How Microsoft Evolved from Active Directory Red Forest to the Enterprise Access Model

petri.com/active-directory-red-forest

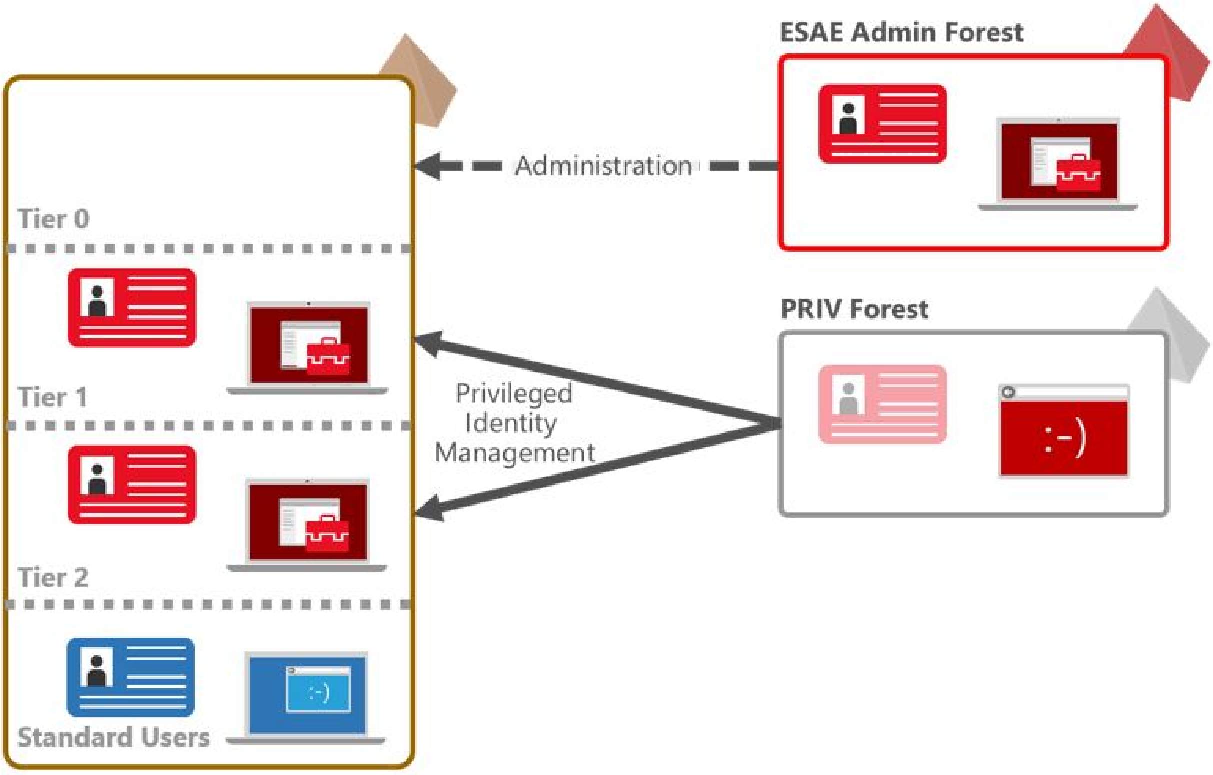
August 29, 2024

Over ten years ago, Microsoft announced the EASE or Active Directory Enhanced Security Admin Environment. Otherwise known as your Active Directory Red Forest, it isolates your privileged access administrative accounts in Active Directory (AD). Over the last four years, Microsoft has accounted for the retirement of the ESAE in favor of a more modern privileged access strategy called the Enterprise Access Model (EAM).

Learn about the history of Active Directory Red Forest and how the enterprise [hybrid] landscape dictated Microsoft's new privileged access management model.

What is Active Directory Red Forest?

The Active Directory Enhanced Security Admin Environment has a few 'aliases' you may know – 'Active Directory Red Forest', 'Admin Forest', or even 'Hardened Forest.' This is Microsoft's legacy architecture built to secure your Windows Server Active Directory environment – namely your privileged accounts. These include accounts in the Schema Admins, Enterprise Admins, Domain Admins, etc. security groups.



Microsoft Active Directory Red Forest (Image Credit: Microsoft)

The purpose was to create an isolated Active Directory forest to house these important accounts. All of your 'Tier-0' (or critically important and vulnerable) accounts were stored here.

However, it is important to note that around four years ago, Microsoft announced the retirement of this architecture and no longer recommends it.

Why was the EASE retired?

Microsoft retired this approach mainly due to the changing and evolving landscape of enterprise networks. Because this solution was built ten years ago when Active Directory on-premises was the mainstream, its limitations, and failings became apparent when more companies onboarded a hybrid approach – including Microsoft Entra ID (previously Azure AD) in their identity and access management plans. This legacy approach, based on macro-segmentation techniques, didn't adequately account for hybrid- or cloud-based environments.

So, is there no reason today to implement an Active Directory Red Forest in your environment? Not necessarily. Microsoft does not rule out the use of the ESAE because it can still be used as an effective model in certain situations. When an organization has strong security and compliance requirements, can allocate sufficient budget dollars to maintaining an isolated forest (and all accompanying software/hardware), and needs to control identity access within the confines of Active Directory, this is still a valid and supported option.

Microsoft's privileged access strategy

Microsoft's privileged access strategy is designed to reduce risks associated with privileged access and protect critical assets. Here are some key points they address with this strategy.

1. **High Impact and Likelihood** – Privileged access is a top security priority because any breach can have significant impacts on your organization.
2. **Zero Trust Principles** – The strategy is built on Zero Trust security principles, which essentially assumes breach and requires explicit validation. No room for error.
3. **Holistic Approach** – No single solution can mitigate all security risks – Instead, use a blend of multiple technologies and software tools to create your security solution.

Why is privileged access important?

Often viewed as the foundational layer of all security assurances, the security of privileged access is critically important. An attacker in control of your privileged accounts can undermine your entire security boundaries.

From a risk perspective, loss of privileged access is a high-impact event with a high likelihood of happening that is growing at an alarming rate across industries.

These targeted data theft incidents resulted in many high-profile breaches at familiar brands (and many unreported incidents). More recently these techniques were adopted by ransomware attackers, fueling an explosive growth of highly profitable human-operated ransomware attacks that intentionally disrupt business operations across many industries.

High business impact

If you've been an IT Pro for even a relatively small number of years, you likely know the scope of a breach of a company's privileged accounts. Attackers with access to these accounts have full control of all enterprise resources, giving them the ability to export confidential data, spread it across the Internet (often for a sum), interrupt key business processes, and cause irreparable damage to computers, servers, and other key network infrastructure.

Targeted data theft is one of the most popular schemes attackers will use – Access and steal sensitive intellectual property (IP) for monetary gain and notoriety (in the wrong circles…).

High likelihood of occurrence

There has been an increasing prevalence of attacks targeting privileged access accounts, mostly due to the increasing amount of modern credential theft and phishing attack schemes. Human-operated ransomware also contributes to the frequency of these types of attacks.

These types of accounts are very attractive to hackers because they provide such a wide-ranging landscape inside an enterprise's systems. This leads to rapid and significant business impact when compromised.

Both the silent impact and attacker monetization limitations on these attacks are disintegrating with the advent of human-operated ransomware, which is growing in volume, impact, and awareness.

1. **Loud and disruptive** – to business processes to payment of extortion demands.
2. **Universally applicable** – Every organization in every industry is financially motivated to continue operations uninterrupted.

The legacy AD tier model

This can be described as a security framework designed to prevent the escalation of privileges within an enterprise's network. Administrative access is spread across three tiers to minimize the risk of unauthorized access attempts.

- **Tier 0** – This tier includes accounts, systems, and groups that contain any level of administrative control of the AD forest. Domain Admins and Enterprise Admins are classic examples. This is the most critical tier and must be secured above all else.
- **Tier 1** – this tier typically contains accounts and systems that manage enterprise devices and servers. Although they are crucial to the enterprise, they do not have the same level of impact if breached.
- **Tier 2** – Everything else funnels into this tier. These accounts include user and computer accounts for your users and devices.

The EAM (Enterprise Access Model)

About four years ago after Microsoft announced the retirement of their Enhanced Secure Admin Environment, they started rolling out the recommended replacement strategy – the Active Directory Enterprise Access Model.

The EAM is a modern security framework that is designed to address the evolving complexities of hybrid and multi-cloud environments by providing a comprehensive approach to access control.

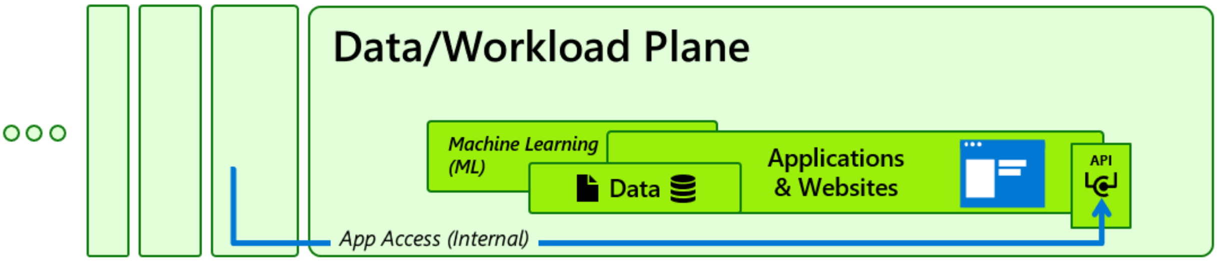
Here are the key points that make up this new strategy.

1. **Holistic Access Control** – This addresses all types of access by external and internal users, applications, privileged accounts, and applications.
2. **Zero Trust Principles** – There's that phrase again – Zero Trust principles include explicit validation, least privilege, and assumption of breach.
3. **Multiple Planes** – Different planes such as the data/workload plane, management plane, and control plane each have specific security measures in place.

4. **Consistent Policy Enforcement** – This ensures consistent policy and security enforcement across all access methods – users, admins, APIs, and even service accounts.
5. **Continuous Auditing** – This is for continuous auditing for configuration vulnerabilities – essential to prevent unauthorized privilege escalation.

Infrastructure – Describing various 'Planes'

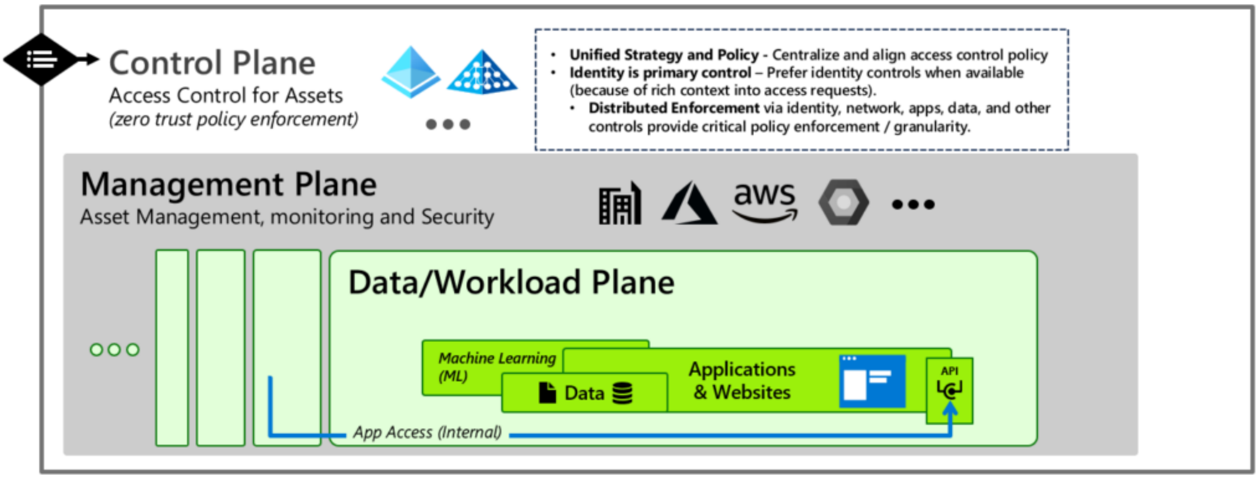
The primary stores of business value that an organization must protect are located in the Data/Workload plane.



The 'Data/Workload' Plane (Image Credit: Microsoft)

The applications and data typically store a large percentage of an organization's Business processes and Intellectual Property (IP).

A management plane is created by an enterprise IT organization managing and supporting the workloads and the infrastructure they are hosted on, being on-premises, on Microsoft Azure, or a hybrid of the two.

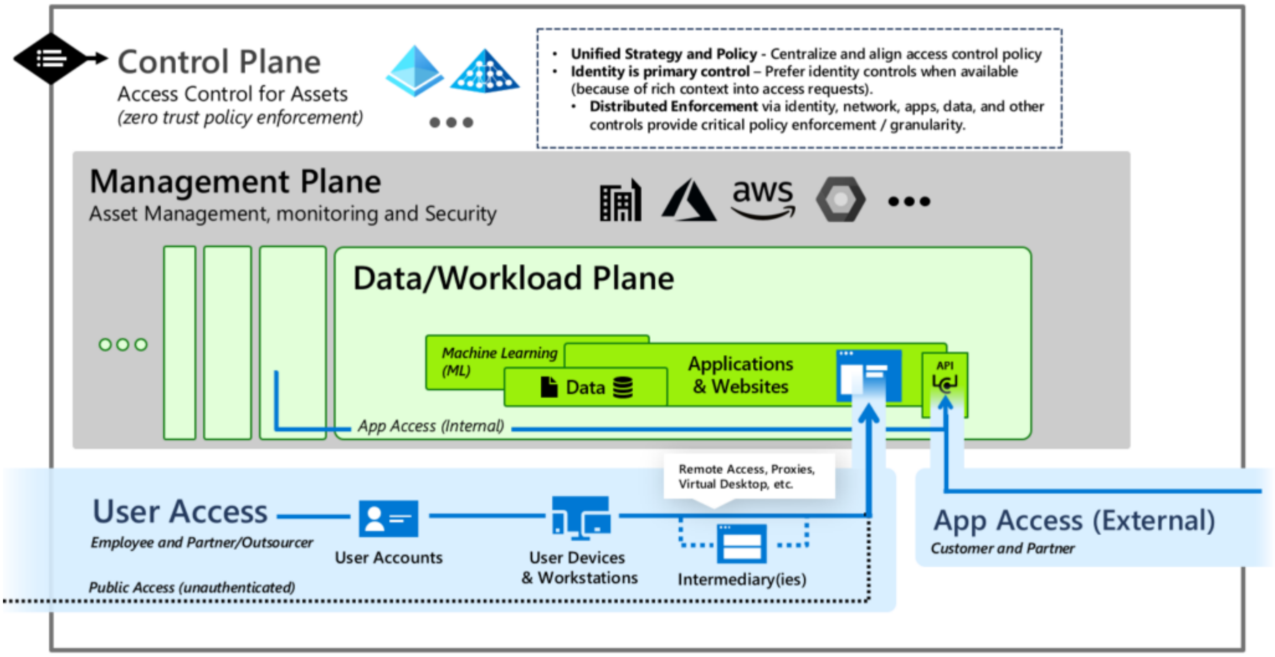


- **Unified Strategy and Policy** - Centralize and align access control policy
- **Identity is primary control** – Prefer identity controls when available (because of rich context into access requests).
  - **Distributed Enforcement** via identity, network, apps, data, and other controls provide critical policy enforcement / granularity.

Incorporating the 'Management' and 'Control' Planes – Image Credit: Microsoft

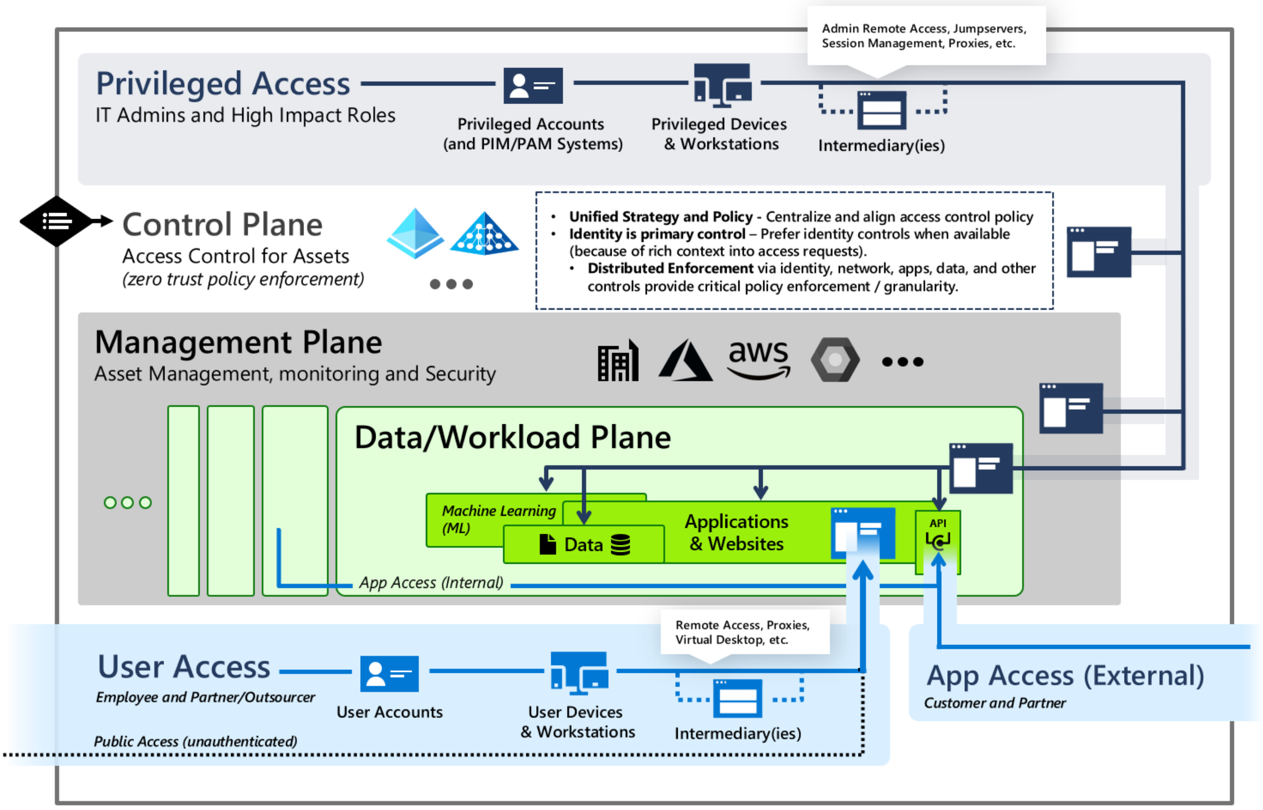
Providing consistent access control to these systems across the enterprise requires a control plane based on central identity systems, often supplemented by network access control (NAC) for older systems.

Each plane has control of the data and workloads by their functions. For these systems to create value for your business, they must be accessible to users, partners, and customers using their normal workstations. This creates user access pathways.


Control Plane
Access Control for Assets
(zero trust policy enforcement)
• Unified Strategy and Policy - Centralize and align access control policy
• Identity is primary control – Prefer identity controls when available (because of rich context into access requests).
• Distributed Enforcement via identity, network, apps, data, and other controls provide critical policy enforcement / granularity.
Management Plane
Asset Management, monitoring and Security
aws
Data/Workload Plane
Machine Learning (ML)
Data
Applications & Websites
API
App Access (Internal)
Remote Access, Proxies, Virtual Desktop, etc.
User Access
Employee and Partner/Outsourcer
User Accounts
User Devices & Workstations
Intermediary(ies)
Public Access (unauthenticated)
App Access (External)
Customer and Partner

Microsoft Active Diretory ESM – Describing 'User Access' pathways (Image Credit: Microsoft)

Finally, all of these systems must be managed by an IT staff, developers, or other IT Pros in the organization – thus privileged access pathways are created.


Admin Remote Access, Jumpservers, Session Management, Proxies, etc.
Privileged Access
IT Admins and High Impact Roles
Privileged Accounts (and PIM/PAM Systems)
Privileged Devices & Workstations
Intermediary(ies)
Control Plane
Access Control for Assets
(zero trust policy enforcement)
Management Plane
Asset Management, monitoring and Security
aws
Data/Workload Plane
Machine Learning (ML)
Data
Applications & Websites
API
App Access (Internal)
Remote Access, Proxies, Virtual Desktop, etc.
User Access
Employee and Partner/Outsourcer
User Accounts
User Devices & Workstations
Intermediary(ies)
Public Access (unauthenticated)
App Access (External)
Customer and Partner

- **Unified Strategy and Policy** - Centralize and align access control policy
- **Identity is primary control** – Prefer identity controls when available (because of rich context into access requests).
  - **Distributed Enforcement** via identity, network, apps, data, and other controls provide critical policy enforcement / granularity.

Microsoft Active Diretory ESM – How the 'Privileged Access' works with the new strategy -(Image Credit: Microsoft)

Providing a strong and consistent access control plan in your organization requires you to:

- Enforce Zero Trust principles
- Include pervasive security and policy enforcement
- Mitigate unauthorized privilege escalation

Recommendations for securing Active Directory

First of all, let me describe an overview of how you can implement Microsoft's Enterprise Access Model in your environment.

- **Assess your environment**

  Identify resources you need to protect and define goals to secure them.
- **Establish Privileged Access Workstations (PAWs)**

  Designate a dedicated device for privileged tasks and lock it down
- **Implement Just-In-Time (JIT) Access**

  Grant elevated privileges on the fly only. You can utilize Entra ID Privileged Identity Management (PIM) for this.
- **Enforce Multi-Factor Authentication (MFA) (PLEASE!)**

  Please, for the love of all that is holy, enable MFA across the board in your enterprise!

- **Leverage Entra ID Conditional Access**
  Apply granular policies to control access based on user identity, location, and network access.
- **Regularly Review and Update Policies**
  Monitor access patterns and adjust your conditional access policies accordingly.
- **Educate Users**
  Provide ongoing training campaigns on password policies, MFA, and the introduction of Passkeys.
- **Leverage Automation**
  Use automation tools to streamline tasks like password resets (self-service password resets) and onboarding/offboarding processes.
- **Regularly Audit and Monitor**
  Review Entra ID sign-in logs, user activities, etc., and adjust policies.
- **Stay Updated**
  Always keep systems patched and security vulnerabilities at bay.

Conclusion

Microsoft's evolution from the Enhanced Security Admin Environment (ESAE) to the Enterprise Access Model reflects a significant shift in addressing modern security challenges and newer hybrid infrastructures. The ESAE, designed for on-premises environments, has been retired in favor of the more adaptable and comprehensive Enterprise Access Model.

This new approach leverages continuous auditing, Zero Trust principles, and consistent policy enforcement to secure privileged access across hybrid and multi-cloud environments. By adopting this modern framework, organizations can better protect their critical assets and stay resilient against evolving threats.

Table of contents