

Windows Server 2022: Secure On-premises and Hybrid Infrastructure

Secure the Windows Server Operating System



Tim Warner

Microsoft Azure Solutions Architect

@TechTrainerTim TechTrainerTim.com



Overview



Configure and manage exploit protection

**Configure and manage Windows Defender
Application Control**

**Configure and manage Windows Defender
for Endpoint**

**Configure and manage Windows Defender
Credential Guard**

Configure SmartScreen

**Implement operating system security by
using Group Policies**



Windows Server 2022: Secure On-premises and Hybrid Infrastructure

Secure the Windows Server Operating System

Secure Hybrid Active Directory Accounts

Configure Hybrid Active Directory Account Security

Remediate Windows Server Security Issues with Azure Services

Secure Windows Server Networking

Secure Windows Server Storage



Windows Server Hybrid Administrator Associate

Take two exams



CERTIFICATION EXAM **AZ-800**
**Administering Windows Server
Hybrid Core Infrastructure**

AND



CERTIFICATION EXAM **AZ-801**
**Configuring Windows Server
Hybrid Advanced Services**

Earn the certification




ASSOCIATE CERTIFICATION
**Microsoft Certified:
Windows Server Hybrid
Administrator Associate**

One-year cert validity



Exercise Files



What do you want to learn?

Timothy
timothywarner316@gmail.com

Troubleshooting with Microsoft Azure Network Watcher

by Tim Warner

Microsoft now gives you packet-level access to your Windows Server and Linux virtual machines (VMs) running in Azure. You'll learn how to use Network Watcher to troubleshoot network security groups (NSGs), perform packet captures, and much more.

[Resume Course](#) [Bookmark](#) [Add to Channel](#)

Table of contents

Description

Transcript

Exercise files

Discussion


Learning Check

Recommended

These exercise files are intended to provide you with the assets you need to create a video-based hands-on experience. With the exercise files, you can follow along with the author and re-create the same solution on your computer. We find this to be even more effective than written lab exercises.

[Download exercise files](#)

Course author

 **Tim Warner**

Timothy Warner is a Microsoft Most Valuable Professional (MVP) in Cloud and Datacenter Management who is based in Nashville, TN.

Course info

Level	Intermediate
Rating	★★★★★
My rating	★★★★★
Duration	2h 12m
Released	31 Oct 2017

Share course

[f](#) [t](#) [g+](#) [in](#)



Exercise Files

The screenshot displays a Windows desktop environment with three overlapping windows:

- File Explorer (Left):** Shows the path `C:\Users\Tim\Downloads\azur`. The file list contains folders named 02, 03, 04, 05, and 06. Folder 02 is selected. The status bar indicates `0 / 5 object(s) selected`.
- Code Editor (Center):** The title bar reads `File Edit Selection View Go Debug ... microsoft-azure-ad-privileged-identity-management-configuring-m4-links.t...`. The active file is `microsoft-azure-ad-privileged-identity-management-configuring-m4-links.txt`. The content of the file is as follows:

```
1 Module 4: Organize and Perform Azure AD PIM Access Reviews↵
2 ↵
3 Microsoft Azure↵
4 https://azure.microsoft.com/en-us/↵
5 ↵
6 Azure Documentation↵
7 https://docs.microsoft.com/en-us/azure/↵
8 ↵
9 Azure AD Privileged Identity Management (PIM) documentation | Microsoft Docs↵
10 https://docs.microsoft.com/en-us/azure/active-directory/
    privileged-identity-management/↵
11 ↵
12 Identity Governance - Azure Active Directory | Microsoft Docs↵
13 https://docs.microsoft.com/en-us/azure/active-directory/governance/
    identity-governance-overview↵
14 ↵
15 Create an access review of Azure resource roles in PIM - Azure Active Directory |
    Microsoft Docs↵
16 https://docs.microsoft.com/en-us/azure/active-directory/
    privileged-identity-management/pim-resource-roles-start-access-review↵
17 ↵
18 Review access to Azure AD roles in PIM - Azure Active Directory | Microsoft Docs↵
19 https://docs.microsoft.com/en-us/azure/active-directory/
    privileged-identity-management/pim-how-to-perform-security-review↵
20 ↵
21 View audit history for Azure AD roles in PIM - Azure Active Directory | Microsoft
    Docs↵
22 https://docs.microsoft.com/en-us/azure/active-directory/
    privileged-identity-management/pim-how-to-use-audit-log↵
```

The status bar at the bottom shows `Spaces: 4 UTF-8 CRLF Plain Text`.
- File Details Window (Right):** Shows the path `02\demos\`. It contains a table with file details:

	Size	Pac
	1 298	
	359	



Exploit Protection

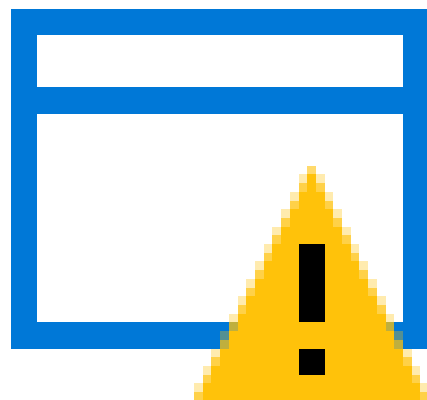


Exploit

A software tool designed to take advantage of a vulnerability in a computer system, typically for malicious purposes such as installing malware



Windows Defender Exploit Guard



Replaces the Enhanced Mitigation Experience Toolkit (EMET)

Host-based, Intelligent Security Graph (ISG)-powered intrusion prevention solution

Provides Attack Surface Reduction (ASR) for Windows concerning the most common hardware/malware attack vectors

Configured in Security app and/or Group Policy



~~Windows~~ Microsoft Defender Protection Products



Microsoft Defender Product Family

Cloud services

- **Defender for Endpoint**
- **Defender for Identity**
- **Defender for Cloud**
 - **Defender for Servers**

System services

- **Defender Exploit Guard**
- **Defender Application Control**
- **Defender SmartScreen**



Windows Defender Application Control



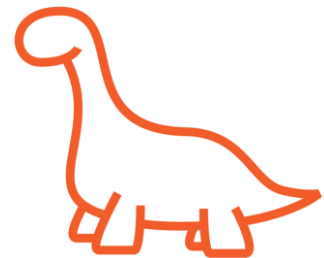
WDAC allows only allowed (trusted) device drivers and software to run on the managed servers



Two enforcement modes: Audit Only and Enforcement Enabled



No system requirements (compare with Credential Guard, which uses HVCI)



Compare with AppLocker (which no longer receives feature improvements)



AppLocker may be useful to support downlevel Windows versions and/or when you don't need DLL or driver enforcement



Microsoft Defender for Endpoint

**ISG-powered
threat-vulnerability
mgmt. client**

**Available for
Windows, macOS,
Android, iOS**

**Centralized
management via
web portal**

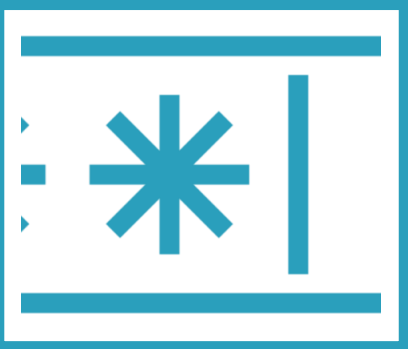
**UI in Windows
Security app**

**Defender for
Servers grants
license**

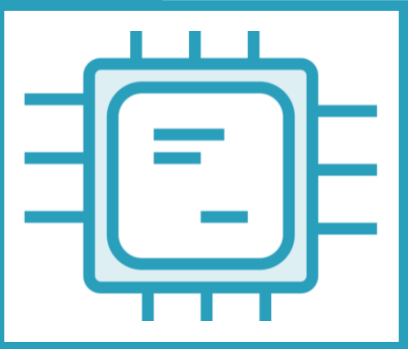
**Integrates with
Sentinel, Intune,
Defender...**



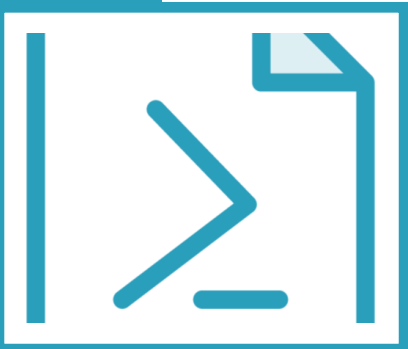
Windows Defender Credential Guard



Protects users against NTLM Pass-the-Hash or Kerberos Pass-the-Ticket attacks (password hashes/tickets stored in memory)



Virtualization-based protection (requires UEFI, TPM, Secure Boot)



Windows Defender Credential Guard hardware readiness tool (PowerShell)



Manage Credential Guard with Group Policy or Intune



SmartScreen



SmartScreen



Reputation-based protection against malicious websites and applications

- Phishing attempts
- Unsigned software

Microsoft-curated proprietary filter lists

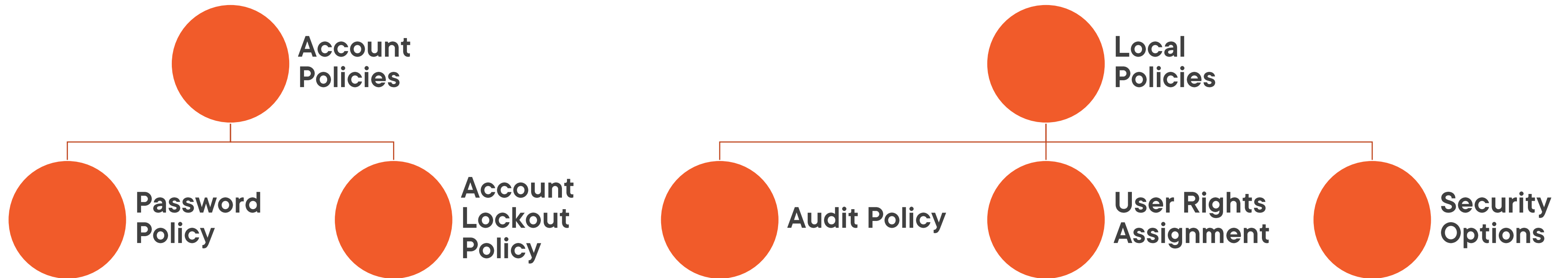
Management through Group Policy and Microsoft Intune



Group Policy-Based OS Security



Group Policy Security Policy Settings



Demo



1

Group Policy security settings

Traditional

App Control / Exploit / Cred Guard

Demo websites and software (EICAR)

SmartScreen

Defender for Cloud / Server

Defender for Endpoint portal



Summary



There was a time when Group Policy was "the only game in town" for enforcing system security

Trends:

- Cloud-based artificial intelligence
- Hybrid cloud integration
- Trusted boot/code allow lists

Lead: "Yeah, but what about protecting our user identities themselves?"



Up Next:

Secure Hybrid Active Directory Accounts

