Privileged Access Workstation (PAW)

Securing privileged access requires a broad range of elements including technical components (host defenses, account protections, identity management) as well as changes to process, and administrative practices.
Useful Links:

- Red Forest Design
- Microsoft: Securing Privileged Access
    - Privileged Access Workstations Overview and Deployment
- Microsoft Blog: PAW Solution – This links contains updated blog posts on how to deploy
    - PAW Deployment Guide
    - PAW Host Buildout
- Secure Privileged Access Blog List

- Session: How Microsoft IT used Win10 and Server2016 to implement Privileged Access
- Session: How to build PAW on same Domain

Instructions

Each security control is listed in a recommended order that should be followed when starting out. Each document is labeled **## - Title**. Each file explains what's going on and how to apply the control.

To alleviate troubleshooting, fully test your environment before continuing to the next section. Literally spend several days living under the new policy to see how things work.

Where a script is concerned, specific instructions and requirements to run the script can be found within the script's comment header.

What is a PAW?

In short, a PAW is one solution to the problem of credential theft, replay and pivoting attacks, and privilege escalation. PAW is a method of administering network devices in a more secure and more hardened environment than what most admins are used to. A successful PAW deployment will contain many security controls aimed to enable a more Defense in Depth security strategy.

Okay, but what is a PAW?

A PAW is the workstation the admin uses to access and administrate the network using privileged credentials. It provides the admin a secure method to perform day-to-day administrative tasks on network devices such as Domain Controllers, member servers, user workstations, networking equipment, and cloud admin portals (like Azure and AWS).

Because the PAW adheres to the Clean Source Security Principal, it prevents the logged-on user from freely surfing the Internet, checking email, running applications outside of the AppLocker whitelist, or insecurely accessing network devices that could expose risk to credential theft. It provides the admin everything they need to do their job.

How is a PAW physically different from a normal workstation where I administer my servers with RDP and MMC?

The PAW is a physical workstation, preferably a laptop, that runs Windows 10 Enterprise Edition (1709+) as the primary host OS. This device is used to administer the network and all the systems on it. It has the Hyper-V role installed that, in addition to security features like Credential Guard, hosts a VM that provides the admin day-to-day Internet access and email. PAWs have several hardware requirements to make for the most secure deployment:

- Windows 10 compatible (no Chromebook or Mac)
- TPM 2.0
- Enough hard drive space, CPU, and RAM resources to have a pleasant experience in your day-to-day VM