

Protecting Tier 0 the Modern Way

 techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/protecting-tier-0-the-modern-way/4052851



Blog Post

How should your Tier 0 Protection look like?

Almost every attack on Active Directory you hear about today – no matter if ransomware is involved or not – (ab)uses credential theft techniques as the key factor for successful compromise. Microsoft's [State of Cybercrime report](#) confirms this statement: "The top finding among ransomware incident response engagements was insufficient privilege access and lateral movement controls."

Despite the fantastic capabilities of modern detection and protection tools (like the Microsoft Defender family of products), we should not forget that prevention is always better than cure (which means that accounts should be protected against credential theft proactively). Microsoft's approach to achieving this goal is the [Enterprise Access Model](#). It adds the aspect of hybrid and multi-cloud identities to the Active Directory Administrative Tier Model. Although first published almost 10 years ago, the AD Administrative Tier Model is still not obsolete. Not having it in place and enforced is extremely risky with today's threat level in mind.

Most attackers follow playbooks and whatever their final goal may be, Active Directory Domain domination (Tier 0 compromise) is a stopover in almost every attack. Hence, **securing Tier 0 is the first critical step towards your Active Directory hardening journey and this article was written to help with it.**

AD Administrative Tier Model Refresher

The AD Administrative Tier Model prevents escalation of privilege by restricting what Administrators can control and where they can log on. In the context of protecting Tier 0, the latter ensures that Tier 0 credentials cannot be exposed to a system belonging to another Tier (Tier 1 or Tier 2).

Tier 0 includes accounts (Admins-, service- and computer-accounts, groups) that have direct or indirect administrative control over all AD-related identities and identity management systems. While direct administrative control is easy to identify (e.g. members of Domain Admins group), indirect control can be hard to spot: e.g. think of a virtualized Domain Controller and what the admin of the virtualization host can do to it, like dumping the memory or copying the Domain Controller's hard disk with all the password hashes. Consequently, virtualization environments hosting Tier 0 computers are Tier 0 systems as well. This also applies to the virtualization Admin accounts.

The three Commandments of AD Administrative Tier Model

Rule #1: **Credentials from a higher-privileged tier** (e.g. Tier 0 Admin or Service account) **must not be exposed to lower-tier systems** (e.g. Tier 1 or Tier 2 systems).

Rule #2: **Lower-tier credentials can use services provided by higher-tiers, but not the other way around.** E.g. Tier 1 and even Tier 2 system still must be able to apply Group Policies.

Rule #3: **Any system or user account that can manage a higher tier is also a member of that tier, whether originally intended or not.**

Implementing the AD Administrative Tier Model

Most guides describe how to achieve these goals by implementing a complex cascade of Group Policies (The local computer configuration must be changed to avoid that higher Tier level administrators can expose their credentials to a down-level computer). This comes with the downside that Group Policies can be bypassed by local administrators and that the Tier Level restriction works only on Active Directory joined Windows computers. The bad news is that there is still no click-once deployment for Tiered Administration, but there is a more robust way to get things done by implementing [Authentication policies](#). Authentication Policies provide a way to contain

high-privilege credentials to systems that are only pertinent to selected users, computers, or services. With these capabilities, you can limit Tier 0 account usage to Tier 0 hosts. That's exactly what we need to achieve to protect Tier 0 identities from credential theft-based attacks.

To be very clear on this: **With Kerberos Authentication Policies you can define a claim which defines where the user is allowed to request a Kerberos Granting Ticket from.**

Optional: Deep Dive in Authentication Policies

Authentication Policies are based on a Kerberos extension called FAST (Flexible Authentication Secure Tunneling) or Kerberos Armoring. FAST provides a protected channel between the Kerberos client and the KDC for the whole pre-authentication conversation by encrypting the pre-authentication messages with a so-called armor key and by ensuring the integrity of the messages.

Kerberos Armoring is disabled by default and must be enabled using Group Policies. Once enabled, it provides the following functionality:

- Protection against offline dictionary attacks. Kerberos armoring protects the user's pre-authentication data (which is vulnerable to offline dictionary attacks when it is generated from a password).
- Authenticated Kerberos errors. Kerberos armoring protects user Kerberos authentications from KDC Kerberos error spoofing, which can downgrade to NTLM or weaker cryptography.
- Disables any authentication protocol except Kerberos for the configured user.
- Compounded authentication in Dynamic Access Control (DAC). This allows authorization based on the combination of both user claims and device claims.

The last bullet point provides the basis for the feature we plan to use for protecting Tier 0: Authentication Policies.

Restricting user logon from specific hosts requires the Domain Controller (specifically the Key Distribution Center (KDC)) to validate the host's identity. When using Kerberos authentication with Kerberos armoring, the KDC is provided with the TGT of the host from which the user is authenticating. That's what we call an armored TGT, the content of which is used to complete an access check to determine if the host is allowed.

Kerberos armoring logon flow (simplified):

1. The computer has already received an armored TGT during computer authentication to the domain.
2. The user logs on to the computer:
 1. An unarmored AS-REQ for a TGT is sent to the KDC.
 2. The KDC queries for the user account in Active Directory and determines if it is configured with an Authentication Policy that restricts initial authentication that requires armored requests.
 3. The KDC fails the request and asks for Pre-Authentication.
 4. Windows detects that the domain supports Kerberos armoring and sends an armored AS-REQ to retry the sign-in request.
 5. The KDC performs an access check by using the configured access control conditions and the client operating system's identity information in the TGT that was used to armor the request. If the access check fails, the domain controller rejects the request.
3. If the access check succeeds, the KDC replies with an armored reply (AS-REP) and the authentication process continues. The user now has an armored TGT.

Looks very much like a normal Kerberos logon? Not exactly: The main difference is the fact that the user's TGT includes the source computer's identity information. Requesting Service Tickets looks similar to what we described above, except that the user's armored TGT is used for protection and restriction.

Implementing a Tier 0 OU Structure and Authentication Policy

The following steps are required to limit Tier 0 account usage (Admins and Service accounts) to Tier 0 hosts:

1. Enable Kerberos Armoring (aka FAST) for DCs and all computers (or at least Tier 0 computers).
2. Before creating an OU structure similar to the one pictured below, you MUST ensure that Tier 0 accounts are the only ones having sensitive permissions on the root level of the domain. Keep in mind that all ACLs configured on the root-level of fabrikam.com will be inherited by the OU called "Admin" in our example.
3. Create the following security groups:
 - Tier 0 Users
 - Tier 0 Computer
4. Constantly update the Authentication policy to ensure that any new T0 Admin or T0 service account is covered.
5. Ensure that any newly created T0 computer account is added to the T0 Computers security group.
6. Configure an Authentication Policy with the following parameters and enforce the Kerberos Authentication policy:

(User) Accounts	Conditions (Computer accounts/groups)	User Sign On
-----------------	---------------------------------------	--------------

T0 Admin accounts	(Member of each({ENTERPRISE DOMAIN CONTROLLERS}) Or Member of any({Tier 0 computers (FABRIKAM\Tier 0 computers)}))	Kerberos only
-------------------	--	---------------

The screenshot below shows the relevant section of the Authentication Policy:

Find more details about how to create Authentication Policies at <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/how-to-configure-protected-accounts#create-a-user-account-audit-for-authentication-policy-with-adac>.

Tier 0 Admin Logon Flow: Privileged Access Workstations (PAWs) are a MUST

As explained at the beginning of the article, attackers can sneak through an open (and MFA protected) RDP connection when the Admin's client computer is compromised. To protect from this type of attack Microsoft has been recommending using PAWs since many years.

In case you ask yourself, what the advantage of restricting the source of a logon attempt through Kerberos Policies is: Most certainly you do not want your T0 Admins to RDP from their – potentially compromised – workplace computers to the DC. Instead, you want them to use a Tier 0 Administrative Jump Host or - even better - a Privileged Access Workstation. With a compromised workplace computer as a source for T0 access it would be easy for an attacker to either use a keylogger to steal the T0 Admin's password, or to simply sneak through the RDP channel once it is open (using a simple password or MFA doesn't make a big difference for this type of attack). Even if an attacker would be able to steal the credential of a Tier 0 user, the attacker could use those credentials from a computer which is defined in the claim. On any other computer, Active Directory will not approve a TGT, even if the user provides the correct credentials. This will give you the easy possibility to monitor the declined requests and react properly.

There are too many ways of implementing the Tier 0 Admin logon flow to describe all of them in a blog. The "classic" (some call it "old-fashioned") approach is a domain-joined PAW which is used for T0 administrative access to Tier 0 systems.

The solution above is straightforward but does not provide any modern cloud-based security features.

"Protecting Tier 0 the modern way" not only refers to using Authentication Policies, but also leverages modern protection mechanisms provided by Azure Entra ID, like Multi-Factor-Authentication, Conditional Access or Identity Protection (to cover just the most important ones).

Our preferred way of protecting the Tier 0 logon flow is via an Intune-managed PAW and Azure Virtual Desktop because this approach is easy to implement and perfectly teams modern protection mechanisms with on-premises Active Directory:

Logon to the AVD is restricted to come from a compliant PAW device only, Authentication Policies do the rest.

Automation through PowerShell

Still sounds painful? While steps 1 – 3 (enable Kerberos FAST, create OU structure, create Tier 0 groups) of Implementing a Tier 0 OU Structure and Authentication Policy are one-time tasks, step 4 and 6 (keep group membership and Authentication policy up-to-date) have turned out to be challenging in complex, dynamic environments. That's why Andreas Lucas (aka Kili69) has developed a PowerShell-based automation tool which ...

- creates the OU structure described above (if not already exists)
- creates the security groups described above (if not already exist)
- creates the Authentication policy described above (if not already exists)
- applies the Tier 0 authentication policy to any Tier 0 user object
- removes any object from the T0 Computers group which is not located in the Tier 0 OU
- removes any user object from the default Active directory Tier 0 groups, if the Authentication policy is not applied (except Built-In Administrator, GMSA and service accounts)

Additional Comments and Recommendations

Prerequisites for implementing Kerberos Authentication Policies

Kerberos Authentication Policies were introduced in Windows Server 2012 R2, hence a Domain functional level of Windows Server 2012 R2 or higher is required for implementation.

Authentication Policy – special Settings

Require rolling NTLM secret for NTLM authentication

Configuration of this feature was moved to the properties of the domain in Active Directory Administrative Center. When enabled, for users with the "Smart card is required for interactive logon" checkbox set, a new random password will be generated according to the password policy. See <https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/whats-new-in-credential-protection#rolling-public-key-only-users-ntlm-secrets> for more details.

Allow NTLM network authentication when user is restricted to selected devices

We do NOT recommend enabling this feature because with NTLM authentication allowed the capabilities of restricting access through Authentication Policies are reduced. In addition to that, we recommend adding privileged users to the [Protected Users security group](#). This special group was designed to harden privileged accounts and introduces a set of protection mechanisms, one of which is making NTLM authentication impossible for the members of this group. See <https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/authentication-policies-and-authentication-policy-silos#about-authentication-policies> for more details.

Have Breakglass Accounts in place

Break Glass accounts are emergency access accounts used to access critical systems or resources when other authentication mechanisms fail or are unavailable. In Active Directory, Break Glass accounts are used to provide emergency access to Active Directory in case normal T0 Admin accounts do not work anymore, e.g. because of a misconfigured Authentication Policy.

Clean Source Principle

The [clean source principle](#) requires all security dependencies to be as trustworthy as the object being secured. Implementation of the clean source principle is beyond the scope of this article, but explained in detail at [Success criteria for privileged access strategy](#) | Microsoft Learn.

Review ACLs on the Root-level of your Domain(s)

The security implications of an account having excessive privileges (e.g. being able to modify permissions at the root-level of the domain) are massive. For that reason, before creating the new OU (named "Admin" in the description above), you must ensure that there are no excessive ACLs (Access Control List) configured on the Root-level of the domain. In addition to that, consider breaking inheritance on the OU called "Admin" in our example.

Updated Feb 19, 2024

Version 5.0

[DagmarHeidecker](#)



Agree with [LegoVader](#) One point where I want your confirmation while leveraging **Entra Governance Service** in elevating a user to domain-admin of the on-prem Active Directory is it may not be exactly **just-in-time**. The reason is we have to wait for the next **Writeback Cycle** of Cloud-Sync.

I believe it is every 20 min.

Remember, there is no **STANDING** domain-admin of AD in our environment. Eligible **HYBRID-USER** will go to Entra-portal and request to be part of such writeback group via access-package to become domain-admin of AD

Am I right ?

- Hi [svhelden](#),

the tiering concept for on-premise environment is just a subset of tiering in cloud-based environments. Here, it is much more complex (as you can see at the Enterprise Access Model [Securing privileged access Enterprise access model - Privileged access](#) | Microsoft Learn).

However, one thing stays identically: if you have a privileged role in Azure (or in AWS), you have to use a PAW to access the administrative portals with that role!

As a side note, as long as you are running your environment hybrid, if an attacker successfully compromise one part (either cloud or on-premise), that one can easily step over to the other part and compromise that as well...

cheers



[testuser7](#)

we create one Entra-group and then **writeback** that group under the built-in "**Domain Admins**" group as child-group.
(member of)

Interesting idea. Obviously this would make your domain security rely on Entra ID, meaning, any Entra admin could become a Tier 0 admin. Thus Entra would be part of Tier 0, too. If the workstation of a Global Admin is compromised, the attacker could use it to break into your AD.

What do others think about that? For me it sounds like a violation of tier boundaries.

- Hi The_Goat ,

Every virtualization host that run T0 VM guests (e.g., Domain Controllers, Certification Authorities or EntraID Connect boxes) will automatically become Tier0.

Although you can protect VM guests using hard disk encryption or even complete VM encryption, this protection will only ensure that you cannot use the VM anywhere else. However, if an attacker can access the running VM or even create a snapshot which consists the running memory of a T0 VM, that one will be able to extract the secrets directly out of the snapshot, e.g., the krbtgt... For that reason, T0 must be extended to the hypervisors that run T0 guests. This includes as well cloud-based hypervisors!

cheers



Hi,

Thanks for the reply.



Cyr-Az

Copper Contributor

Oct 31, 2024

@The_Goat let's put it like this : anyone with access to the vmware host or console is capable of intercepting your domain controllers network communications or to copy/modify its data. So this is a clear no-no, unless the vmware admins are considered tier0 admins and the vmware hosts are considered tier0.



matthiasheil

Copper Contributor

Oct 31, 2024

Hi The_Goat, I 'd say for Hyper-V you may protect, or more precise have to protect virtual DCs as shielded VMs. In Vmware there should be comparable features



The_Goat

Copper Contributor

Oct 31, 2024

Hi and thanks for this article.

I just wanted to know your thoughts on hosting tier0 domaincontrollers(vms) on tier1 vmware hosts.

Is this recommended? I would think that this is a security risk.

//Goat

- 
[testuser7](#)
Brass Contributor

Oct 31, 2024

thanks [LegoVader](#) for confirming where 3rd party PAM would fit.

Actually, I was just toying with the idea what [Alexmags1337](#) brought forth. That is excellent. So let me elaborate it and help you help me.


So what you are saying is, we create one Entra-group and then **writeback** that group under the built-in **"Domain Admins"** group as child-group. (member of)

Now with the help of Governance entitlement packages of Entra, an eligible user will be added to this written-back group

The group will be written back to AD and now this user can use his PAW (which again will be the modern PAW as explained in this blog by protecting the Tier 0 logon flow via an [Intune-managed PAW](#) and [Azure Virtual Desktop](#)).

So this way we can utilize the Entra solution to realize just-in-time PIM for AD

Did I interpret you correctly ?

- 
[Alexmags1337](#)
Copper Contributor

Oct 29, 2024

If you have Entra ID you already have two PAM solutions. For IT admins there's PIM for Entra roles and security groups (likely already in use). For standard users there's ID Governance entitlement packages (which can be time based). Even Entra ID access reviews can be used periodically empty temporary exception groups. Entra Cloud Sync can write back security groups managed in Entra ID to AD Domain Services. See how far you can get with your existing tech.

- 
[testuser7](#)
Brass Contributor

Oct 29, 2024

Excellent !!! Thanks [LegoVader](#) and [KiliMuc](#) This design of PAW will definitely fly in my org.

One more question on same line.. We are also adding PAM solution like CyberArk or PAM360 in the mix.

Which tier is the most adequate tier for installing PAM without breaking the guidelines of EAM and 3 commandments.

My understanding is tier0 is the most appropriate.

- Hi [testuser7](#) ,

the cloud-based PAW must be a physical device and is defined as THE clean keyboard (meaning this box has best protection and detection assigned and will ensure no one can interfere the connections to your targets). In that case, you can use that ONE physical clean keyboard to reach out to T0 AVDs AND T1 AVDs from which you will do you administrative work for the corresponding tiers.

cheers

- [testuser7](#) of course you can use the same physical device to connect to Tier 0 and Tier 1. The PAW must be managed from the highest security level (Tier 0) but from this computer it is allowed to connect to downlevel (Tier 1 computer) via AvD.

It's hard to break out from the AvD session into the source computer, but it is easy to break in into the AvD session from the source computer. This means the PAW logged on user must be trustworthy, then you can connect to Tier 0 and Tier 1

It makes no sense to stable the PAWs on your table, the users will not accept this, and they will deny all the security restrictions.

I hope this answers your question.



Intune-managed PAW and Azure Virtual Desktop

We like this approach.

Can the same physical PAW be used to connect to any Tier1 server along with Tier0 server ?? We can not do proliferation of physical PAWs. It is not very user-friendly experience.



follow-up on my proposals in the comments above, while not helping with the tier and protection model, this looks very promising for hardening your Windows Server 2025:

<https://techcommunity.microsoft.com/t5/windows-server-insiders/announcing-windows-server-2025-security-baseline-preview/mp/4257686>

Config Items / OsConfig Repository:

<https://github.com/microsoft/osconfig/tree/main>



Hello [@NateBarkei](#) , [@ckuever0983](#) ,

for me the solution was to set "KDC Support for claims, compound authentication and Kerberos amoring" to "Always provide claims".

Best Regards,

Peter



Hi I made a script to implement tiered admin model OU structure, groups and OU permissions. Have a look to get you started. Remix it to your needs [alexmag's ADTiersOfJoy: Active Directory Tiered Administration Model \(github.com\)](#)



[svhelden](#)

Thanks for answering.

Ah, understood. You are absolutely right. My fault!

Greetings

Jörg



[JMaletzky](#). Shouldn't "the RDP-Port of T0-PAWs" be disabled? You must use the PAWs physically. With an RDP connection from a non-T0-system to the PAW you would break the isolation (by entering your T0 credentials on the keyboard of a non-T0 device).

I think that "NLA must be enforced on every T0 system" obviously applies to T0 servers but not PAWs.

```
{},"cachedText":{"lastModified":"1731977288000","locale":"en-US","namespaces":{"components/community/NavbarDropdownToggle":{"__ref":"CachedAsset:text:en_US-components/community/NavbarDropdownToggle-1731977288000"},"cachedText":{"lastModified":"1731977288000","locale":"en-US","namespaces":{"shared/client/components/users/UserAvatar":{"__ref":"CachedAsset:text:en_US-shared/client/components/users/UserAvatar-1731977288000"},"cachedText":{"lastModified":"1731977288000","locale":"en-US","namespaces":{"shared/client/components/ranks/UserRankLabel":{"__ref":"CachedAsset:text:en_US-shared/client/components/ranks/UserRankLabel-1731977288000"},"cachedText":{"lastModified":"1731977288000","locale":"en-US","namespaces":{"components/users/UserRegistrationDate":{"__ref":"CachedAsset:text:en_US-components/users/UserRegistrationDate-1731977288000"},"cachedText":{"lastModified":"1731977288000","locale":"en-US","namespaces":{"shared/client/components/nodes/NodeAvatar":{"__ref":"CachedAsset:text:en_US-shared/client/components/nodes/NodeAvatar-1731977288000"},"cachedText":{"lastModified":"1731977288000","locale":"en-US","namespaces":{"shared/client/components/nodes/NodeDescription":{"__ref":"CachedAsset:text:en_US-shared/client/components/nodes/NodeDescription-1731977288000"},"cachedText":{"lastModified":"1731977288000","locale":"en-US","namespaces":{"components/tags/TagView/TagViewChip":{"__ref":"CachedAsset:text:en_US-
```

```

components/tags/TagView/TagViewChip-1731977288000"},"cachedText":{"lastModified":"1731977288000","locale":"en-US","namespaces":{"shared/client/components/nodes/NodeIcon"},"":{"__ref":"CachedAsset:text:en_US-shared/client/components/nodes/NodeIcon-1731977288000"},"CachedAsset:pages-1734787623375":
{"__typename":"CachedAsset","id":"pages-1734787623375","value":{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"BlogViewAllPostsPage","type":"BLOG","urlPath":"/category/:categoryId/blog/:boardId/all-
posts(/:after/:before)?","__typename":"PageDescriptor"},"__typename":"PageResource"},
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"CasePortalPage","type":"CASE_PORTAL","urlPath":"/caseportal","__typename":"PageDescriptor"},"__typename":"PageResource"},
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"CreateGroupHubPage","type":"GROUP_HUB","urlPath":"/groups/create","__typename":"PageDescriptor"},"__typename":"PageResourc
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"CaseViewPage","type":"CASE_DETAILS","urlPath":"/case/:caseId/:caseNumber","__typename":"PageDescriptor"},"__typename":"PageI
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"InboxPage","type":"COMMUNITY","urlPath":"/inbox","__typename":"PageDescriptor"},"__typename":"PageResource"},
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"HelpFAQPage","type":"COMMUNITY","urlPath":"/help","__typename":"PageDescriptor"},"__typename":"PageResource"},
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"IdeaMessagePage","type":"IDEA_POST","urlPath":"/idea/:boardId:messageSubject/:messageId","__typename":"PageDescriptor"},"__ty
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"IdeaViewAllIdeasPage","type":"IDEA","urlPath":"/category/:categoryId/ideas/:boardId/all-
ideas(/:after/:before)?","__typename":"PageDescriptor"},"__typename":"PageResource"},
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"LoginPage","type":"USER","urlPath":"/signin","__typename":"PageDescriptor"},"__typename":"PageResource"},
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"BlogPostPage","type":"BLOG","urlPath":"/category/:categoryId/blogs/:boardId/create","__typename":"PageDescriptor"},"__typename":"P
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"UserBlogPermissions.Page","type":"COMMUNITY","urlPath":"/c/user-blog-
permissions/page","__typename":"PageDescriptor"},"__typename":"PageResource"},
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"ThemeEditorPage","type":"COMMUNITY","urlPath":"/designer/themes","__typename":"PageDescriptor"},"__typename":"PageResource"
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"TkbViewAllArticlesPage","type":"TKB","urlPath":"/category/:categoryId/kb/:boardId/all-
articles(/:after/:before)?","__typename":"PageDescriptor"},"__typename":"PageResource"},
{"lastUpdatedTime":1730142000000,"localOverride":null,"page":
{"id":"AllEvents","type":"CUSTOM","urlPath":"/Events","__typename":"PageDescriptor"},"__typename":"PageResource"},
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"OccasionEditPage","type":"EVENT","urlPath":"/event/:boardId:messageSubject/:messageId/edit","__typename":"PageDescriptor"},"__ty
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"OAuthAuthorizationAllowPage","type":"USER","urlPath":"/auth/authorize/allow","__typename":"PageDescriptor"},"__typename":"PageRe
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"PageEditorPage","type":"COMMUNITY","urlPath":"/designer/pages","__typename":"PageDescriptor"},"__typename":"PageResource"},
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"PostPage","type":"COMMUNITY","urlPath":"/category/:categoryId/:boardId/create","__typename":"PageDescriptor"},"__typename":"Page
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"ForumBoardPage","type":"FORUM","urlPath":"/category/:categoryId/discussions/:boardId","__typename":"PageDescriptor"},"__typenam
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"TkbBoardPage","type":"TKB","urlPath":"/category/:categoryId/kb/:boardId","__typename":"PageDescriptor"},"__typename":"PageResour
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"EventPostPage","type":"EVENT","urlPath":"/category/:categoryId/events/:boardId/create","__typename":"PageDescriptor"},"__typename
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"UserBadgesPage","type":"COMMUNITY","urlPath":"/users/login/:userId/badges","__typename":"PageDescriptor"},"__typename":"PageI
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"GroupHubMembershipAction","type":"GROUP_HUB","urlPath":"/membership/join/:nodeId/:membershipType","__typename":"PageDescr
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"IdeaReplyPage","type":"IDEA_REPLY","urlPath":"/idea/:boardId:messageSubject/:messageId/comments/:replyId","__typename":"PageI
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"UserSettingsPage","type":"USER","urlPath":"/mysettings/userSettingsTab","__typename":"PageDescriptor"},"__typename":"PageResou
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"GroupHubsPage","type":"GROUP_HUB","urlPath":"/groups","__typename":"PageDescriptor"},"__typename":"PageResource"},
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"ForumPostPage","type":"FORUM","urlPath":"/category/:categoryId/discussions/:boardId/create","__typename":"PageDescriptor"},"__type
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"OccasionRsvpActionPage","type":"OCCASION","urlPath":"/event/:boardId:messageSubject/:messageId/rsvp/:responseType","__typena
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"VerifyUserEmailPage","type":"USER","urlPath":"/verifyemail/:userId/verifyEmailToken","__typename":"PageDescriptor"},"__typename":"
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"AllOccasionsPage","type":"OCCASION","urlPath":"/category/:categoryId/events/:boardId/all-

```



```

events(/:after/:before)?", "__typename": "PageDescriptor"}, "__typename": "PageResource"},
{"id": "EventBoardPage", "type": "EVENT", "urlPath": "/category/:categoryId/events/:boardId", "__typename": "PageDescriptor"}, {"id": "EventBoardPage", "type": "EVENT", "urlPath": "/category/:categoryId/events/:boardId", "__typename": "PageDescriptor"}, {"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "TkbReplyPage", "type": "TKB_REPLY", "urlPath": "/kb/:boardId/messageSubject/:messageId/comments/:replyId", "__typename": "PageDes
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "IdeaBoardPage", "type": "IDEA", "urlPath": "/category/:categoryId/ideas/:boardId", "__typename": "PageDescriptor"}, {"id": "IdeaBoardPage", "type": "IDEA", "urlPath": "/category/:categoryId/ideas/:boardId", "__typename": "PageRe
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "CommunityGuideLinesPage", "type": "COMMUNITY", "urlPath": "/communityguidelines", "__typename": "PageDescriptor"}, {"id": "CommunityGuideLinesPage", "type": "COMMUNITY", "urlPath": "/communityguidelines", "__typename": "P
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "CaseCreatePage", "type": "SALESFORCE_CASE_CREATION", "urlPath": "/caseportal/create", "__typename": "PageDescriptor"}, {"id": "CaseCreatePage", "type": "SALESFORCE_CASE_CREATION", "urlPath": "/caseportal/create", "__typena
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "TkbEditPage", "type": "TKB", "urlPath": "/kb/:boardId/messageSubject/:messageId/edit", "__typename": "PageDescriptor"}, {"id": "TkbEditPage", "type": "TKB", "urlPath": "/kb/:boardId/messageSubject/:messageId/edit", "__typename": "P
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page": {"id": "KhorosSignInPage", "type": "USER", "urlPath": "/kh-
signin", "__typename": "PageDescriptor"}, {"id": "KhorosSignInPage", "type": "USER", "urlPath": "/kh-
signin", "__typename": "PageDescriptor"}, {"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "ForgotPasswordPage", "type": "USER", "urlPath": "/forgotpassword", "__typename": "PageDescriptor"}, {"id": "ForgotPasswordPage", "type": "USER", "urlPath": "/forgotpassword", "__typename": "PageResource"},
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "IdeaEditPage", "type": "IDEA", "urlPath": "/idea/:boardId/messageSubject/:messageId/edit", "__typename": "PageDescriptor"}, {"id": "IdeaEditPage", "type": "IDEA", "urlPath": "/idea/:boardId/messageSubject/:messageId/edit", "__typename": "PageDescriptor"}, {"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "TagPage", "type": "COMMUNITY", "urlPath": "/tag/:tagName", "__typename": "PageDescriptor"}, {"id": "TagPage", "type": "COMMUNITY", "urlPath": "/tag/:tagName", "__typename": "PageResource"},
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "BlogBoardPage", "type": "BLOG", "urlPath": "/category/:categoryId/blog/:boardId", "__typename": "PageDescriptor"}, {"id": "BlogBoardPage", "type": "BLOG", "urlPath": "/category/:categoryId/blog/:boardId", "__typename": "PageRe
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "OccasionMessagePage", "type": "OCCASION_TOPIC", "urlPath": "/event/:boardId/messageSubject/:messageId", "__typename": "PageDes
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "ManageContentPage", "type": "COMMUNITY", "urlPath": "/managecontent", "__typename": "PageDescriptor"}, {"id": "ManageContentPage", "type": "COMMUNITY", "urlPath": "/managecontent", "__typename": "PageResourc
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "ClosedMembershipNodeNonMembersPage", "type": "GROUP_HUB", "urlPath": "/closedgroup/:groupHubId", "__typename": "PageDescriptc
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "CommunityPage", "type": "COMMUNITY", "urlPath": "/", "__typename": "PageDescriptor"}, {"id": "CommunityPage", "type": "COMMUNITY", "urlPath": "/", "__typename": "PageResource"},
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "ForumMessagePage", "type": "FORUM_TOPIC", "urlPath": "/discussions/:boardId/messageSubject/:messageId", "__typename": "PageDes
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "IdeaPostPage", "type": "IDEA", "urlPath": "/category/:categoryId/ideas/:boardId/create", "__typename": "PageDescriptor"}, {"id": "IdeaPostPage", "type": "IDEA", "urlPath": "/category/:categoryId/ideas/:boardId/create", "__typename": "Pa
{"lastUpdatedTime": 1730142000000, "localOverride": null, "page":
{"id": "CommunityHub.Page", "type": "CUSTOM", "urlPath": "/Directory", "__typename": "PageDescriptor"}, {"id": "CommunityHub.Page", "type": "CUSTOM", "urlPath": "/Directory", "__typename": "PageResource"},
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "BlogMessagePage", "type": "BLOG_ARTICLE", "urlPath": "/blog/:boardId/messageSubject/:messageId", "__typename": "PageDescriptor"}, {"id": "BlogMessagePage", "type": "BLOG_ARTICLE", "urlPath": "/blog/:boardId/messageSubject/:messageId", "__typename": "PageDescriptor"}, {"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "RegistrationPage", "type": "USER", "urlPath": "/register", "__typename": "PageDescriptor"}, {"id": "RegistrationPage", "type": "USER", "urlPath": "/register", "__typename": "PageResource"},
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "EditGroupHubPage", "type": "GROUP_HUB", "urlPath": "/group/:groupHubId/edit", "__typename": "PageDescriptor"}, {"id": "EditGroupHubPage", "type": "GROUP_HUB", "urlPath": "/group/:groupHubId/edit", "__typename": "PageRe
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "ForumEditPage", "type": "FORUM", "urlPath": "/discussions/:boardId/messageSubject/:messageId/edit", "__typename": "PageDescriptor"}, {"id": "ForumEditPage", "type": "FORUM", "urlPath": "/discussions/:boardId/messageSubject/:messageId/edit", "__typename": "PageDescriptor"}, {"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "ResetPasswordPage", "type": "USER", "urlPath": "/resetpassword/:userId/resetPasswordToken", "__typename": "PageDescriptor"}, {"id": "ResetPasswordPage", "type": "USER", "urlPath": "/resetpassword/:userId/resetPasswordToken", "__typen
{"lastUpdatedTime": 1730142000000, "localOverride": null, "page":
{"id": "AllBlogs.Page", "type": "CUSTOM", "urlPath": "/blogs", "__typename": "PageDescriptor"}, {"id": "AllBlogs.Page", "type": "CUSTOM", "urlPath": "/blogs", "__typename": "PageResource"},
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "TkbMessagePage", "type": "TKB_ARTICLE", "urlPath": "/kb/:boardId/messageSubject/:messageId", "__typename": "PageDescriptor"}, {"id": "TkbMessagePage", "type": "TKB_ARTICLE", "urlPath": "/kb/:boardId/messageSubject/:messageId", "__typ
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "BlogEditPage", "type": "BLOG", "urlPath": "/blog/:boardId/messageSubject/:messageId/edit", "__typename": "PageDescriptor"}, {"id": "BlogEditPage", "type": "BLOG", "urlPath": "/blog/:boardId/messageSubject/:messageId/edit", "__typenami
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "ManageUsersPage", "type": "USER", "urlPath": "/users/manage/:tab?:manageUsersTab?", "__typename": "PageDescriptor"}, {"id": "ManageUsersPage", "type": "USER", "urlPath": "/users/manage/:tab?:manageUsersTab?", "__typename": "PageDescriptor"}, {"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "ForumReplyPage", "type": "FORUM_REPLY", "urlPath": "/discussions/:boardId/messageSubject/:messageId/replies/:replyId", "__typename": "PageDescriptor"}, {"id": "ForumReplyPage", "type": "FORUM_REPLY", "urlPath": "/discussions/:boardId/messageSubject/:messageId/replies/:replyId", "__typename
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "PrivacyPolicyPage", "type": "COMMUNITY", "urlPath": "/privacypolicy", "__typename": "PageDescriptor"}, {"id": "PrivacyPolicyPage", "type": "COMMUNITY", "urlPath": "/privacypolicy", "__typename": "PageResource"},
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "NotificationPage", "type": "COMMUNITY", "urlPath": "/notifications", "__typename": "PageDescriptor"}, {"id": "NotificationPage", "type": "COMMUNITY", "urlPath": "/notifications", "__typename": "PageResource"},
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "UserPage", "type": "USER", "urlPath": "/users/login/:userId", "__typename": "PageDescriptor"}, {"id": "UserPage", "type": "USER", "urlPath": "/users/login/:userId", "__typename": "PageResource"},
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "OccasionReplyPage", "type": "OCCASION_REPLY", "urlPath": "/event/:boardId/messageSubject/:messageId/comments/:replyId", "__typen
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":
{"id": "ManageMembersPage", "type": "GROUP_HUB", "urlPath": "/group/:groupHubId/manage/:tab?", "__typename": "PageDescriptor"}, {"id": "ManageMembersPage", "type": "GROUP_HUB", "urlPath": "/group/:groupHubId/manage/:tab?", "__typen
{"lastUpdatedTime": 1734787623375, "localOverride": null, "page":

```

```

{"id":"SearchResultsPage","type":"COMMUNITY","urlPath":"/search","__typename":"PageDescriptor"},"__typename":"PageResource"},
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"BlogReplyPage","type":"BLOG_REPLY","urlPath":"/blog/:boardId:messageSubject:messageId/replies/:replyId","__typename":"PageDes
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"GroupHubPage","type":"GROUP_HUB","urlPath":"/group/:groupHubId","__typename":"PageDescriptor"},"__typename":"PageResource"
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"TermsOfServicePage","type":"COMMUNITY","urlPath":"/termsofservice","__typename":"PageDescriptor"},"__typename":"PageResource"
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"CategoryPage","type":"CATEGORY","urlPath":"/category/:categoryId","__typename":"PageDescriptor"},"__typename":"PageResource"},
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"ForumViewAllTopicsPage","type":"FORUM","urlPath":"/category/:categoryId/discussions/:boardId/all-
topics/(/:after|/:before)?","__typename":"PageDescriptor"},"__typename":"PageResource"},
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"TkbPostPage","type":"TKB","urlPath":"/category/:categoryId/kbs/:boardId/create","__typename":"PageDescriptor"},"__typename":"PageF
{"lastUpdatedTime":1734787623375,"localOverride":null,"page":
{"id":"GroupHubPostPage","type":"GROUP_HUB","urlPath":"/group/:groupHubId/:boardId/create","__typename":"PageDescriptor"},"__typenar
components/context/AppContext/AppContextProvider-0":{"__typename":"CachedAsset","id":"text:en_US-
components/context/AppContext/AppContextProvider-0","value":{"noCommunity":"Cannot find community","noUser":"Cannot find current
user","noNode":"Cannot find node with id {nodeId}","noMessage":"Cannot find message with id
{messageId}"},"localOverride":false},"CachedAsset:text:en_US-shared/client/components/common/Loading/LoadingDot-0":
{"__typename":"CachedAsset","id":"text:en_US-shared/client/components/common/Loading/LoadingDot-0","value":
{"title":"Loading..."},"localOverride":false},"User:user:-1":
{"__typename":"User","id":"user:-1","uid":-1,"login":"Deleted","email":"","avatar":null,"rank":null,"kudosWeight":1,"registrationData":
{"__typename":"RegistrationData","status":"ANONYMOUS","registrationTime":null,"confirmEmailStatus":false,"registrationAccessLevel":"VIEW
[]"},"ssold":null,"profileSettings":{"__typename":"ProfileSettings","dateDisplayStyle":
{"__typename":"InheritableStringSettingWithPossibleValues","key":"layout.friendly_dates_enabled","value":"false","localValue":"true","possible
["true","false"]},"dateDisplayFormat":{"__typename":"InheritableStringSetting","key":"layout.format_pattern_date","value":"MMM dd
yyyy","localValue":"MM-dd-yyyy"},"language":
{"__typename":"InheritableStringSettingWithPossibleValues","key":"profile.language","value":"en-US","localValue":"en","possibleValues":
["en-US"]},"deleted":false},"Theme:customTheme1":{"__typename":"Theme","id":"customTheme1"},"Category:category:cis":
{"__typename":"Category","id":"category:cis","entityType":"CATEGORY","displayId":"cis","nodeType":"category","depth":4,"title":"Core
Infrastructure and Security","shortTitle":"Core Infrastructure and Security","parent":
{"__ref":"Category:category:MicrosoftSecurityandCompliance"},"Category:category:top":
{"__typename":"Category","id":"category:top","displayId":"top","nodeType":"category","depth":0,"title":"Top","entityType":"CATEGORY","shortTi
{"__typename":"Category","id":"category:communities","displayId":"communities","nodeType":"category","depth":1,"parent":
{"__ref":"Category:category:top"},"title":"Communities","entityType":"CATEGORY","shortTitle":"Communities"},"Category:category:products-
services":{"__typename":"Category","id":"category:products-services","displayId":"products-
services","nodeType":"category","depth":2,"parent":
{"__ref":"Category:category:communities"},"title":"Products","entityType":"CATEGORY","shortTitle":"Products"},"Category:category:MicrosoftS
{"__typename":"Category","id":"category:MicrosoftSecurityandCompliance","displayId":"MicrosoftSecurityandCompliance","nodeType":"categ
{"__ref":"Category:category:products-services"},"title":"Security, Compliance, and
Identity","entityType":"CATEGORY","shortTitle":"Security, Compliance, and Identity","categoryPolicies":
{"__typename":"CategoryPolicies","canReadNode":
{"__typename":"PolicyResult","failureReason":null}},"Blog:board:CoreInfrastructureandSecurityBlog":
{"__typename":"Blog","id":"board:CoreInfrastructureandSecurityBlog","entityType":"BLOG","displayId":"CoreInfrastructureandSecurityBlog","nc
Infrastructure and Security Blog","description":"","avatar":null,"profileSettings":{"__typename":"ProfileSettings","language":null,"parent":
{"__ref":"Category:category:cis"},"ancestors":{"__typename":"CoreNodeConnection","edges":{"__typename":"CoreNodeEdge","node":
{"__ref":"Community:community:gxucf89792"},"{"__typename":"CoreNodeEdge","node":{"__ref":"Category:category:communities"}},
{"__typename":"CoreNodeEdge","node":{"__ref":"Category:category:products-services"},"{"__typename":"CoreNodeEdge","node":
{"__ref":"Category:category:MicrosoftSecurityandCompliance"},"{"__typename":"CoreNodeEdge","node":
{"__ref":"Category:category:cis"}},{"__typename":"UserContext":
{"__typename":"NodeUserContext","canAddAttachments":false,"canUpdateNode":false,"canPostMessages":false,"isSubscribed":false},"board
{"__typename":"BoardPolicies","canPublishArticleOnCreate":{"__typename":"PolicyResult","failureReason":
{"__typename":"FailureReason","message":"error.lithium.policies.forums.policy_can_publish_on_create_workflow_action.accessDenied","key
[]}}},"shortTitle":"Core Infrastructure and Security Blog","tagProperties":{"__typename":"TagNodeProperties","tagsEnabled":
{"__typename":"PolicyResult","failureReason":null},"requireTags":true,"tagType":"FREEFORM_ONLY"},"AssociatedImage":
{"url":"https://techcommunity.microsoft.com/t5/s/gxucf89792/images/cmstNC05WEo0bcl"},"
{"__typename":"AssociatedImage","url":"https://techcommunity.microsoft.com/t5/s/gxucf89792/images/cmstNC05WEo0bcl","height":512,"widthl
{"__typename":"Rank","id":"rank:4","position":5,"name":"Microsoft","color":"333333","icon":{"__ref":"AssociatedImage":
{"url":"https://techcommunity.microsoft.com/t5/s/gxucf89792/images/cmstNC05WEo0bcl"},"rankStyle":"OUTLINE"},"User:user:259504":
{"__typename":"User","id":"user:259504","uid":259504,"login":"DagmarHeidecker","deleted":false,"avatar":
{"__typename":"UserAvatar","url":"https://techcommunity.microsoft.com/t5/s/gxucf89792/m_assets/avatars/default/avatar-8.svg"},"rank":
{"__ref":"Rank:rank:4"},"email":"","messagesCount":9,"biography":null,"topicsCount":4,"kudosReceivedCount":45,"kudosGivenCount":1,"kudos
{"__typename":"RegistrationData","status":null,"registrationTime":"2019-01-02T03:09:08.721-
08:00","confirmEmailStatus":null,"followersCount":null,"solutionsCount":0},"BlogTopicMessage:message:4052851":
{"__typename":"BlogTopicMessage","uid":4052851,"subject":"Protecting Tier 0 the Modern
Way","id":"message:4052851","revisionNum":21,"author":{"__ref":"User:user:259504"},"depth":0,"hasGivenKudo":false,"board":

```

```
{ "__ref": "Blog:board:CoreInfrastructureandSecurityBlog"}, "conversation":
{ "__ref": "Conversation:conversation:4052851"}, "messagePolicies": { "__typename": "MessagePolicies", "canPublishArticleOnEdit":
{ "__typename": "PolicyResult", "failureReason":
{ "__typename": "FailureReason", "message": "error.lithium.policies.forums.policy_can_publish_on_edit_workflow_action.accessDenied", "key": "t
[]}}, "canModerateSpamMessage": { "__typename": "PolicyResult", "failureReason":
{ "__typename": "FailureReason", "message": "error.lithium.policies.feature.moderation_spam.action.moderate_entity.allowed.accessDenied", "ke
[]}}, "contentWorkflow":
{ "__typename": "ContentWorkflow", "state": "PUBLISH", "scheduledPublishTime": null, "scheduledTimezone": null, "userContext":
{ "__typename": "MessageWorkflowContext", "canSubmitForReview": null, "canEdit": false, "canRecall": null, "canSubmitForPublication": null, "canRe
{ "__ref": "ModerationData:moderation_data:4052851"}, "teaser": "
```

Almost every attack on Active Directory you hear about today – no matter if ransomware is involved or not – (ab)uses credential theft techniques as the key factor for successful compromise. Microsoft's [State of Cybercrime report](#) confirms this statement: "The top finding among ransomware incident response engagements was insufficient privilege access and lateral movement controls."

\n\n

Despite the fantastic capabilities of modern detection and protection tools (like the Microsoft Defender family of products), we should not forget that prevention is always better than cure (which means that accounts should be protected against credential theft proactively). Microsoft's approach to achieving this goal is the [Enterprise Access Model](#). It adds the aspect of hybrid and multi-cloud identities to the Active Directory Administrative Tier Model. Although first published almost 10 years ago, the AD Administrative Tier Model is still not obsolete. Not having it in place and enforced is extremely risky with today's threat level in mind.

\n\n

Most attackers follow playbooks and whatever their final goal may be, Active Directory Domain domination (Tier 0 compromise) is a stopover in almost every attack. Hence, **securing Tier 0 is the first critical step towards your Active Directory hardening journey and this article was written to help with it.**

", "body": "

How should your Tier 0 Protection look like?

\n

\n\n

Almost every attack on Active Directory you hear about today – no matter if ransomware is involved or not – (ab)uses credential theft techniques as the key factor for successful compromise. Microsoft's [State of Cybercrime report](#) confirms this statement: "The top finding among ransomware incident response engagements was insufficient privilege access and lateral movement controls."

\n\n

Despite the fantastic capabilities of modern detection and protection tools (like the Microsoft Defender family of products), we should not forget that prevention is always better than cure (which means that accounts should be protected against credential theft proactively). Microsoft's approach to achieving this goal is the [Enterprise Access Model](#). It adds the aspect of hybrid and multi-cloud identities to the Active Directory Administrative Tier Model. Although first published almost 10 years ago, the AD Administrative Tier Model is still not obsolete. Not having it in place and enforced is extremely risky with today's threat level in mind.

\n\n

Most attackers follow playbooks and whatever their final goal may be, Active Directory Domain domination (Tier 0 compromise) is a stopover in almost every attack. Hence, **securing Tier 0 is the first critical step towards your Active Directory hardening journey and this article was written to help with it.**

\n\n

AD Administrative Tier Model Refresher

\n

The AD Administrative Tier Model prevents escalation of privilege by restricting what Administrators can control and where they can log on. In the context of protecting Tier 0, the latter ensures that Tier 0 credentials cannot be exposed to a system belonging to another Tier (Tier 1 or Tier 2).

\n\n

Tier 0 includes accounts (Admins-, service- and computer-accounts, groups) that have direct or indirect administrative control over all AD-related identities and identity management systems. While direct administrative control is easy to identify (e.g. members of Domain Admins group), indirect control can be hard to spot: e.g. think of a virtualized Domain Controller and what the admin of the virtualization host can do to it, like dumping the memory or copying the Domain Controller's hard disk with all the password hashes. Consequently, virtualization environments hosting Tier 0 computers are Tier 0 systems as well. This also applies to the virtualization Admin accounts.

\n\n

The three Commandments of AD Administrative Tier Model

\n

Rule #1: **Credentials from a higher-privileged tier** (e.g. Tier 0 Admin or Service account) **must not be exposed to lower-tier systems** (e.g. Tier 1 or Tier 2 systems).

\n

Rule #2: **Lower-tier credentials can use services provided by higher-tiers, but not the other way around.** E.g. Tier 1 and even Tier 2 system still must be able to apply Group Policies.

\n

Rule #3: **Any system or user account that can manage a higher tier is also a member of that tier, whether originally intended or not.**

\n

\n\n

Implementing the AD Administrative Tier Model

\n

Most guides describe how to achieve these goals by implementing a complex cascade of Group Policies (The local computer configuration must be changed to avoid that higher Tier level administrators can expose their credentials to a down-level computer). This comes with the downside that Group Policies can be bypassed by local administrators and that the Tier Level restriction works only on Active Directory joined Windows computers. The bad news is that there is still no click-once deployment for Tiered Administration, but there is a more robust way to get things done by implementing Authentication policies. Authentication Policies provide a way to contain high-privilege credentials to systems that are only pertinent to selected users, computers, or services. With these capabilities, you can limit Tier 0 account usage to Tier 0 hosts. That's exactly what we need to achieve to protect Tier 0 identities from credential theft-based attacks.

\n\n

To be very clear on this: **With Kerberos Authentication Policies you can define a claim which defines where the user is allowed to request a Kerberos Granting Ticket from.**

\n\n

Optional: Deep Dive in Authentication Policies

\n

Authentication Policies are based on a Kerberos extension called FAST (Flexible Authentication Secure Tunneling) or Kerberos Armoring. FAST provides a protected channel between the Kerberos client and the KDC for the whole pre-authentication conversation by encrypting the pre-authentication messages with a so-called armor key and by ensuring the integrity of the messages.

\n

Kerberos Armoring is disabled by default and must be enabled using Group Policies. Once enabled, it provides the following functionality:

\n

\n

- Protection against offline dictionary attacks. Kerberos armoring protects the user's pre-authentication data (which is vulnerable to offline dictionary attacks when it is generated from a password).

\n

- Authenticated Kerberos errors. Kerberos armoring protects user Kerberos authentications from KDC Kerberos error spoofing, which can downgrade to NTLM or weaker cryptography.

\n

- Disables any authentication protocol except Kerberos for the configured user.

\n

- Compounded authentication in Dynamic Access Control (DAC). This allows authorization based on the combination of both user claims and device claims.

\n

\n

The last bullet point provides the basis for the feature we plan to use for protecting Tier 0: Authentication Policies.

\n\n

Restricting user logon from specific hosts requires the Domain Controller (specifically the Key Distribution Center (KDC)) to validate the host's identity. When using Kerberos authentication with Kerberos armoring, the KDC is provided with the TGT of the host from which the user is authenticating. That's what we call an armored TGT, the content of which is used to complete an access check to determine if the host is allowed.

\n\n

\n

Kerberos armoring logon flow (simplified):

T0 Admin accounts	\n (Member of each({ENTERPRISE DOMAIN CONTROLLERS}) Or Member of any({Tier 0 computers (FABRIKAM\\Tier 0 computers)})) \n	Kerberos only
-------------------	---	---------------

\n

\n

The screenshot below shows the relevant section of the Authentication Policy:

\n

\n\n

Find more details about how to create Authentication Policies at <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/how-to-configure-protected-accounts#create-a-user-account-audit-for-authentication-policy-with-adac>.

\n\n

Tier 0 Admin Logon Flow: Privileged Access Workstations (PAWs) are a MUST

\n

As explained at the beginning of the article, attackers can sneak through an open (and MFA protected) RDP connection when the Admin's client computer is compromised. To protect from this type of attack Microsoft has been recommending using PAWs since many years.

\n\n

In case you ask yourself, what the advantage of restricting the source of a logon attempt through Kerberos Policies is: Most certainly you do not want your T0 Admins to RDP from their – potentially compromised – workplace computers to the DC. Instead, you want them to use a Tier 0 Administrative Jump Host or - even better - a Privileged Access Workstation. With a compromised workplace computer as a source for T0 access it would be easy for an attacker to either use a keylogger to steal the T0 Admin's password, or to simply sneak through the RDP channel once it is open (using a simple password or MFA doesn't make a big difference for this type of attack). Even if an attacker would be able to steal the credential of a Tier 0 user, the attacker could use those credentials from a computer which is defined in the claim. On any other computer, Active Directory will not approve a TGT, even if the user provides the correct credentials. This will give you the easy possibility to monitor the declined requests and react properly.

\n\n

There are too many ways of implementing the Tier 0 Admin logon flow to describe all of them in a blog. The "classic" (some call it "old-fashioned") approach is a domain-joined PAW which is used for T0 administrative access to Tier 0 systems.

\n\n

\n

The solution above is straightforward but does not provide any modern cloud-based security features.

\n

"Protecting Tier 0 the modern way" not only refers to using Authentication Policies, but also leverages modern protection mechanisms provided by Azure Entra ID, like Multi-Factor-Authentication, Conditional Access or Identity Protection (to cover just the most important ones).

\n\n

Our preferred way of protecting the Tier 0 logon flow is via an Intune-managed PAW and Azure Virtual Desktop because this approach is easy to implement and perfectly teams modern protection mechanisms with on-premises Active Directory:

\n

\n\n

Logon to the AVD is restricted to come from a compliant PAW device only, Authentication Policies do the rest.

\n\n

Automation through PowerShell

\n

Still sounds painful? While steps 1 – 3 (enable Kerberos FAST, create OU structure, create Tier 0 groups) of Implementing a Tier 0 OU Structure and Authentication Policy are one-time tasks, step 4 and 6 (keep group membership and Authentication policy up-to-date) have turned out to be challenging in complex, dynamic environments. That's why Andreas Lucas (aka Kili69) has developed a PowerShell-based automation tool which ...

\n

\n

- creates the OU structure described above (if not already exists)

- \n
- creates the security groups described above (if not already exist)
- \n
- creates the Authentication policy described above (if not already exists)
- \n
- applies the Tier 0 authentication policy to any Tier 0 user object
- \n
- removes any object from the T0 Computers group which is not located in the Tier 0 OU
- \n
- removes any user object from the default Active directory Tier 0 groups, if the Authentication policy is not applied (except Built-In Administrator, GMSA and service accounts)
- \n

\n\n

Additional Comments and Recommendations

\n

Prerequisites for implementing Kerberos Authentication Policies

\n

Kerberos Authentication Policies were introduced in Windows Server 2012 R2, hence a Domain functional level of Windows Server 2012 R2 or higher is required for implementation.

\n\n

Authentication Policy – special Settings

\n

Require rolling NTLM secret for NTLM authentication

\n

Configuration of this feature was moved to the properties of the domain in Active Directory Administrative Center. When enabled, for users with the “Smart card is required for interactive logon” checkbox set, a new random password will be generated according to the password policy. See <https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/whats-new-in-credential-protection#rolling-public-key-only-users-ntlm-secrets> for more details.

\n\n

Allow NTLM network authentication when user is restricted to selected devices

\n

We do NOT recommend enabling this feature because with NTLM authentication allowed the capabilities of restricting access through Authentication Policies are reduced. In addition to that, we recommend adding privileged users to the [Protected Users security group](#). This special group was designed to harden privileged accounts and introduces a set of protection mechanisms, one of which is making NTLM authentication impossible for the members of this group. See <https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/authentication-policies-and-authentication-policy-silos#about-authentication-policies> for more details.

\n\n

Have Breakglass Accounts in place

\n

Break Glass accounts are emergency access accounts used to access critical systems or resources when other authentication mechanisms fail or are unavailable. In Active Directory, Break Glass accounts are used to provide emergency access to Active Directory in case normal T0 Admin accounts do not work anymore, e.g. because of a misconfigured Authentication Policy.

\n\n

Clean Source Principle

\n

The [clean source principle](#) requires all security dependencies to be as trustworthy as the object being secured. Implementation of the clean source principle is beyond the scope of this article, but explained in detail at [Success criteria for privileged access strategy.](#) | [Microsoft Learn](#).

\n\n

Review ACLs on the Root-level of your Domain(s)

\n

The security implications of an account having excessive privileges (e.g. being able to modify permissions at the root-level of the domain are massive. For that reason, before creating the new OU (named "Admin" in the description above), you must ensure that there are no excessive ACLs (Access Control List) configured on the Root-level of the domain. In addition to that, consider breaking inheritance on the OU called "Admin" in our example.

\n\n","body@stringLength":"24600","rawBody":."

How should your Tier 0 Protection look like?

\n

\n\n

Almost every attack on Active Directory you hear about today – no matter if ransomware is involved or not – (ab)uses credential theft techniques as the key factor for successful compromise. Microsoft's [State of Cybercrime report](#) confirms this statement: "The top finding among ransomware incident response engagements was insufficient privilege access and lateral movement controls."

\n\n

Despite the fantastic capabilities of modern detection and protection tools (like the Microsoft Defender family of products), we should not forget that prevention is always better than cure (which means that accounts should be protected against credential theft proactively). Microsoft's approach to achieving this goal is the [Enterprise Access Model](#). It adds the aspect of hybrid and multi-cloud identities to the Active Directory Administrative Tier Model. Although first published almost 10 years ago, the AD Administrative Tier Model is still not obsolete. Not having it in place and enforced is extremely risky with today's threat level in mind.

\n\n

Most attackers follow playbooks and whatever their final goal may be, Active Directory Domain domination (Tier 0 compromise) is a stopover in almost every attack. Hence, **securing Tier 0 is the first critical step towards your Active Directory hardening journey and this article was written to help with it.**

\n\n

AD Administrative Tier Model Refresher

\n

The AD Administrative Tier Model prevents escalation of privilege by restricting what Administrators can control and where they can log on. In the context of protecting Tier 0, the latter ensures that Tier 0 credentials cannot be exposed to a system belonging to another Tier (Tier 1 or Tier 2).

\n\n

Tier 0 includes accounts (Admins-, service- and computer-accounts, groups) that have direct or indirect administrative control over all AD-related identities and identity management systems. While direct administrative control is easy to identify (e.g. members of Domain Admins group), indirect control can be hard to spot: e.g. think of a virtualized Domain Controller and what the admin of the virtualization host can do to it, like dumping the memory or copying the Domain Controller's hard disk with all the password hashes. Consequently, virtualization environments hosting Tier 0 computers are Tier 0 systems as well. This also applies to the virtualization Admin accounts.

\n\n

The three Commandments of AD Administrative Tier Model

\n

Rule #1: **Credentials from a higher-privileged tier** (e.g. Tier 0 Admin or Service account) **must not be exposed to lower-tier systems** (e.g. Tier 1 or Tier 2 systems).

\n

Rule #2: **Lower-tier credentials can use services provided by higher-tiers, but not the other way around.** E.g. Tier 1 and even Tier 2 system still must be able to apply Group Policies.

\n

Rule #3: **Any system or user account that can manage a higher tier is also a member of that tier, whether originally intended or not.**

\n

\n\n

Implementing the AD Administrative Tier Model

\n

Most guides describe how to achieve these goals by implementing a complex cascade of Group Policies (The local computer configuration must be changed to avoid that higher Tier level administrators can expose their credentials to a down-level computer). This comes with the downside that Group Policies can be bypassed by local administrators and that the Tier Level restriction works only on Active Directory joined Windows computers. The bad news is that there is still no click-once deployment for Tiered Administration, but there is a more robust way to get things done by implementing [Authentication policies](#). Authentication Policies provide a way to contain

high-privilege credentials to systems that are only pertinent to selected users, computers, or services. With these capabilities, you can limit Tier 0 account usage to Tier 0 hosts. That's exactly what we need to achieve to protect Tier 0 identities from credential theft-based attacks.

\n\n

To be very clear on this: **With Kerberos Authentication Policies you can define a claim which defines where the user is allowed to request a Kerberos Granting Ticket from.**

\n\n

Optional: Deep Dive in Authentication Policies

\n

Authentication Policies are based on a Kerberos extension called FAST (Flexible Authentication Secure Tunneling) or Kerberos Armoring. FAST provides a protected channel between the Kerberos client and the KDC for the whole pre-authentication conversation by encrypting the pre-authentication messages with a so-called armor key and by ensuring the integrity of the messages.

\n

Kerberos Armoring is disabled by default and must be enabled using Group Policies. Once enabled, it provides the following functionality:

\n

\n

- Protection against offline dictionary attacks. Kerberos armoring protects the user's pre-authentication data (which is vulnerable to offline dictionary attacks when it is generated from a password).

\n

- Authenticated Kerberos errors. Kerberos armoring protects user Kerberos authentications from KDC Kerberos error spoofing, which can downgrade to NTLM or weaker cryptography.

\n

- Disables any authentication protocol except Kerberos for the configured user.

\n

- Compounded authentication in Dynamic Access Control (DAC). This allows authorization based on the combination of both user claims and device claims.

\n

\n

The last bullet point provides the basis for the feature we plan to use for protecting Tier 0: Authentication Policies.

\n\n

Restricting user logon from specific hosts requires the Domain Controller (specifically the Key Distribution Center (KDC)) to validate the host's identity. When using Kerberos authentication with Kerberos armoring, the KDC is provided with the TGT of the host from which the user is authenticating. That's what we call an armored TGT, the content of which is used to complete an access check to determine if the host is allowed.

\n\n

\n

Kerberos armoring logon flow (simplified):

\n

\n

1. The computer has already received an armored TGT during computer authentication to the domain.

\n

2. The user logs on to the computer:\n

\n

1. An unarmored AS-REQ for a TGT is sent to the KDC.

\n

2. The KDC queries for the user account in Active Directory and determines if it is configured with an Authentication Policy that restricts initial authentication that requires armored requests.

\n

3. The KDC fails the request and asks for Pre-Authentication.

\n

4. Windows detects that the domain supports Kerberos armoring and sends an armored AS-REQ to retry the sign-in request.

\n

5. The KDC performs an access check by using the configured access control conditions and the client operating system's identity information in the TGT that was used to armor the request. If the access check fails, the domain controller rejects the request.

\n

\n

\n

3. If the access check succeeds, the KDC replies with an armored reply (AS-REP) and the authentication process continues. The user now has an armored TGT.

ln

ln

Looks very much like a normal Kerberos logon? Not exactly: The main difference is the fact that the user's TGT includes the source computer's identity information. Requesting Service Tickets looks similar to what we described above, except that the user's armored TGT is used for protection and restriction.

\n\n

Implementing a Tier 0 OU Structure and Authentication Policy

\ln

The following steps are required to limit Tier 0 account usage (Admins and Service accounts) to Tier 0 hosts:

\n

ln

1. Enable Kerberos Armoring (aka FAST) for DCs and all computers (or at least Tier 0 computers).

ln

2. Before creating an OU structure similar to the one pictured below, you **MUST** ensure that Tier 0 accounts are the only ones having sensitive permissions on the root level of the domain. Keep in mind that all ACLs configured on the root-level of fabrikam.com will be inherited by the OU called “Admin” in our example.

ln

\ln

\\n\\n

3. Create the following security groups:

ln

- Tier 0 Users

\n

- Tier 0 Computer

\ln

4. Constantly update the Authentication policy to ensure that any new T0 Admin or T0 service account is covered.

\ln

5. Ensure that any newly created T0 computer account is added to the T0 Computers security group.

\\n

6. Configure an Authentication Policy with the following parameters and enforce the Kerberos Authentication policy:

\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n

(User) Accounts	Conditions (Computer accounts/groups)	User Sign On
T0 Admin accounts	\n (Member of each({ENTERPRISE DOMAIN CONTROLLERS}) Or Member of any({Tier 0 computers (FABRIKAM\\Tier 0 computers)})) \n	Kerberos only

\\n

ln

The screenshot below shows the relevant section of the Authentication Policy:

ln

\n\n

Find more details about how to create Authentication Policies at <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/how-to-configure-protected-accounts#create-a-user-account-audit-for-authentication-policy-with-adac>.

\\n\\n

Tier 0 Admin Logon Flow: Privileged Access Workstations (PAWs) are a MUST

ln

As explained at the beginning of the article, attackers can sneak through an open (and MFA protected) RDP connection when the Admin's client computer is compromised. To protect from this type of attack Microsoft has been recommending using [PAWs](#) since many years.

\n\n

In case you ask yourself, what the advantage of restricting the source of a logon attempt through Kerberos Policies is: Most certainly you do not want your T0 Admins to RDP from their – potentially compromised – workplace computers to the DC. Instead, you want them to use a Tier 0 Administrative Jump Host or - even better - a [Privileged Access Workstation](#). With a compromised workplace computer as a source for T0 access it would be easy for an attacker to either use a keylogger to steal the T0 Admin's password, or to simply sneak through the RDP channel once it is open (using a simple password or MFA doesn't make a big difference for this type of attack). Even if an attacker would be able to steal the credential of a Tier 0 user, the attacker could use those credentials from a computer which is defined in the claim. On any other computer, Active Directory will not approve a TGT, even if the user provides the correct credentials. This will give you the easy possibility to monitor the declined requests and react properly.

\n\n

There are too many ways of implementing the Tier 0 Admin logon flow to describe all of them in a blog. The "classic" (some call it "old-fashioned") approach is a domain-joined PAW which is used for T0 administrative access to Tier 0 systems.

\n\n

\n

The solution above is straightforward but does not provide any modern cloud-based security features.

\n

"Protecting Tier 0 the modern way" not only refers to using Authentication Policies, but also leverages modern protection mechanisms provided by Azure Entra ID, like [Multi-Factor-Authentication](#), [Conditional Access](#) or [Identity Protection](#) (to cover just the most important ones).

\n\n

Our preferred way of protecting the Tier 0 logon flow is via an [Intune-managed PAW](#) and [Azure Virtual Desktop](#) because this approach is easy to implement and perfectly teams modern protection mechanisms with on-premises Active Directory:

\n

\n\n

Logon to the AVD is restricted to come from a compliant PAW device only, Authentication Policies do the rest.

\n\n

Automation through PowerShell

\n

Still sounds painful? While steps 1 – 3 (enable Kerberos FAST, create OU structure, create Tier 0 groups) of Implementing a Tier 0 OU Structure and Authentication Policy are one-time tasks, step 4 and 6 (keep group membership and Authentication policy up-to-date) have turned out to be challenging in complex, dynamic environments. That's why Andreas Lucas (aka Kili69) has developed a [PowerShell-based automation tool](#) which ...

\n

\n

- creates the OU structure described above (if not already exists)

\n

- creates the security groups described above (if not already exist)

\n

- creates the Authentication policy described above (if not already exists)

\n

- applies the Tier 0 authentication policy to any Tier 0 user object

\n

- removes any object from the T0 Computers group which is not located in the Tier 0 OU

\n

- removes any user object from the default Active directory Tier 0 groups, if the Authentication policy is not applied (except Built-In Administrator, GMSA and service accounts)

\n

\n\n

Additional Comments and Recommendations

\n

Prerequisites for implementing Kerberos Authentication Policies

\n

Kerberos Authentication Policies were introduced in Windows Server 2012 R2, hence a Domain functional level of Windows Server 2012 R2 or higher is required for implementation.

\n\n

Authentication Policy – special Settings

\n

Require rolling NTLM secret for NTLM authentication

\n

Configuration of this feature was moved to the properties of the domain in Active Directory Administrative Center. When enabled, for users with the “Smart card is required for interactive logon” checkbox set, a new random password will be generated according to the password policy. See <https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/whats-new-in-credential-protection#rolling-public-key-only-users-ntlm-secrets> for more details.

\n\n

Allow NTLM network authentication when user is restricted to selected devices

\n

We do NOT recommend enabling this feature because with NTLM authentication allowed the capabilities of restricting access through Authentication Policies are reduced. In addition to that, we recommend adding privileged users to the [Protected Users security group](#). This special group was designed to harden privileged accounts and introduces a set of protection mechanisms, one of which is making NTLM authentication impossible for the members of this group. See <https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/authentication-policies-and-authentication-policy-silos#about-authentication-policies> for more details.

\n\n

Have Breakglass Accounts in place

\n

Break Glass accounts are emergency access accounts used to access critical systems or resources when other authentication mechanisms fail or are unavailable. In Active Directory, Break Glass accounts are used to provide emergency access to Active Directory in case normal T0 Admin accounts do not work anymore, e.g. because of a misconfigured Authentication Policy.

\n\n

Clean Source Principle

\n

The [clean source principle](#) requires all security dependencies to be as trustworthy as the object being secured. Implementation of the clean source principle is beyond the scope of this article, but explained in detail at [Success criteria for privileged access strategy | Microsoft Learn](#).

\n\n

Review ACLs on the Root-level of your Domain(s)

\n

The security implications of an account having excessive privileges (e.g. being able to modify permissions at the root-level of the domain) are massive. For that reason, before creating the new OU (named “Admin” in the description above), you must ensure that there are no excessive ACLs (Access Control List) configured on the Root-level of the domain. In addition to that, consider breaking inheritance on the OU called “Admin” in our example.

```
\n\n","kudosSumWeight":18,"repliesCount":56,"postTime":"2024-02-19T04:15:10.476-08:00","images":\n{"__typename":"AssociatedImageConnection","edges":\n[{"__typename":"AssociatedImageEdge","cursor":"MjQuMTB8Mi4xfG98MjV8X05WX3wx","node":{"__ref":"AssociatedImage":\n{"url":"https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MjkwNGlFQTgwMDNEMUFFMTBDNkVB?revision=21\"}}},{\"__typename\":\"AssociatedImageEdge\",\"cursor\":\"MjQuMTB8Mi4xfG98MjV8X05WX3wy\",\"node\":\n{\"__ref\":\"AssociatedImage\":\n{\"url\":\"https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MDI2Mmk4RTYwNjEwMzI1QUM3RTJB?revision=21\"}}},{\"__typename\":\"AssociatedImageEdge\",\"cursor\":\"MjQuMTB8Mi4xfG98MjV8X05WX3wz\",\"node\":\n{\"__ref\":\"AssociatedImage\":\n{\"url\":\"https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MDI3N2kyODU1MzE0OTgzMEVGRTE4?revision=21\"}}},{\"__typename\":\"AssociatedImageEdge\",\"cursor\":\"MjQuMTB8Mi4xfG98MjV8X05WX3w0\",\"node\":\n{\"__ref\":\"AssociatedImage\":\n{\"url\":\"https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MDI4N2lEQjAyQ0E0QzkwODJDQ0U3?revision=21\"}}},{\"__typename\":\"AssociatedImageEdge\",\"cursor\":\"MjQuMTB8Mi4xfG98MjV8X05WX3w1\",\"node\":\n{\"__ref\":\"AssociatedImage\":\n{\"url\":\"https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MDI4OWk2MDZBQ0ZDMEI0Mzg2OEVB?revision=21\"}}},{\"__typename\":\"AssociatedImageEdge\",\"cursor\":\"MjQuMTB8Mi4xfG98MjV8X05WX3w2\",\"node\":
```

```
{ "__ref": "AssociatedImage":
{"url": "https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MDI5NmIERkMzNzM2RUVDNEVEQkJG?
revision=21"}}, {"__typename": "AssociatedImageEdge", "cursor": "MjQuMTB8Mi4xfG98MjV8X05WX3w3", "node":
{"__ref": "AssociatedImage":
{"url": "https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MDI5N2k4OTUyQUExRDA4NzE4OEFC?
revision=21"}}, {"totalCount": 7, "pageInfo":
{"__typename": "PageInfo", "hasNextPage": false, "endCursor": null, "hasPreviousPage": false, "startCursor": null}, {"attachments":
{"__typename": "AttachmentConnection", "pageInfo":
{"__typename": "PageInfo", "hasNextPage": false, "endCursor": null, "hasPreviousPage": false, "startCursor": null, "edges": [], "tags":
{"__typename": "TagConnection", "pageInfo":
{"__typename": "PageInfo", "hasNextPage": false, "endCursor": null, "hasPreviousPage": false, "startCursor": null, "edges":
[{"__typename": "TagEdge", "cursor": "MjQuMTB8Mi4xfG98MTB8X05WX3w3", "node":
{"__typename": "Tag", "id": "tag:DagmarHeidecker", "text": "DagmarHeidecker", "time": "2021-06-29T13:40:47.229-
07:00", "lastActivityTime": null, "messagesCount": null, "followersCount": null}], "timeToRead": 9, "rawTeaser": "
Almost every attack on Active Directory you hear about today – no matter if ransomware is involved or not – (ab)uses credential theft
techniques as the key factor for successful compromise. Microsoft's State of Cybercrime report confirms this statement: "The top finding
among ransomware incident response engagements was insufficient privilege access and lateral movement controls."
}
```

\n\n

Despite the fantastic capabilities of modern detection and protection tools (like the Microsoft Defender family of products), we should not forget that prevention is always better than cure (which means that accounts should be protected against credential theft proactively). Microsoft's approach to achieving this goal is the [Enterprise Access Model](#). It adds the aspect of hybrid and multi-cloud identities to the Active Directory Administrative Tier Model. Although first published almost 10 years ago, the AD Administrative Tier Model is still not obsolete. Not having it in place and enforced is extremely risky with today's threat level in mind.

\n\n

Most attackers follow playbooks and whatever their final goal may be, Active Directory Domain domination (Tier 0 compromise) is a stopover in almost every attack. Hence, **securing Tier 0 is the first critical step towards your Active Directory hardening journey and this article was written to help with it.**

```
", "introduction": "", "coverImage": null, "coverImageProperties":
{"__typename": "CoverImageProperties", "style": "STANDARD", "titlePosition": "BOTTOM", "altText": "", "currentRevision":
{"__ref": "Revision:revision:4052851_21"}, {"latestVersion": {"__typename": "FriendlyVersion", "major": "5", "minor": "0"}, "metrics":
{"__typename": "MessageMetrics", "views": 83372, "visibilityScope": "PUBLIC", "canonicalUrl": null, "seoTitle": null, "seoDescription": null, "placeholder":
{"__typename": "UserConnection", "edges": [], "nonCoAuthorContributors": {"__typename": "UserConnection", "edges": [], "coAuthors":
{"__typename": "UserConnection", "edges": [], "blogMessagePolicies":
{"__typename": "BlogMessagePolicies", "canDoAuthoringActionsOnBlog": {"__typename": "PolicyResult", "failureReason":
{"__typename": "FailureReason", "message": "error.lithium.policies.blog.action_can_do_authoring_action.accessDenied", "key": "error.lithium.pol
[]}}, {"archivalData": null, "customFields": [], "revisions": {"constraints": {"isPublished": {"eq": true}, "first": 1}}:
{"__typename": "RevisionConnection", "totalCount": 21}, {"Conversation:conversation:4052851":
{"__typename": "Conversation", "id": "conversation:4052851", "solved": false, "topic":
{"__ref": "BlogTopicMessage:message:4052851"}, {"lastPostingActivityTime": "2024-11-04T05:13:15.746-08:00", "lastPostTime": "2024-11-
04T05:13:15.746-08:00", "unreadReplyCount": 56, "isSubscribed": false, "ModerationData:moderation_data:4052851":
{"__typename": "ModerationData", "id": "moderation_data:4052851", "status": "APPROVED", "rejectReason": null, "isReportedAbuse": false, "rejectL
{"url": "https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MjkWNGIFQTgwMDNEMUFFMTBDNBKV?
revision=21"}:
{"__typename": "AssociatedImage", "url": "https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MjkWNGIFQTgw
revision=21", "title": "DagmarHeidecker_0-
1708345486896.png", "associationType": "BODY", "width": 890, "height": 423, "altText": null, "AssociatedImage":
{"url": "https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MDI2Mmk4RTYwNjEwMzI1QUM3RTJB?
revision=21"}:
{"__typename": "AssociatedImage", "url": "https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MDI2Mmk4RTY
revision=21", "title": "DagmarHeidecker_0-
1707459813959.png", "associationType": "BODY", "width": 523, "height": 405, "altText": null, "AssociatedImage":
{"url": "https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MDI3N2kyODU1MzE0OTgzMEVGRTE4?
revision=21"}:
{"__typename": "AssociatedImage", "url": "https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MDI3N2kyODU
revision=21", "title": "DagmarHeidecker_0-
1707463029173.png", "associationType": "BODY", "width": 940, "height": 455, "altText": null, "AssociatedImage":
{"url": "https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MDI4N2IEQjAyQ0E0QzkwODJDQ0U3?
revision=21"}:
{"__typename": "AssociatedImage", "url": "https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MDI4N2IEQjAyC
revision=21", "title": "DagmarHeidecker_0-
1707463188790.png", "associationType": "BODY", "width": 940, "height": 470, "altText": null, "AssociatedImage":
{"url": "https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MDI4OWk2MDZBQ0ZDMEI0Mzg2OEVB?
revision=21"}:
{"__typename": "AssociatedImage", "url": "https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MDI4OWk2MDZ
revision=21", "title": "DagmarHeidecker_0-
```

1707463910563.png","associationType":"BODY","width":939,"height":366,"altText":null},"AssociatedImage":
{\"url\":\"https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MDI5NmIERkMzNzM2RUVDNEVEQkJG?revision=21\"}":
{\"__typename\":\"AssociatedImage\",\"url\":\"https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MDI5NmIERkMzNzM2RUVDNEVEQkJG?revision=21\",\"title\":\"DagmarHeidecker_0-1707468206441.png\",\"associationType\":\"BODY\",\"width\":940,\"height\":291,\"altText\":null,\"AssociatedImage\":
{\"url\":\"https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MDI5N2k4OTUyQUExRDA4NzE4OEFC?revision=21\"}":
{\"__typename\":\"AssociatedImage\",\"url\":\"https://techcommunity.microsoft.com/t5/s/gxcuf89792/images/bS00MDUyODUxLTU1MDI5N2k4OTUyQUExRDA4NzE4OEFC?revision=21\",\"title\":\"DagmarHeidecker_1-1707468256678.png\",\"associationType\":\"BODY\",\"width\":939,\"height\":400,\"altText\":null,\"Revision:revision:4052851_21\":
{\"__typename\":\"Revision\",\"id\":\"revision:4052851_21\",\"lastEditTime\":\"2024-02-19T08:04:58.862-08:00\"},\"CachedAsset:theme:customTheme1-1734787622921\":{\"__typename\":\"CachedAsset\",\"id\":\"theme:customTheme1-1734787622921\",\"value\":{\"id\":\"customTheme1\",\"animation\":
{\"fast\":\"150ms\",\"normal\":\"250ms\",\"slow\":\"500ms\",\"slowest\":\"750ms\",\"function\":\"cubic-bezier(0.07, 0.91, 0.51, 1)\",\"__typename\":\"AnimationThemeSettings\"},\"avatar\":{\"borderRadius\":\"50%\",\"collections\":
[\"default\"],\"__typename\":\"AvatarThemeSettings\"},\"basics\":{\"browserIcon\":{\"imageAssetName\":\"favicon-1730836283320.png\",\"imageLastModified\":\"1730836286415\",\"__typename\":\"ThemeAsset\"},\"customerLogo\":
{\"imageAssetName\":\"favicon-1730836271365.png\",\"imageLastModified\":\"1730836274203\",\"__typename\":\"ThemeAsset\"},\"maximumWidthOfPageContent\":\"1300px\",\"oneC
{\"borderRadiusSm\":\"3px\",\"borderRadius\":\"3px\",\"borderRadiusLg\":\"5px\",\"paddingY\":\"5px\",\"paddingYLg\":\"7px\",\"paddingYHero\":\"var(--lia-bs-btn-padding-y-lg)\",\"paddingX\":\"12px\",\"paddingXLg\":\"16px\",\"paddingXHero\":\"60px\",\"fontStyle\":\"NORMAL\",\"fontWeight\":\"700\",\"textTransform\":\"NONE\",\"disab
-lia-bs-white\"},\"primaryTextHoverColor\":\"var(--lia-bs-white)\",\"primaryTextActiveColor\":\"var(--lia-bs-white)\",\"primaryBgColor\":\"var(--lia-bs-primary)\",\"primaryBgHoverColor\":\"hsl(var(--lia-bs-primary-h), var(--lia-bs-primary-s), calc(var(--lia-bs-primary-l) * 0.85))\",\"primaryBgActiveColor\":\"hsl(var(--lia-bs-primary-h), var(--lia-bs-primary-s), calc(var(--lia-bs-primary-l) * 0.7))\",\"primaryBorder\":\"1px solid transparent\",\"primaryBorderHover\":\"1px solid transparent\",\"primaryBorderActive\":\"1px solid transparent\",\"primaryBorderFocus\":\"1px solid var(--lia-bs-white)\",\"primaryBoxShadowFocus\":\"0 0 0 1px var(--lia-bs-primary), 0 0 0 4px hsla(var(--lia-bs-primary-h), var(--lia-bs-primary-s), var(--lia-bs-primary-l), 0.2)\",\"secondaryTextColor\":\"var(--lia-bs-gray-900)\",\"secondaryTextHoverColor\":\"hsl(var(--lia-bs-gray-900-h), var(--lia-bs-gray-900-s), calc(var(--lia-bs-gray-900-l) * 0.95))\",\"secondaryTextActiveColor\":\"hsl(var(--lia-bs-gray-900-h), var(--lia-bs-gray-900-s), calc(var(--lia-bs-gray-900-l) * 0.9))\",\"secondaryBgColor\":\"var(--lia-bs-gray-200)\",\"secondaryBgHoverColor\":\"hsl(var(--lia-bs-gray-200-h), var(--lia-bs-gray-200-s), calc(var(--lia-bs-gray-200-l) * 0.96))\",\"secondaryBgActiveColor\":\"hsl(var(--lia-bs-gray-200-h), var(--lia-bs-gray-200-s), calc(var(--lia-bs-gray-200-l) * 0.92))\",\"secondaryBorder\":\"1px solid transparent\",\"secondaryBorderHover\":\"1px solid transparent\",\"secondaryBorderActive\":\"1px solid transparent\",\"secondaryBorderFocus\":\"1px solid transparent\",\"secondaryBoxShadowFocus\":\"0 0 0 1px var(--lia-bs-primary), 0 0 0 4px hsla(var(--lia-bs-primary-h), var(--lia-bs-primary-s), var(--lia-bs-primary-l), 0.2)\",\"tertiaryTextColor\":\"var(--lia-bs-gray-900)\",\"tertiaryTextHoverColor\":\"hsl(var(--lia-bs-gray-900-h), var(--lia-bs-gray-900-s), calc(var(--lia-bs-gray-900-l) * 0.95))\",\"tertiaryTextActiveColor\":\"hsl(var(--lia-bs-gray-900-h), var(--lia-bs-gray-900-s), calc(var(--lia-bs-gray-900-l) * 0.9))\",\"tertiaryBgColor\":\"transparent\",\"tertiaryBgHoverColor\":\"transparent\",\"tertiaryBgActiveColor\":\"hsla(var(--lia-bs-black-h), var(--lia-bs-black-s), var(--lia-bs-black-l), 0.04)\",\"tertiaryBorder\":\"1px solid transparent\",\"tertiaryBorderHover\":\"1px solid hsla(var(--lia-bs-black-h), var(--lia-bs-black-s), var(--lia-bs-black-l), 0.08)\",\"tertiaryBorderActive\":\"1px solid transparent\",\"tertiaryBorderFocus\":\"1px solid transparent\",\"tertiaryBoxShadowFocus\":\"0 0 0 1px var(--lia-bs-primary), 0 0 0 4px hsla(var(--lia-bs-primary-h), var(--lia-bs-primary-s), var(--lia-bs-primary-l), 0.2)\",\"destructiveTextColor\":\"var(--lia-bs-danger)\",\"destructiveTextHoverColor\":\"hsl(var(--lia-bs-danger-h), var(--lia-bs-danger-s), calc(var(--lia-bs-danger-l) * 0.95))\",\"destructiveTextActiveColor\":\"hsl(var(--lia-bs-danger-h), var(--lia-bs-danger-s), calc(var(--lia-bs-danger-l) * 0.9))\",\"destructiveBgColor\":\"var(--lia-bs-gray-200)\",\"destructiveBgHoverColor\":\"hsl(var(--lia-bs-gray-200-h), var(--lia-bs-gray-200-s), calc(var(--lia-bs-gray-200-l) * 0.96))\",\"destructiveBgActiveColor\":\"hsl(var(--lia-bs-gray-200-h), var(--lia-bs-gray-200-s), calc(var(--lia-bs-gray-200-l) * 0.92))\",\"destructiveBorder\":\"1px solid transparent\",\"destructiveBorderHover\":\"1px solid transparent\",\"destructiveBorderActive\":\"1px solid transparent\",\"destructiveBorderFocus\":\"1px solid transparent\",\"destructiveBoxShadowFocus\":\"0 0 0 1px var(--lia-bs-primary), 0 0 0 4px hsla(var(--lia-bs-primary-h), var(--lia-bs-primary-s), var(--lia-bs-primary-l), 0.2)\",\"__typename\":\"ButtonsThemeSettings\"},\"border\":{\"color\":\"hsla(var(--lia-bs-black-h), var(--lia-bs-black-s), var(--lia-bs-black-l), 0.08)\",\"mainContent\":\"NONE\",\"sideContent\":\"LIGHT\",\"radiusSm\":\"3px\",\"radius\":\"5px\",\"radiusLg\":\"9px\",\"radius50\":\"100vw\",\"__typename\":\"Bor
{\"xs\":\"0 0 0 1px hsla(var(--lia-bs-gray-900-h), var(--lia-bs-gray-900-s), var(--lia-bs-gray-900-l), 0.08), 0 3px 0 1px hsla(var(--lia-bs-gray-900-h), var(--lia-bs-gray-900-s), var(--lia-bs-gray-900-l), 0.16)\",\"sm\":\"0 2px 4px hsla(var(--lia-bs-gray-900-h), var(--lia-bs-gray-900-s), var(--lia-bs-gray-900-l), 0.12)\",\"md\":\"0 5px 15px hsla(var(--lia-bs-gray-900-h), var(--lia-bs-gray-900-s), var(--lia-bs-gray-900-l), 0.3)\",\"lg\":\"0 10px 30px hsla(var(--lia-bs-gray-900-h), var(--lia-bs-gray-900-s), var(--lia-bs-gray-900-l), 0.3)\",\"__typename\":\"BoxShadowThemeSettings\"},\"cards\":{\"bgColor\":\"var(--lia-panel-bg-color)\",\"borderRadius\":\"var(--lia-panel-border-radius)\",\"boxShadow\":\"var(--lia-box-shadow-xs)\",\"__typename\":\"CardsThemeSettings\"},\"chip\":
{\"maxWidth\":\"300px\",\"height\":\"30px\",\"__typename\":\"ChipThemeSettings\"},\"coreTypes\":{\"defaultMessageLinkColor\":\"var(--lia-bs-link-color)\",\"defaultMessageLinkDecoration\":\"none\",\"defaultMessageLinkFontStyle\":\"NORMAL\",\"defaultMessageLinkFontWeight\":\"400\",\"defaultM
-lia-bs-font-family-base\"},\"forumFontWeight\":\"var(--lia-default-message-font-weight)\",\"forumLineHeight\":\"var(--lia-bs-line-height-base)\",\"forumFontStyle\":\"var(--lia-default-message-font-style)\",\"forumMessageLinkColor\":\"var(--lia-default-message-link-color)\",\"forumMessageLinkDecoration\":\"var(--lia-default-message-link-decoration)\",\"forumMessageLinkFontStyle\":\"var(--lia-default-message-link-font-style)\",\"forumMessageLinkFontWeight\":\"var(--lia-default-message-link-font-weight)\",\"forumSolvedColor\":\"#148563\",\"blogColor\":\"#1CBAA0\",\"blogFontFamily\":\"var(--lia-bs-font-family-base)\",\"blogFontWeight\":\"var(--lia-default-message-font-weight)\",\"blogLineHeight\":\"1.75\",\"blogFontStyle\":\"var(--lia-default-message-font-style)\",\"blogMessageLinkColor\":\"var(--lia-default-message-link-color)\",\"blogMessageLinkDecoration\":\"var(--lia-default-message-link-decoration)\",\"blogMessageLinkFontStyle\":\"var(--lia-default-message-link-font-style)\",\"blogMessageLinkFontWeight\":\"var(--lia-default-

lia-border-radius-50)","hamburgerColor":"var(--lia-nav-controller-icon-color)","hamburgerHoverColor":"var(--lia-nav-controller-icon-color)","hamburgerBgColor":"transparent","hamburgerBgHoverColor":"transparent","hamburgerBorder":"none","hamburgerBorderHover":"none","lia-nav-link-color","collapseMenuDividerOpacity":0.16,"__typename":"NavbarThemeSettings"},"pager":{"textColor":"var(--lia-bs-link-color)","textFontWeight":"var(--lia-font-weight-md)","textFontSize":"var(--lia-bs-font-size-sm)","__typename":"PagerThemeSettings"},"panel":{"bgColor":"var(--lia-bs-white)","borderRadius":"var(--lia-bs-border-radius)","borderColor":"var(--lia-bs-border-color)","boxShadow":"none","__typename":"PanelThemeSettings"},"popover":{"arrowHeight":"8px","arrowWidth":"16px","maxWidth":"300px","minWidth":"100px","headerBg":"var(--lia-bs-white)","borderColor":"var(--lia-bs-border-color)","borderRadius":"var(--lia-bs-border-radius)","boxShadow":"0 0.5rem 1rem hsla(var(--lia-bs-black-h), var(--lia-bs-black-s), var(--lia-bs-black-l), 0.15)","__typename":"PopoverThemeSettings"},"prism":{"color":"#000000","bgColor":"#f5f2f0","fontFamily":"var(--font-family-monospace)","fontSize":"var(--lia-bs-font-size-base)","fontWeightBold":"var(--lia-bs-font-weight-bold)","fontStyleItalic":"italic","tabSize":2,"highlightColor":"#b3d4fc","commentColor":"#62707e","punctuationColor":"#6f6f6f","namespaceOpacity":0,100%,0.5},"keywordColor":"#0076a9","functionColor":"#d3284b","variableColor":"#c14700","__typename":"PrismThemeSettings"},"rte":{"bgColor":"var(--lia-bs-white)","borderRadius":"var(--lia-panel-border-radius)","boxShadow":"var(--lia-panel-box-shadow)","customColor1":"#bfded2","customColor2":"#fbee8","customColor3":"#f8cac6","customColor4":"#eeca9","customColor5":"#c2e0f4","diffChangedColor":"hsla(43, 97%, 63%, 0.4)","diffNoneColor":"hsla(0, 0%, 80%, 0.4)","diffRemovedColor":"hsla(9, 74%, 47%, 0.4)","specialMessageHeaderMarginTop":"40px","specialMessageHeaderMarginBottom":"20px","specialMessageItemMarginTop":"0","special":{"bgColor":"var(--lia-bs-gray-200)","bgHoverColor":"var(--lia-bs-gray-400)","borderRadius":"var(--lia-bs-border-radius-sm)","color":"var(--lia-bs-body-color)","hoverColor":"var(--lia-bs-body-color)","fontWeight":"var(--lia-font-weight-md)","fontSize":"var(--lia-font-size-xxs)","textTransform":"UPPERCASE","letterSpacing":"0.5px","__typename":"TagsThemeSettings"},"toasts":{"borderRadius":"var(--lia-bs-border-radius)","paddingX":"12px","__typename":"ToastsThemeSettings"},"typography":{"fontFamilyBase":"Segoe UI","fontStyleBase":"NORMAL","fontWeightBase":"400","fontWeightLight":"300","fontWeightNormal":"400","fontWeightMd":"500","fontWeightB":{"source":"SERVER","name":"Segoe UI","styles":[{"style":"NORMAL","weight":"400","__typename":"FontStyleData"}, {"style":"NORMAL","weight":"300","__typename":"FontStyleData"}, {"style":"NORMAL","weight":"600","__typename":"FontStyleData"}, {"style":"NORMAL","weight":"700","__typename":"FontStyleData"}, {"style":"ITALIC","weight":"400","__typename":"FontStyleData"}]","assetNames":["SegoeUI-normal-400.woff2","SegoeUI-normal-300.woff2","SegoeUI-normal-600.woff2","SegoeUI-normal-700.woff2","SegoeUI-italic-400.woff2"],"__typename":"CustomFont"},"source":"SERVER","name":"MWF Fluent Icons","styles":[{"style":"NORMAL","weight":"400","__typename":"FontStyleData"}]","assetNames":["MWFFluentIcons-normal-400.woff2"],"__typename":"CustomFont"},"__typename":"TypographyThemeSettings"},"unstyledListItem":{"marginBottomSm":"5px","marginBottomMd":"10px","marginBottomLg":"15px","marginBottomXl":"20px","marginBottomXxl":"25px","__typename":"YiqThemeSettings"},"colorLightness":{"primaryDark":0.36,"primaryLight":0.74,"primaryLighter":0.89,"primaryLightest":0.95,"infoDark":0.39,"infoLight":0.72,"infoLighter":0.85,"infoLight components/common/EmailVerification-1731977288000":{"__typename":"CachedAsset","id":"text:en_US-components/common/EmailVerification-1731977288000","value":{"email.verification.title":"Email Verification Required","email.verification.message.update.email":"To participate in the community, you must first verify your email address. The verification email was sent to {email}. To change your email, visit My Settings.","email.verification.message.resend.email":"To participate in the community, you must first verify your email address. The verification email was sent to {email}. Resend email."},"localOverride":false},"CachedAsset:text:en_US-shared/client/components/common>Loading>LoadingDot-1731977288000":{"__typename":"CachedAsset","id":"text:en_US-shared/client/components/common>Loading>LoadingDot-1731977288000","value":{"title":"Loading..."},"localOverride":false},"CachedAsset:quilt:o365.prod:pages/blogs/BlogMessagePage:board:CoreInfrastructureandSecurityf1734787621243":{"__typename":"CachedAsset","id":"quilt:o365.prod:pages/blogs/BlogMessagePage:board:CoreInfrastructureandSecurityBlog-1734787621243","value":{"id":"BlogMessagePage","container":{"id":"Common","headerProps":{"backgroundImageProps":null,"backgroundColor":null,"addComponents":null,"removeComponents":["community.widget.bannerWidget"],"componentOrder":null,"__typename":"QuiltContainerSectionProps"},"headerComponentProps":{"community.widget.breadcrumbWidget":{"disableLastCrumbForDesktop":false},"footerProps":null,"footerComponentProps":null,"items":[{"id":"blog-article","layout":"ONE_COLUMN","bgColor":null,"showTitle":null,"showDescription":null,"textPosition":null,"textColor":null,"sectionEditLevel":"L":{"main":[{"id":"blogs.widget.blogArticleWidget","className":"lia-blog-container","props":null,"__typename":"QuiltComponent"}],"__typename":"OneSectionColumns"},"id":"section-1729184836777","layout":"MAIN_SIDE","bgColor":"transparent","showTitle":false,"showDescription":false,"textPosition":"CENTER","textColor":"var(--lia-bs-body-color)","sectionEditLevel":null,"bgImage":null,"disableSpacing":null,"edgeToEdgeDisplay":null,"fullHeight":null,"showBorder":null,"__typename":"QuiltComponent"},"id":"custom.widget.Social_Sharing","className":null,"props":{"widgetVisibility":"signedInOrAnonymous","useTitle":true,"useBackground":true,"title":"Share","lazyLoad":false},"__typename":"QuiltComponent"},"pages/blogs/BlogMessagePage-1731977288000":{"__typename":"CachedAsset","id":"text:en_US-pages/blogs/BlogMessagePage-1731977288000","value":{"title":{"contextMessageSubject"}|{communityTitle},"errorMissing":"This blog post cannot be found","name":"Blog Message Page","section.blog-article.title":"Blog Post","section.section-1729184836777.title":"","section.section-1729184836777.description":"","section.Cnclde.title":"Blog Post","section.tifEmD.description":"","section.tifEmD.title":"","localOverride":false},"CachedAsset:quiltWrapper:o365.prod:Common:1734787567344":{"__typename":"CachedAsset","id":"quiltWrapper:o365.prod:Common:1734787567344","value":{"id":"Common","header":{"backgroundImageProps":{"assetName":null,"backgroundSize":"COVER","backgroundRepeat":"NO_REPEAT","backgroundPosition":"CENTER_CENTER","lastModified":{"id":"community.widget.navbarWidget","props":{"showUserName":true,"showRegisterLink":true,"useIconLanguagePicker":true,"useLabelLanguagePicker":true,"className":"QuiltComponent


```

component-edit-mode__OnCcm","links":{"sideLinks":[],"mainLinks":[{"children":[],"linkType":"INTERNAL","id":"gxcuf89792","params":
{},"routeName":"CommunityPage"},{"children":[],"linkType":"EXTERNAL","id":"external-link","url":"/Directory","target":"SELF"},{"children":
[{"linkType":"INTERNAL","id":"microsoft365","params":{"categoryId":"microsoft365"},"routeName":"CategoryPage"},
{"linkType":"INTERNAL","id":"microsoft-teams","params":{"categoryId":"MicrosoftTeams"},"routeName":"CategoryPage"},
{"linkType":"INTERNAL","id":"windows","params":{"categoryId":"Windows"},"routeName":"CategoryPage"},
{"linkType":"INTERNAL","id":"microsoft-securityand-compliance","params":
{"categoryId":"MicrosoftSecurityandCompliance"},"routeName":"CategoryPage"},{"linkType":"INTERNAL","id":"outlook","params":
{"categoryId":"Outlook"},"routeName":"CategoryPage"},{"linkType":"INTERNAL","id":"planner","params":
{"categoryId":"Planner"},"routeName":"CategoryPage"},{"linkType":"INTERNAL","id":"windows-server","params":{"categoryId":"Windows-
Server"},"routeName":"CategoryPage"},{"linkType":"INTERNAL","id":"azure","params":
{"categoryId":"Azure"},"routeName":"CategoryPage"},{"linkType":"INTERNAL","id":"exchange","params":
{"categoryId":"Exchange"},"routeName":"CategoryPage"},{"linkType":"INTERNAL","id":"microsoft-endpoint-manager","params":
{"categoryId":"microsoft-endpoint-manager"},"routeName":"CategoryPage"},{"linkType":"INTERNAL","id":"s-q-l-server","params":
{"categoryId":"SQL-Server"},"routeName":"CategoryPage"},{"linkType":"EXTERNAL","id":"external-link-
2","url":"/Directory","target":"SELF"},{"linkType":"EXTERNAL","id":"communities","url":"/","target":"BLANK"},{"children":
[{"linkType":"INTERNAL","id":"education-sector","params":{"categoryId":"EducationSector"},"routeName":"CategoryPage"},
{"linkType":"INTERNAL","id":"a-i","params":{"categoryId":"AI"},"routeName":"CategoryPage"},{"linkType":"INTERNAL","id":"i-t-ops-
talk","params":{"categoryId":"ITOpsTalk"},"routeName":"CategoryPage"},{"linkType":"INTERNAL","id":"partner-community","params":
{"categoryId":"PartnerCommunity"},"routeName":"CategoryPage"},{"linkType":"INTERNAL","id":"microsoft-mechanics","params":
{"categoryId":"MicrosoftMechanics"},"routeName":"CategoryPage"},{"linkType":"INTERNAL","id":"healthcare-and-life-sciences","params":
{"categoryId":"HealthcareAndLifeSciences"},"routeName":"CategoryPage"},{"linkType":"INTERNAL","id":"public-sector","params":
{"categoryId":"PublicSector"},"routeName":"CategoryPage"},{"linkType":"INTERNAL","id":"io-t","params":
{"categoryId":"IoT"},"routeName":"CategoryPage"},{"linkType":"INTERNAL","id":"driving-adoption","params":
{"categoryId":"DrivingAdoption"},"routeName":"CategoryPage"},{"linkType":"INTERNAL","id":"s-m-b","params":
{"categoryId":"SMB"},"routeName":"CategoryPage"},{"linkType":"INTERNAL","id":"startupsat-microsoft","params":
{"categoryId":"StartupsatMicrosoft"},"routeName":"CategoryPage"},{"linkType":"EXTERNAL","id":"external-link-
1","url":"/Directory","target":"SELF"},{"linkType":"EXTERNAL","id":"communities-1","url":"/","target":"SELF"},{"children":
[],"linkType":"EXTERNAL","id":"external","url":"/Blogs","target":"SELF"},{"children":[],"linkType":"EXTERNAL","id":"external-
1","url":"/Events","target":"SELF"},{"children":[{"linkType":"INTERNAL","id":"microsoft-learn-1","params":
{"categoryId":"MicrosoftLearn"},"routeName":"CategoryPage"},{"linkType":"INTERNAL","id":"microsoft-learn-blog","params":
{"boardId":"MicrosoftLearnBlog","categoryId":"MicrosoftLearn"},"routeName":"BlogBoardPage"},{"linkType":"EXTERNAL","id":"external-
10","url":"https://learningroomdirectory.microsoft.com/","target":"BLANK"},{"linkType":"EXTERNAL","id":"external-
3","url":"https://docs.microsoft.com/learn/dynamics365/WT.mc_id=techcom_header-webpage-m365","target":"BLANK"},
{"linkType":"EXTERNAL","id":"external-4","url":"https://docs.microsoft.com/learn/m365/?wt.mc_id=techcom_header-webpage-
m365","target":"BLANK"},{"linkType":"EXTERNAL","id":"external-5","url":"https://docs.microsoft.com/learn/topics/sci/?
wt.mc_id=techcom_header-webpage-m365","target":"BLANK"},{"linkType":"EXTERNAL","id":"external-
6","url":"https://docs.microsoft.com/learn/powerplatform/?wt.mc_id=techcom_header-webpage-powerplatform","target":"BLANK"},
{"linkType":"EXTERNAL","id":"external-7","url":"https://docs.microsoft.com/learn/github/?wt.mc_id=techcom_header-webpage-
github","target":"BLANK"},{"linkType":"EXTERNAL","id":"external-8","url":"https://docs.microsoft.com/learn/teams/?
wt.mc_id=techcom_header-webpage-teams","target":"BLANK"},{"linkType":"EXTERNAL","id":"external-
9","url":"https://docs.microsoft.com/learn/dotnet/?wt.mc_id=techcom_header-webpage-dotnet","target":"BLANK"},
{"linkType":"EXTERNAL","id":"external-2","url":"https://docs.microsoft.com/learn/azure/?WT.mc_id=techcom_header-webpage-
m365","target":"BLANK"},{"linkType":"INTERNAL","id":"microsoft-learn","params":
{"categoryId":"MicrosoftLearn"},"routeName":"CategoryPage"},{"children":[],"linkType":"INTERNAL","id":"community-info-center","params":
{"categoryId":"Community-Info-Center"},"routeName":"CategoryPage"}],"style":{"boxShadow":"var(--lia-bs-box-shadow-
sm)","controllerHighlightColor":"hsla(30, 100%,
50%)","linkFontWeight":"400","dropdownDividerMarginBottom":"10px","hamburgerBorderHover":"none","linkBoxShadowHover":"none","linkFo
-lia-border-radius-50"},"hamburgerBgColor":"transparent","hamburgerColor":"var(--lia-nav-controller-icon-
color)","linkTextBorderBottom":"none","brandLogoHeight":"30px","linkBgHoverColor":"transparent","linkLetterSpacing":"normal","collapseMenu
solid var(--lia-bs-border-
color)","hamburgerBorder":"none","dropdownPaddingX":"10px","brandMarginRightSm":"10px","linkBoxShadow":"none","collapseMenuDividerI
-lia-nav-link-color)","linkColor":"var(--lia-bs-body-color)","linkJustifyContent":"flex-
start","dropdownPaddingTop":"10px","controllerHighlightTextColor":"var(--lia-yiq-dark)","controllerTextColor":"var(--lia-nav-controller-icon-
color)","background":{"imageName":"","color":"var(--lia-bs-
white)","size":"COVER","repeat":"NO_REPEAT","position":"CENTER_CENTER","imageLastModified":""},"linkBorderRadius":"var(--lia-bs-
border-radius-sm)","linkHoverColor":"var(--lia-bs-body-color)","position":"FIXED","linkBorder":"none","linkTextBorderBottomHover":"2px
solid var(--lia-bs-body-color)","brandMarginRight":"30px","hamburgerHoverColor":"var(--lia-nav-controller-icon-
color)","linkBorderHover":"none","collapseMenuMarginLeft":"20px","linkFontStyle":"NORMAL","controllerTextHoverColor":"var(--lia-nav-
controller-icon-hover-
color)","linkPaddingX":"10px","linkPaddingY":"5px","paddingTop":"15px","linkTextTransform":"NONE","dropdownBorderColor":"hsla(var(--
lia-bs-black-h), var(--lia-bs-black-s), var(--lia-bs-black-l), 0.08)","controllerBgHoverColor":"hsla(var(--lia-bs-black-h), var(--lia-bs-black-s),
var(--lia-bs-black-l), 0.1)","linkBgColor":"transparent","linkDropdownPaddingX":"var(--lia-nav-link-
px)","linkDropdownPaddingY":"9px","controllerIconColor":"var(--lia-bs-body-
color)","dropdownDividerMarginTop":"10px","linkGap":"10px","controllerIconHoverColor":"var(--lia-bs-body-
color)","showSearchIcon":false,"languagePickerStyle":"iconAndLabel"},"__typename":"QuiltComponent"},
{"id":"community.widget.breadcrumbWidget","props":{"backgroundColor":"transparent","linkHighlightColor":"var(--lia-bs-
primary)","visualEffects":{"showBottomBorder":true},"linkTextColor":"var(--lia-bs-gray-700)","__typename":"QuiltComponent"},

```

```

{"id":"custom.widget.HeroBanner","props":
{"widgetVisibility":"signedInOrAnonymous","useTitle":true,"usePageWidth":false,"useBackground":false,"cMax_items":3,"title":"","lazyLoad":fal
{"backgroundImageProps":
{"assetName":null,"backgroundSize":"COVER","backgroundRepeat":"NO_REPEAT","backgroundPosition":"CENTER_CENTER","lastModified
[{"id":"custom.widget.MicrosoftFooter","props":
{"widgetVisibility":"signedInOrAnonymous","useTitle":true,"useBackground":false,"title":"","lazyLoad":false},"__typename":"QuiltComponent"}],
components/common/ActionFeedback-1731977288000":{"__typename":"CachedAsset","id":"text:en_US-
components/common/ActionFeedback-1731977288000","value":{"joinedGroupHub.title":"Welcome","joinedGroupHub.message":"You are
now a member of this group and are subscribed to updates.","groupHubInviteNotFound.title":"Invitation Not
Found","groupHubInviteNotFound.message":"Sorry, we could not find your invitation to the group. The owner may have canceled the
invite.","groupHubNotFound.title":"Group Not Found","groupHubNotFound.message":"The grouphub you tried to join does not exist. It
may have been deleted.","existingGroupHubMember.title":"Already Joined","existingGroupHubMember.message":"You are already a
member of this group.","accountLocked.title":"Account Locked","accountLocked.message":"Your account has been locked due to multiple
failed attempts. Try again in {lockoutTime} minutes.","editedGroupHub.title":"Changes Saved","editedGroupHub.message":"Your group
has been updated.","leftGroupHub.title":"Goodbye","leftGroupHub.message":"You are no longer a member of this group and will not
receive future updates.","deletedGroupHub.title":"Deleted","deletedGroupHub.message":"The group has been
deleted.","groupHubCreated.title":"Group Created","groupHubCreated.message":"{groupHubName} is ready to
use","accountClosed.title":"Account Closed","accountClosed.message":"The account has been closed and you will now be redirected to
the homepage","resetTokenExpired.title":"Reset Password Link has Expired","resetTokenExpired.message":"Try resetting your password
again","invalidUrl.title":"Invalid URL","invalidUrl.message":"The URL you're using is not recognized. Verify your URL and try
again.","accountClosedForUser.title":"Account Closed","accountClosedForUser.message":"{userName}'s account is
closed","inviteTokenInvalid.title":"Invitation Invalid","inviteTokenInvalid.message":"Your invitation to the community has been canceled or
expired.","inviteTokenError.title":"Invitation Verification Failed","inviteTokenError.message":"The url you are utilizing is not recognized.
Verify your URL and try again","pageNotFound.title":"Access Denied","pageNotFound.message":"You do not have access to this area of
the community or it doesn't exist","eventAttending.title":"Responded as Attending","eventAttending.message":"You'll be notified when
there's new activity and reminded as the event approaches","eventInterested.title":"Responded as
Interested","eventInterested.message":"You'll be notified when there's new activity and reminded as the event
approaches","eventNotFound.title":"Event Not Found","eventNotFound.message":"The event you tried to respond to does not
exist."},"localOverride":false},"CachedAsset:component:custom.widget.HeroBanner-en-1734787692513":
{"__typename":"CachedAsset","id":"component:custom.widget.HeroBanner-en-1734787692513","value":{"component":
{"id":"custom.widget.HeroBanner","template":{"id":"HeroBanner","markupLanguage":"REACT","style":null,"texts":
{"searchPlaceholderText":"Search this
community","followActionText":"Follow","unfollowActionText":"Following","searchOnHoverText":"Please enter your search term(s) and then
press return key to complete a search."},"defaults":{"config":{"applicablePages":
[],"dynamicByCoreNode":null,"description":null,"fetchContent":null,"__typename":"ComponentConfiguration"},"props":
{"id":"max_items","dataType":"NUMBER","list":false,"defaultValue":"3","label":"Max Items","description":"The maximum number of items
to display in the
carousel","possibleValues":null,"control":"INPUT","__typename":"PropDefinition"},"__typename":"ComponentProperties"},"components":
[{"id":"custom.widget.HeroBanner","form":{"fields":
[{"id":"widgetChooser","validation":null,"noValidation":null,"dataType":"STRING","list":null,"control":null,"defaultValue":null,"label":null,"descripti
{"id":"title","validation":null,"noValidation":null,"dataType":"STRING","list":null,"control":null,"defaultValue":null,"label":null,"description":null,"pos
{"id":"useTitle","validation":null,"noValidation":null,"dataType":"BOOLEAN","list":null,"control":null,"defaultValue":null,"label":null,"description":nu
{"id":"useBackground","validation":null,"noValidation":null,"dataType":"BOOLEAN","list":null,"control":null,"defaultValue":null,"label":null,"descri
{"id":"widgetVisibility","validation":null,"noValidation":null,"dataType":"STRING","list":null,"control":null,"defaultValue":null,"label":null,"descriptio
{"id":"moreOptions","validation":null,"noValidation":null,"dataType":"STRING","list":null,"control":null,"defaultValue":null,"label":null,"description'
{"id":"cMax_items","validation":null,"noValidation":null,"dataType":"NUMBER","list":false,"control":"INPUT","defaultValue":"3","label":"Max
Items","description":"The maximum number of items to display in the carousel","possibleValues":null,"__typename":"FormField"},"layout":
{"rows":[{"id":"widgetChooserGroup","type":"fieldset","as":null,"items":
[{"id":"widgetChooser","className":null,"__typename":"FormFieldRef"},"props":null,"legend":null,"description":null,"className":null,"viewVar
{"id":"titleGroup","type":"fieldset","as":null,"items":[{"id":"title","className":null,"__typename":"FormFieldRef"},
{"id":"useTitle","className":null,"__typename":"FormFieldRef"},"props":null,"legend":null,"description":null,"className":null,"viewVariant":null
{"id":"useBackground","type":"fieldset","as":null,"items":
[{"id":"useBackground","className":null,"__typename":"FormFieldRef"},"props":null,"legend":null,"description":null,"className":null,"viewVai
{"id":"widgetVisibility","type":"fieldset","as":null,"items":
[{"id":"widgetVisibility","className":null,"__typename":"FormFieldRef"},"props":null,"legend":null,"description":null,"className":null,"viewVari
{"id":"moreOptionsGroup","type":"fieldset","as":null,"items":
[{"id":"moreOptions","className":null,"__typename":"FormFieldRef"},"s","props":null,"legend":null,"description":null,"className":null,"viewVariar
{"id":"componentPropsGroup","type":"fieldset","as":null,"items":
[{"id":"cMax_items","className":null,"__typename":"FormFieldRef"},"props":null,"legend":null,"description":null,"className":null,"viewVariar
[],__typename":"Component"},"grouping":"CUSTOM","__typename":"ComponentTemplate"},"properties":{"config":{"applicablePages":
[],"dynamicByCoreNode":null,"description":null,"fetchContent":null,"__typename":"ComponentConfiguration"},"props":
[{"id":"max_items","dataType":"NUMBER","list":false,"defaultValue":"3","label":"Max Items","description":"The maximum number of items
to display in the
carousel","possibleValues":null,"control":"INPUT","__typename":"PropDefinition"},"__typename":"ComponentProperties"},"form":{"fields":
[{"id":"widgetChooser","validation":null,"noValidation":null,"dataType":"STRING","list":null,"control":null,"defaultValue":null,"label":null,"descripti
{"id":"title","validation":null,"noValidation":null,"dataType":"STRING","list":null,"control":null,"defaultValue":null,"label":null,"description":null,"pos
{"id":"useTitle","validation":null,"noValidation":null,"dataType":"BOOLEAN","list":null,"control":null,"defaultValue":null,"label":null,"description":nu

```

```

{"id":"useBackground","validation":null,"noValidation":null,"dataType":"BOOLEAN","list":null,"control":null,"defaultValue":null,"label":null,"descri
{"id":"widgetVisibility","validation":null,"noValidation":null,"dataType":"STRING","list":null,"control":null,"defaultValue":null,"label":null,"description
{"id":"moreOptions","validation":null,"noValidation":null,"dataType":"STRING","list":null,"control":null,"defaultValue":null,"label":null,"description"
{"id":"cMax_items","validation":null,"noValidation":null,"dataType":"NUMBER","list":false,"control":"INPUT","defaultValue":"3","label":"Max
Items","description":"The maximum number of items to display in the carousel","possibleValues":null,"__typename":"FormField"},"layout":
{"rows":[{"id":"widgetChooserGroup","type":"fieldset","as":null,"items":
[{"id":"widgetChooser","className":null,"__typename":"FormFieldRef"},"props":null,"legend":null,"description":null,"className":null,"viewVar
{"id":"titleGroup","type":"fieldset","as":null,"items":[{"id":"title","className":null,"__typename":"FormFieldRef"},
{"id":"useTitle","className":null,"__typename":"FormFieldRef"},"props":null,"legend":null,"description":null,"className":null,"viewVariant":nul
{"id":"useBackground","type":"fieldset","as":null,"items":
[{"id":"useBackground","className":null,"__typename":"FormFieldRef"},"props":null,"legend":null,"description":null,"className":null,"viewVai
{"id":"widgetVisibility","type":"fieldset","as":null,"items":
[{"id":"widgetVisibility","className":null,"__typename":"FormFieldRef"},"props":null,"legend":null,"description":null,"className":null,"viewVari
{"id":"moreOptionsGroup","type":"fieldset","as":null,"items":
[{"id":"moreOptions","className":null,"__typename":"FormFieldRef"},"props":null,"legend":null,"description":null,"className":null,"viewVariar
{"id":"componentPropsGroup","type":"fieldset","as":null,"items":
[{"id":"cMax_items","className":null,"__typename":"FormFieldRef"},"props":null,"legend":null,"description":null,"className":null,"viewVariar
{"fields":
[{"id":"widgetChooser","validation":null,"noValidation":null,"dataType":"STRING","list":null,"control":null,"defaultValue":null,"label":null,"descripti
{"id":"title","validation":null,"noValidation":null,"dataType":"STRING","list":null,"control":null,"defaultValue":null,"label":null,"description":null,"pos
{"id":"useTitle","validation":null,"noValidation":null,"dataType":"BOOLEAN","list":null,"control":null,"defaultValue":null,"label":null,"description":nu
{"id":"useBackground","validation":null,"noValidation":null,"dataType":"BOOLEAN","list":null,"control":null,"defaultValue":null,"label":null,"descri
{"id":"widgetVisibility","validation":null,"noValidation":null,"dataType":"STRING","list":null,"control":null,"defaultValue":null,"label":null,"descriptio
{"id":"moreOptions","validation":null,"noValidation":null,"dataType":"STRING","list":null,"control":null,"defaultValue":null,"label":null,"description"
{"id":"cMax_items","validation":null,"noValidation":null,"dataType":"NUMBER","list":false,"control":"INPUT","defaultValue":"3","label":"Max
Items","description":"The maximum number of items to display in the carousel","possibleValues":null,"__typename":"FormField"},"layout":
{"rows":[{"id":"widgetChooserGroup","type":"fieldset","as":null,"items":
[{"id":"widgetChooser","className":null,"__typename":"FormFieldRef"},"props":null,"legend":null,"description":null,"className":null,"viewVar
{"id":"titleGroup","type":"fieldset","as":null,"items":[{"id":"title","className":null,"__typename":"FormFieldRef"},
{"id":"useTitle","className":null,"__typename":"FormFieldRef"},"props":null,"legend":null,"description":null,"className":null,"viewVariant":nul
{"id":"useBackground","type":"fieldset","as":null,"items":
[{"id":"useBackground","className":null,"__typename":"FormFieldRef"},"props":null,"legend":null,"description":null,"className":null,"viewVai
{"id":"widgetVisibility","type":"fieldset","as":null,"items":
[{"id":"widgetVisibility","className":null,"__typename":"FormFieldRef"},"props":null,"legend":null,"description":null,"className":null,"viewVari
{"id":"moreOptionsGroup","type":"fieldset","as":null,"items":
[{"id":"moreOptions","className":null,"__typename":"FormFieldRef"},"props":null,"legend":null,"description":null,"className":null,"viewVariar
{"id":"componentPropsGroup","type":"fieldset","as":null,"items":
[{"id":"cMax_items","className":null,"__typename":"FormFieldRef"},"props":null,"legend":null,"description":null,"className":null,"viewVariar
en-1734787692513":{"__typename":"CachedAsset","id":"component:custom.widget.Social_Sharing-en-1734787692513","value":
{"component":{"id":"custom.widget.Social_Sharing","template":{"id":"Social_Sharing","markupLanguage":"HANDLEBARS","style":".social-
share {\n .sharing-options {\n position: relative;\n margin: 0;\n padding: 0;\n line-height: 10px;\n display: flex;\n justify-content: left;\n gap:
5px;\n list-style-type: none;\n li {\n text-align: left;\n a {\n min-width: 30px;\n min-height: 30px;\n display: block;\n padding: 1px;\n .social-
share-linkedin {\n img {\n background-color: rgb(0, 119, 181);\n }\n }\n .social-share-facebook {\n img {\n background-color: rgb(59, 89,
152);\n }\n }\n .social-share-x {\n img {\n background-color: rgb(0, 0, 0);\n }\n }\n .social-share-rss {\n img {\n background-color: rgb(0, 0,
0);\n }\n }\n .social-share-reddit {\n img {\n background-color: rgb(255, 69, 0);\n }\n }\n .social-share-email {\n img {\n background-color:
rgb(132, 132, 132);\n }\n }\n a {\n img {\n height: 2rem;\n }\n }\n }\n }\n }","texts":null,"defaults":{"config":{"applicablePages":
[],"dynamicByCoreNode":false,"description":"Adds buttons to share to various social media
websites","fetchedContent":null,"__typename":"ComponentConfiguration"},"props":
[], "__typename":"ComponentProperties"},"components":[{"id":"custom.widget.Social_Sharing","form":null,"config":null,"props":
[], "__typename":"Component"}],"grouping":"CUSTOM","__typename":"ComponentTemplate"},"properties":{"config":{"applicablePages":
[],"dynamicByCoreNode":false,"description":"Adds buttons to share to various social media
websites","fetchedContent":null,"__typename":"ComponentConfiguration"},"props":
[], "__typename":"ComponentProperties"},"form":null,"__typename":"Component","localOverride":false},"globalCss":
{"css":".custom_widget_Social_Sharing_social-share_c7xxz_1 {\n .custom_widget_Social_Sharing_sharing-options_c7xxz_2 {\n position:
relative;\n margin: 0;\n padding: 0;\n line-height: 0.625rem;\n display: flex;\n justify-content: left;\n gap: 0.3125rem;\n list-style-type:
none;\n li {\n text-align: left;\n a {\n min-width: 1.875rem;\n min-height: 1.875rem;\n display: block;\n padding: 0.0625rem;\n
.custom_widget_Social_Sharing_social-share-linkedin_c7xxz_18 {\n img {\n background-color: rgb(0, 119, 181);\n }\n }\n
.custom_widget_Social_Sharing_social-share-facebook_c7xxz_23 {\n img {\n background-color: rgb(59, 89, 152);\n }\n }\n
.custom_widget_Social_Sharing_social-share-x_c7xxz_28 {\n img {\n background-color: rgb(0, 0, 0);\n }\n }\n
.custom_widget_Social_Sharing_social-share-rss_c7xxz_33 {\n img {\n background-color: rgb(0, 0, 0);\n }\n }\n
.custom_widget_Social_Sharing_social-share-reddit_c7xxz_38 {\n img {\n background-color: rgb(255, 69, 0);\n }\n }\n
.custom_widget_Social_Sharing_social-share-email_c7xxz_43 {\n img {\n background-color: rgb(132, 132, 132);\n }\n }\n a {\n img {\n
height: 2rem;\n }\n }\n }\n }\n }\n }","tokens":{"social-share":"custom_widget_Social_Sharing_social-share_c7xxz_1","sharing-
options":"custom_widget_Social_Sharing_sharing-options_c7xxz_2","social-share-linkedin":"custom_widget_Social_Sharing_social-
share-linkedin_c7xxz_18","social-share-facebook":"custom_widget_Social_Sharing_social-share-facebook_c7xxz_23","social-share-
x":"custom_widget_Social_Sharing_social-share-x_c7xxz_28","social-share-rss":"custom_widget_Social_Sharing_social-share-
rss_c7xxz_33","social-share-reddit":"custom_widget_Social_Sharing_social-share-reddit_c7xxz_38","social-share-

```


list": "custom_widget_MicrosoftFooter_c-list_f95yq_78", "f-bare": "custom_widget_MicrosoftFooter_f-bare_f95yq_78", "c-uhff-base": "custom_widget_MicrosoftFooter_c-uhff-base_f95yq_94", "c-uhff-ccpa": "custom_widget_MicrosoftFooter_c-uhff-ccpa_f95yq_107"}}, {"form": null, "localOverride": false}, {"CachedAsset": {"text": "en_US-components/community/Breadcrumb-1731977288000": {"__typename": "CachedAsset", "id": "text:en_US-components/community/Breadcrumb-1731977288000", "value": {"navLabel": "Breadcrumbs", "dropdown": "Additional parent page navigation"}, "localOverride": false}, {"CachedAsset": {"text": "en_US-components/messages/MessageBanner-1731977288000": {"__typename": "CachedAsset", "id": "text:en_US-components/messages/MessageBanner-1731977288000", "value": {"messageMarkedAsSpam": "This post has been marked as spam", "messageMarkedAsSpam@board:TKB": "This article has been marked as spam", "messageMarkedAsSpam@board:BLOG": "This post has been marked as spam", "messageMarkedAsSpam@board:FORUM": "This discussion has been marked as spam", "messageMarkedAsSpam@board:OCCASION": "This event has been marked as spam", "messageMarkedAsSpam@board:IDEA": "This idea has been marked as spam", "manageSpam": "Manage Spam", "messageMarkedAsAbuse": "This post has been marked as abuse", "messageMarkedAsAbuse@board:TKB": "This article has been marked as abuse", "messageMarkedAsAbuse@board:BLOG": "This post has been marked as abuse", "messageMarkedAsAbuse@board:FORUM": "This discussion has been marked as abuse", "messageMarkedAsAbuse@board:OCCASION": "This event has been marked as abuse", "messageMarkedAsAbuse@board:IDEA": "This idea has been marked as abuse", "preModCommentAuthorText": "This comment will be published as soon as it is approved", "preModCommentModeratorText": "This comment is awaiting moderation", "messageMarkedAsOther": "This post has been rejected due to other reasons", "messageMarkedAsOther@board:TKB": "This article has been rejected due to other reasons", "messageMarkedAsOther@board:BLOG": "This post has been rejected due to other reasons", "messageMarkedAsOther@board:FORUM": "This discussion has been rejected due to other reasons", "messageMarkedAsOther@board:OCCASION": "This event has been rejected due to other reasons", "messageMarkedAsOther@board:IDEA": "This idea has been rejected due to other reasons"}, "localOverride": false}, {"CachedAsset": {"text": "en_US-components/messages/MessageView/MessageViewStandard-1731977288000": {"__typename": "CachedAsset", "id": "text:en_US-components/messages/MessageView/MessageViewStandard-1731977288000", "value": {"anonymus": "Anonymous", "author": "{messageAuthorLogin}", "authorBy": "{messageAuthorLogin}", "board": "{messageBoardTitle}", "replyToUser": "to {parentAuthor}", "showMoreReplies": "Show More", "replyText": "Reply", "repliesText": "Replies", "markedAsSolved": "Marked as Solved", "movedMessagePlaceholder.BLOG": "{count, plural, =0 {This comment has been} other {These comments have been}}", "movedMessagePlaceholder.TKB": "{count, plural, =0 {This comment has been} other {These comments have been}}", "movedMessagePlaceholder.FORUM": "{count, plural, =0 {This reply has been} other {These replies have been}}", "movedMessagePlaceholder.IDEA": "{count, plural, =0 {This comment has been} other {These comments have been}}", "movedMessagePlaceholder.OCCASION": "{count, plural, =0 {This comment has been} other {These comments have been}}", "movedMessagePlaceholder.UrlText": "moved.", "messageStatus": "Status: ", "statusChanged": "Status changed: {previousStatus} to {currentStatus}", "statusAdded": "Status added: {status}", "statusRemoved": "Status removed: {status}", "labelExpand": "expand replies", "labelCollapse": "collapse replies", "unhelpfulReason.reason1": "Content is outdated", "unhelpfulReason.reason2": "Article is missing information", "unhelpfulReason.reason3": "Content is for a different Product", "unhelpfulReason.reason4": "Doesn't match what I was searching for"}, "localOverride": false}, {"CachedAsset": {"text": "en_US-components/messages/MessageReplyCallToAction-1731977288000": {"__typename": "CachedAsset", "id": "text:en_US-components/messages/MessageReplyCallToAction-1731977288000", "value": {"leaveReply": "Leave a reply...", "leaveReply@board:BLOG@message:root": "Leave a comment...", "leaveReply@board:TKB@message:root": "Leave a comment...", "leaveReply@board:IDEA@message:root": "Leave a comment...", "leaveReply@board:OCCASION@message:root": "Leave a comment...", "repliesTurnedOff.FORUM": "Replies are turned off for this topic", "repliesTurnedOff.BLOG": "Comments are turned off for this topic", "repliesTurnedOff.TKB": "Comments are turned off for this topic", "repliesTurnedOff.IDEA": "Comments are turned off for this topic", "repliesTurnedOff.OCCASION": "Comments are turned off for this topic", "infoText": "Stop poking me!"}, "localOverride": false}, {"Category: {"category": "Exchange": {"__typename": "Category", "id": "category:Exchange", "categoryPolicies": {"__typename": "CategoryPolicies", "canReadNode": {"__typename": "PolicyResult", "failureReason": null}}, "Category: {"category": "Planner": {"__typename": "Category", "id": "category:Planner", "categoryPolicies": {"__typename": "CategoryPolicies", "canReadNode": {"__typename": "PolicyResult", "failureReason": null}}, "Category: {"category": "Outlook": {"__typename": "Category", "id": "category:Outlook", "categoryPolicies": {"__typename": "CategoryPolicies", "canReadNode": {"__typename": "PolicyResult", "failureReason": null}}, "Category: {"category": "Community-Info-Center": {"__typename": "Category", "id": "category:Community-Info-Center", "categoryPolicies": {"__typename": "CategoryPolicies", "canReadNode": {"__typename": "PolicyResult", "failureReason": null}}, "Category: {"category": "EducationSector": {"__typename": "Category", "id": "category:EducationSector", "categoryPolicies": {"__typename": "CategoryPolicies", "canReadNode": {"__typename": "PolicyResult", "failureReason": null}}, "Category: {"category": "DrivingAdoption": {"__typename": "Category", "id": "category:DrivingAdoption", "categoryPolicies": {"__typename": "CategoryPolicies", "canReadNode": {"__typename": "PolicyResult", "failureReason": null}}, "Category: {"category": "Azure": {"__typename": "Category", "id": "category:Azure", "categoryPolicies": {"__typename": "CategoryPolicies", "canReadNode": {"__typename": "PolicyResult", "failureReason": null}}, "Category: {"category": "Windows-Server": {"__typename": "Category", "id": "category:Windows-Server", "categoryPolicies": {"__typename": "CategoryPolicies", "canReadNode": {"__typename": "PolicyResult", "failureReason": null}}, "Category: {"category": "SQL-Server": {"__typename": "Category", "id": "category:SQL-Server", "categoryPolicies": {"__typename": "CategoryPolicies", "canReadNode": {"__typename": "PolicyResult", "failureReason": null}}, "Category: {"category": "MicrosoftTeams": {"__typename": "Category", "id": "category:MicrosoftTeams", "categoryPolicies": {"__typename": "CategoryPolicies", "canReadNode": {"__typename": "PolicyResult", "failureReason": null}}, "Category: {"category": "PublicSector": {"__typename": "Category", "id": "category:PublicSector", "categoryPolicies": {"__typename": "CategoryPolicies", "canReadNode": {"__typename": "PolicyResult", "failureReason": null}}, "Category: {"category": "microsoft365": {"__typename": "Category", "id": "category:microsoft365", "categoryPolicies": {"__typename": "CategoryPolicies", "canReadNode": {"__typename": "PolicyResult", "failureReason": null}}, "Category: {"category": "IoT": {"__typename": "Category", "id": "category:IoT", "categoryPolicies": {"__typename": "CategoryPolicies", "canReadNode": {"__typename": "PolicyResult", "failureReason": null}}}

```

{"__typename":"Category","id":"category:IoT","categoryPolicies":{"__typename":"CategoryPolicies","canReadNode":
{"__typename":"PolicyResult","failureReason":null}},"Category:category:HealthcareAndLifeSciences":
{"__typename":"Category","id":"category:HealthcareAndLifeSciences","categoryPolicies":
{"__typename":"CategoryPolicies","canReadNode":{"__typename":"PolicyResult","failureReason":null}},"Category:category:SMB":
{"__typename":"Category","id":"category:SMB","categoryPolicies":{"__typename":"CategoryPolicies","canReadNode":
{"__typename":"PolicyResult","failureReason":null}},"Category:category:ITOpsTalk":
{"__typename":"Category","id":"category:ITOpsTalk","categoryPolicies":{"__typename":"CategoryPolicies","canReadNode":
{"__typename":"PolicyResult","failureReason":null}},"Category:category:microsoft-endpoint-manager":
{"__typename":"Category","id":"category:microsoft-endpoint-manager","categoryPolicies":
{"__typename":"CategoryPolicies","canReadNode":
{"__typename":"PolicyResult","failureReason":null}},"Category:category:MicrosoftLearn":
{"__typename":"Category","id":"category:MicrosoftLearn","categoryPolicies":{"__typename":"CategoryPolicies","canReadNode":
{"__typename":"PolicyResult","failureReason":null}},"Blog:board:MicrosoftLearnBlog":
{"__typename":"Blog","id":"board:MicrosoftLearnBlog","blogPolicies":{"__typename":"BlogPolicies","canReadNode":
{"__typename":"PolicyResult","failureReason":null}},"boardPolicies":{"__typename":"BoardPolicies","canReadNode":
{"__typename":"PolicyResult","failureReason":null}},"Category:category:AI":
{"__typename":"Category","id":"category:AI","categoryPolicies":{"__typename":"CategoryPolicies","canReadNode":
{"__typename":"PolicyResult","failureReason":null}},"Category:category:MicrosoftMechanics":
{"__typename":"Category","id":"category:MicrosoftMechanics","categoryPolicies":{"__typename":"CategoryPolicies","canReadNode":
{"__typename":"PolicyResult","failureReason":null}},"Category:category:StartupsatMicrosoft":
{"__typename":"Category","id":"category:StartupsatMicrosoft","categoryPolicies":{"__typename":"CategoryPolicies","canReadNode":
{"__typename":"PolicyResult","failureReason":null}},"Category:category:PartnerCommunity":
{"__typename":"Category","id":"category:PartnerCommunity","categoryPolicies":{"__typename":"CategoryPolicies","canReadNode":
{"__typename":"PolicyResult","failureReason":null}},"Category:category:Windows":
{"__typename":"Category","id":"category:Windows","categoryPolicies":{"__typename":"CategoryPolicies","canReadNode":
{"__typename":"PolicyResult","failureReason":null}},"CachedAsset:text:en_US-components/community/Navbar-1731977288000":
{"__typename":"CachedAsset","id":"text:en_US-components/community/Navbar-1731977288000","value":{"community":{"Community
Home","inbox":"Inbox","manageContent":"Manage Content","tos":"Terms of Service","forgotPassword":"Forgot
Password","themeEditor":"Theme Editor","edit":"Edit Navigation Bar","skipContent":"Skip to content","gxcuf89792":"Tech
Community","external-1":"Events","s-m-b":"Small and Medium Businesses","windows-server":"Windows Server","education-
sector":"Education Sector","driving-adoption":"Driving Adoption","microsoft-learn":"Microsoft Learn","s-q-l-server":"SQL Server","partner-
community":"Microsoft Partner Community","microsoft365":"Microsoft 365","external-9":".NET","external-8":"Teams","external-
7":"Github","products-services":"Products","external-6":"Power Platform","communities-1":"Topics","external-5":"Security, Compliance &
Identity","planner":"Planner","external-4":"Microsoft 365","external-3":"Dynamics 365","azure":"Azure","healthcare-and-life-
sciences":"Healthcare and Life Sciences","external-2":"Azure","microsoft-mechanics":"Microsoft Mechanics","microsoft-learn-
1":"Community","external-10":"Learning Room Directory","microsoft-learn-blog":"Blog","windows":"Windows","i-t-ops-talk":"ITOps
Talk","external-link-1":"View All","microsoft-securityand-compliance":"Security, Compliance, and Identity","public-sector":"Public
Sector","community-info-center":"Lounge","external-link-2":"View All","microsoft-teams":"Microsoft Teams","external":"Blogs","microsoft-
endpoint-manager":"Microsoft Intune and Configuration Manager","startupsat-microsoft":"Startups at
Microsoft","exchange":"Exchange","a-i":"AI and Machine Learning","io-t":"Internet of Things (IoT)","outlook":"Outlook","external-
link":"Community Hubs","communities":"Products"},"localOverride":false},"CachedAsset:text:en_US-
components/community/NavbarHamburgerDropdown-1731977288000":{"__typename":"CachedAsset","id":"text:en_US-
components/community/NavbarHamburgerDropdown-1731977288000","value":{"hamburgerLabel":"Side
Menu"},"localOverride":false},"CachedAsset:text:en_US-components/community/BrandLogo-1731977288000":
{"__typename":"CachedAsset","id":"text:en_US-components/community/BrandLogo-1731977288000","value":
{"logoAlt":"Khoros","themeLogoAlt":"Brand Logo"},"localOverride":false},"CachedAsset:text:en_US-
components/community/NavbarTextLinks-1731977288000":{"__typename":"CachedAsset","id":"text:en_US-
components/community/NavbarTextLinks-1731977288000","value":{"more":"More"},"localOverride":false},"CachedAsset:text:en_US-
components/authentication/AuthenticationLink-1731977288000":{"__typename":"CachedAsset","id":"text:en_US-
components/authentication/AuthenticationLink-1731977288000","value":{"title.login":"Sign
In","title.registration":"Register","title.forgotPassword":"Forgot Password","title.multiAuthLogin":"Sign
In"},"localOverride":false},"CachedAsset:text:en_US-components/nodes/NodeLink-1731977288000":
{"__typename":"CachedAsset","id":"text:en_US-components/nodes/NodeLink-1731977288000","value":{"place":"Place
{name}}","localOverride":false},"CachedAsset:text:en_US-components/messages/MessageCoverImage-1731977288000":
{"__typename":"CachedAsset","id":"text:en_US-components/messages/MessageCoverImage-1731977288000","value":
{"coverImageTitle":"Cover Image"},"localOverride":false},"CachedAsset:text:en_US-shared/client/components/nodes/NodeTitle-
1731977288000":{"__typename":"CachedAsset","id":"text:en_US-shared/client/components/nodes/NodeTitle-1731977288000","value":
{"nodeTitle":{"nodeTitle, select, community {Community} other {{nodeTitle}}}"},"localOverride":false},"CachedAsset:text:en_US-
components/messages/MessageTimeToRead-1731977288000":{"__typename":"CachedAsset","id":"text:en_US-
components/messages/MessageTimeToRead-1731977288000","value":{"minReadText":{"min} MIN
READ"},"localOverride":false},"CachedAsset:text:en_US-components/messages/MessageSubject-1731977288000":
{"__typename":"CachedAsset","id":"text:en_US-components/messages/MessageSubject-1731977288000","value":{"noSubject":{"no
subject}}","localOverride":false},"CachedAsset:text:en_US-components/users/UserLink-1731977288000":
{"__typename":"CachedAsset","id":"text:en_US-components/users/UserLink-1731977288000","value":{"authorName":"View Profile:
{author},"anonymous":"Anonymous"},"localOverride":false},"CachedAsset:text:en_US-shared/client/components/users/UserRank-
1731977288000":{"__typename":"CachedAsset","id":"text:en_US-shared/client/components/users/UserRank-1731977288000","value":
{"rankName":{"rankName},"userRank":"Author rank {rankName}}","localOverride":false},"CachedAsset:text:en_US-

```

```
components/messages/MessageTime-1731977288000":{"__typename":"CachedAsset","id":"text:en_US-
components/messages/MessageTime-1731977288000","value":{"postTime":"Published: {time}","lastPublishTime":"Last Update:
{time}","conversation.lastPostingActivityTime":"Last posting activity time: {time}","conversation.lastPostTime":"Last post time:
{time}","moderationData.rejectTime":"Rejected time: {time}"},"localOverride":false},"CachedAsset:text:en_US-
components/messages/MessageBody-1731977288000":{"__typename":"CachedAsset","id":"text:en_US-
components/messages/MessageBody-1731977288000","value":{"showMessageBody":"Show More","mentionsErrorTitle":{"mentionsType,
select, board {Board} user {User} message {Message} other {} No Longer Available"},"mentionsErrorMessage":"The {mentionsType} you
are trying to view has been removed from the community.","videoProcessing":"Video is being processed. Please try again in a few
minutes"},"bannerTitle":"Video provider requires cookies to play the video. Accept to continue or {url} it directly on the provider's
site"},"buttonTitle":"Accept","urlText":"watch"},"localOverride":false},"CachedAsset:text:en_US-
components/messages/MessageCustomFields-1731977288000":{"__typename":"CachedAsset","id":"text:en_US-
components/messages/MessageCustomFields-1731977288000","value":{"CustomField.default.label":{"Value of
{name}}"},"localOverride":false},"CachedAsset:text:en_US-components/messages/MessageRevision-1731977288000":
{"__typename":"CachedAsset","id":"text:en_US-components/messages/MessageRevision-1731977288000","value":
{"lastUpdatedDatePublished":{"publishCount, plural, one{Published} other{Updated}} {date}","lastUpdatedDateDraft":"Created
{date}","version":"Version {major}.{minor}}"},"localOverride":false},"CachedAsset:text:en_US-
shared/client/components/common/QueryHandler-1731977288000":{"__typename":"CachedAsset","id":"text:en_US-
shared/client/components/common/QueryHandler-1731977288000","value":{"title":"Query
Handler"},"localOverride":false},"CachedAsset:text:en_US-components/messages/MessageReplyButton-1731977288000":
{"__typename":"CachedAsset","id":"text:en_US-components/messages/MessageReplyButton-1731977288000","value":{"repliesCount":
{count}},"title":"Reply","title@board:BLOG@message:root":"Comment","title@board:TKB@message:root":"Comment","title@board:IDEA@me
components/messages/MessageAuthorBio-1731977288000":{"__typename":"CachedAsset","id":"text:en_US-
components/messages/MessageAuthorBio-1731977288000","value":{"sendMessage":"Send Message","actionMessage":"Follow this blog
board to get notified when there's new activity","coAuthor":"CO-PUBLISHER","contributor":"CONTRIBUTOR","userProfile":"View
Profile","iconlink":"Go to {name} {type}}"},"localOverride":false},"CachedAsset:text:en_US-
components/customComponent/CustomComponent-1731977288000":{"__typename":"CachedAsset","id":"text:en_US-
components/customComponent/CustomComponent-1731977288000","value":{"errorMessage":"Error rendering component id:
{customComponentId},"bannerTitle":"Video provider requires cookies to play the video. Accept to continue or {url} it directly on the
provider's site"},"buttonTitle":"Accept","urlText":"watch"},"localOverride":false},"CachedAsset:text:en_US-
components/community/NavbarDropdownToggle-1731977288000":{"__typename":"CachedAsset","id":"text:en_US-
components/community/NavbarDropdownToggle-1731977288000","value":{"ariaLabelClosed":"Press the down arrow to open the
menu"},"localOverride":false},"CachedAsset:text:en_US-shared/client/components/users/UserAvatar-1731977288000":
{"__typename":"CachedAsset","id":"text:en_US-shared/client/components/users/UserAvatar-1731977288000","value":{"altText":{"login}'s
avatar","altTextGeneric":"User's avatar"},"localOverride":false},"CachedAsset:text:en_US-
shared/client/components/ranks/UserRankLabel-1731977288000":{"__typename":"CachedAsset","id":"text:en_US-
shared/client/components/ranks/UserRankLabel-1731977288000","value":{"altTitle":"Icon for {rankName}
rank"},"localOverride":false},"CachedAsset:text:en_US-components/users/UserRegistrationDate-1731977288000":
{"__typename":"CachedAsset","id":"text:en_US-components/users/UserRegistrationDate-1731977288000","value":{"noPrefix":
{date},"withPrefix":"Joined {date}}"},"localOverride":false},"CachedAsset:text:en_US-shared/client/components/nodes/NodeAvatar-
1731977288000":{"__typename":"CachedAsset","id":"text:en_US-shared/client/components/nodes/NodeAvatar-1731977288000","value":
{"altTitle":"Node avatar for {nodeTitle}}"},"localOverride":false},"CachedAsset:text:en_US-
shared/client/components/nodes/NodeDescription-1731977288000":{"__typename":"CachedAsset","id":"text:en_US-
shared/client/components/nodes/NodeDescription-1731977288000","value":{"description":
{description}}},"localOverride":false},"CachedAsset:text:en_US-components/tags/TagView/TagViewChip-1731977288000":
{"__typename":"CachedAsset","id":"text:en_US-components/tags/TagView/TagViewChip-1731977288000","value":{"tagLabelName":"Tag
name {tagName}}"},"localOverride":false},"CachedAsset:text:en_US-shared/client/components/nodes/NodeIcon-1731977288000":
{"__typename":"CachedAsset","id":"text:en_US-shared/client/components/nodes/NodeIcon-1731977288000","value":
{"contentType":"Content Type {style, select, FORUM {Forum} BLOG {Blog} TKB {Knowledge Base} IDEA {Ideas} OCCASION {Events}
other {} icon"},"localOverride":false}}},"page":"/blogs/BlogMessagePage/BlogMessagePage","query":
{"boardId":"coreinfrastructureandsecurityblog","messageSubject":"protecting-tier-0-the-modern-
way","messageId":"4052851"},"buildId":"E37e9rqmzENIUrf3G1YvE","runtimeConfig":
{"buildInformationVisible":false,"logLevelApp":"info","logLevelMetrics":"info","openTelemetryClientEnabled":false,"openTelemetryConfigName":
auth-idp","apolloDevToolsEnabled":false,"isFallback":false,"isExperimentalCompile":false,"dynamicIds":
["./components/community/Navbar/NavbarWidget.tsx","./components/community/Breadcrumb/BreadcrumbWidget.tsx","./components/customC
{"id":"analytics","src":"https://techcommunity.microsoft.com/t5/s/gxcuf89792/pagescripts/1729284608000/analytics.js?
page.id=BlogMessagePage&entity.id=board%3ACoreinfrastructureandsecurityblog&entity.id=message%3A4052851","strategy":"afterInteractiv
Protecting Tier 0 the Modern Way | Microsoft Community Hub
```