Moving on from Active Directory Red Forest

semperis.com/blog/good-riddance-red-forest-understanding-microsofts-new-privileged-access-management-strategy

January 25, 2021

Darren Mar-Elia | VP of Products

As far back as 2012, Microsoft released the first version of its important “Mitigating Pass-the-Hash and Credential Theft” whitepapers. In this first version, Microsoft defined the problem of lateral movement and privilege escalation within a Windows Active Directory on-premises environment and included best practices for mitigating these kinds of attacks at the time. Two years later, Microsoft released version 2 of that document, which significantly increased the guidance based on the current state of Windows.
The company also introduced concepts such as Privileged Access Workstations (PAWs) and Admin Tiering (see figure below).

Admin Tiering as introduced in “Mitigating Pass-the-Hash and Other Credential Theft, version 2”

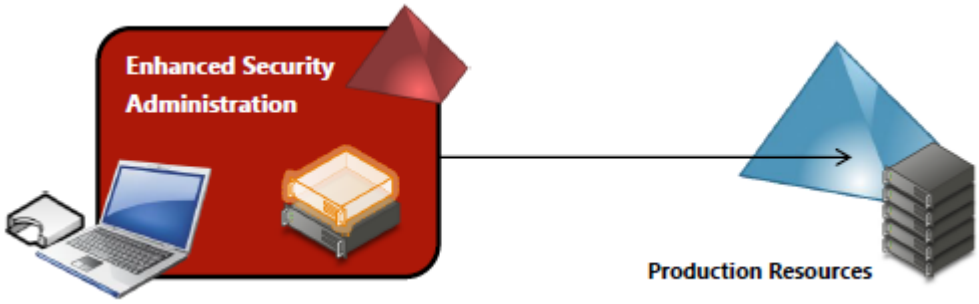
Admin Tiering introduced the concept of separating “areas of concern” when it came to administration. Admin accounts that managed AD and domain controllers could never log into regular workstations and servers. Server Admin accounts couldn’t log into domain controllers and workstations, etc. This approach limited the ability for lateral movement attacks to move up in privilege level. It wasn’t perfect, but it worked—
when implemented.

Related reading

Active Directory Security: Top Risks & Best Practices

Enter Red Forest

About 10 years ago, Microsoft built on the notion presented in these two "Mitigating Pass-the-Hash and Credential Theft" whitepapers by introducing the concept of a Red Forest, also known as Enhanced Security Admin Environment (ESAE). A Red Forest is basically a separate AD forest, trusted by your production AD forests, where all your administrative credentials would reside:



Enhanced Security Admin Environment (aka "Red Forest"), a separate AD forest that is trusted by production AD forests, where all administrative credentials reside

In principle, the Red Forest concept seemed like a good approach. Get your admin credentials out of the forest, where the potential attacker is roaming around, and ensure they only live securely in the separate Red Forest. In practice, the Red Forest was a clunky approach to the problem. Many management tools work poorly—or not at all—across forest boundaries. The Red Forest didn't account for any administrative accounts (e.g., application administrators) beyond infrastructure administrators. And finally, having to maintain another separate forest infrastructure was a lot of overhead for a relatively modest gain.

And…Exit the Red Forest

As a result of these constraints, and likely expedited by revelations from the recent SolarWinds attack, Microsoft recently retired the concept of the Red Forest. As of today, building a Red Forest is no longer the standard approach for isolating and protecting privileged access in a Windows/Active Directory world. So, what is the new standard?

Adoption Has Lagged

Well, as you can imagine, the SolarWinds attack highlighted the risks that on-prem identity systems like Active Directory pose to the cloud resources that they are integrally tied to in most organizations today. It is not uncommon for shops to be authenticating and

authorizing to Azure cloud resources using a combination of on-prem AD identities and federation solutions such as PingFederate and ADFS, instead of using Azure AD directly.

This means that, as usual, the weakest link in the chain of protecting cloud identities and applications, and especially privileged access, continues to be those on-prem resources that we've been trying to protect for 20+ years. And while approaches such as Admin Tiering and Red Forest have been around for a while, the reality is that many shops never implemented these approaches, or only partially implemented them. That might sound difficult to imagine, so let me repeat that.

Well–known strategies for mitigating privileged access risk have been under-deployed in most Microsoft shops.

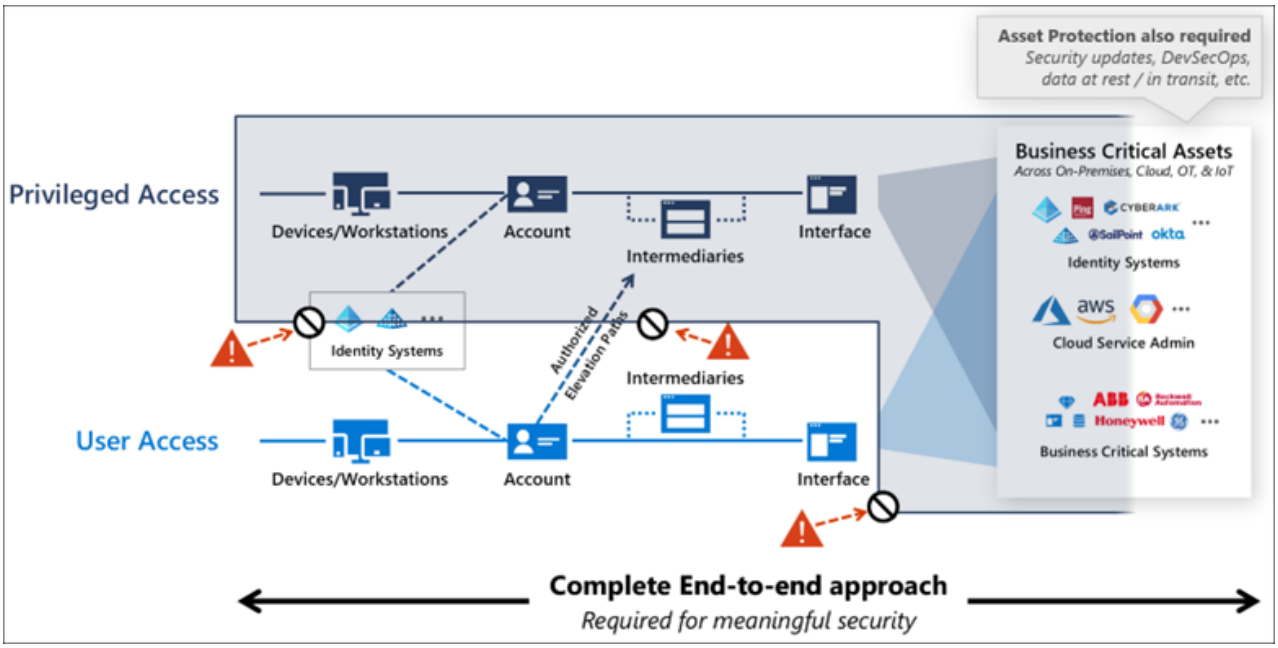
The reasons for this oversight are many and varied, but most have to do with the cost and complexity of implementing these approaches. The result has been that many shops continue to have woefully inadequate controls for preventing the spread of what is essentially a 15–year–old risk. Given that the SolarWinds attack showed how attackers could use weaknesses in on-prem privileged access management to move "vertically" into cloud systems such as Office 365, Microsoft felt compelled to re-define what privileged access looks like in the modern era.

The Future of Privileged Access?

In December 2020, Microsoft unveiled its new privileged access strategy. This strategy uses the principles of Zero Trust and "the Cloud" as its foundations. Microsoft even states in its new strategy documents that "Cloud is a source of security." You would be rightly skeptical of this statement, given that Microsoft is one of the largest cloud providers in the world. "So I have to invest in the cloud to be secure?"

The way I view this new approach is that it represents an evolution of the previous pass-the-hash and Red Forest strategies. Despite the emphasis on your acquisition of revenue–generating cloud services from Azure, the new approach makes some sense. That said, I'm not convinced that shops that were hesitant to do something as simple as Admin Tiering will now dive into complex zone-based Zero-Trust–based implementations that involve many moving parts. But let's tease it apart a bit and dig into what Microsoft is proposing.

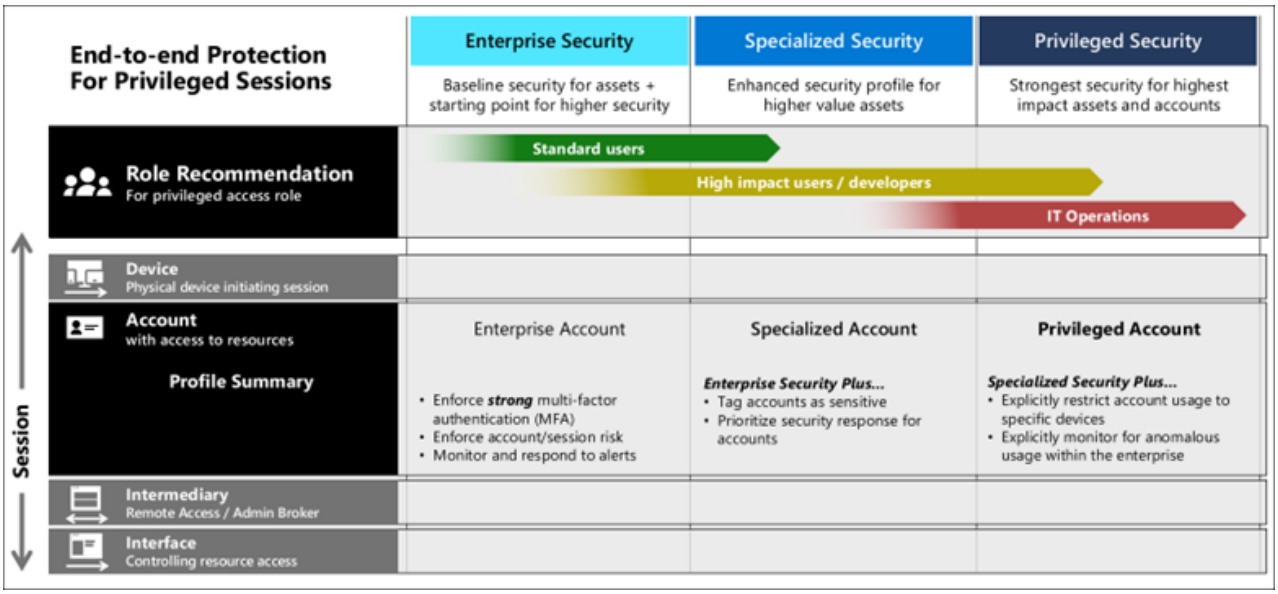
The first thing to understand is that Microsoft is looking at the tiering model a bit differently and, I would argue, more holistically than before. Whereas before, Admin Tiering and Red Forests were focused on privileged access and administration by IT pros, this new model takes into account the full landscape of a modern organization—including not only IT administration but also line-of-business application administration and the various pools of business data that live in most organizations, as you can see here:



Microsoft diagram of access tiers tied to control, management, and data/workload "planes"

This diagram underscores the concept that user access to resources and data must be kept separate from privileged access, with appropriate controls for access one tier from another. Further, Microsoft breaks access into three levels: **Enterprise**, **Specialized and Privileged**, where most users fall into the Enterprise category, leaving Specialized for specific classes of users such as developers, executives, and other specialized functions that are potentially higher risk to the business. And of course, Privileged are those users managing these environments, such as members of Azure Global Admins or the familiar built-in AD groups like Domain Admins and Enterprise Admins.

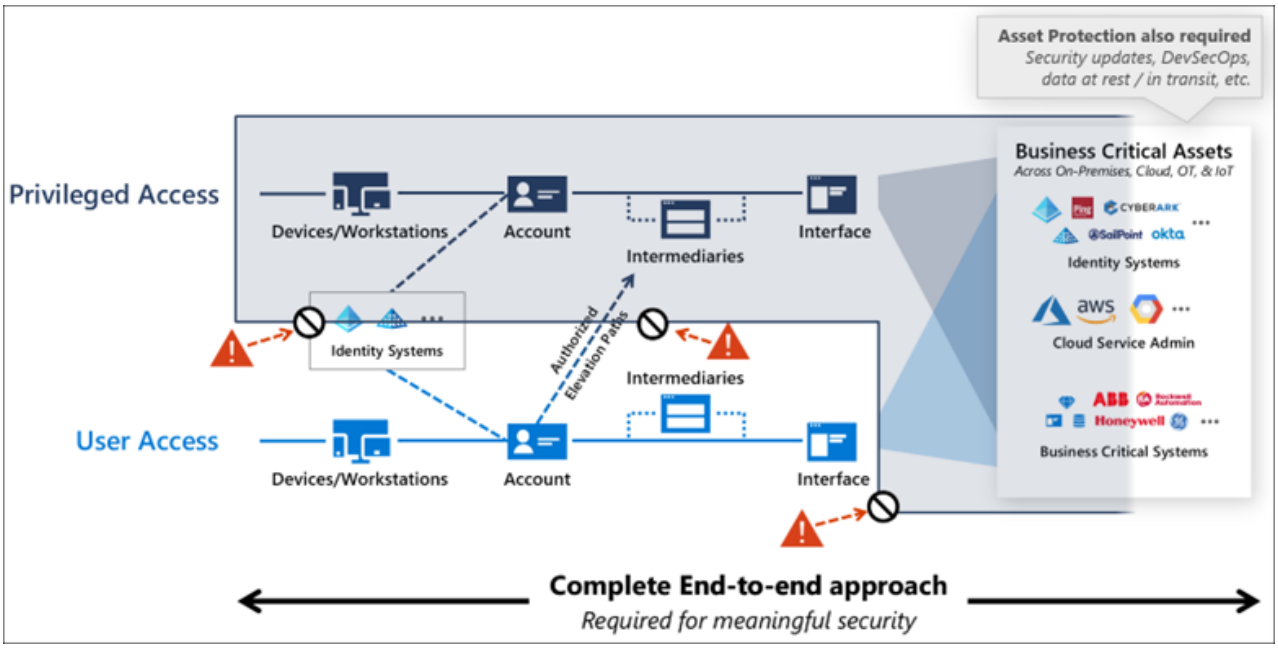
For each security level, Microsoft specifies security controls to ensure that the user accessing the resource is who they say they are. This is where some heavy pitching of Azure services shows up. As you can see from the diagram below, all users essentially should be using MFA and Zero Trust protections, which is of course a big lift for many enterprises today that primarily focus MFA on privileged access:



The new privileged access strategy recommended by Microsoft provides straightforward role-based access guidelines.

As you can see from the figure above, this strategy also introduces the concept of **intermediaries** and **interfaces**. Intermediaries, in a more familiar parlance, are things like jump servers or bastion hosts (aka PAWS), VPNs, or other secure jumping–off points for privileged access. Interfaces are precisely as they imply—the end–user applications, tools, and utilities (e.g., PowerShell remoting) used to access resources. Those interfaces might go through various application proxies or other levels of indirection to enforce secure access to those resources. This access is also further secured using Zero Trust technologies that enforce device and user security—policies such as being on a managed device, in a known location, being a known user, performing routine user behaviors, using MFA, conditional access, and just-in-time administration.

So far, most of this guidance seems straightforward, albeit skewed heavily toward consumption of many Azure security services to implement the model. But I must admit that as I followed the strategy, Microsoft started to lose me with the complexity introduced by “planes” (not the kind you fly in). This is best explained using Microsoft’s diagram:



Microsoft diagram of access tiers tied to control, management, and data/workload “planes”

This diagram is explained as the evolution of the old Admin Tiering model, but frankly it just confused me. It made no real connection back to the previous diagrams I showed depicting Enterprise, Specialized, and Privileged access. The model seemed to just rise up out of whole cloth—without explaining how I get from those three tiers of access to Privileged Access, Control Plane, Management Plane, and User Access, which are then mapped to Tiers 0, 1 and 2. Just confusing.

Implementing the New Strategy…Or Not

If I ignore that particular break from reality and focus on the principles I discussed above, this approach makes some sense and seems a logical extension of the previous concepts that have been around for years. And if you read it agnostically, many of the principles of using Zero Trust policy enforcement, intermediaries, just-in-time administration, and MFA can be implemented without opening your wallet to Microsoft in particular. And if you decide to go down the Microsoft path, they provide some pretty good implementation guidance called **Rapid Modernization Plan (RAMP).**

I’m not sure that “rapid” will be part of any wholesale implementation of this new strategy, given the complexities of most enterprise environments. My main concern about this whole new strategy is the complexity it introduces. The model has many moving parts to implement to ensure it’s working as expected—and we all know that complexity often kills security. My immediate reaction here is that if many shops were reluctant to implement something as relatively simple as Admin Tiering, how do we expect them to implement what is essentially a much more complex strategy? I think it’s a legitimate question.

I have no doubt Microsoft’s response is that you can rely on Azure services to solve much of this, but that doesn’t remove the need to manage all those services well, implement them consistently, and monitor them religiously over time. I’m not a fan of putting all my

security eggs in the technology basket, even when that technology comes from a trusted partner like Microsoft. You need to balance your own organization's business and security needs with the realities of what the technology can and can't do. It's an old trope, but security is about people, process, and technology. Relying on just one leg of that stool will always fail.

Finally, I wonder if this new strategy doesn't represent a somewhat unrealistic view of where most enterprises are today in the cloud implementation journey. Despite their best efforts, most enterprises still live and die by on-prem Active Directory to authenticate and authorize their users, technologies like Group Policy to secure and lock down their desktops and servers, and a dizzying array of on-prem and cloud line-of-business applications.

This new Microsoft strategy somewhat relies on a lift and shift of many of these technologies to corresponding cloud technologies. That will not happen overnight (understatement), if at all, and as such, what do enterprises do in the meantime? One suggestion might be to finally implement some of the guidance Microsoft has had in place for over 10 years around tier administration, PAWs, and similar technologies, then begin to augment that with some of these newer cloud technologies. That's what I would do anyway.