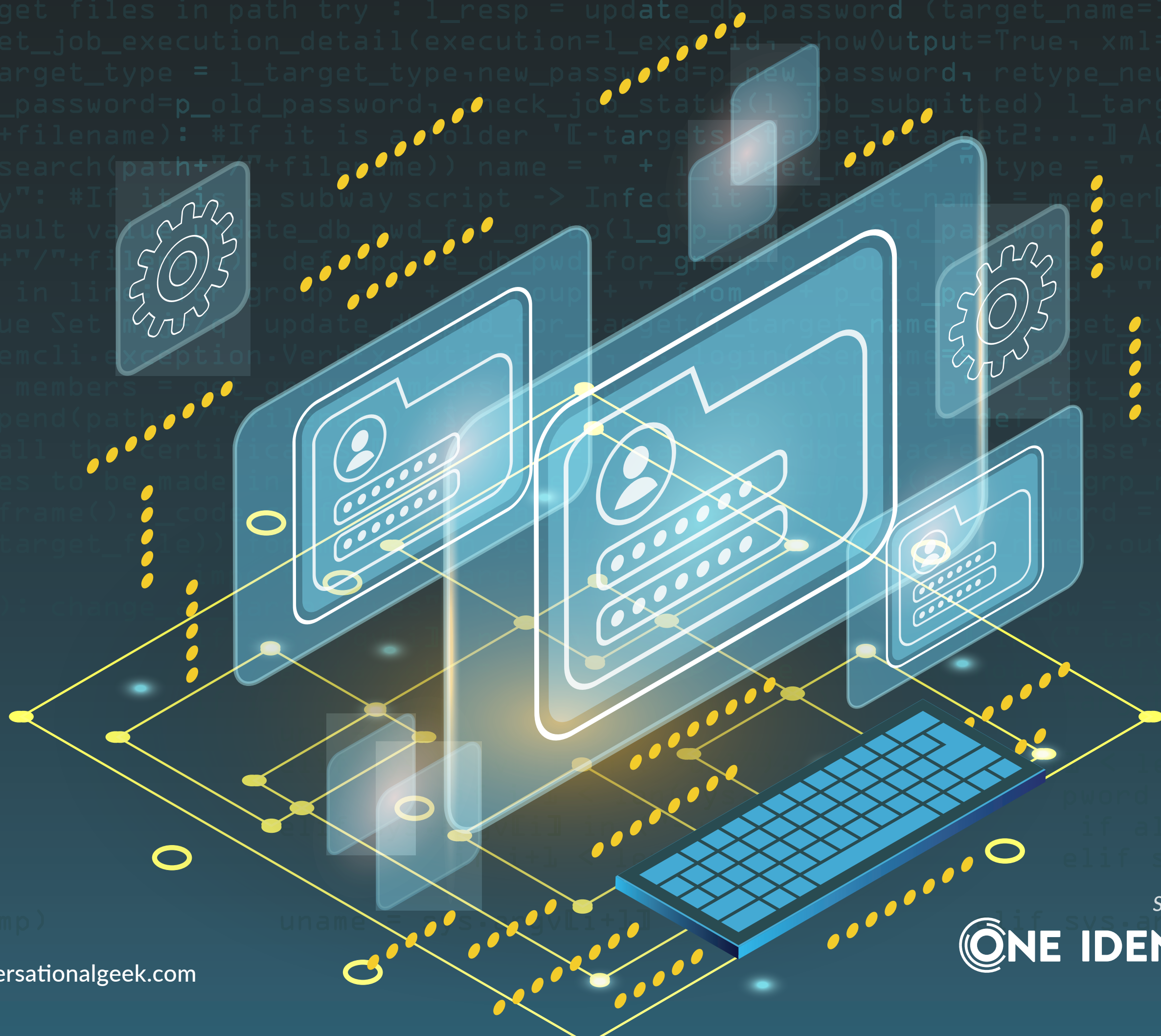
ConversationalGeek®

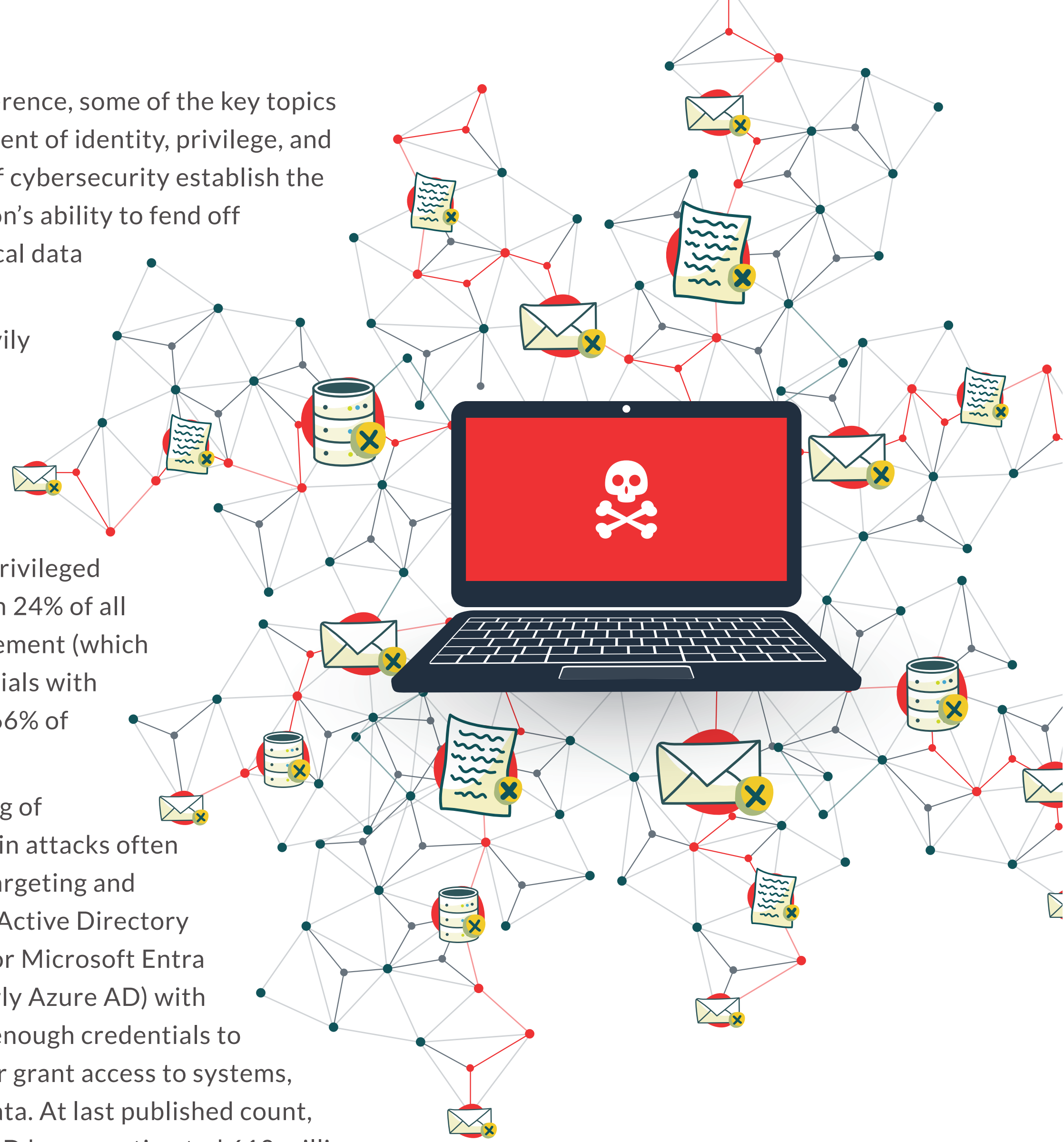
Solving the 3 MOST IMPACTFUL AD *and* Entra ID Group Management Challenges



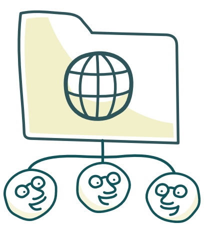
Sponsored by ONE IDENTITY by Quest

www.conversationalgeek.com

At a recent Gartner IAM conference, some of the key topics revolved around the management of identity, privilege, and access. These core elements of cybersecurity establish the foundation of your organization's ability to fend off cyberattacks and protect critical data from being misused.



Today's cyberattacks rely heavily on an attacker's ability to gain privileged access beyond that of a low-level user. Tactics like *privilege elevation* and *lateral movement* are critical aspects of every attack, with privileged elevation estimated to occur in 24% of all cyberattacks[1] and lateral movement (which requires some form of credentials with elevated access) occurring in 66% of ransomware attacks[2].



The gaining of privileges in attacks often involves targeting and accessing Active Directory (AD) and/or Microsoft Entra ID (formerly Azure AD) with elevated-enough credentials to modify the directory to further grant access to systems, resources, applications, and data. At last published count, according to Microsoft, Entra ID has an estimated 610 million monthly users worldwide[3]. And with on-premises AD remaining the world's primary directory service, many of the organizations relying on Entra ID do so by synchronizing it with their on-premises AD in a hybrid environment. Add to this Entra ID's support for AWS and Google Workspace, and you quickly realize that a single misconfigured privilege can potentially provide a threat actor with access to many parts of your computing environment.

The foundation for AD and Entra ID providing privileged access to resources – whether on-premises or in the cloud – is *groups*. Whether we're talking about some level of administrative rights to the entire environment, or to virtualization platforms, applications, data, or other cloud resources, achieving a known-secure state of identity, privilege, and access within AD and Entra ID comes down to the practical management of the groups that exist within those environments.

But the reality of today is that, despite IT and Security teams clearly understanding the role groups play within the process of providing access to resources, in many organizations the management of groups remains at the lowest priority level, making groups a very real security risk.

[1] Reliaquest, *Annual Cyberthreat Report* (2024)
[2] Coveware, *Quarterly Ransomware Reports* (1Q 2024)
[3] Microsoft, Q4 2023 Earnings Call

Why are Groups A PROBLEM?

Looking past the administrative entropy that, no doubt, exists within countless groups across every organization, groups create a single, serious problem – *overpermissioned users*.

In essence, the end result is users have too much access to resources they shouldn't because IT doesn't have a handle on what the actual security impact will be by doing something as simple as adding a user to a group, nesting a group, or assigning permissions to a group.

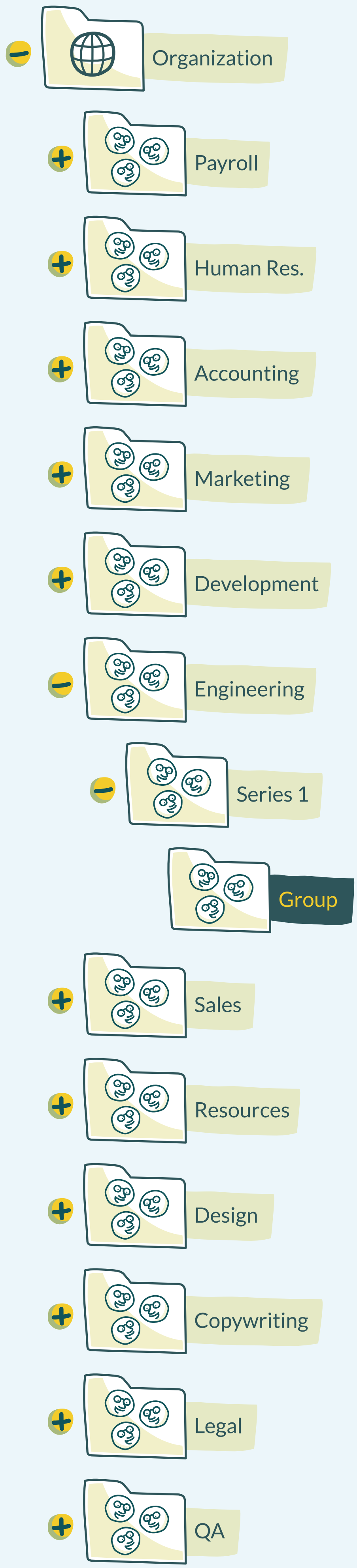
And all this comes at a time when organizations are focused on removing standing permissions, establishing Zero Trust models, and implementing an identity fabric approach to security – all to stop threat actors from taking advantage of any and all elevated privileges during a cyberattack. In essence, the organization is so focused on the larger initiatives, the lack of attention paid to the simple act of properly securing groups benefits the attacker.

Add to this the fact that cyber insurers are quickly becoming savvy to the fact that privileged access (something granted by group membership) is the most critical factor in a cyberattack (that is, "*no privileged access, no successful cyberattack*"). In response, they are improving their list of requirements around identity and privileged access, ensuring that potential insured organizations have a tight grip on how permissions are assigned and who gets them – all in the name of minimizing the risk of a successful cyberattack that could result in a claim against an issued policy.

But groups come with their own challenges...

What are the Group CHALLENGES?

But groups come with their own challenges – some created by the nature of the functionality of groups and some created by human nature and our lack of forward thinking that results in anything but a secure state of identity, privilege, and access. In this eBook, we'll take a look at three specific group management challenges – *Group Glut, Harnessing Nested Groups, and Permission Elevation and Permission Creep* – and help you to understand why these problems exist and how to address them. Let's first take a look at each of the challenges, and then see how to solve these issues in one motion.



Challenge 1 - Group Glut

Organizations have been creating groups without oversight to provide access to resources for the past 24 years (since AD's inception). It's probably safe to guess that every organization has *at least* one group that no one is exactly sure why it exists, nor the reasons for its specific group membership.

Multiply this by as many as 24 years that your organization has been running AD. Then add in the fact that you now sync with Entra ID – which adds on even more groups of its own and others specifically to grant permissions to cloud-based resources – and you come to quickly realize there are a ton of groups that IT has little-to-no insight into why they exist, why members exist within the group, and how the groups are used.

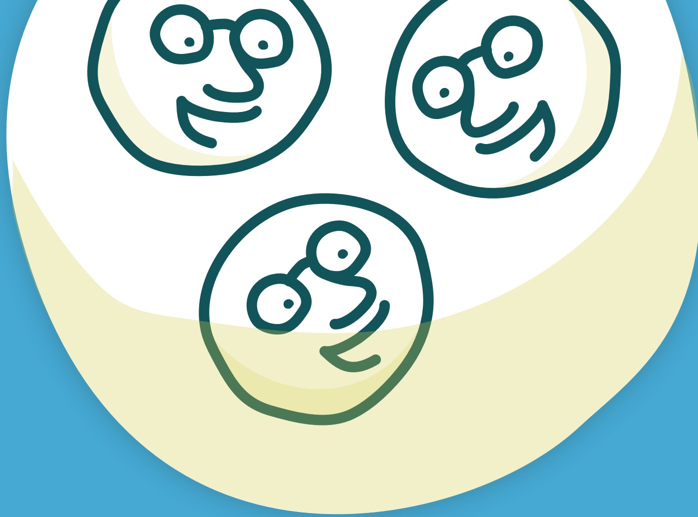
Why Does Group Glut Exist?

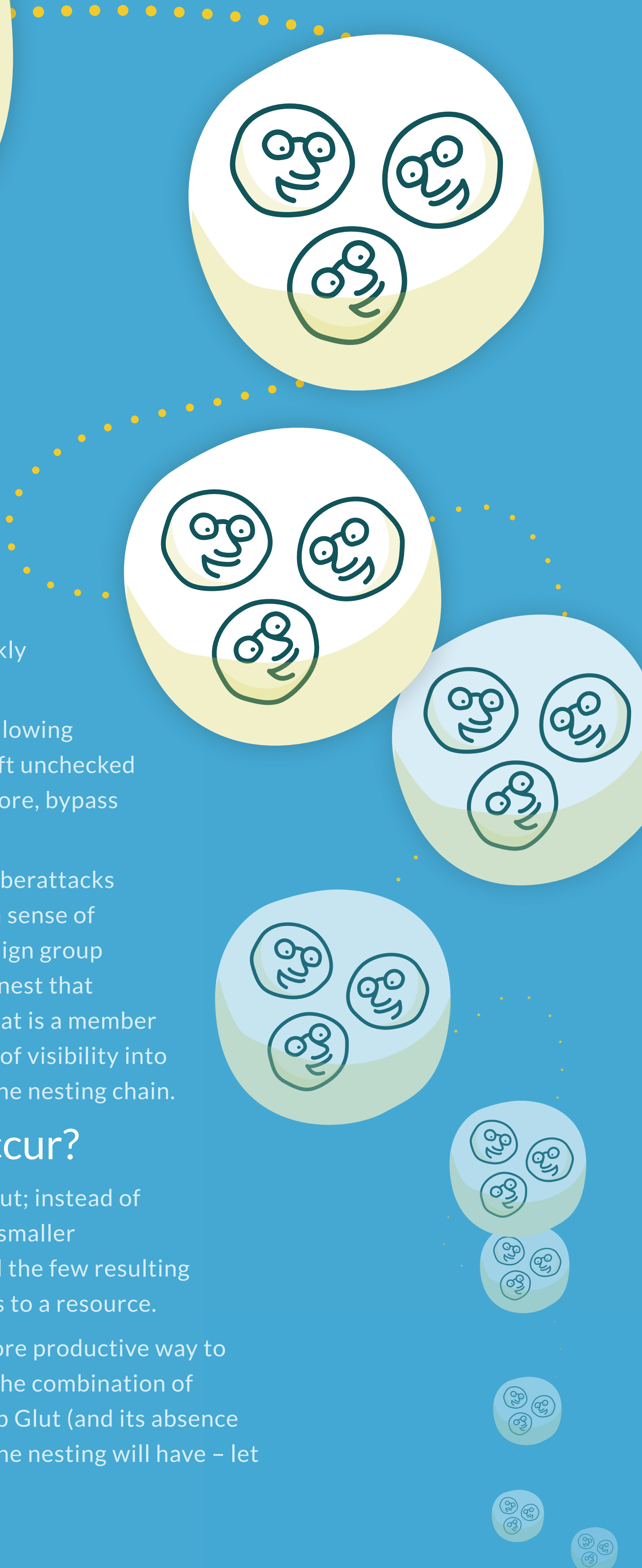
It's simple – IT is right on top of a request for a new group to provide access to some new application, data store, or other resource. But, as it always happens, attention is taken quickly away and placed on the next big initiative or fire to be put out. Eventually, the months pass, staffing changes over time, and with no documentation as to why that group was created years ago, no one has the proper context to make a decision around what to do about the group.

NAME	TYPE
en-Dale	Security Group
en-Kate	Security Group
en-Tom	Security Group
en-Dave	Security Group
en-Staff	Security Group
en-Sam	Security Group
en-Bethany	Security Group
en-Zack	Security Group

One of the aspects of this particular challenge is that age-old issue of the permissions assigned to a group not being stored (or at least documented) within the directory (be it AD or Entra ID). Think about it – it would help a lot if, years after a group's creation, you could see, say, the UNC share or the web application the group is assigned permissions to; it would likely provide just enough context to help decide whether the group is needed any longer or not.

In short, there's no formal group lifecycle management that includes change management (to document the creation of groups, adding of members, and assignment of permissions) and formal periodic group attestation (to verify a group is still needed, its membership is correct, and its assigned permissions are correct).





Challenge 2 - Harnessing Nested Groups

The idea of nesting groups empowers the creation of permission hierarchies; it's not uncommon for organizations to have several levels of nesting to facilitate the establishment of roles and subsequent granting of access quickly and consistently.

But it's not all goodness that nesting brings. The very idea of allowing multiple groups to exist as members of other groups – when left unchecked – can create unforeseen permission inheritance (which, therefore, bypass security controls) which leads to overpermissioning of users.

Additionally, threat actors take advantage of nesting during cyberattacks as a means of establishing persistence while also maintaining a sense of stealth. For example, a threat actor can create a seemingly benign group with an equally benign user as its only member. They can then nest that group in a second benign group that is nested within a third, that is a member of Domain Admins. This repeated use of nesting creates a lack of visibility into exactly which users are granted permissions anywhere along the nesting chain.

Why Does Unsanctioned Nesting Occur?

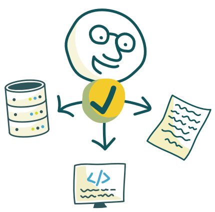
Nesting was designed to be a response to addressing Group Glut; instead of having countless members in a single group, let's organize the smaller sub-groupings of users into their own groups and then just add the few resulting groups into the initial group that has been granted permissions to a resource.

In and of itself, it's not a bad thing; nesting can actually be a more productive way to get the right people the right access to needed resources. It's the combination of leveraging nested groups with the previously mentioned Group Glut (and its absence of oversight) that results in a lack of visibility into the impact the nesting will have – let alone the fact that the nesting exists in the first place.

Challenge 3 - Permission Elevation and Permission Creep

This last group challenge is the natural result of the first two – both Group Glut and Nested Groups, when done without thought given to how the changes today will impact the organization's security tomorrow, result in unnecessary and undesired *permission creep* and *permission elevation*.

You may be wondering if there's a difference – *there is*.



Permission creep is the gradual accumulation of access permissions beyond what a user needs over time. For example, a user in accounting who belongs to a group that has rights to access the accounting application is later granted rights to an Accounts Payable application because the four other people in the group use that app. Now the accounting user also has access to the AP application, even though it's not part of their role within the organization.

Permissions Elevation refers to the specific elevation of rights assigned to a user that grants them access to resources normally reserved for IT or a technical user. This could be the rights of a local administrator, access to manage some or all of the directory, a Domain Admin (for local AD), any of the built-in roles within Entra ID, and any other kind of access that could be deemed sensitive or critical to the organization.

Why Does Permissions Elevation and Creep Occur?

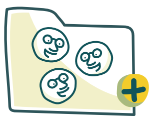
Like the previous two challenges, these unintended and unsanctioned increases in a user's permissions all come down to IT's lack of visibility into the impact a simple change to a group will have on a user's access.

Solving your Group Management Challenges

Each of these challenges exist because the management of groups isn't seen as something that impacts anything more than the immediate need to address a service desk ticket to give someone permissions to a resource. There needs to be a bit more forward thinking about how a group will be (and should be) used throughout its lifecycle – a ***Group Management Lifecycle***.

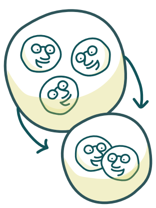
Whether this is accomplished manually, using Entra ID Permissions Management, or using a third-party solution, the idea is this: there needs to be a larger sense of vigilance around every aspect of group management with an understanding that a single change to a group can have tremendous impact on the organization's overall security.

At a minimum, a group management lifecycle should include the following:

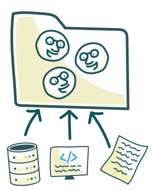


Group Creation – Is there another group that already exists that meets the need or is a new group warranted?

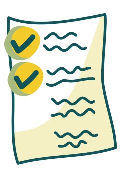
Group Owner – The group should have a designated person responsible for any changes that impact the group and its membership. This should be someone close to the usage of the permissions granted to the group like a department head, or line of business owner, rather than IT.



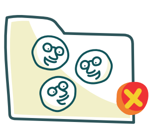
Membership Changes – There should be some established process (that may include requiring approval of changes from the group's Owner) when changes are made to a group's membership.



Permission Changes – The group's Owner should be involved in all assignments of permissions, with the changes detailed using some form of change management.

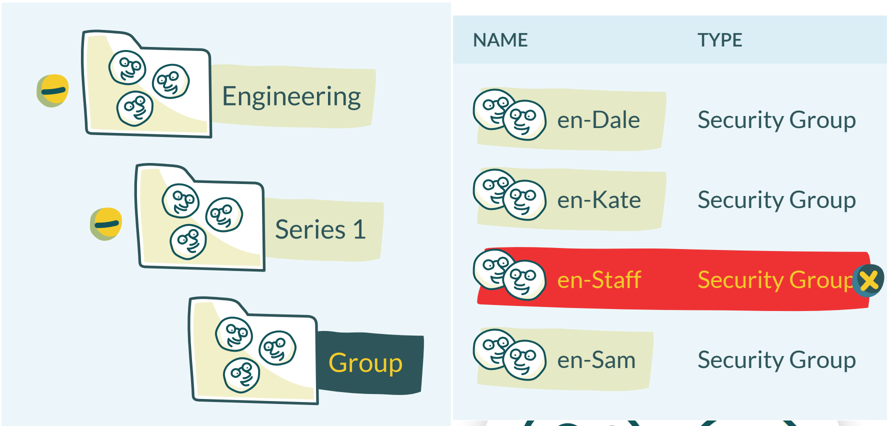


Attestation – Periodically (at least annually), each group's Owner should review and attest to the current state of the group, its membership, and assigned permissions. Should anything be amiss, it can be remediated to bring the group back into an approved state.

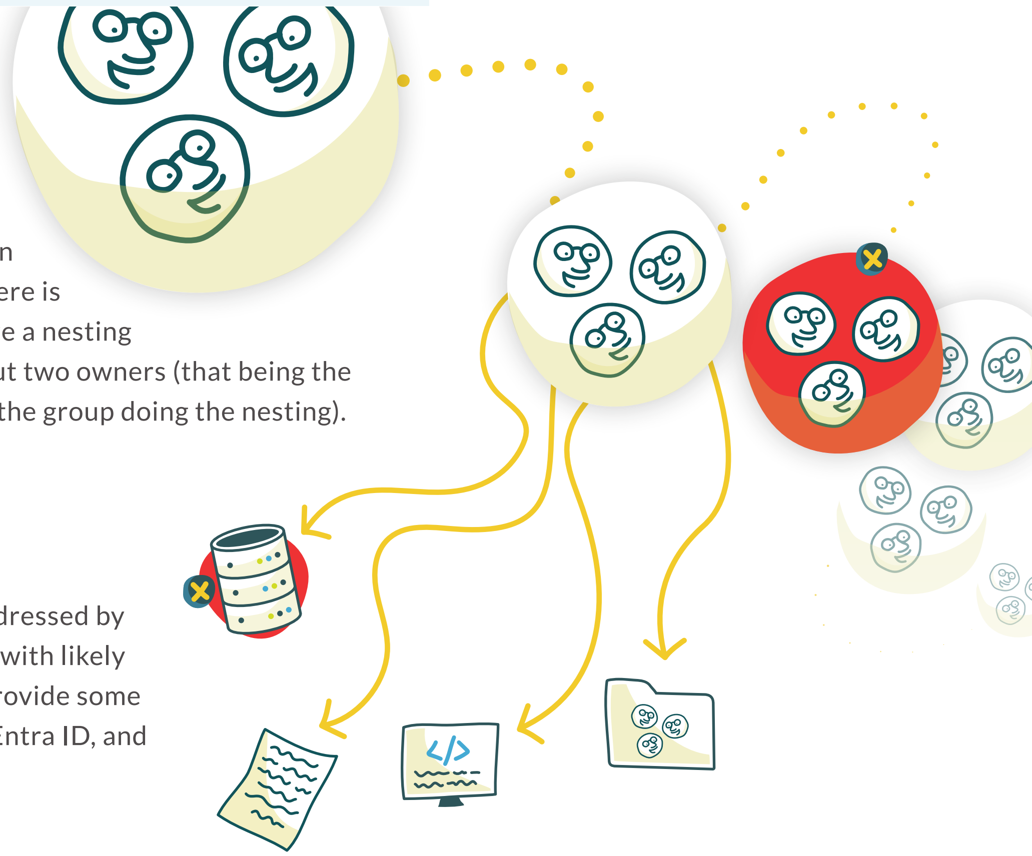


Group Deletion – Should the group be determined (during attestation) to no longer be of use, it should be deleted, with the deletion documented.

What Happens to Group Management Challenges?



Group Glut ceases to exist, as groups aren't haphazardly created, group Owners ensure only approved members exist, and once a group is no longer needed, it's deleted from the directory.



Nested Groups as a whole are no longer a problem, as each group within the nested chain has an owner and there is some workflow and approval to ensure a nesting change is approved by not just one, but two owners (that being the owner of the group being nested and the group doing the nesting).

Permission Elevation and Creep are addressed by getting a handle on the previous two, with likely reserved Ownership of groups that provide some level of administrative access to AD/Entra ID, and any other critical resources.

You begin this journey by acknowledging the risk that groups create to your organization's cybersecurity stance. In doing so, you find yourself also recognizing that the proper lack of lifecycle management of groups is to blame. The manifestations of group glut and over-nesting are only the result of a lack of policy, process, and oversight designed to ensure the use of groups isn't just about productivity, but also about maintaining a particular state of cybersecurity.

By putting a group management lifecycle in place – through both the use of carefully thought-out process and solutions designed to help implement and enforce those processes, your organization will improve its security stance, and establish a new security standard on which future delegation of privileges via groups will be measured against.

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Access Management (AM), Privileged Access Management (PAM) and Active Directory Management (AD Mgmt) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing more than 500-million-plus identities for more than 11,000 organizations worldwide.

For more information, visit: www.oneidentity.com/products/active-roles