CYBERARK

SOLUTION BRIEF

SECURING MICROSOFT ENHANCED SECURITY ADMINISTRATIVE ENVIRONMENTS (ESAE) WITH CYBERARK PRIVILEGED ACCESS SECURITY

WHY CYBERARK?

- Comprehensive privileged access controls protect Tier-0 environments via session isolation, monitoring, threat detection, analytics, and support for multi-factor authentication
- Cost effective alternative to Privileged Access Workstations (PAWs) to secure ESAE
- Protect beyond Active Directory integrated systems and extends to all enterprise systems (*NIX, SSH-based, etc.)

OUT-OF-THE-BOX-INTEGRATIONS

- Cloud: Amazon Web Services and Microsoft Azure
- Virtualization: VMWare ESX
- Networking: Riverbed and Cisco
- Mainframe: AS400 and Z/OS / OS390

For a complete list of integrations, please visit www.cyberark.com/integrations

Microsoft's Enhanced Security Administrative Environment (ESAE) architecture is an advanced methodology for securing Active Directory within an enterprise. Through various controls and workflows, the goal of ESAE is to limit an attacker's ability to gain control over "Tier-0" assets – the ultimate target for nefarious characters – as this provides them with untethered access to domain-joined IT infrastructure. The core of the ESAE approach is the deployment of a hardened administrative Active Directory forest, often referred to as a "Red Forest", for the purpose of administering the production domain. One of the most commonly used techniques in advanced attacks is to exploit privileged accounts and their associated credentials, especially those that provide access to the domain controller wherein all Windows authentication requests take place.

Establishing Credential Boundaries

Critical to the overall strength of an ESAE deployment is the hardening of the control relationships between credentials, assets, and humans. Credential boundaries are a logical and technological set of controls that are used to simplify adherence to least privilege, as well as limit privileged credential exposure and escalation. CyberArk facilitates seamless deployment of credential boundaries by simplifying privilege delegation and credential management, allowing IT administrators to concentrate on their work and not having to concern themselves on which accounts they should be using. This enables faster adoption of ESAE concepts with less administrative overhead, and the end result ultimately creates a first step in minimizing the attack surface – but organizations shouldn't stop at credential use segmentation to maintain an optimal security posture.

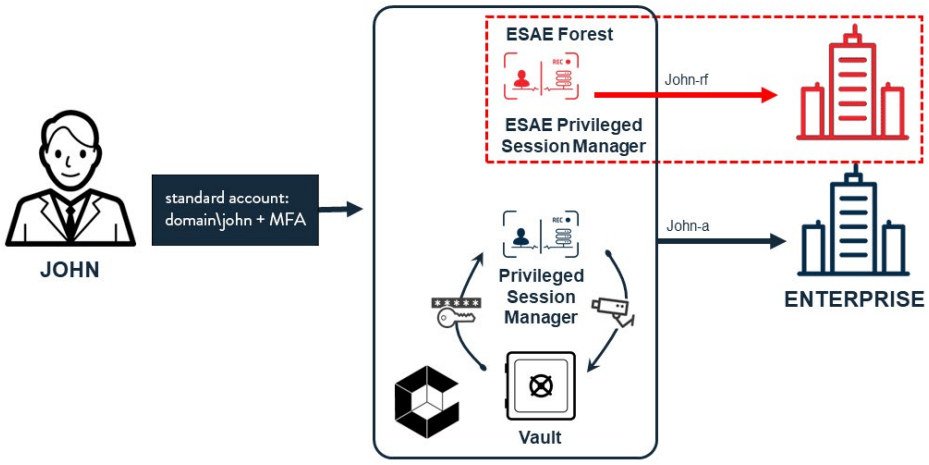

Figure 1. A standard CyberArk deployment securing privileged access workstations (PAWs) with separate administrative accounts and PAWs for Domain Administrators.

"Direct control of enterprise identities in the environment. Tier 0 includes accounts, groups, and other assets that have direct or indirect administrative control of the Active Directory Forest, Domains, or Domain Controllers, and all the assets in it. The security sensitivity of all Tier 0 assets is equivalent as they are all effectively in control of each other."

- Tier 0 model as defined by Microsoft

Securing Privileged Access

CyberArk goes beyond the use of credential boundaries and assists organizations in meeting the goals of another piece of the ESAE approach; the Microsoft Privileged Access Workstations (PAWs). PAWs are dedicated and hardened administrative operating systems that seek to facilitate secure use of privileged credentials. CyberArk flexibly provides controls with the same intent via CyberArk Privileged Session Manager, both as an addition to PAW workflows and in some circumstances as a replacement for the PAWs entirely.

Privileged Session Manager provides advanced session isolation, recording, and control of privileged activity within an ESAE environment. The solution leverages a next-gen proxy server to eliminate the exposure of privileged credentials to administrators' desktops, and provide session recordings with a full, detailed audit trail for analysis and forensic review. The controls within Privileged Session Manager are also enforceable on non-Windows assets, allowing comprehensive control over the entire IT landscape.

Furthermore, CyberArk Privileged Threat Analytics delivers detailed analysis on domain-level administrator activities, enabling security operations teams to detect indications of an attack before irreparable damage is done. The solution can monitor the network, seeking out anomalies that indicate in-progress attacks that leverage the Windows authentication protocol Kerberos (e.g PAC manipulation, Overpass-the-Hash and Golden Ticket) which can provide unrestricted access to the organization's entire IT infrastructure. By querying the Active Directly and performing on-going analytics on network traffic and adminstraitor actvities in real-time, security operations teams can be provided with the critical intelligence needed to quickly respond to advanced attacks within ESAE.

The Benefits of Securing ESAE with CyberArk

The CyberArk Privileged Access Security Solution allows organizations to secure and protect ESAE architectures by:

- Reducing the exposure of privileged credentials and assets
- Acting as a single interface for various security zones and tiers within an environment
- Providing enhanced auditing and recording of activities within the ESAE and production environments
- Delivering targeted analytics and threat detection within ESAE
- Facilitating the application of ESAE concepts and controls to the entire enterprise, including non-Windows assets

CyberArk provides a comprehensive solution designed to proactively protect against advanced attacks that exploit administrative privileges to gain access to an organizations most critical assets, steal sensitive data and damage critical systems. The solution helps organizations reduce the attack surface by eliminating unnecessary local administrator privileges and strengthening the security of privileged access. Products in the solution can be managed independently, or combined for a cohesive and comprehensive privileged access security solution.

For more information, please visit www.cyberark.com.