POP – Privileged Access Workstation (PAW): Fundamentals

Help prevent the compromise of privileged account credentials from cyber-attacks

Benefits

- Highly secured and usable workstations to protect all types of admin accounts
- Dedicated domain accounts for admins which are restricted to high trust clients to avoid accidental credential exposure
- Built in a secure lab with known good media, and easily deployed using Microsoft Deployment Toolkit
- Automated creation of Active Directory structures and policies that harden and protect the PAWs and admin accounts
- Increased security by preventing vulnerable applications in software from being successfully exploited by attackers
- Can restrict Internet browsing and other high-risk activities of administrative account users

Duration:

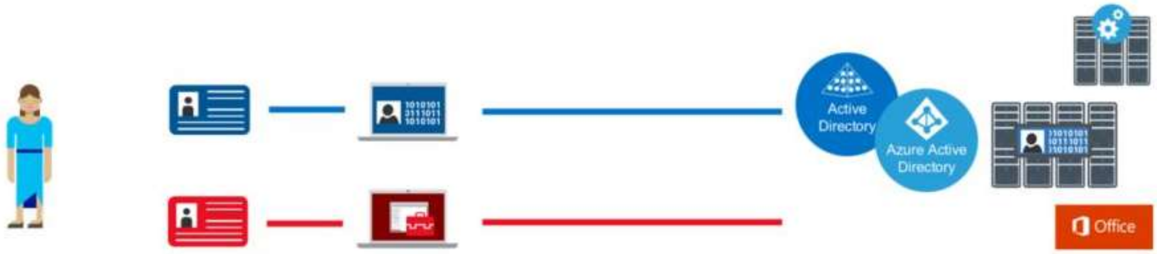
- 4 days

Overview

Cyber-attacks continue to increase in persistence and sophistication.
Attackers use a variety of techniques to steal credentials, constantly seeking administrative access to fully control corporate and government computing environments. Loss of privileged user accounts results in attackers having access to most or all of an organization's electronic documents, presentations, applications, databases, and other intellectual property.
Additionally, attackers can implant backdoors on any system, which can often evade antimalware and intrusion detection systems. Organizations should seek to protect admin accounts as one of their most valuable assets. The only safe recovery from an admin compromise is building a brand new environment, which can be extremely difficult, slow, and expensive.

Credential Hygiene and PAW

Credential hygiene is the recommended practice of verifying that privileged user accounts only log on to workstations and servers that are sufficiently trusted and are not used to perform high-risk activities such as Internet browsing. This is critical because an administrator who uses a low-trust workstation might unwittingly access attacker-controlled malware that might be used to steal the administrator's credentials.
Privileged Access Workstation (PAW) enforces credential hygiene by separating administrative accounts from normal user accounts (such as those for email and web browsing) and compartmentalizing logon access for each type of administrative account.
Microsoft Services provides a 4 days engagement to assist you in creating a PAW in Pre-Production (Lab) environment and supporting Active Directory configurations as described at: http://aka.ms/cyberpaw. We provide you a hardened, standardized administrative image, and assistance with deployment to a single administrator' machine in Pre-Production environment.



PAW Solution Details

Technologies Used in this Solution

- *Windows 10, Build 1607 (x64-based processor) or later*
- *Windows Server 2016 RTM (or 2012 R2) Active Directory Domain Services*
- *Group Policy-based Security Baselines applied to all systems*
- *Microsoft Deployment Toolkit 2013 server with Update 2*
- *BitLocker*
- *Credential Guard*
- *EMET*
- *Windows Defender*

Environment Requirements

Customer will need to provide:

- *Conference room with projection display*
- *Lab environment*

The POP - Privileged Access Workstation (PAW): Fundamentals is a four day engagement with a Microsoft Premier Field Engineer working alongside the customer's Security and Active Directory staff. The deliverables will consist of training, knowledge transfer and implementation of PAW in a customer provided lab.

Advanced Protection Technologies

Administrators log on to dedicated physical workstations that are hardened to improve their ability to resist remote attacks, local privilege escalation attacks, and physical compromise. The solution employs hardened configuration policies, Credential Guard to protect privileged user credentials, Windows BitLocker Drive Encryption for system integrity, and the Enhanced Mitigation Experience Toolkit (EMET) for improved exploit-technique protections.

Solution Delivery and Content

This solution uses extensive automation to provide consistency during the deployment of each PAW, and to configure the customer's Pre-Production Active Directory with the necessary structure and policies to enforce the security controls necessary for modern credential theft mitigation.

Agenda

This service is a four day engagement with a Microsoft Premier Field Engineer working alongside the customer's Security and Active Directory staff. The deliverables will consist of training, knowledge transfer and implementation of the PAW in a customer provided lab. An example agenda is as follows:

Day 1

- POP PAW Engagement Workshop - PowerPoint Module reviewing the current threat landscape and PAW deployment
- Building MDT server using prepared ISO

Day 2

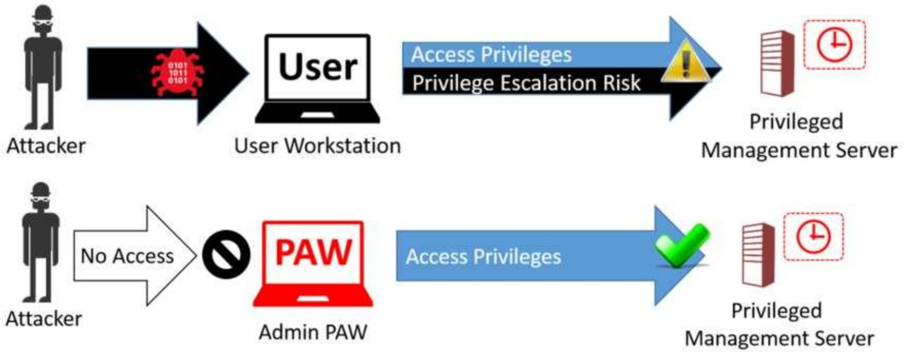
- Tier Model Overview - Demonstrating the Tier model environment to customer
- Initial Deployment - Test deployment of PAW to test driver import and deployment
- Test deployment - Stabilizing deployment process

Day 3

- PAW Deployment Testing - Functional Testing

Day 4

- PAW Education on Tier model - Demonstrating how the model works



For more information about Consulting and Support solutions from Microsoft, contact your Microsoft Services representative or visit www.microsoft.com/services