Active Directory is used and trusted by over 90% of the world for your internal security, and identity management. This authentication protects your administrative rights and restricted information within the enterprise. Because of its popularity, Active Directory is now a prime target for hackers to try to compromise enterprise systems. Since Windows 2012R2, the modernization of Active Directory has provided us a number of changes to our best practices to help us resist current AD attacks. Here are some of the ways we can secure our enterprises.

Microsoft Active Directory Red Forest Design or Enhanced Security Security Environment (ESEA). To keep it brief and simple, it’s basically a tiered approach to secure your administrative rights by watching the watchers. This model was created to reduce the possibility of a damaging domain compromise by building resilience into the forest and eliminating common AD hacking strategies. Remodeling your AD with this model can be an intimidating task, but approaching it by making changes in several steps can ease the burden. I approached it by implementing each step as an implementation project with change controls. To read more: (<https://social.technet.microsoft.com/wiki/contents/articles/37509.active-directory-red-forest-design-aka-enhanced-security-administrative-environment-esae.aspx>  
  
<https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material#ESAE_BM> )

1. LAPS or Microsoft’s Local Administrator Password Solution. Securing local account credentials is critical to ensuring both administrative systems and user workstations are prepared for a shift to higher security. This solution solves the issue of shared-credential local administrator accounts by providing each local account with a unique, complex password and storing it in AD on a “need to know basis”. <https://technet.microsoft.com/en-us/mt227395.aspx>
2. PAW or Priveleged Access Workstations. Isolating administrative systems is a fundamental principle of the ESEA architecture. This architecture eliminates the risks of shared-use workstations by separating an individual’s user and administrative logins to separate contexts and preventing user-targeted attacks. (<https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations>)
3. PAM or Privileged Access Management. Microsoft Identity Manager (MIM) and Privileged Access Managemen (PAM). These tools create a fully separate forest with a one-way trust for management of all production domains and ensures that if a production administrative account ever got compromised does not compromise the entire enterprise or network.   
   (<https://social.technet.microsoft.com/wiki/contents/articles/28754.microsoft-identity-manager-2016-resources.aspx>)  
   (<https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services>)
4. JEA + JIT (Just Enough Administration and Just In Time Administration) - These 2 concepts are designed to limit administrative availability by giving just enough administrative rights to do something for a certain amount of time. This limits what an attacker can do and how long they can do something with those rights if an account ever got compromised. MIM contains tools for this with an auditable features to put these concepts into action.  
   (<https://docs.microsoft.com/en-us/previous-versions//dn896648(v=technet.10)>)

These steps were gathered through a lot of research through Microsoft MVPs, their blogs, and other AD security websites. For insights to AD security, I highly recommend the below link. You can learn from a Microsoft Certified Solutions Master for Directory Services in which there are less than 100 in the world.

https://adsecurity.org/