PAM

I’m looking to explain the differences between the offerings to a customer.

MIM and Windows Server are part of the Microsoft securing privileged access suite of offerings.

Historically, years ago Microsoft gave guidance on how to secure privileged access, but because Microsoft didn’t have technologies to provide – for instance – the just-in-time admin access control, or monitoring of AD domain controller requests – customers were forced to rely upon adding expensive third party products to augment their Windows Server investments.   Thus an ecosystem grew up alongside Windows of add-on tools like these.  As with other investments Microsoft have been making, the features we’ve been adding in the last few years through product evolution and acquisitions rounds out the security controls for privileged access in Windows, reducing a customer’s need to bring in third party products.

Specifically, Windows Server 2016 adds new foundational capabilities for privileged identity and access management in AD DS and Kerberos, that enable reducing the risk of attacks targeting administrators in Windows domains, through time-limited group memberships.  MIM provides workflow, user interfaces, etc for managing those memberships in AD DS with “just in time” admin access.  A customer can deploy an isolated bastion environment with Windows Server and MIM, and use that to control administrative access across existing domains and forests.  This solution was designed in line with Microsoft’s “assume breach” guidance which Anders and others presented at last year’s Ignite, and is a part of the overall securing privileged access roadmap alongside other technologies such as ATA, JEA, PAWs, Azure AD PIM, described here: https://technet.microsoft.com/en-us/library/mt631194(v=ws.11).aspx

Fundamentally, the assume breach mindset requires that customers isolate the control of their administrative accounts from any existing Active Directory that might already have been compromised.  Some third party products implement that isolation by managing those accounts in a database table embedded in their product AND centralizing all administrator authentication into their product, but this unfortunately requires the customer to not only build out a whole ‘nother set of HA strategies to deal with this, but also change every administrator’s interaction model, disrupting existing tools and client apps.  By contrast, our approach is that authentication in the bastion environment with Windows Server and MIM is the already familiar Active Directory: customers can use their EXISTING skills and tools for HA, and existing Kerberos tickets that admins get and use for accessing workloads like Exchange or VM management or file server work just the same as they did, from the client apps and tools the customer is already using.  Furthermore, many third party PIM products were focused on implementing the privileged access controls through password sharing and password vaulting, but we want customers to not be limited to passwords for authentication: with WS 2016 they can use physical smartcards, virtual smartcards, and any other authentication in the future supported in AD.   We also augment the authentication in AD itself with callouts to Azure MFA when a user activates their privileged roles, so that even if a credential is stolen the attacker cannot simply replay it.

The securing privileged access roadmap emphasizes customer’s time to value, and orders MIM and Windows Server alongside of other controls mentioned above.  A customer should consider when selecting technology vendors the cost of acquisition, time of deployment, and cost/time of continued maintenance.   In the case of MIM and Windows Server, customers who are already using either FIM Service or Azure AD Premium for scenarios like SSPR or SSGM probably already have the necessary licenses they need to deploy MIM and Windows Server for PAM.   Some enterprise customers were shocked to learn the cost quoted by vendors of third party PIM products, as compared to the cost of deploying Microsoft’s offerings.