The Evolution of Active Directory Red Forest

ravenswoodtechnology.com/is-the-active-directory-red-forest-dead-time-to-shift-to-the-enterprise-access-model

Burke Matsuo

August 8, 2024

A red forest is designed to increase the security of Windows Server Active Directory Domain Services (AD DS) by protecting privileged credentials from compromise. Privileged identities, such as members of the Domain Admins and Enterprise Admins groups, are created as separate accounts and abstracted from the existing AD DS forests. These accounts are created in a discreet, hardened red forest that's used to manage one or more of an organization's production forests.

You may have also heard red forests referred to as bastion, administrative, or Tier 0 forests. In this article, we'll discuss what an AD red forest is, what led to Microsoft retiring the architecture, Microsoft's replacement strategy, and some considerations for implementing an overall enterprise access strategy for your organization.

The Rise of the Microsoft ESAE Model

Partner with Microsoft experts you can trust

If it's time to take that first step toward leveling up your organization's security, get in touch with Ravenswood to start the conversation.

Get in Touch

Microsoft Services introduced its AD DS red forest offering, the Enhanced Security Admin Environment (ESAE), more than 10 years ago. ESAE was designed to protect administrative credentials in AD DS. Deployment of ESAE forests has also been used to regain control of compromised AD DS environments.

Privileged access workstations (PAWs) are deployed in conjunction with the implementation of an ESAE forest. PAWs are used for administration of an ESAE forest, as they provide a "clean keyboard," preserving the clean source principle. This ensures privileged administration takes place from a device that's managed at the same level of security assurance as the assets being administered.

To learn more about how PAWs help increase security, check out our blog post, "Use Privileged Access Workstations to Increase Security."

The Demise of the ESAE Model

In December 2020, Microsoft announced the retirement of the ESAE model as a default recommendation and replaced it with a modernized privileged access strategy. This updated strategy includes the Enterprise Access Model (EAM), which addresses asset protection outside of traditional AD DS. We'll discuss the EAM in the next section.

Many factors likely contributed to the decision to retire the ESAE model, such as:

- Limited scope of protection
- Complexity
- Cost

Let's look at each of these factors in greater detail.

Limited Scope of Protection

What about protection of privileged accounts used to administer Microsoft Entra ID and resources in Azure and other cloud providers? These accounts weren't included in the ESAE architecture. At the time the ESAE model was designed, most organizations hadn't started their journeys to the public cloud.

Complexity

An ESAE environment is a complex, hardened environment that can be challenging when issues arise. Organizations have inadvertently locked themselves out of their environments and needed Microsoft's assistance to get back in.

The ESAE architecture calls for heavy use of IPSec to secure communications between the PAWs, domain controllers, and supporting infrastructure. IPSec is fraught with complexity and can be very difficult to troubleshoot.

In the article "Enhanced Security Admin Environment," Microsoft notes that organizations using this architecture sustain "extra risk" due to the technical complexity and encourages organizations with this architecture to "apply extra rigor to monitor, identify, and mitigate any associated risks."

Cost

The ESAE implementation requires a separate AD DS forest to be created and physical PAWs to be deployed. The cost of building and operating such a complex environment also contributed to the ESAE architecture's retirement.

Privileged Access Strategy

As the number of cloud-only and cloud-hybrid organizations increased, Microsoft recognized the need to update its guidance for securing privileged access. Microsoft's updated strategy can be found in its Securing Privileged Administration documentation.

Zero Trust

In August 2020, the NIST Special Publication 800-207 "Zero Trust Architecture" was published to define Zero Trust, identify its components, and describe its use cases.

The Zero Trust model dictates that trust is never a given and all requests must be verified. Microsoft's updated privileged access strategy was built using the zero trust principles of explicit validation, least privilege, and assume breach.

Explicit Validation

Every authentication and authorization decision needs to be validated using all available information. Users should log in with strong authentication, the security posture of their device should be checked for compliance with organizational policies, and the applications used to access an organization's resources should be validated. The network on which the traffic flows should be secured by implementing network segmentation, and the network traffic should be monitored for threats. To learn more about explicit validation, please see Microsoft's Rapid Modernization Plan (RaMP).

Least Privilege

Using the principle of least privilege, users are granted only the minimum permissions needed to perform their duties and only during the period in which they need them. This can be accomplished using Just Enough Administration (JEA). Access is granted just-in-time (JIT) and is timebound.

Assume Breach

This principle indicates the environment has either already been compromised or that a compromise is imminent. The decision to trust shouldn't be made based on the origination of a request, and every request must be verified as if it came from an untrusted network. To say it another way, requests shouldn't be automatically trusted just because they were initiated from within an organization's internal network.

Network segmentation should also be employed to reduce the affected "blast radius" if an attacker were to successfully breach the environment. This helps to limit potential disruptions in the event of an attack.

Enterprise Access Model (EAM)

The EAM is a major part of Microsoft's privileged access strategy. The EAM evolved out of what Microsoft now calls the "legacy AD tier model." The concepts of mitigating privileged escalation are still present but have been broadened to address organizations that have moved either partially or completely to the cloud.

Legacy AD Tier Model

The legacy AD tier model was designed to protect against privilege escalation for AD DS. The following are the legacy AD tiers:

- Tier 0 – Systems such as AD DS, Public Key Infrastructure (PKI), Active Directory Federation Services (AD FS), Entra Connect, and all applications or accounts that can exert control on these sensitive resources

- Tier 1 – Applications, data, member servers, and the systems and accounts that can exert control on them
- Tier 2 – End users, end-user devices, and the systems and accounts that can exert control over them

Although Microsoft reclassified the tiering model as legacy guidance, it indicates there are situations where, if an organization can't perform a cloud migration, using a tiered approach is still a "high priority" recommendation.

EAM

The EAM was designed to modernize the original legacy AD tier model and include protections for organizations that have assets on premises and in the cloud. The EAM is depicted in Figure 1, with the legacy AD tiers superimposed, and includes the following changes:

- Tier 0 becomes the control plane
- Tier 1 splits into the management and data/workload planes
- Tier 2 splits into user access and app access

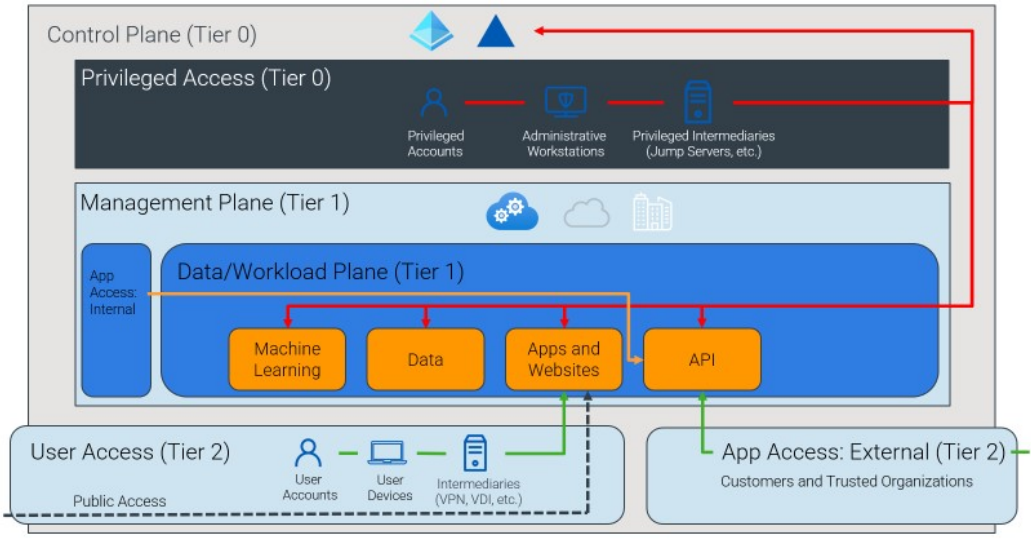
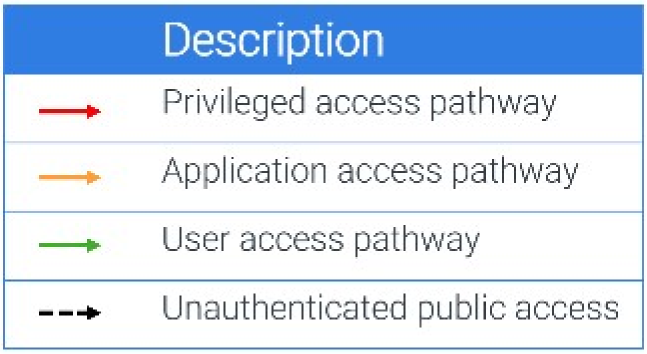

Control Plane (Tier 0)
Privileged Access (Tier 0)
Privileged Accounts
Administrative Workstations
Privileged Intermediaries (Jump Servers, etc.)
Management Plane (Tier 1)
App Access: Internal
Data/Workload Plane (Tier 1)
Machine Learning
Data
Apps and Websites
API
User Access (Tier 2)
Public Access
User Accounts
User Devices
Intermediaries (VPN, VDI, etc.)
App Access: External (Tier 2)
Customers and Trusted Organizations

Figure 1 – Enterprise Access Model



	Description
🟥 →	Privileged access pathway
🟧 →	Application access pathway
🟩 →	User access pathway
- - →	Unauthenticated public access

Let's briefly discuss the major components of the EAM.

Control Plane

The control plane evolved from the legacy "Tier 0." It now encompasses everything related to identity, access control, and networking. Azure role-based access control (Azure RBAC) and Azure Resource Manager (ARM) are examples of control plane components.

Privileged Access

Privileged access is comprised of IT administrators and staff in roles considered to be "High Impact." This includes users that have root-level access to cloud providers, access to systems that are "sensitive," and accounts requiring additional security.

Management Plane

Privileged access is comprised of IT administrators and staff in roles considered to be "High Impact." This includes users that have root-level access to cloud providers, access to systems that are "sensitive," and accounts requiring additional security.

Data/Workload Plane

The data/workload plane is where critical organizational data and intellectual property (IP) reside. This might include product designs, customer data, application data, and secret formulas. Exposure of this data could damage the company's brand or reputation. The data/workload plane also sprouted from the legacy "Tier 1."

User Access and App Access

This is how end users and customers, both internal and external, access the resources in the data/workload plane. This plane evolved from the legacy "Tier 2."

Intermediaries and Interfaces

Intermediaries are technologies used to facilitate access to an organization's environment remotely and/or to increase the security of the remote sessions. Some examples are VPN, Azure Bastion, Entra ID Privileged Identity Management (PIM), third-party Privileged Access Management (PAM), and jump servers. According to Microsoft, each intermediary carries from zero to some level of privilege escalation risk and varies in attack surface and attack value.

Interfaces are applications or web portals such as the Azure Portal, AWS console, and scripting consoles. Interfaces are used to access and perform administration of assets in public cloud providers such as Azure, AWS, and Google.

For more information on intermediaries and interfaces, please see our blog post "Use Privileged Access Workstations to Increase Security."

Should you Implement a Red Forest?

Organizations can still benefit from the foundation that Microsoft put into the ESAE forest architecture, but perhaps without all the complexity. Implementing an ESAE-style red forest that strikes a balance between security and usability could be a favorable path forward.

Even though the ESAE architecture is no longer recommended for most organizations, Microsoft continues to run an ESAE-like architecture for its own environment.

When considering whether to implement an ESAE-style red forest, be realistic and assess whether your organization has the resources to manage this new forest, as well as PAWs.

Ravenswood’s Tier 0 Administrative Model

Ravenswood uses parts of the ESAE’s solid foundational elements and incorporates fundamentals of the EAM to deliver a Tier 0 administrative model to our customers. The protection of accounts used to manage critical cloud-based infrastructure and AD DS administrative accounts is solved for.

As part of our Tier 0 administrative offering, privileged identities are abstracted into a hardened Tier 0 admin forest. These accounts aren’t privileged within the Tier 0 forest itself and are granted JIT access to the AD DS forests that they protect. Access is also timebound and the maximum duration is customizable.

Do you have multiple AD forests that need to be protected? By moving the administrative accounts to a separate Tier 0 forest, the number of accounts can be significantly reduced. Instead of every administrator requiring multiple accounts in each protected forest, one account can be temporarily elevated for each individual domain.

Our model uses native Microsoft functionality and doesn’t require additional PAM software.

Conclusion

Although the ESAE architecture is no longer a default Microsoft recommendation, there are specific cases in which a Tier 0 admin forest is still valid. Microsoft’s ESAE architecture is complex and can be difficult to maintain. It’s a solid architecture that addressed the security of on-premises AD but wasn’t designed for cloud-only or hybrid organizations.

The EAM’s advantage over the legacy AD tier model is that it addresses more than just AD DS. EAM addresses the protection of assets in cloud providers, systems located on premises, remote access, accounts, and devices. Unfortunately, tiering within AD DS that was present in the legacy AD tier model appears to have been omitted from the EAM and is found only in Microsoft’s legacy PAW guidance.

Could your organization benefit from JIT privileged access in AD DS, removal of permanent membership in privileged groups, and the potential reduction in the number of privileged accounts? If your organization is like many that plan to use AD DS for the foreseeable future, perhaps an ESAE-style administrative forest should be part of your overall enterprise access strategy.

Ravenswood’s Tier 0 admin forest design considers Microsoft’s updated privileged access strategy and builds upon it to assist customers with increasing their security posture.

Admin forests can result in additional cost, complexity, and management demands that organizations need to accept prior to moving forward. For organizations that don’t want to deploy an admin forest but would like to rapidly increase their security posture, we can develop a strategy to help mitigate many of the risks.

If your organization would like assistance with increasing the security posture of your AD DS and Azure environment, please let us know!