in the app blade you can see that.

 **Schalk van Wyk** 55:15  
Yeah, like.

 **Nicolas Blank** 55:34  
Password is expired, but the most scalable method of doing that, and I'm going to suggest to you since you know how to code, is to either use PowerShell or the language of your choice to interrogate graph for all the apps in your tenant, then dum all the.  
The dates for your secrets and then you'll see which which is expired and unexpired. And to be yeah, yeah, yeah, yeah. So and I think Matt's actually got a term for that, which is when something crashes into you.

 **Schalk van Wyk** 55:58  
What do you event? Wait for the event.

 **Nicolas Blank** 56:12  
Yeah.

 **Matthew Levy** 56:12  
What?

 **Nicolas Blank** 56:14  
Crash management, you know if you if you wait for the user to tell you that it's broken.

 **Matthew Levy** 56:20  
Oh, oh, scream. Scream theory. Screen. Not the screen theory. Yeah, that one. I can't remember. You wait for the user to scream, basically.

 **Nicolas Blank** 56:26  
Yeah, yeah.  
Yeah, Rhino's got his hand up and then we need to to end the call. So let's just give Rhino to a the the talking stick.

 **Schalk van Wyk** 56:31  
Sure.

 **Nicolas Blank** 56:41  
And he left. All right. I I do want to respect everybody's time. I'm sorry, folks, that we are out of time. However, thank you so much for joining. It's lovely to to get the interactivity that we have. Thank you everyone for asking the questions that you did. Shaun, you did a magnificent job taking something that's so broad.  
And so complicated in making it so accessible. So thank you very much.

 **Schalk van Wyk** 57:05  
Pleasure. Thanks everyone.

 **Nicolas Blank** 57:08  
And with that, have a wonderful day. Oh, Rinot, if you're there, do you want to ask the question quick?

 **Shaun Hardneck** 57:11  
Have a good afternoon. Oh.  
Mm.

 **Matthew Levy** 57:23  
Struggling with the mute button, I arrogant.

 **Nicolas Blank** 57:27  
Yes, it is. It's all right. We'll give you a moment to try that.  
If you maybe want to put into text if it's if it's not too long to put into text.  
Oh, there we go.  
I wanted to ask if anyone has been able to authenticate other Microsoft tenants through external ID and I'm going to ask for a quick yes or no from you Shaun, just because of the the amount of time that we have.

 **Shaun Hardneck** 58:14  
Uh, no, but.

 **Nicolas Blank** 58:15  
Or if you like, you could also continue the chat via I am and then that way we can end the call for everybody else.

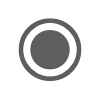
 **Shaun Hardneck** 58:23  
I I haven't, but interesting one and.  
But I suppose you can. It's possible, so it's not not impossible through external ID.  
You can just federate, allow certain users to access your tenant file, not external. Yeah, synchronized identities. Use that. Yeah, there's option. There's options to achieve that rate end.

 **Schalk van Wyk** 58:51  
That was a bad question. Good question.

 **Nicolas Blank** 58:55  
Shaun, are you happy for folks to reach out to you via via LinkedIn? Your your your details are on the meetup site.

 **Shaun Hardneck** 59:00  
Yes, perfectly fine. Happy to chat if anyone has got questions.

 **Nicolas Blank** 59:03  
All right.  
All right. So I'm going to direct everyone to do that just for the sake of time. So I'm going to end the call and Shaun is very.  
Happy to be contacted on this, so thank you again Shaun. Cheers all.

 **Nicolas Blank** stopped transcription