Cutting Down the AD Red Forest

blog.netwrix.com/2023/02/06/active-directory-red-forest

Microsoft recently updated its guidance for how organizations should approach privileged access in Active Directory (AD). A key component is shifting from the tiered access model (TAM) and the Enhanced Security Admin Environment (ESAE) (also known as the Active Directory Red Forest) to the Enterprise Access Model (EAM). This article explains the drawbacks of the older models and the key principles of EAM.

Handpicked related content:

[Free Guide] Privileged Access Management Best Practices

Limitations of the Red Forest Model

Organizations can and do use an AD Red Forest to protect their most privileged credentials. However, they often run into two serious issues:

- High cost. Using the Red Forest Microsoft model can be quite expensive in terms of both resources and time. You need to:
  Build an administrative forest.
  Populate it with the right accounts.
  Arrange access to the right systems.
  Manage the forest closely, updating it as employees come and go and your IT infrastructure evolves.
  Keep it patched, backed up, and monitored on a separate infrastructure.
- Inability to secure modern IT environments. The Red Forest security model was designed for on-premises Active Directory environments. But today, most organizations today have complex hybrid IT ecosystems, often with multiple cloud platforms and identity management providers outside the scope of AD, including but not limited to Azure AD. It's vital to control privileged access across the entire modern IT ecosystem.

However, keep in mind that Microsoft does not rule out the use of Red Forest altogether. It can be an effective model in certain situations, such as when an organization has stringent requirements, can allocate sufficient budget and needs to access control only within the boundaries of Active Directory.

Limitations of the Tiered Access Model

TAM, like ESAE, is based on the Bell LaPadula model from the '70s. TAM still exists, although it has been refactored. It is possible to apply TAM to Azure AD by mapping tiered access functions to Azure AD. In particular, there are several highly privileged roles in Azure AD that merit stronger controls, such as cloud-only accounts with PIM enabled, FIDO2 authentication tokens and Azure managed workstations.

Unfortunately, after pinpointing the Tier Zero equivalents in Azure AD, security gets muddled by the application of Conditional Access policies. Plus, the separation you get in AD does not translate into Azure AD, resulting in a transition that is not seamless.

The Enterprise Access Model

The big advantage with the Enterprise Access Model is that control is not entirely rooted in nor exclusively controlled from Active Directory. Instead, access is predicated on three key layers:

- Control plane — You have a control plane in your identity systems (Active Directory and Azure AD), networks and other locations where access is managed. Management of the control plane is tightly constrained to highly trusted devices and credentials.
- Management plane — This is how we to manage data, applications and services (equivalent to the previous Tier One). We partition access as much as possible across whatever vector is appropriate, such as:
    - Local, hosted, or cloud-based systems
    - IaaS, PaaS, SaaS
    - Other apps and platforms
    - Organizational hierarchy
- Data/workload plane — This layer controls access for users, including employees, contractors, partners and customers. This naturally includes the devices and workstations that they use, which we can manage using Microsoft Intune, which is part of Microsoft Endpoint Manager. For more information about device management, check out this excellent Blue Security podcast.

Core Principles of the Enterprise Admin Model

The enterprise access model represents an acceptance that the world does not live within Active Directory. Instead, it uses modern principles and controls to focus on what really matters — giving people the access they need, restricting or blocking access where it makes sense given the context, and exercising great care in how we provide privileged access, particularly when it comes to managing the control plane. Here are some of the key principles and benefits of EAM.

Enforcement of the least privilege principle

Advanced cloud-based controls that use artificial intelligence (AI) and machine learning (ML) to detect and respond to attacks are great, but least privilege remains the foundation of security. After all, having the most sophisticated webcam doorbell is pointless if we habitually leave the door open.

Accordingly, we need to ensure we tightly control access using a least-privilege model. IT pros generally focus on managing user access because that is the most common daily interaction with the systems we manage. But business users are not our only concern.

We also have to closely manage administrative accounts, service accounts and application accounts, and monitor their behavior, especially around access to critical resources — especially the management interfaces for our control planes.

An assume breach mindset

The Enterprise Access Model goes hand-in-hand with an assume breach mindset. Years ago, organizations had mostly isolated IT environments, so it was convenient and fairly secure to authenticate devices, users, applications and other entities once and then trust them implicitly. Today, however, the workforce is mobile and systems are highly connected, so it's important to shift to a Zero Trust architecture. This approach involves using a variety of signals to make policy-based decisions about access, including the results of technologies like user and entity behavior analytics (UEBA). This approach can enhance security while also delivering on the user expectation for a seamless experience and the ability to work from anywhere.

For example, let's say you're requesting access to our backend payment system. Your account has the appropriate access permissions and you're using a device that the company owns and manages, but you have skipped updates for the past month and disabled your screen lock. As a result, we may block your access outright, or require additional verification, such as multi-factor authentication (MFA). Or we might allow access to non-sensitive material only and record your session.

Consistent enforcement

Policies need to be applied consistently, regardless of the location of users or resources. In practice, this requires gating access to resources through Azure AD as much as possible; AD becomes a legacy backend infrastructure and users have minimal interaction with it. In particular, as noted above, devices need to be managed through Intune.

You can see the trajectory coming together with modern access controls like passwordless access, which contribute to a more seamless user experience.

Mitigating the risk of privilege escalation

To prevent attackers from gaining unauthorized access, we must ensure that we have tight controls around:

- The accounts to which we provide privileges
- The devices from which those accounts can access our control interfaces

Make sure to use network segregation, such as local network rules or features like management groups, network security groups, and Azure policy. Do not re-use service accounts for multiple services, and control who can manage service principals and enterprise apps in Azure AD and scope of that control.

In particular, vendors frequently request a higher level of privilege than their applications actually require. Don't be afraid to provide a robust challenge to requests for things like Domain Admin membership, since granting that right would enable an adversary who compromises the application to gain elevated rights.

Defense in depth

A strong security strategy involves everything from protective controls to monitoring and responding to active threats. The NIST Cybersecurity Framework lays out the following five key elements:

- Identify — Identify all equipment, data and software in your company, including smartphones, laptops and point-of-sale devices, and all sensitive and regulated data. Then create and share a company cybersecurity policy that covers the responsibilities and roles of vendors, employees and anyone with access to sensitive information.
- Protect — To prevent cyberattacks from succeeding, be sure to:
    - Encrypt sensitive data.
    - Control who logs into your network and uses your devices.
    - Store sensitive and regulated data only in secure locations.
    - Perform regular backups and store them securely.
    - Update security software periodically.
    - Create formal policies for safely disposing old devices and electronic files.
    - Prepare for unexpected events that may put data at risk, such as weather emergencies.
    - Train everyone who uses your network and devices about cybersecurity.
- Detect — Continuously monitor your network for suspicious connections and other activity.
- Respond — Ensure you can respond quickly and effectively to threats by creating plans for:
    - Notifying employees, customers and others whose data may be at risk
    - Reporting the attack to relevant authorities
    - Investigating and containing attacks
    - Keeping business operations running
    - Updating your cybersecurity policy and plan according to lessons learned
- Recover — Minimize downtime and business losses by repairing and restoring affected devices and data. Be sure you have a plan to keep customers and employees informed about your progress.

How Netwrix Can Help

The enterprise access model isn't the only way to manage privileged access. If you don't have the resources, time or energy to implement the EAM, consider using Netwrix's privileged access management (PAM) software. Reliable, intuitive and fast, it empowers you to:

- Discover standing privileged accounts and replace them with temporary, on-demand access.
- Reduce the risk of audit findings and business disruptions by managing and tracking all privileged activity in one centralized hub.
- Boost administrative accountability with session monitoring.

Request a one-to-one demo today to experience the Netwrix difference.

Netwrix also provides products that enable you to improve your cybersecurity more broadly, including:

FAQ

What is Active Directory Red Forest?

Red Forest is the common name for the Enhanced Security Admin Environment (ESAE) architecture. Implementation involves setting up a 3-tier model and placing administrative accounts in Tier 0.

Why is Red Forest no longer recommended?

Microsoft replaced Red Forest because it is too expensive for most organizations and it is limited to on-premises Active Directory, with provision for the cloud.

What is the Enterprise Access Model (EAM)?

The Enterprise Access Model replaces the Red Forest with a strategy that controls access across modern hybrid environments.

Joe Dibley
Security Researcher at Netwrix and member of the Netwrix Security Research Team. Joe is an expert in Active Directory, Windows, and a wide variety of enterprise software platforms and technologies, Joe researches new security risks, complex attack techniques, and associated mitigations and detections.