

The logo for The Experts Conference (TEC) is displayed. The letters 'T' and 'E' are in a bold, orange, sans-serif font. The letter 'C' is in a bold, light blue, sans-serif font. A thin white vertical line is positioned to the right of the 'C'.

**TEC**

**The Experts  
Conference**

*Sponsored by Quest®*

# TEC

## The Experts Conference

*Sponsored by Quest®*



**Sean Metcalf**

Founder/CTO Trimarc

## Defending the Identity Nexus

#TEC2022



# About

- Founder & CTO @ Trimarc ([Trimarc.io](https://Trimarc.io)), a professional services company that helps organizations better secure their Active Directory, Azure AD, & VMware environments.
- Microsoft Certified Master (MCM) Directory Services
- Microsoft MVP
- Speaker: Black Hat, Blue Hat, Blue Team Con, BSides Charm, BSides DC, BSides PR, DEF CON, DerbyCon, TEC
- Security Consultant / Researcher
- AD Enthusiast - Own & Operate [ADSecurity.org](https://ADSecurity.org) (Microsoft platform security info)

# About

- Founder & CTO @ Trimarc ([Trimarc.io](https://Trimarc.io)), a professional services company that helps organizations better secure their Active Directory, Azure AD, & VMware environments.
- Microsoft Certified Master (MCM) Directory Services
- *Former* Microsoft MVP
- Speaker: Black Hat, Blue Hat, Blue Team Con, BSides Charm, BSides DC, BSides PR, DEF CON, DerbyCon, TEC
- Security Consultant / Researcher
- AD Enthusiast - Own & Operate [ADSecurity.org](https://ADSecurity.org) (Microsoft platform security info)



# Agenda

- Introduction
- Connected Systems
- The Identity Nexus
- Azure AD
- Attacking the Identity Nexus (Attack Scenarios)
- Mitigations
- Conclusion

# The Identity Nexus



#TEC2022

**TEC**

**The Experts  
Conference**  
*Sponsored by Quest®*

# Common Systems

PKI

Active Directory

VMware

PTA

AAD  
SSSO

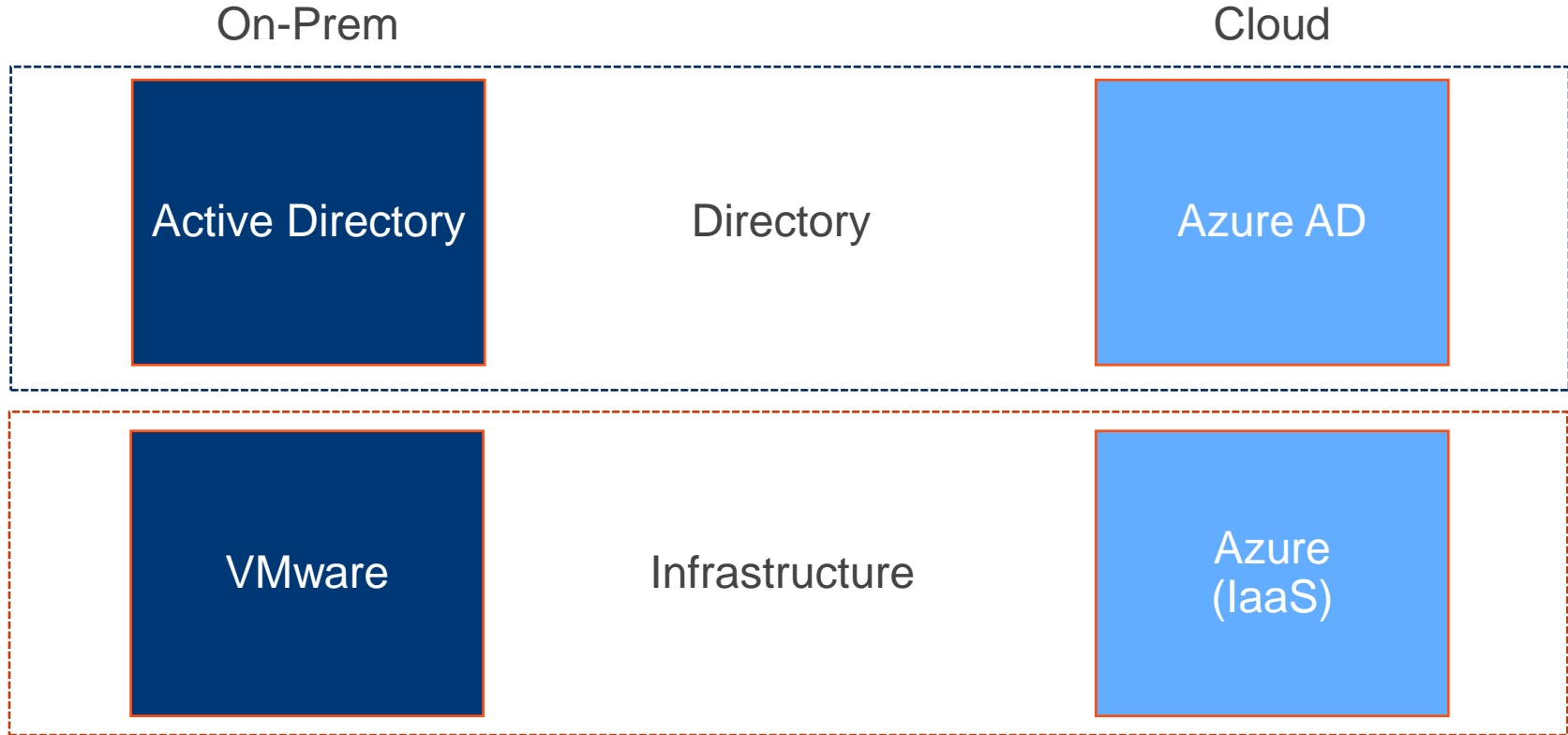
AAD  
Connect

ADFS

Azure AD

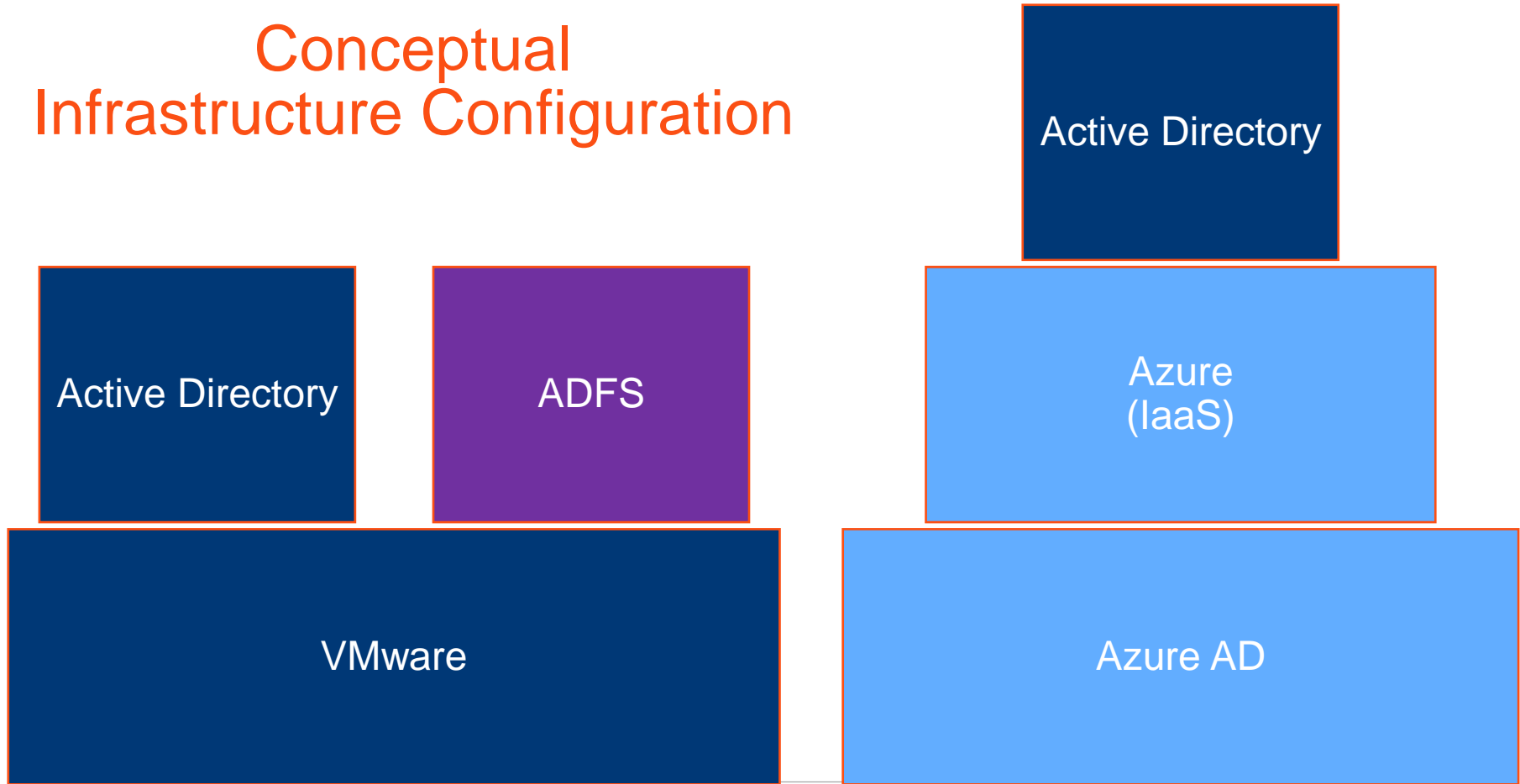
Azure  
(IaaS)

# The Identity Nexus

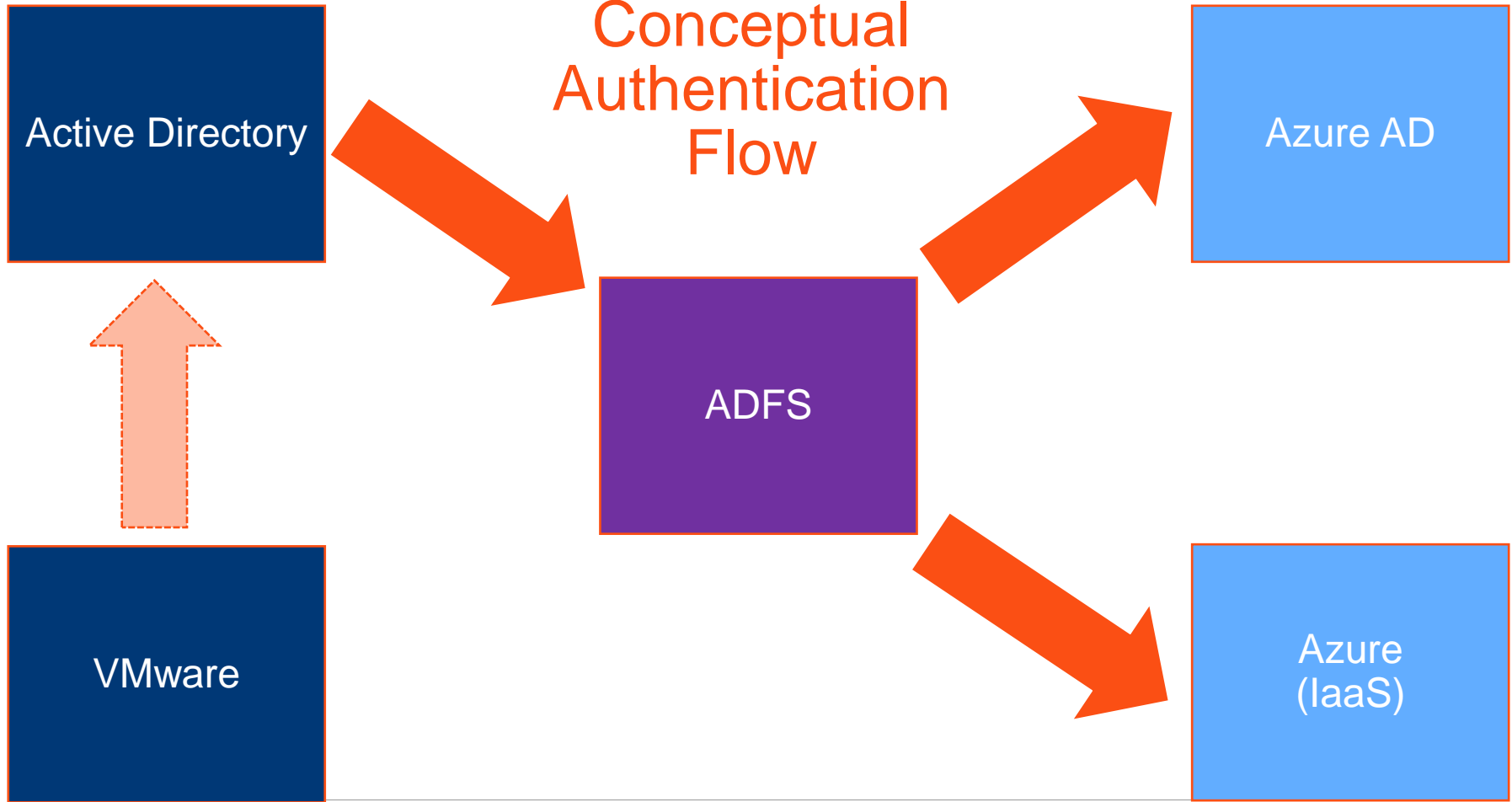




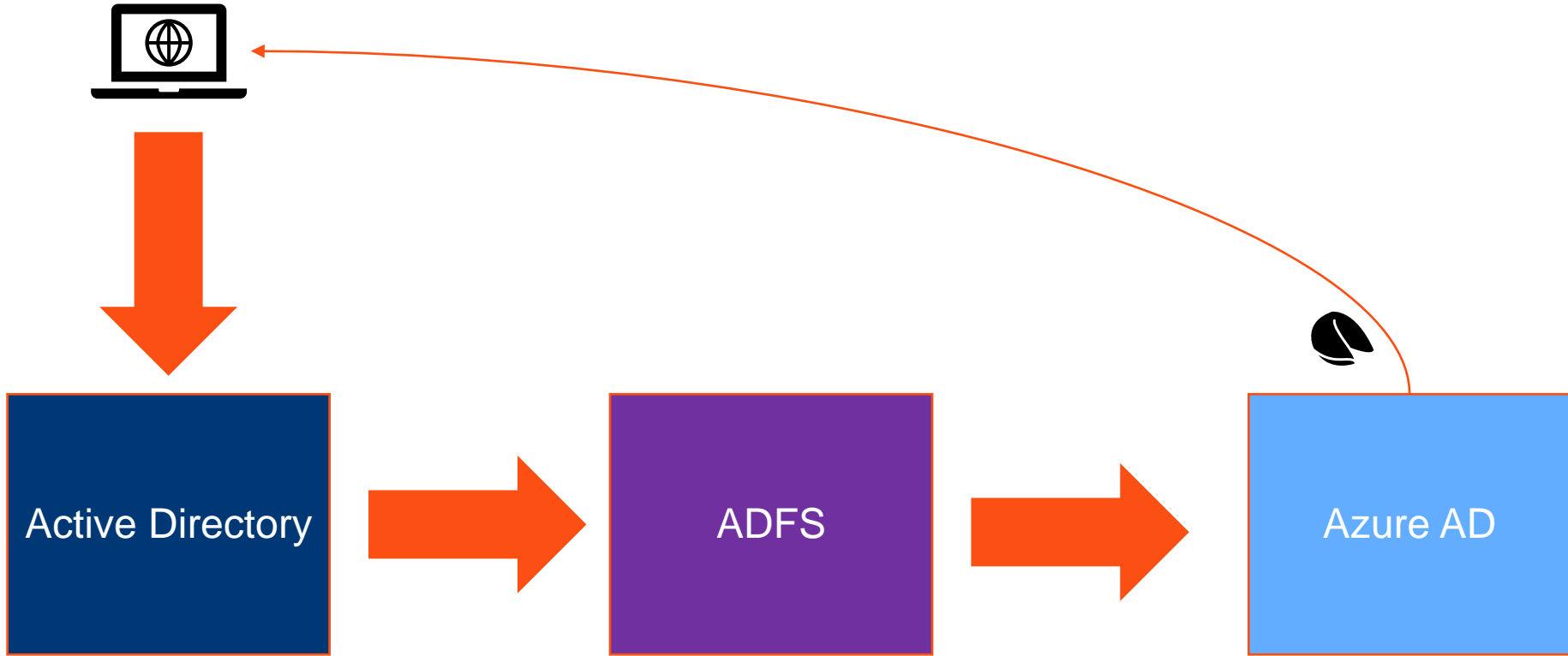
# Conceptual Infrastructure Configuration



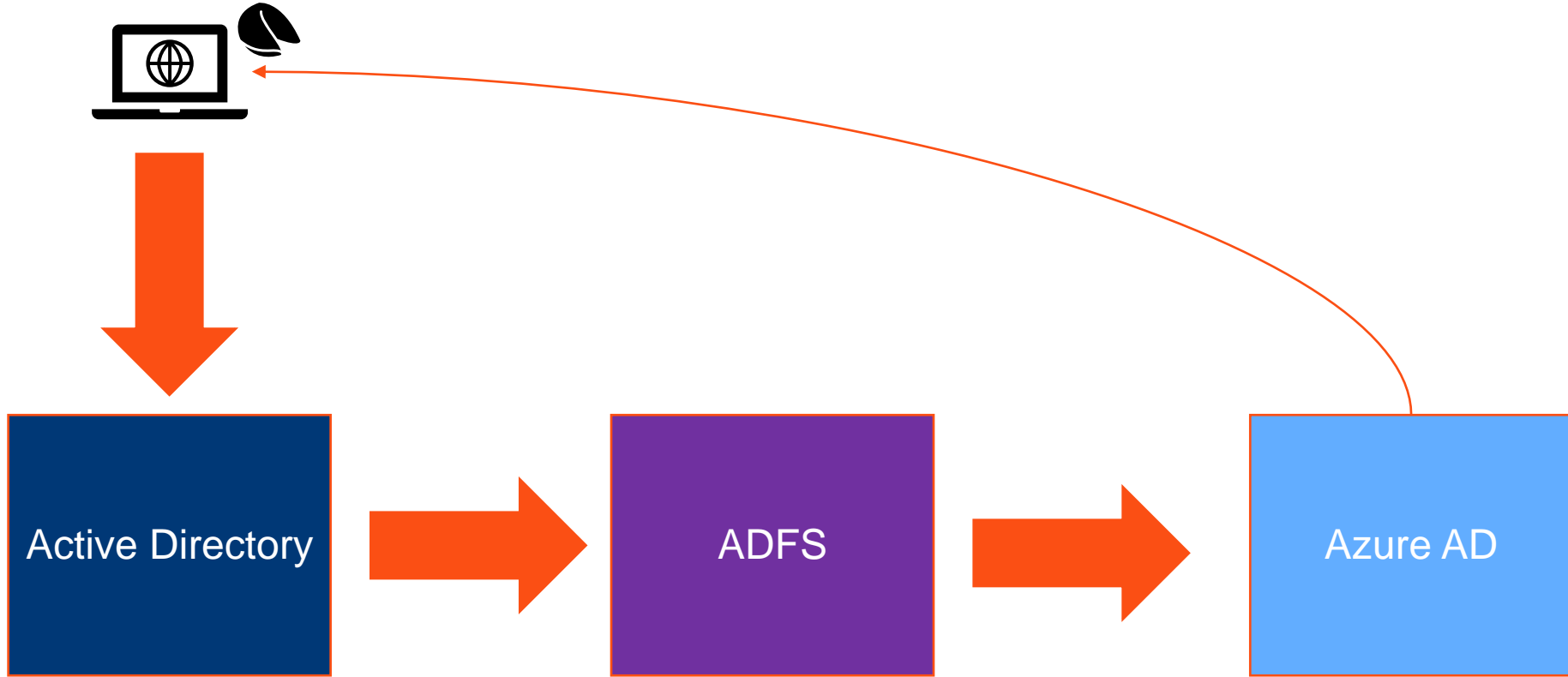
# Conceptual Authentication Flow



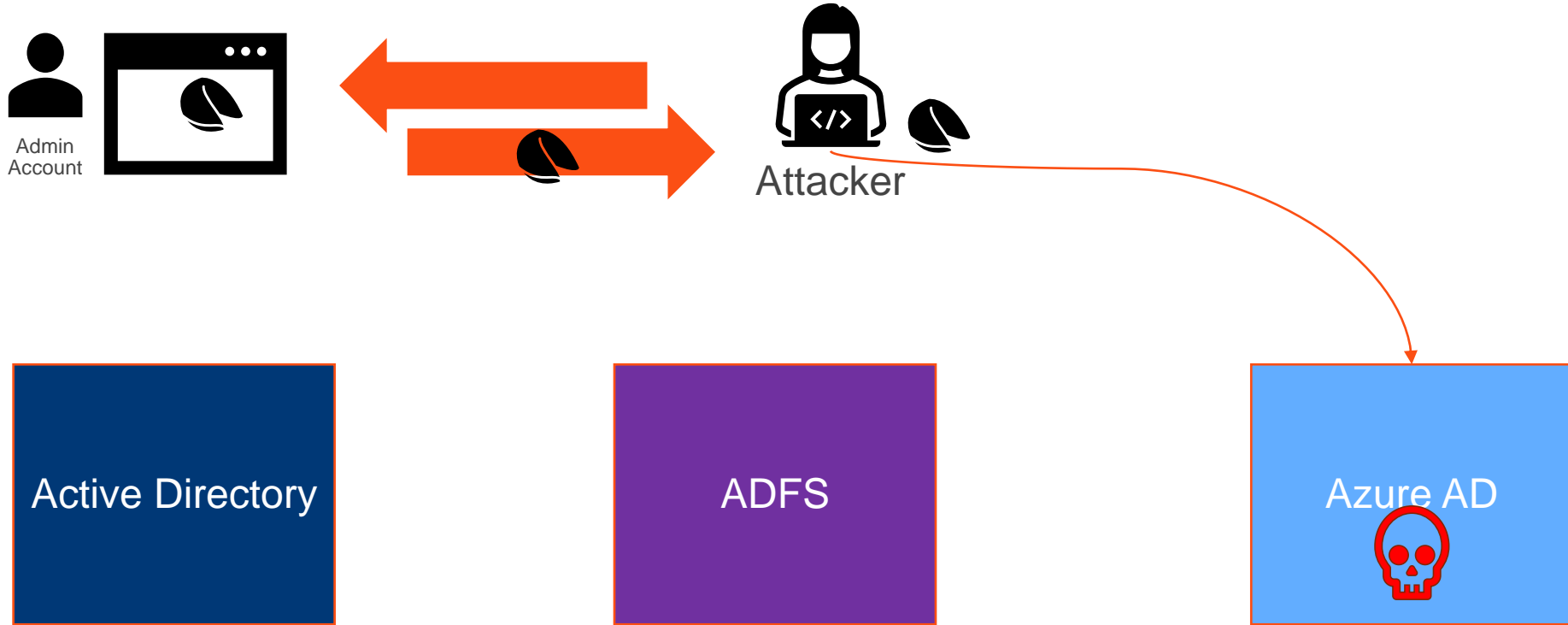
# Session Tokens (Cookies)



# Session Tokens (Cookies)



# Session Tokens (Cookies)





# The Root of Microsoft Cloud: Azure AD

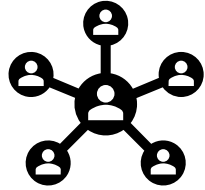
**TEC**

**The Experts  
Conference**

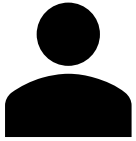
*Sponsored by Quest®*



# Background: Conceptual Comparison



Active  
Directory



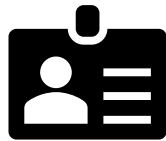
Account



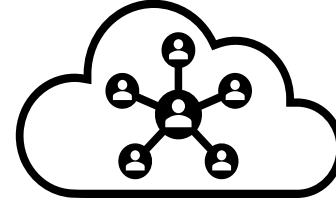
Service  
Account



Groups



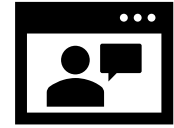
Permissions



Azure AD



Account



Application



Service  
Principal

# Background

## Highly Sensitive Application Permissions:

- **Directory.ReadWrite.All**: Effective Global Admin rights to AAD
- **RoleManagement.ReadWrite.Directory**: Ability to add members to Global Administrator and other roles
- **Application.ReadWrite.All**: Provides full rights to applications which could result in compromise if there are apps with highly privileged permissions
- **AppRoleAssignment.ReadWrite.All**: Provides the application the right to grant additional permissions to itself!
- **RoleManagement.ReadWrite.Directory\***  
(more on this one later)

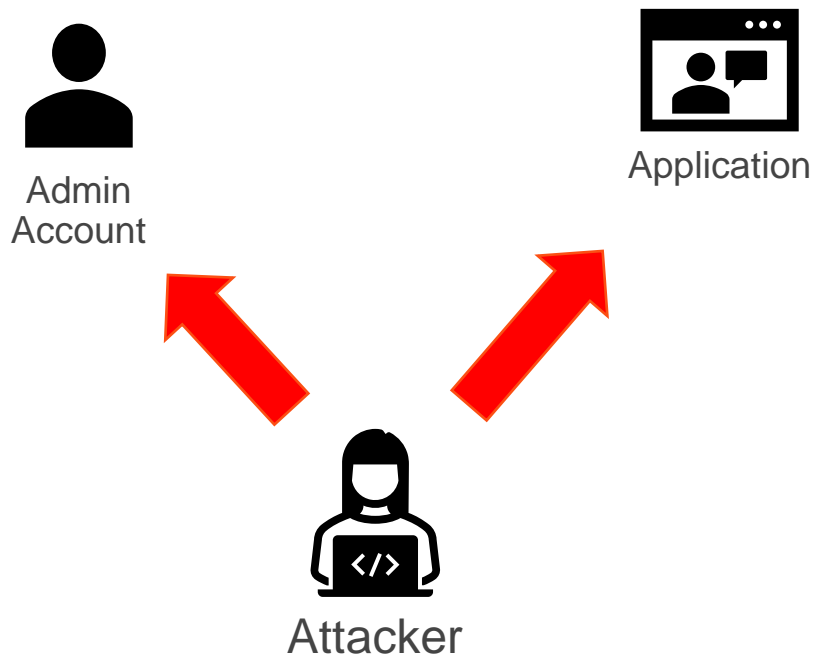
# Background

## ⊗ Caution

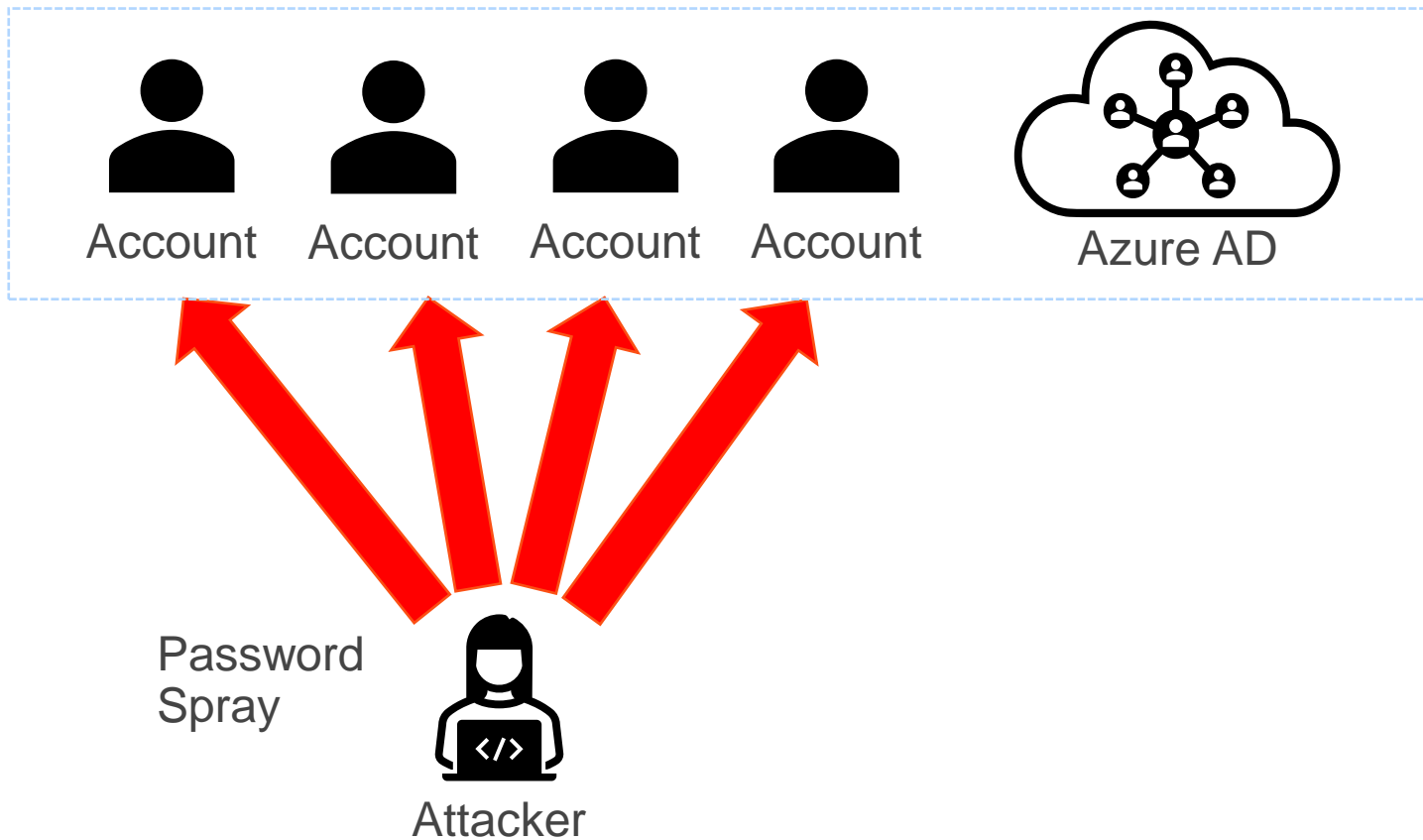
Permissions that allow granting authorization, such as *AppRoleAssignment.ReadWrite.All*, allow an application to grant additional privileges to itself, other applications, or any user. Likewise, permissions that allow managing credentials, such as *Application.ReadWrite.All*, allow an application to act as other entities, and use the privileges they were granted. Use caution when granting any of these permissions.

<https://learn.microsoft.com/en-us/graph/permissions-reference>

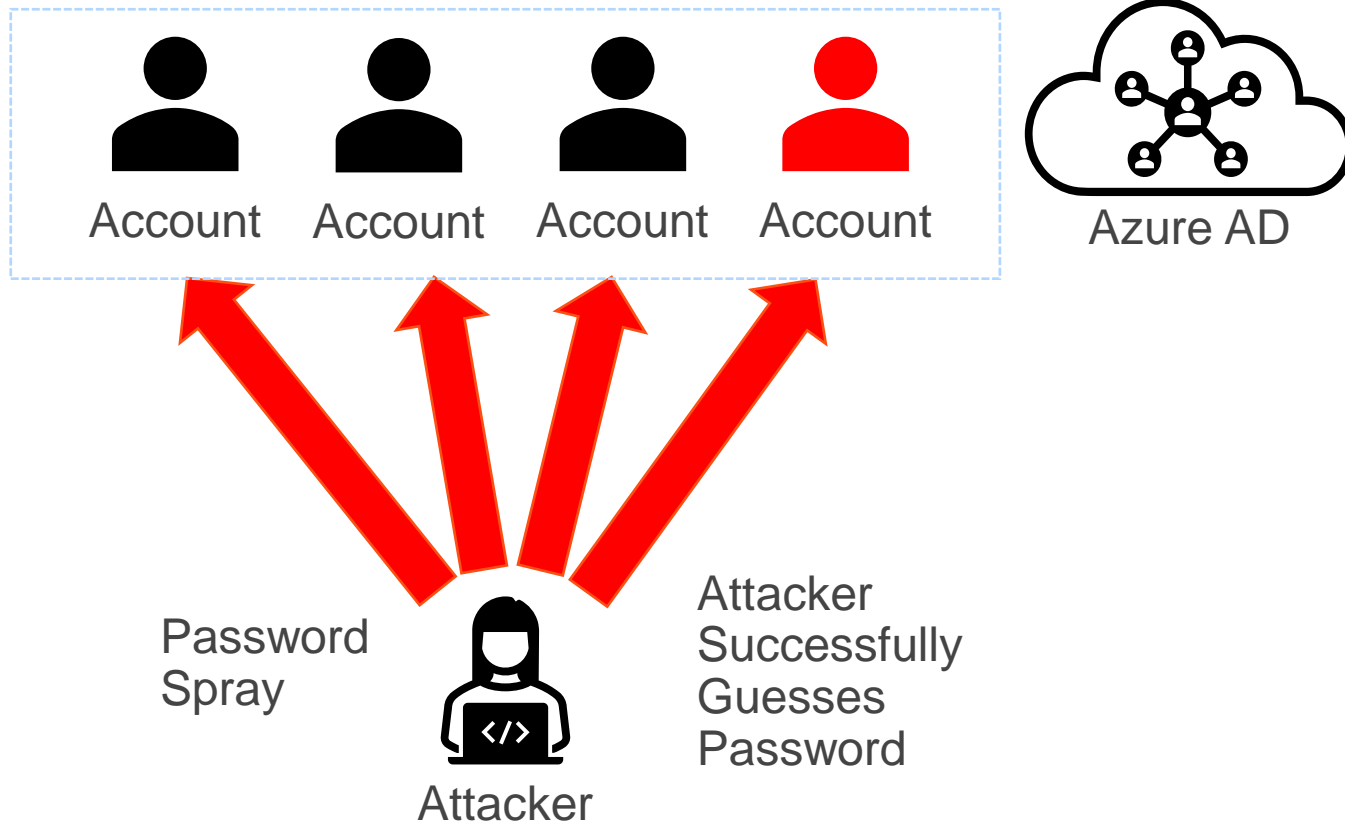
# Attacking Azure AD



# Attacking Azure AD Accounts

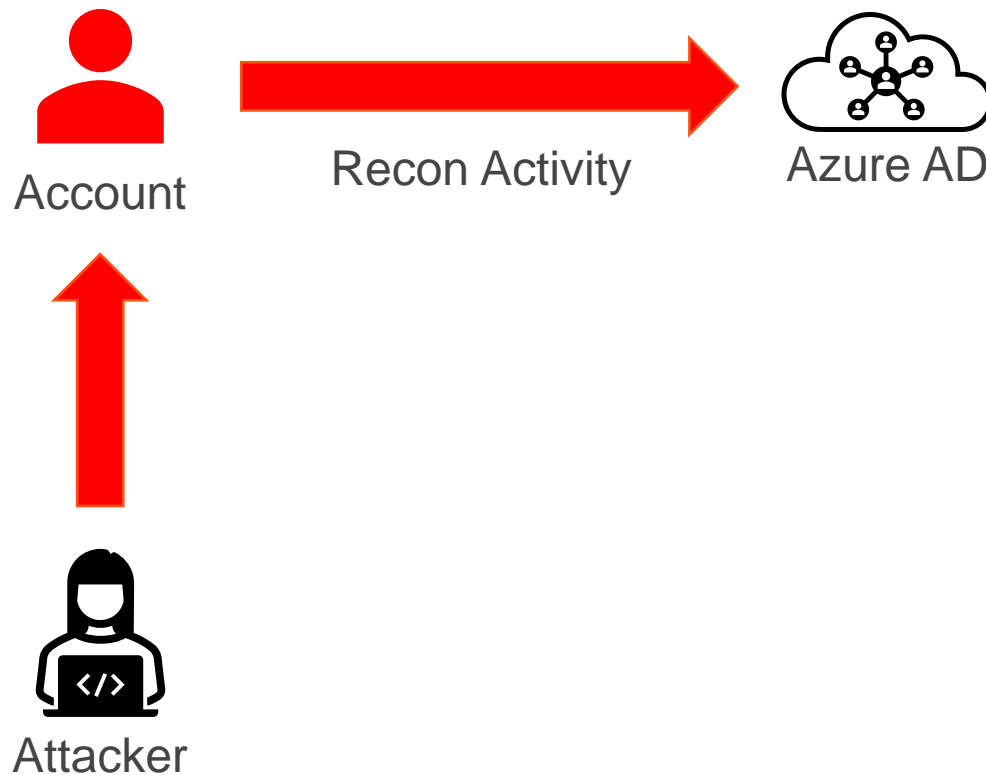


# Attacking Azure AD Accounts

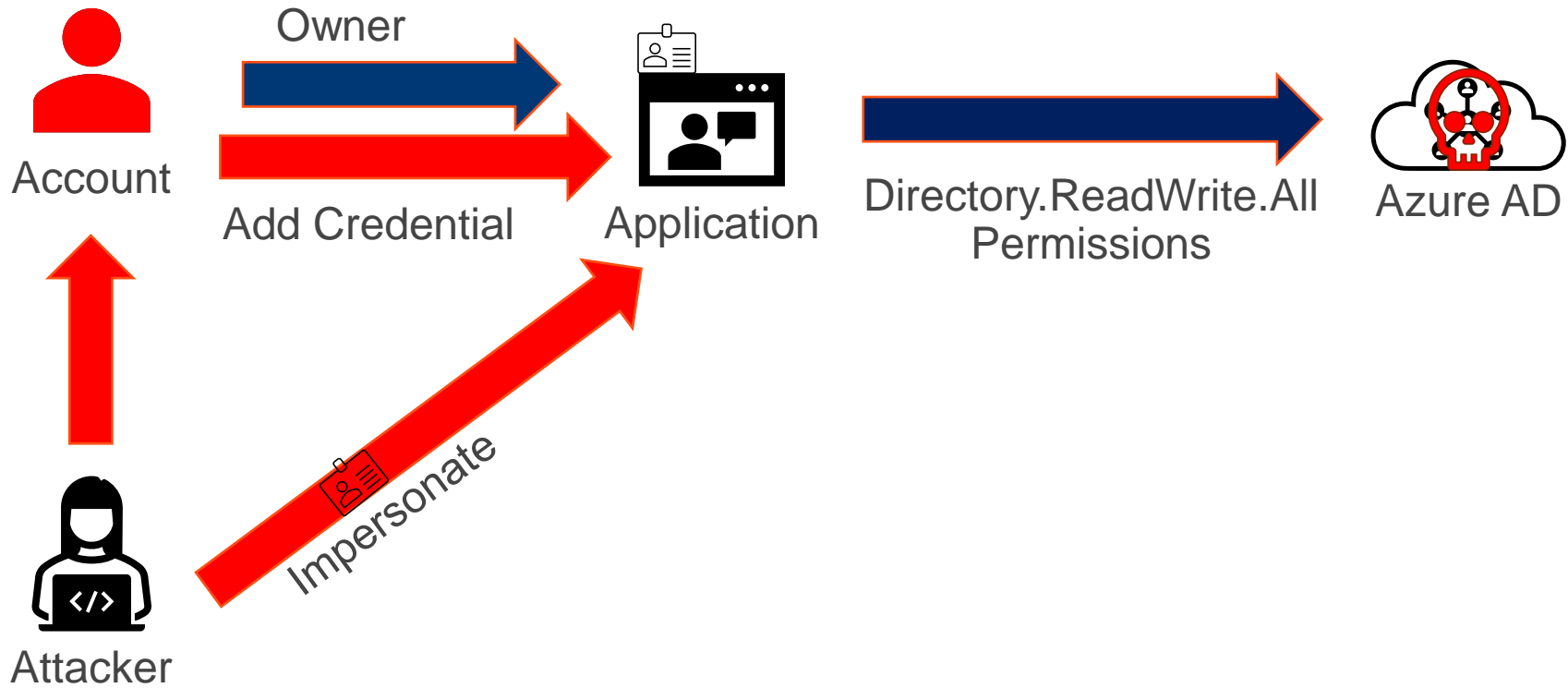




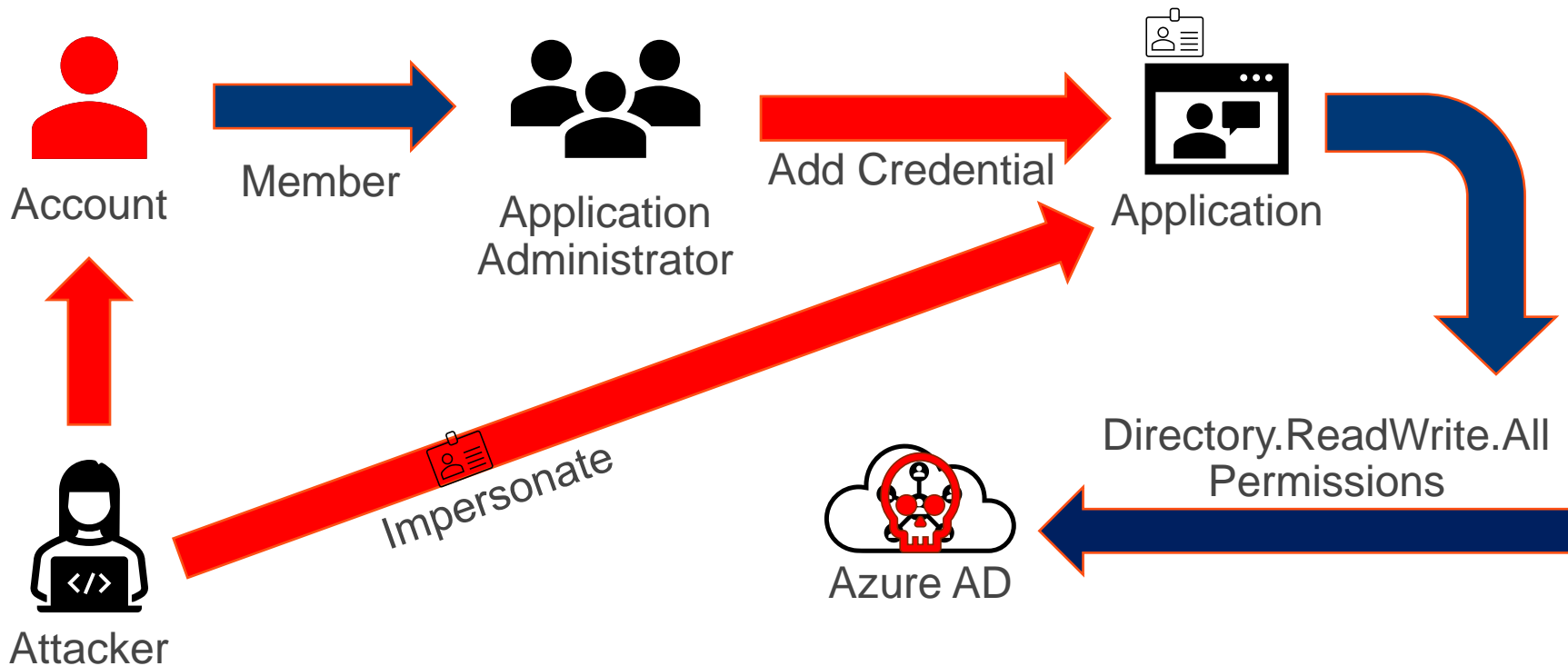
# Attacking Azure AD Accounts



# Compromise Azure AD through Application Permissions



# Compromise Azure AD through Application Permissions



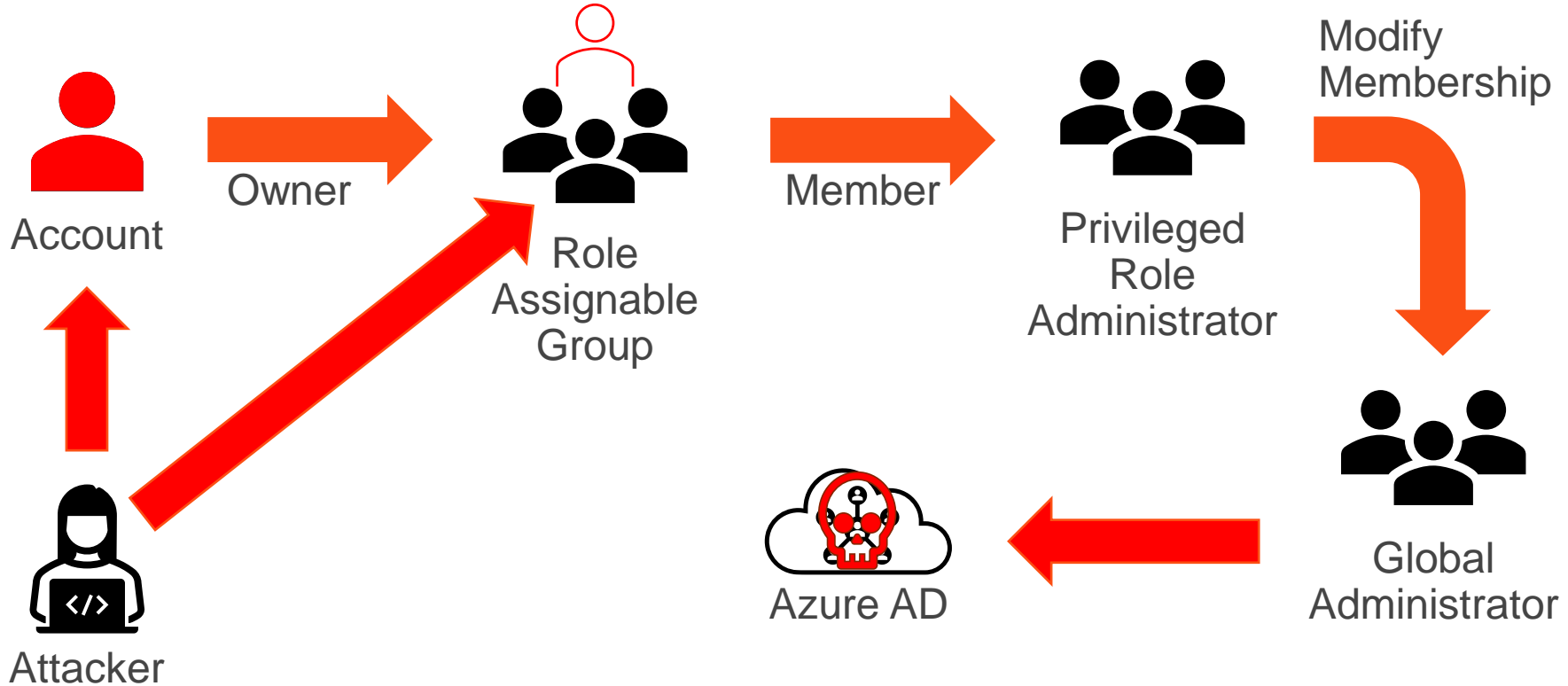
# Role Assignable Groups (RAGs)

- Role Assignable Groups are Security or Microsoft 365 group with the `isAssignableToRole` property set to true and cannot be dynamic.
- Role Assignable Groups were created to solve the potential issue where groups are added to an Azure AD role and a group admin could modify membership.
- Only Global Administrators or Privileged Role Administrators can create Role Assignable Groups and manage them (membership).
- Role Assignable Group owners can manage them.
- There is an application permission (Graph: `RoleManagement.ReadWrite.Directory`) that provides management rights as well.
- 500 role-assignable groups maximum in an Azure AD tenant (creation maximum).
- NOTE:  
Only a Privileged Authentication Administrator or a Global Administrator can change the credentials or reset MFA or modify sensitive attributes for members & owners of a role-assignable group.

# Attacking Role Assignable Groups (RAG)

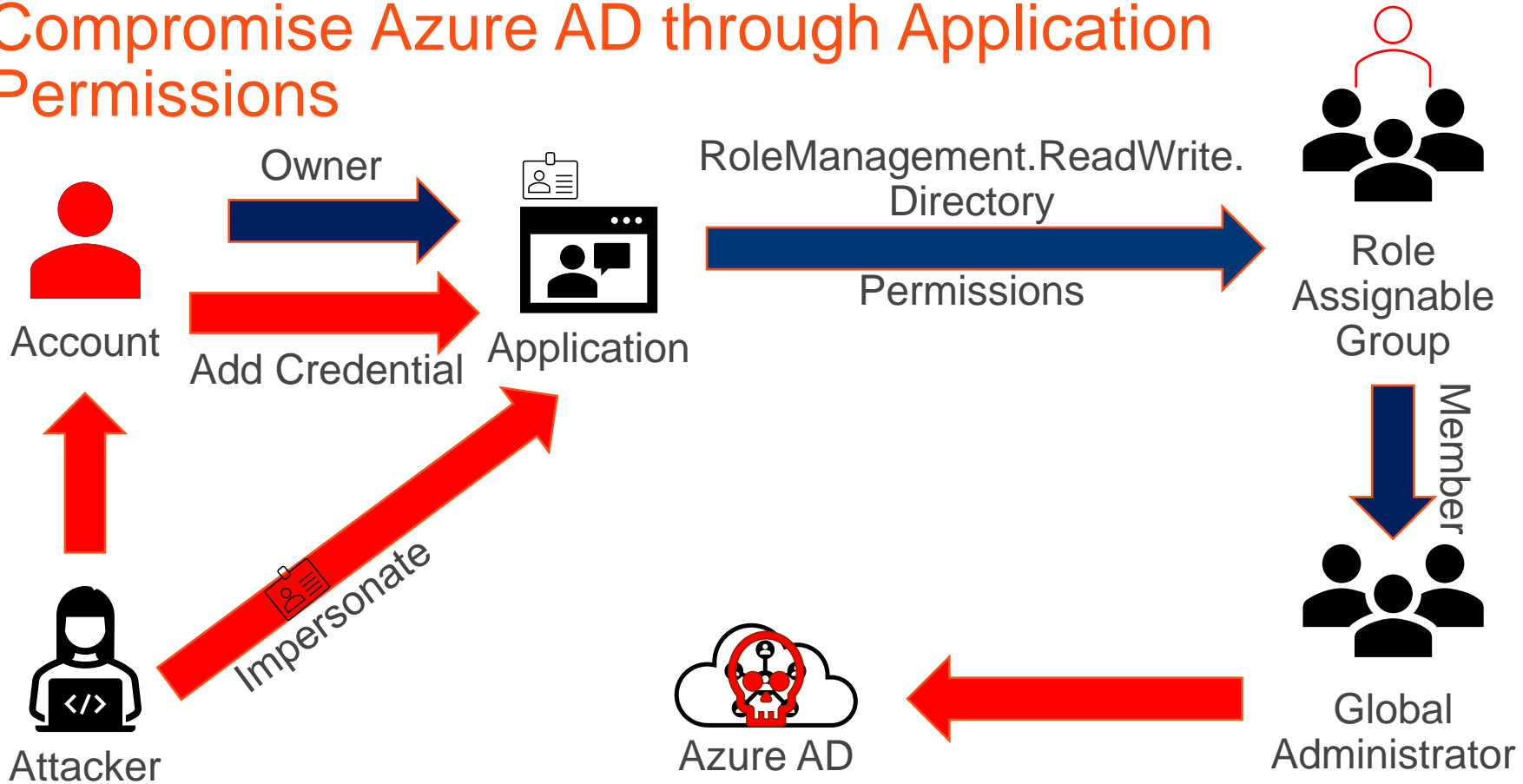
- Check RAG owners & Application permissions (*RoleManagement.ReadWrite.Directory*) to identify target accounts
- Identify Role Assignable Groups that are eligible/permanent members of privileged Azure AD roles.
- Compromise account to gain rights to modify RAG membership

# Compromise Azure AD through Role Assignable Group Configuration





# Compromise Azure AD through Application Permissions



# Role Assignable Group Security Check Logic

## IF

- There is at least one Role Assignable Group
- *AND*
  - At least one of them is eligible/permanent member of privileged Azure AD role
- *AND*
  - There is an owner for a Role Assignable Group
- *OR*
  - There are Role Assignable Group application permissions configured (RoleManagement.ReadWrite.Directory)

*Action: Review configuration and ensure it is appropriate.*

# Azure AD Permissions Security Check Logic

IF

- There is a highly privileged application
- *AND*
  - There is at least 1 member (eligible/permanent) of the AAD role “Application Administrator”

*OR*

- There is at least 1 member (eligible/permanent) of the AAD role “Cloud Application Administrator”

Questions to ask:

- Is the member a regular user account?
- Is the member an admin account?
- Is it already a member of a highly privileged AAD role?

# Azure AD Permissions Security Check Logic

IF

- There is a highly privileged application

AND

- There is an owner configured on that application

Questions to ask:

- Is the owner a regular user account?
- Is the owner an admin account?
- Is it already a member of a highly privileged AAD role?

# Common Azure AD Security Issues

- Customer using PIM, but all members are permanent, not eligible.
- Highly privileged applications with regular user as owner and/or regular user in App/Cloud App Admin role(s).
- Missing MFA on Admin Accounts with highly privileged AAD role rights.
- Users can consent to application permissions.
- Guest/external user accounts have the ability to invite other guests and have effectively the same visibility to the tenant as AAD users.
- Legacy authentication is not blocked through Conditional Access policies (Security Defaults).



# Attacking the Identity Nexus

# How We Think About Identity



# What Identity Actually Is

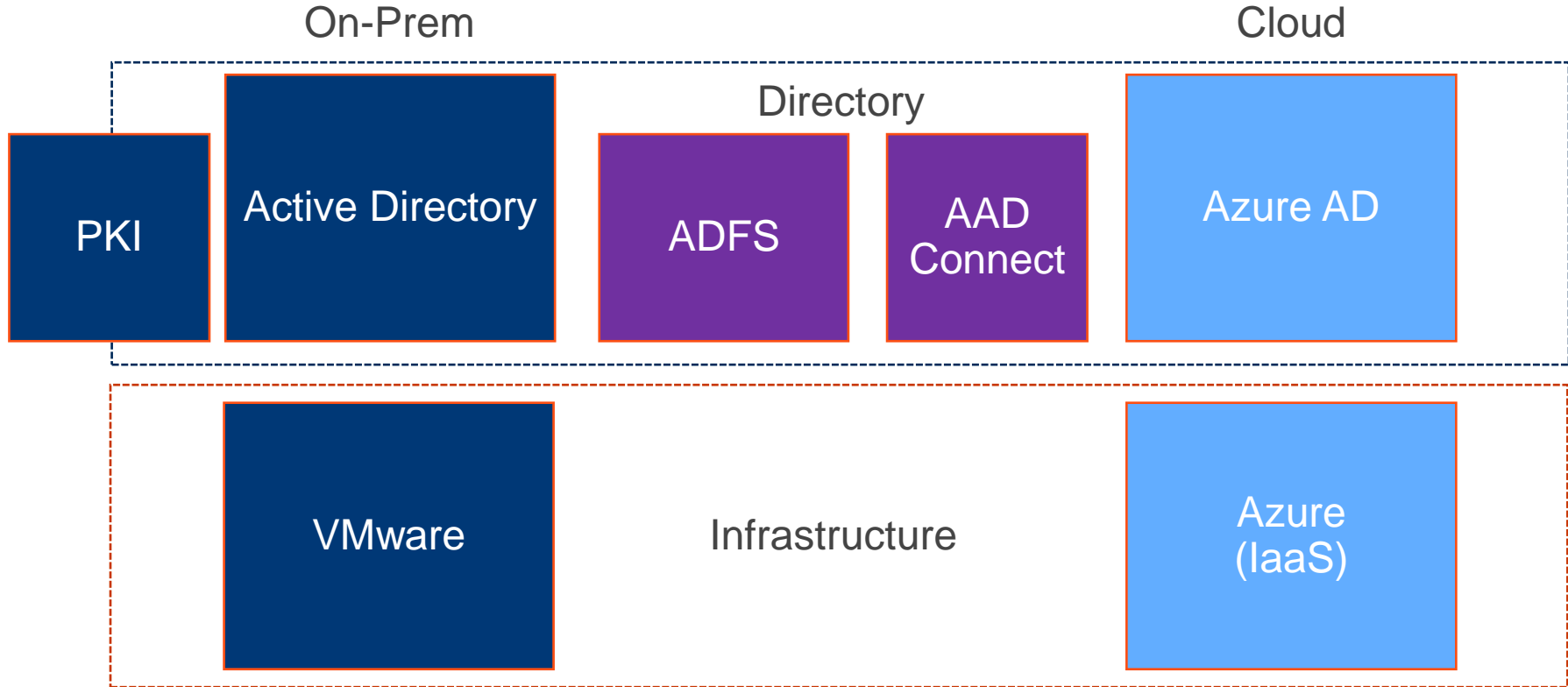




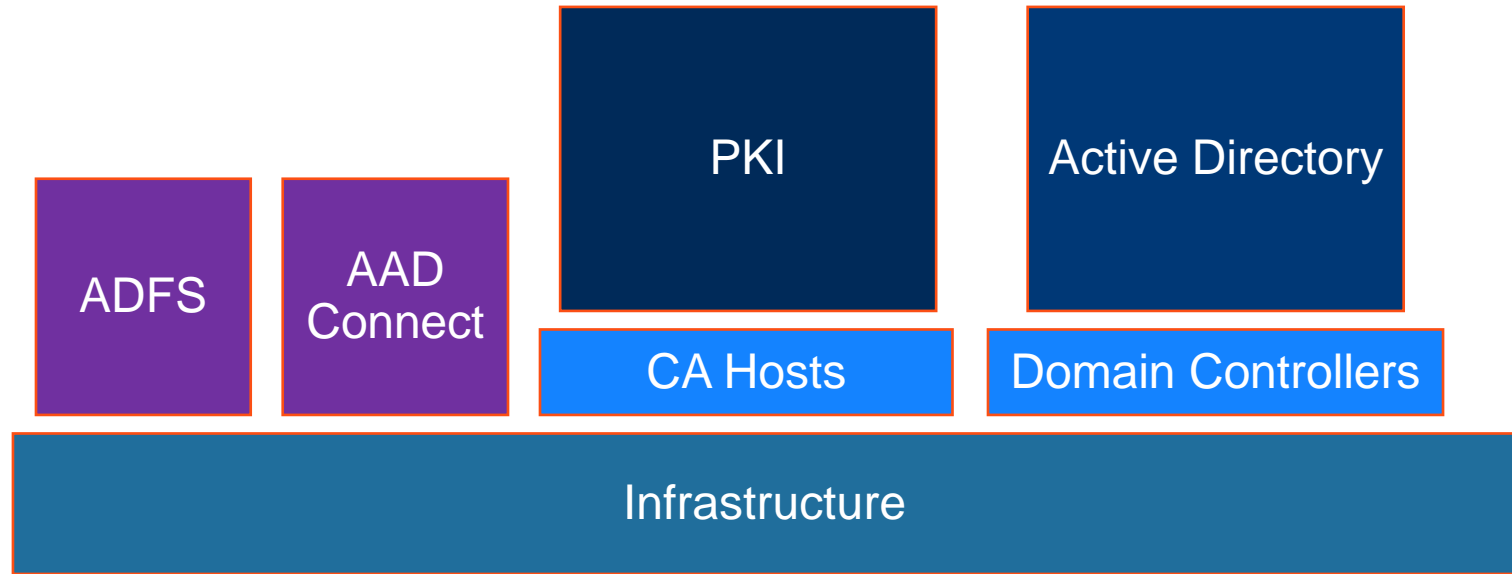
Or this



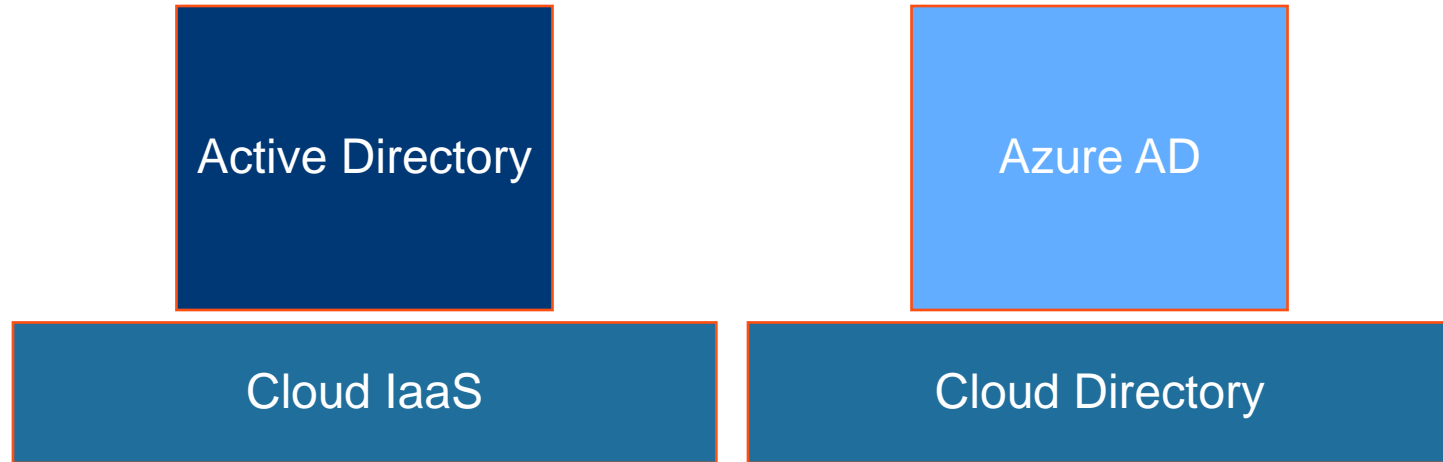
# The Identity Nexus



# On-Premises Systems



# Cloud Systems



# Attack Scenario

---

1. Password Vaults
2. VMware & AD
3. VMware & Azure AD
4. From Azure AD to AD
5. ADFS
6. Azure AD Connect
7. IPMI
8. Red Forest

**TEC**

**The Experts  
Conference**

*Sponsored by Quest®*

# Background: Enterprise Password Vault

- Being deployed more broadly to improve administrative security.
- Typically CyberArk or Thycotic SecretServer.
- “Reconciliation” DA account to bring accounts back into compliance/control.
- Password vault maintains admin accounts for AD & Azure AD.
- Additional components to augment security like a “Session Manager”.

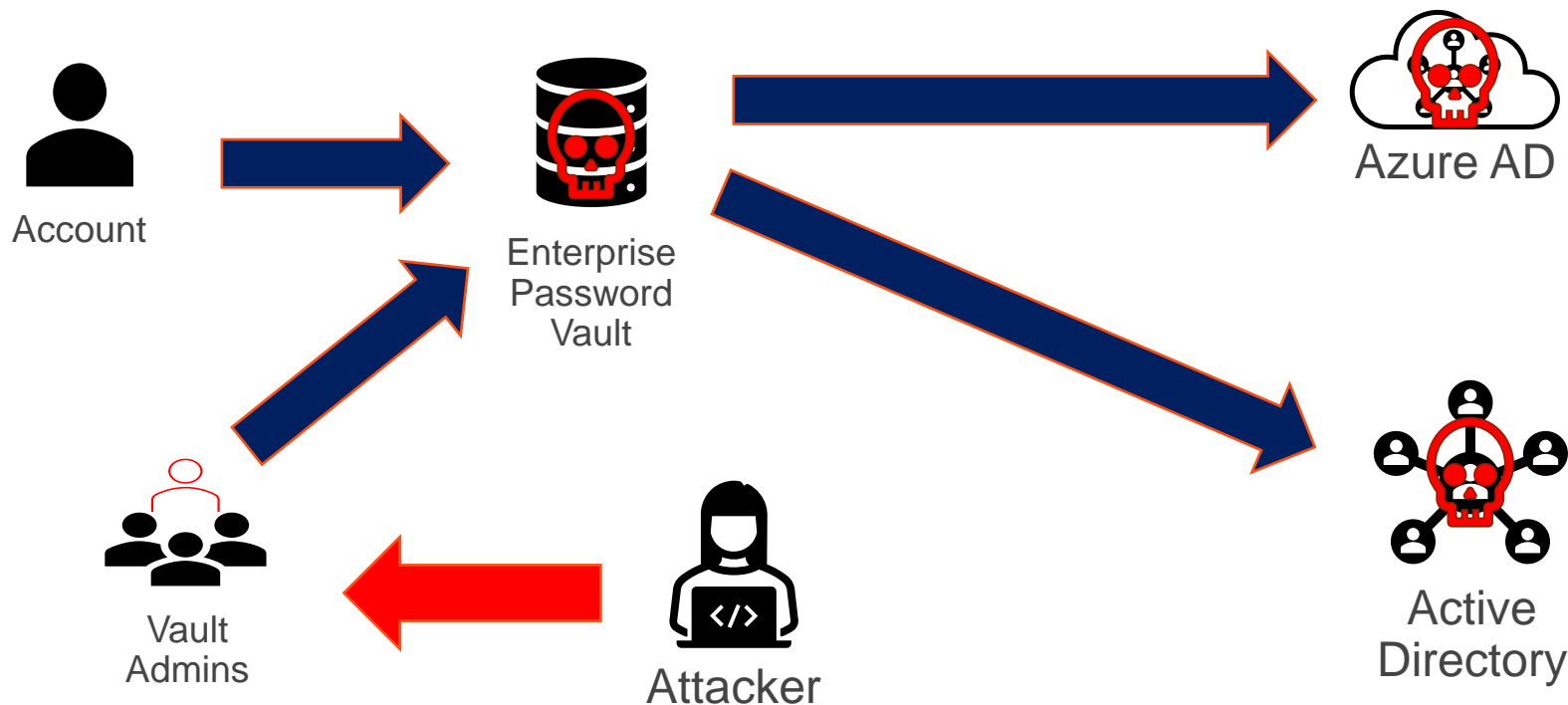


There's Something  
About Password Vaults

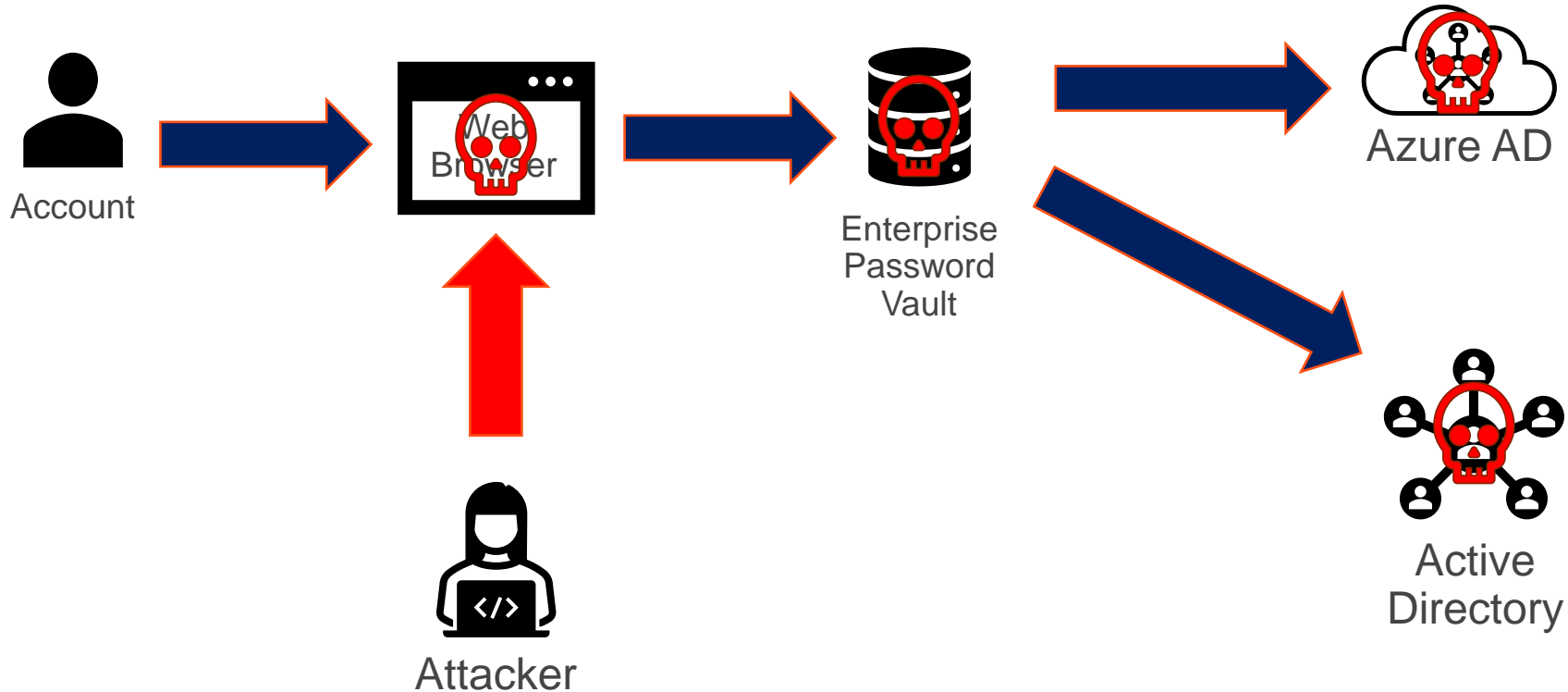
Your Passwords. Our Passion. Our Purpose.



# Attack Scenario: Password Vault

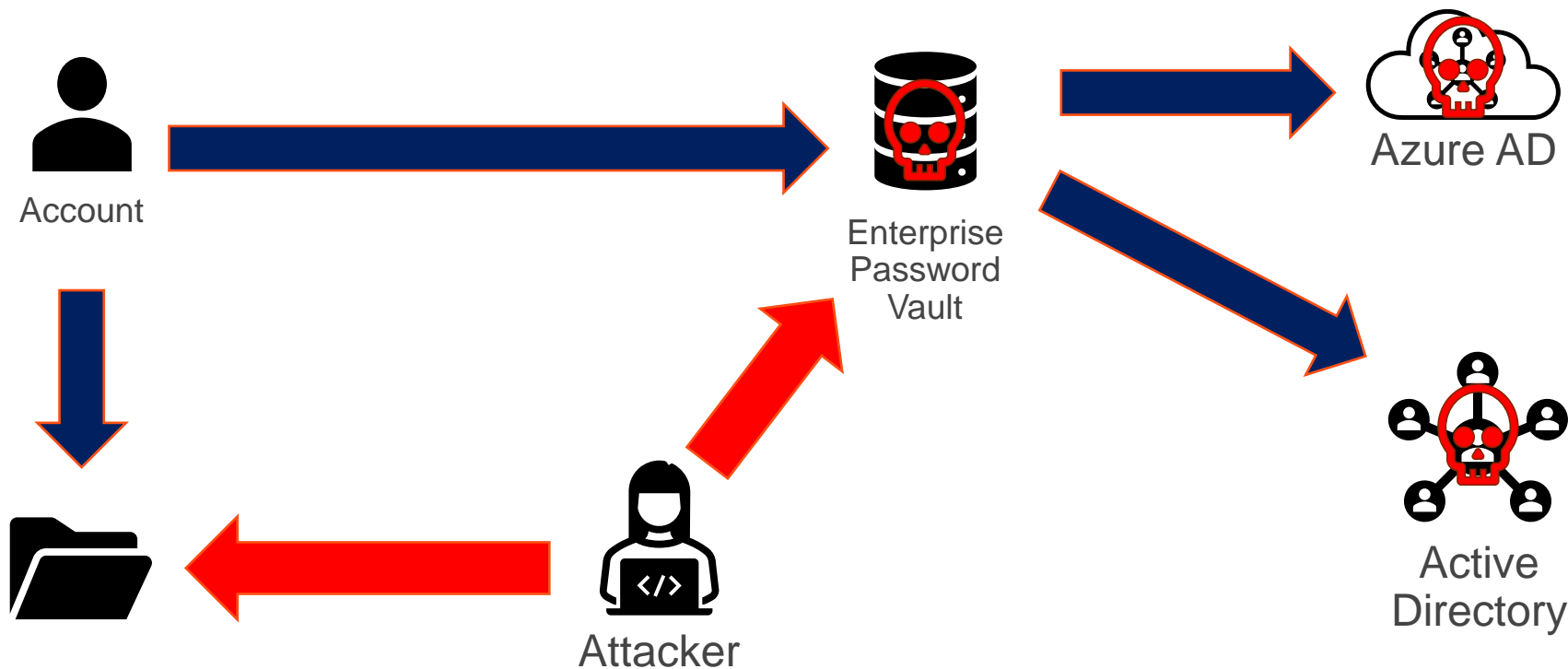


# Attack Scenario: Password Vault

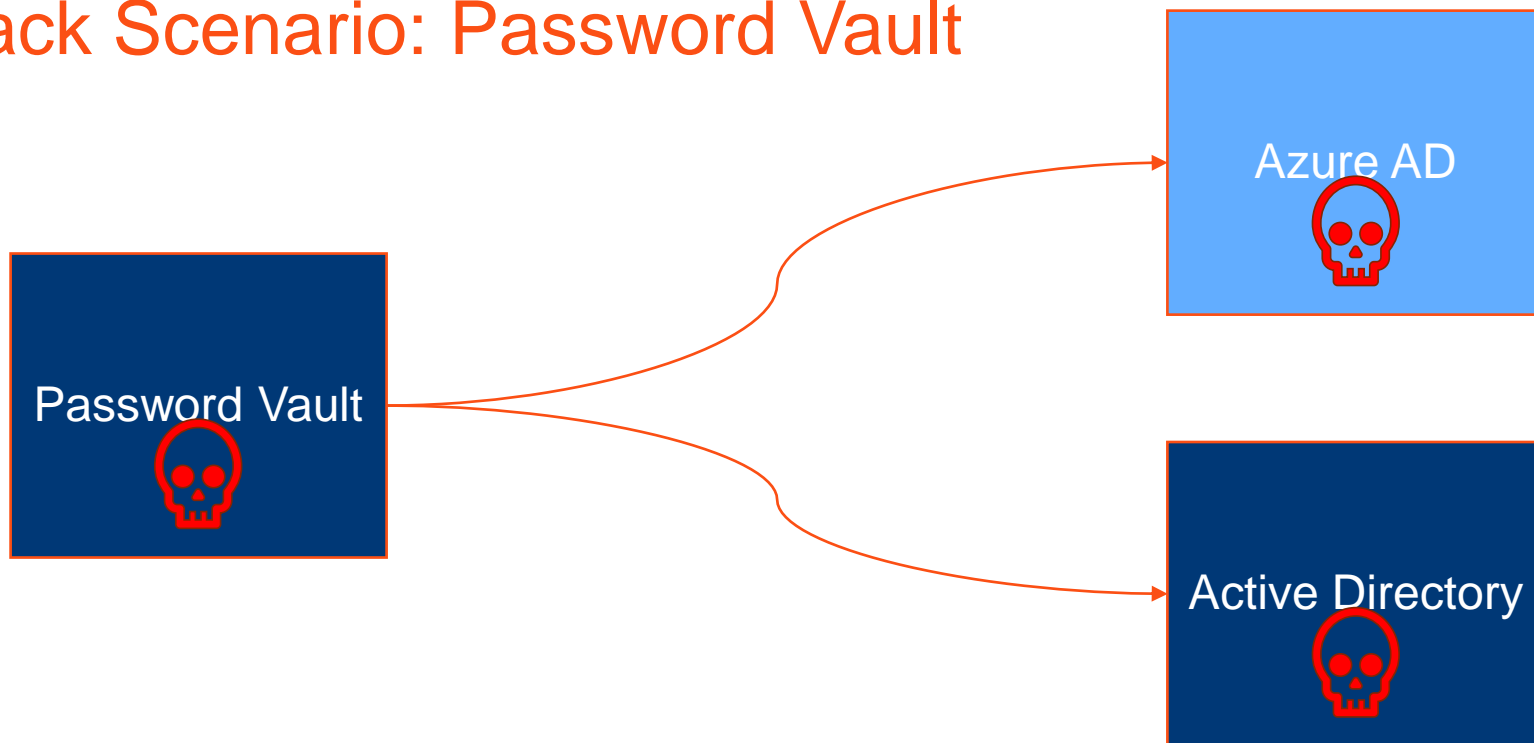




# Attack Scenario: Password Vault



# Attack Scenario: Password Vault



*Compromise AD & Azure AD by Compromising the Password Vault*

# Attack Scenario Key Takeaways

- Enterprise Password Vaults are often not secured appropriately
- Attackers can compromise the vault through:
  - The account used to connect to the vault (typically a user account)
  - An account that is a member of the vault admins group (often a user account)
  - Local admin rights to access the vault directly (DPAPI, etc.)
  - A file on a share (or local computer) that provides vault admin credentials



# Attack Scenario Key Mitigation

- Ensure only Tier 0 admin accounts are members of password vault admin groups.
- Restrict access to the system and related computers.
- AD admins should only connect from an admin system (workstation or server) specific to AD administration.
- AD admins should only connect with credentials other than regular user or AD admin credentials. We refer to this as a “transition account.”
- Ensure credentials are not stored in files or scripts on network shares or personal storage.

# Attack Scenario

---

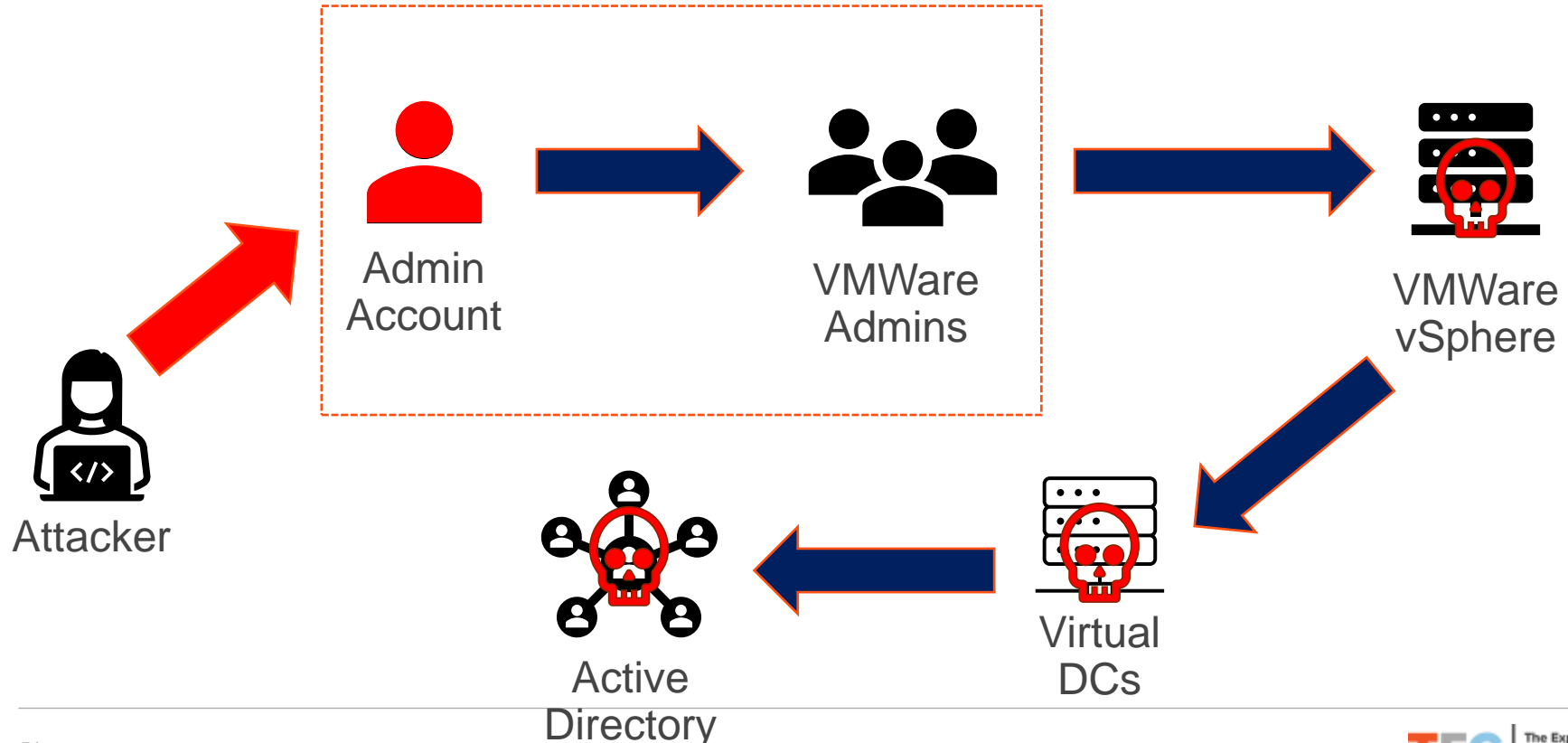
1. Password Vaults
2. VMware & AD
3. VMware & Azure AD
4. From Azure AD to AD
5. ADFS
6. Azure AD Connect
7. IPMI
8. Red Forest

**TEC**

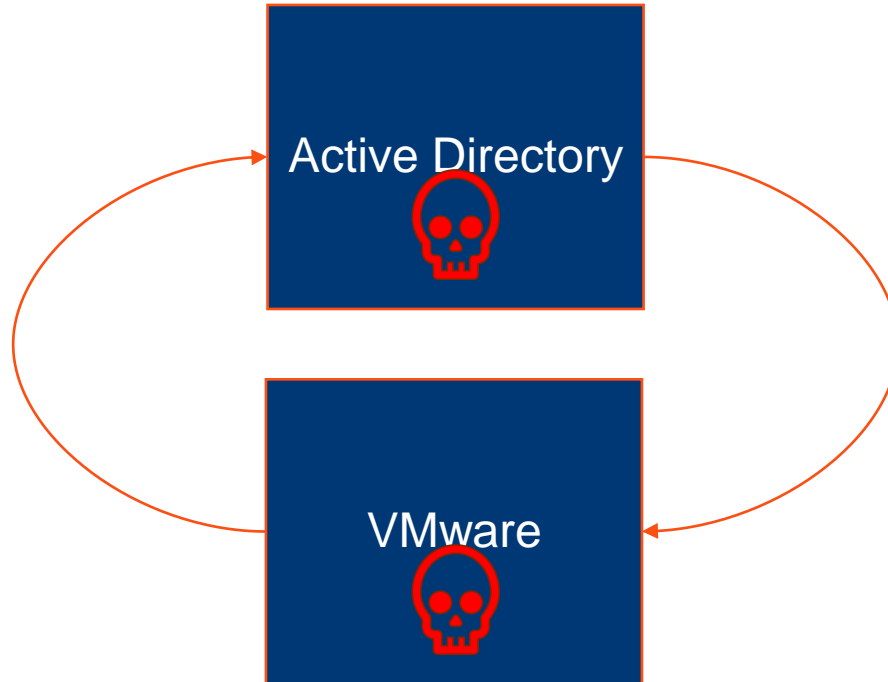
**The Experts  
Conference**

*Sponsored by Quest®*

# Attack Scenario: AD Admin Group to AD



# Attack Scenario: AD Admin Group to AD



*Compromise AD by getting admin rights to VMware through VMware group in AD*

#TEC2022

# Attack Scenario Key Takeaways

- The VMware admins group is typically in Active Directory.
- This group often contains regular user accounts.
- Since Domain Controllers are typically hosted on virtual infrastructure, compromise of VMware administration results in AD compromise.



# Attack Scenario Key Mitigation

- Protect Admin groups to protect VMware.
- Ensure only admin accounts are used for administration.
- Ensure admin accounts are well protected.
- Don't use AD groups for VMware administration if the group and associated accounts can't be securely managed and used.

# Attack Scenario

---

1. Password Vaults
2. VMware & AD
- 3. VMware, AD, & Azure AD**
4. From Azure AD to AD
5. ADFS
6. Azure AD Connect
7. IPMI
8. Red Forest


**TEC**

**The Experts  
Conference**

*Sponsored by Quest®*

# Azure AD User Administrator Role

Can manage all aspects of users and groups, including resetting passwords for limited admins.



User Administrator permission	Notes
Create users and groups Create and manage user views Manage Office support tickets Update password expiration policies	
Manage licenses Manage all user properties except User Principal Name	Applies to all users, including all admins
Delete and restore Disable and enable Manage all user properties including User Principal Name Update (FIDO) device keys	Applies to users who are non-admins or in any of the following roles: <ul style="list-style-type: none"><li>Helpdesk Administrator</li><li>User with no role</li><li>User Administrator</li></ul>
Invalidate refresh Tokens Reset password	For a list of the roles that a User Administrator can reset passwords for and invalidate refresh tokens, see <a href="#">Who can reset passwords</a> .
Update sensitive attributes	For a list of the roles that a User Administrator can update sensitive attributes for, see <a href="#">Who can update sensitive attributes</a> .

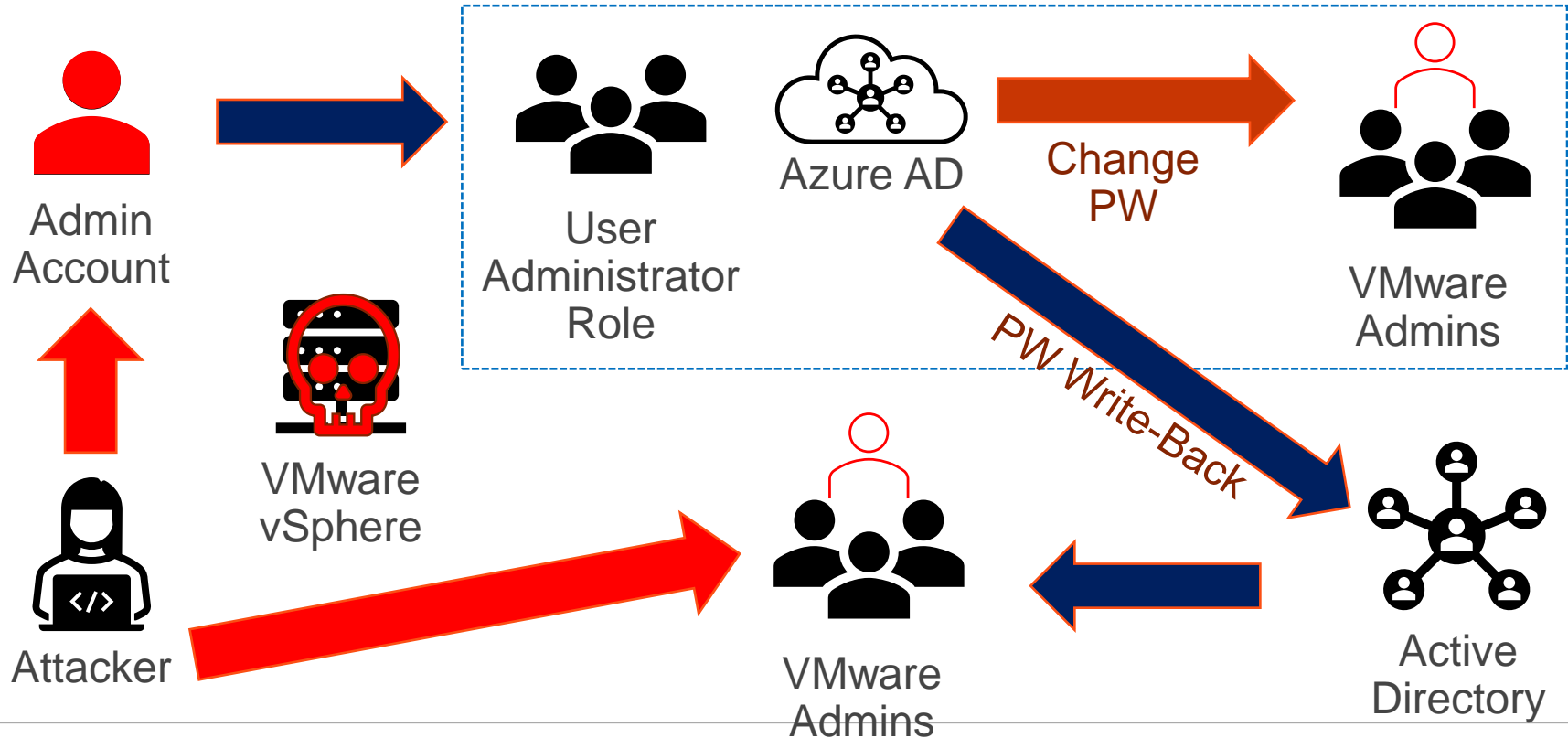
microsoft.directory/groups/members/update



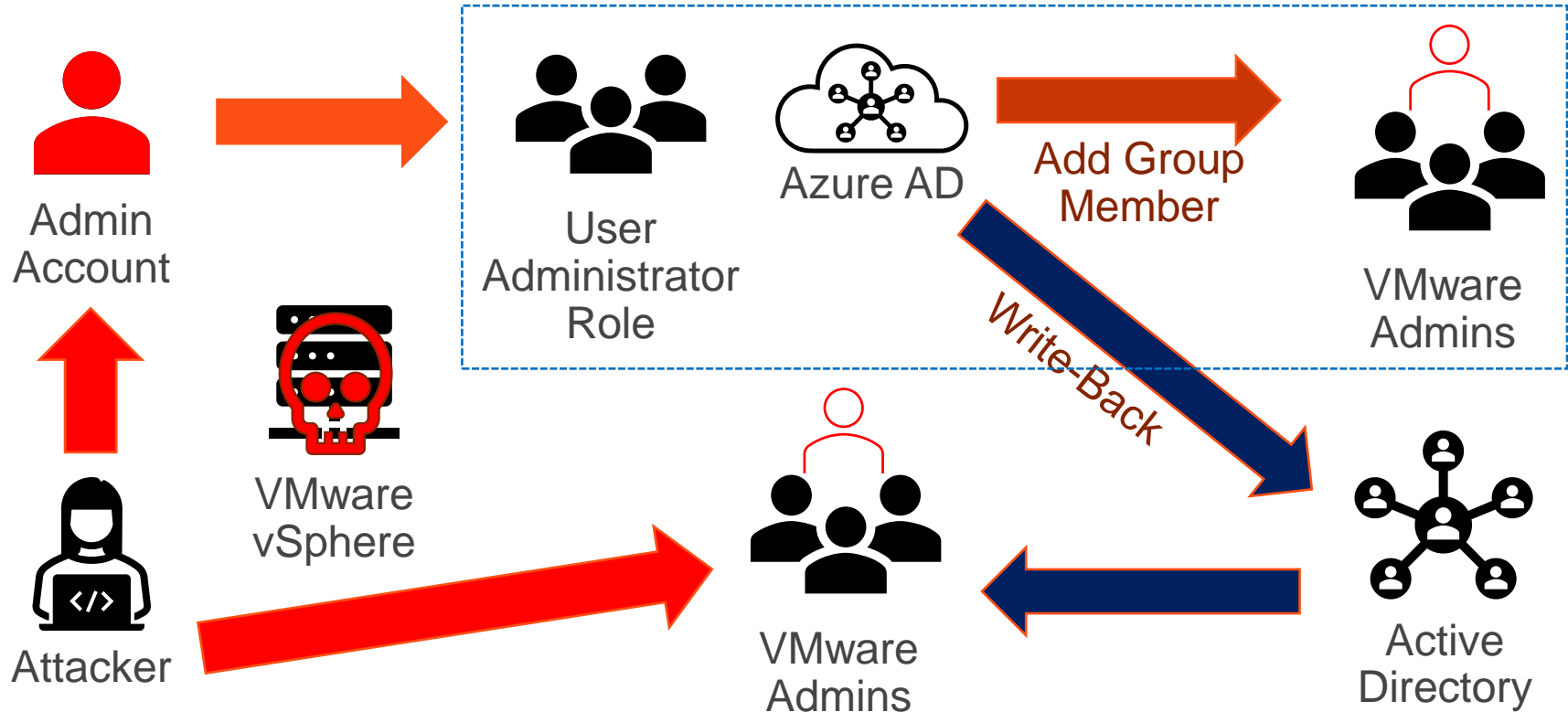
Update members of Security groups and Microsoft 365 groups, excluding role-assignable groups

<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#user-administrator>

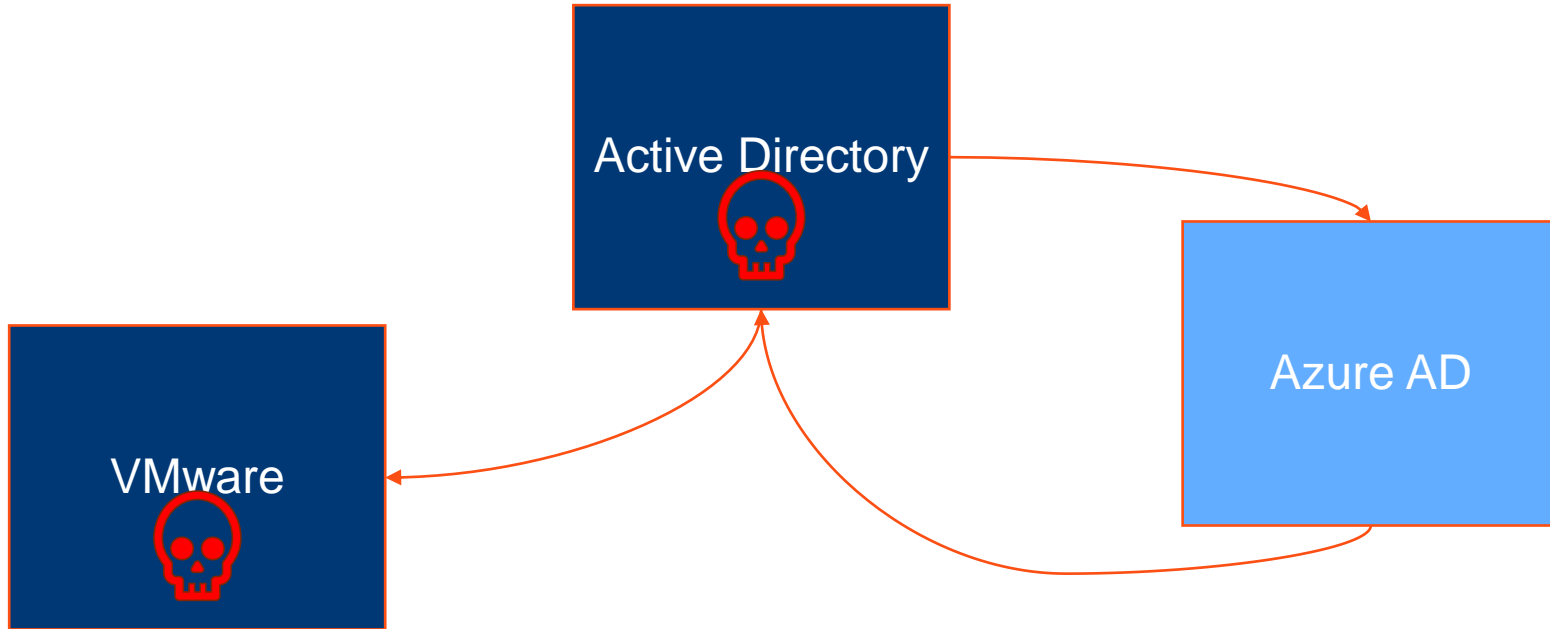
# Attack Scenario: AD to Azure AD to VMWare



# Attack Scenario: AD to Azure AD to VMWare



# Attack Scenario: AD to Azure AD to VMWare



*Compromise AD (& VMware) by getting VMware admin rights through Azure AD rights*

# Attack Scenario Key Takeaways

- Synchronization of admin groups to cloud directory environments can introduce unintended consequences.
- Write-back is a useful feature, but now imbues admins in Azure AD with on-prem superpowers.
- Review the Azure AD roles and ensure only admin accounts are members.
- Leverage PIM (eligible) to ensure that accounts don't have full-time rights.

# Attack Scenario Key Mitigation

- Ensure only admin accounts are used for administration and that they are well protected.
- Preferably use PIM (eligible) for all Azure AD roles.
- Require MFA for all Azure AD admins.
- Do not synchronize on-prem admin accounts to Azure AD.  
(simpler if properly separated in top-level admin OU)
- Do not synchronize on-prem admin groups to Azure AD.  
(simpler if properly separated in top-level admin OU)
- If write-back is configured, think through potential issues.



# Attack Scenario

---

1. Password Vaults
2. VMware & AD
3. VMware & Azure AD
- 4. Azure AD = Azure + AD**
5. ADFS
6. Azure AD Connect
7. IPMI
8. Red Forest

**TEC**

**The Experts  
Conference**

*Sponsored by Quest®*

# Background: From Azure AD to Azure to AD

The header of the article page. It features the VMware logo (a red shield with a white 'T') in the top right. Navigation links include "Search...", "Featured", "Posts", "Videos", and "Presentations".

## From Azure AD to Active Directory (via Azure) – An Unanticipated Attack Path

May 27, 2020

Updated: Jun 17, 2021

While Azure leverages Azure Active Directory for some things, Azure AD roles don't directly affect Azure (or Azure RBAC) typically. This article details a known configuration (at least to those who have dug into Azure AD configuration options) where it's possible for a Global Administrator (aka Company Administrator) in Azure Active Directory to gain control of Azure through a tenant option. This is "by design" as a "break-glass" (emergency) option that can be used to (re)gain Azure admin rights if such access is lost.

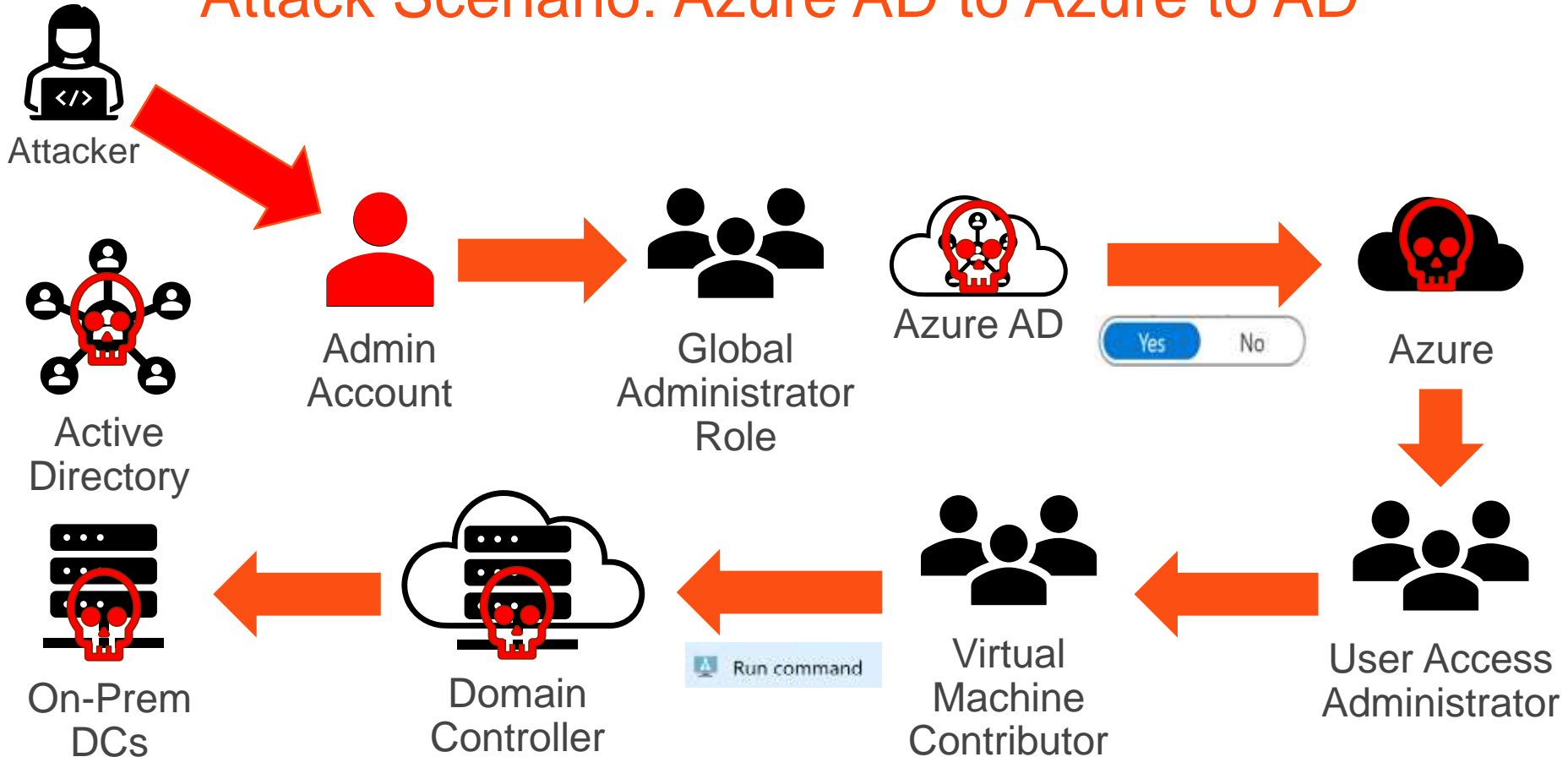
In this post I explore the danger associated with this option how it is currently configured (as of May 2020).

The key takeaway here is that if you don't carefully protect and control Global Administrator role membership and associated accounts, you could lose positive control of systems hosted in all Azure subscriptions as well as Office 365 service data.

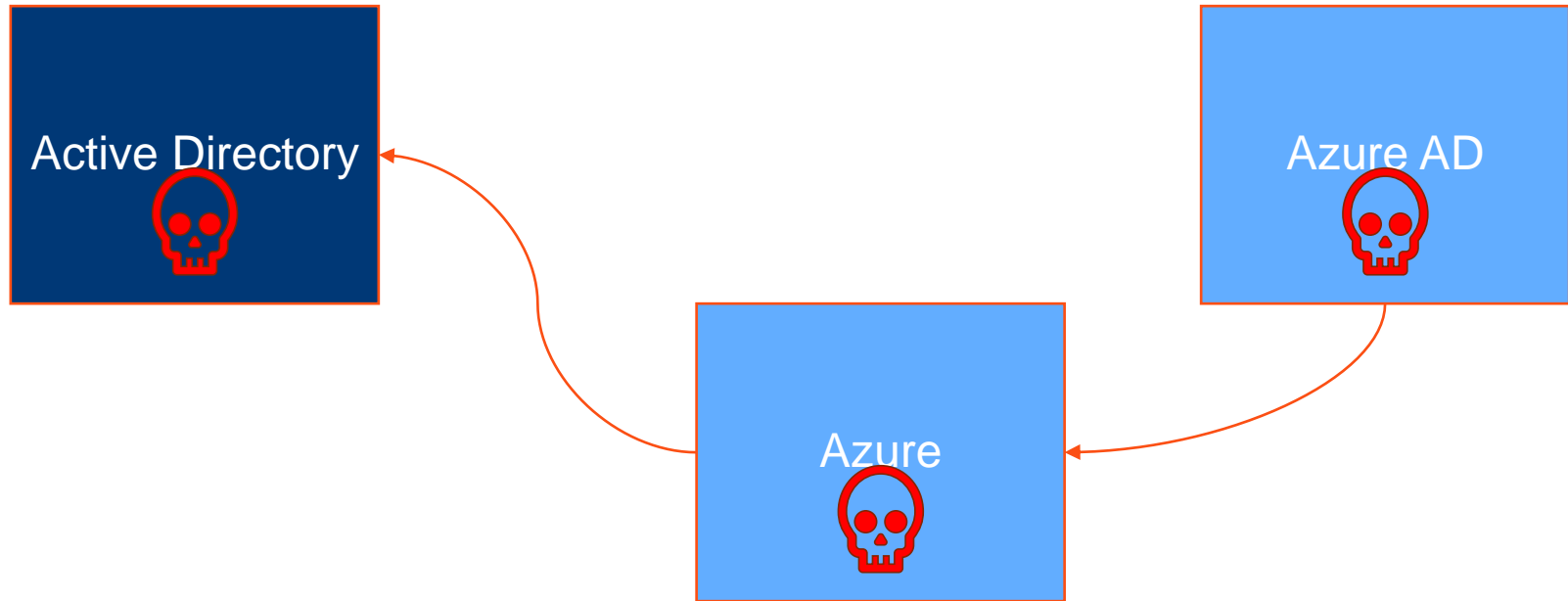
Note:  
Most of the research around this issue was performed during August 2019 through December 2019 and Microsoft may have incorporated changes since then in functionality and/or capability.

<https://www.hub.trimarcsecurity.com/post/from-azure-ad-to-active-directory-via-azure-an-unanticipated-attack-path>

# Attack Scenario: Azure AD to Azure to AD



# Attack Scenario: Azure AD to Azure to AD



*Compromise AD (& Azure & Azure AD) by getting Global Admin rights in Azure AD*

# Attack Scenario Key Takeaways

- An attacker that can gain admin rights to one environment can often pivot to another.
- Hosting Domain Controllers on virtual infrastructure such as VMware & cloud requires trust in that platform as well as additional protections around compromised accounts & monitoring.
- Jumping from Azure AD to Azure to on-prem Active Directory is possible given how most enterprises are configured and if the Global Admins group isn't well protected.

## Attack Scenario Key Mitigation

- Severely restrict membership in Global Admins.
- Use PIM (eligible) for Azure AD roles.
- Require MFA for all Global Admins (preferably all Azure AD role members).
- Closely monitor membership of the “User Access Administrator” Azure role (root level).
- Place Domain Controllers and other sensitive systems in another Azure tenant.



# Attack Scenario

---

1. Password Vaults
2. VMware & AD
3. VMware & Azure AD
4. From Azure AD to AD
- 5. ADFS**
6. Azure AD Connect
7. IPMI
8. Red Forest

**TEC**

**The Experts  
Conference**

*Sponsored by Quest®*

# Background

## Attacking Federation

DEF CON 25 (July 2017)



# How to steal identities – federated style

Federation is effectively Cloud Kerberos.

Own the Federation server, own organizational cloud services.

Token & Signing certificates  $\sim$  KRBGTGT (think Golden Tickets)



## Attacking Federation: Forging SAML

### THREAT RESEARCH BLOG POST

Golden SAML: Newly Discovered Attack Technique Forges Authentication to Cloud Apps

<https://www.cyberark.com/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-cloud-apps/>

### ADFSpoof

A python tool to forge AD FS security tokens.

Created by Doug Bienstock (@doughsec) while at Mandiant FireEye.

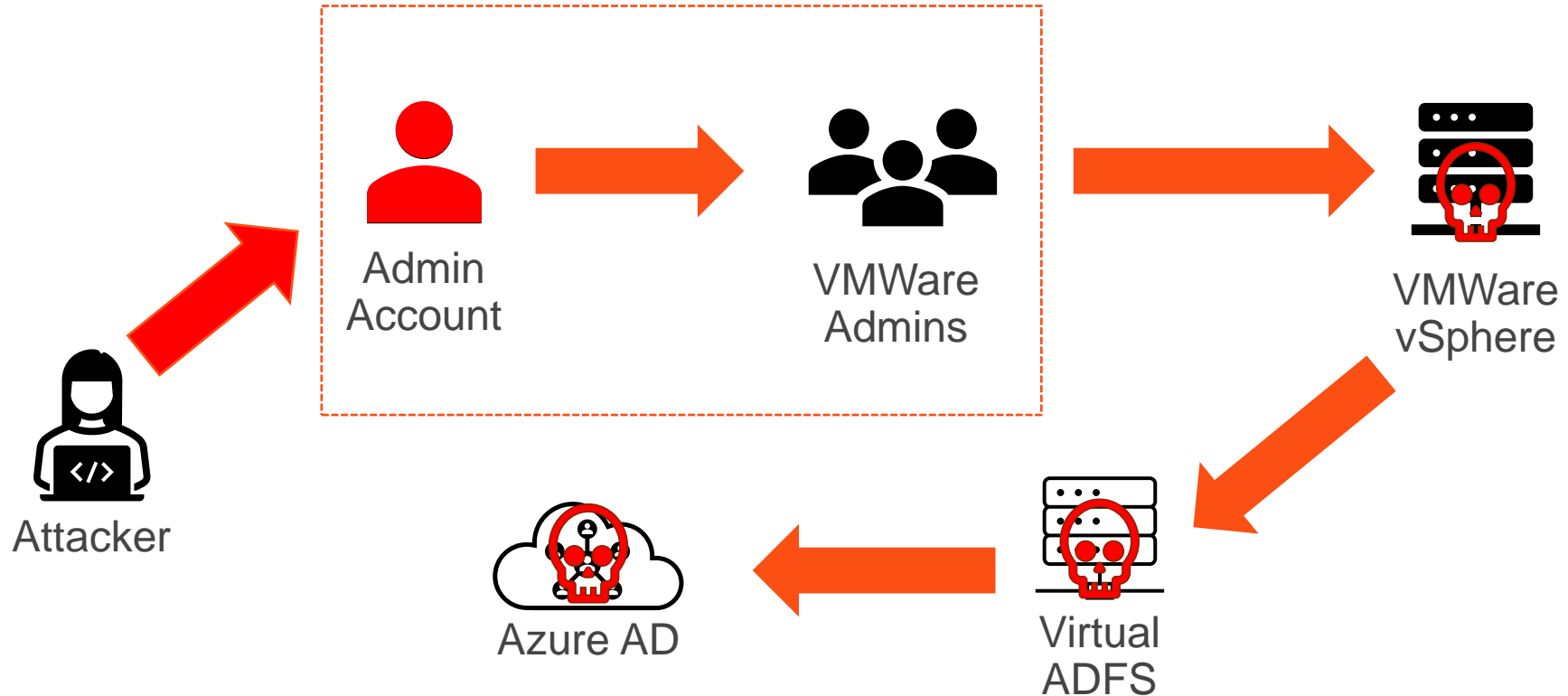
### Detailed Description

ADFSpoof has two main functions:

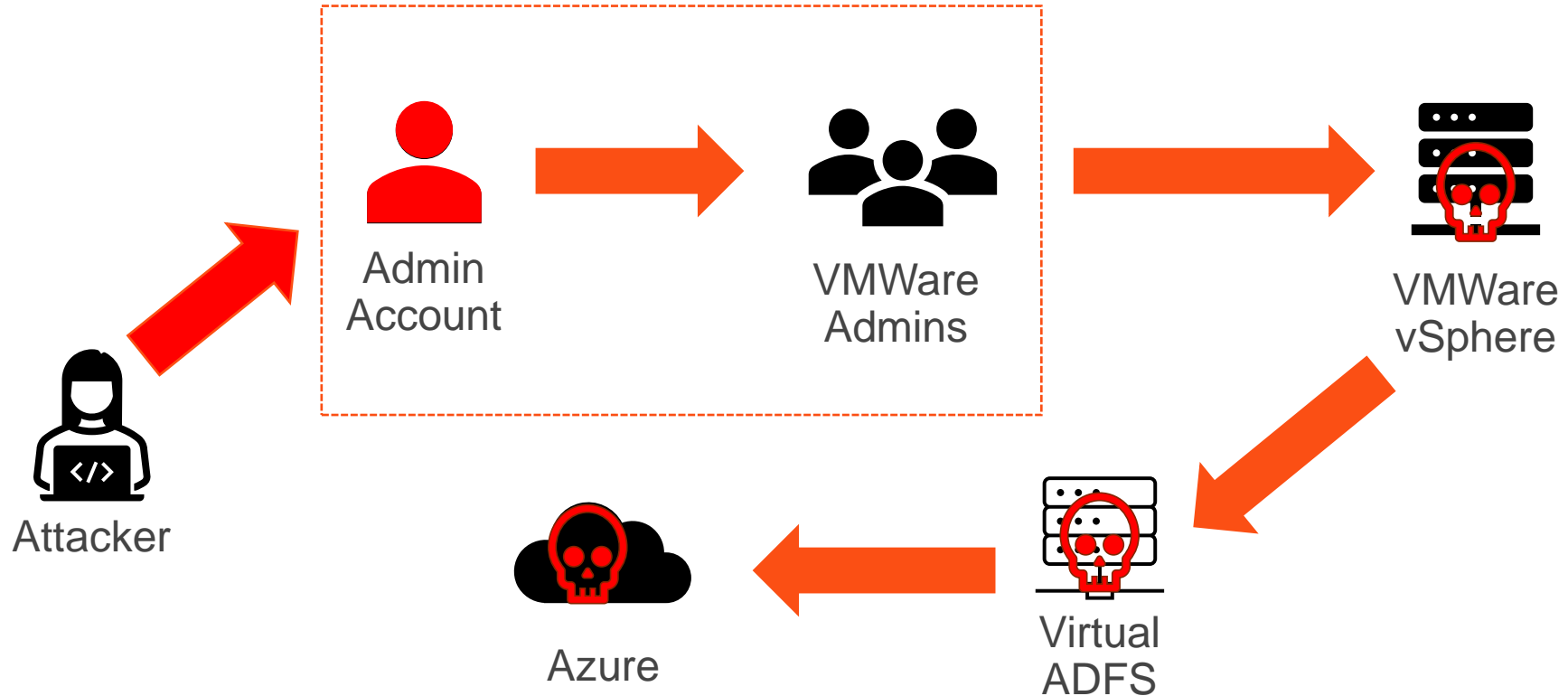
1. Given the EncryptedPFX blob from the AD FS configuration database and DKM decryption key from Active Directory, produce a usable key/cert pair for token signing.
2. Given a signing key, produce a signed security token that can be used to access a federated application.

10 This tool is meant to be used in conjunction with ADFSdump. ADFSdump runs on an AD FS server and outputs important information that you will need to use ADFSpoof.

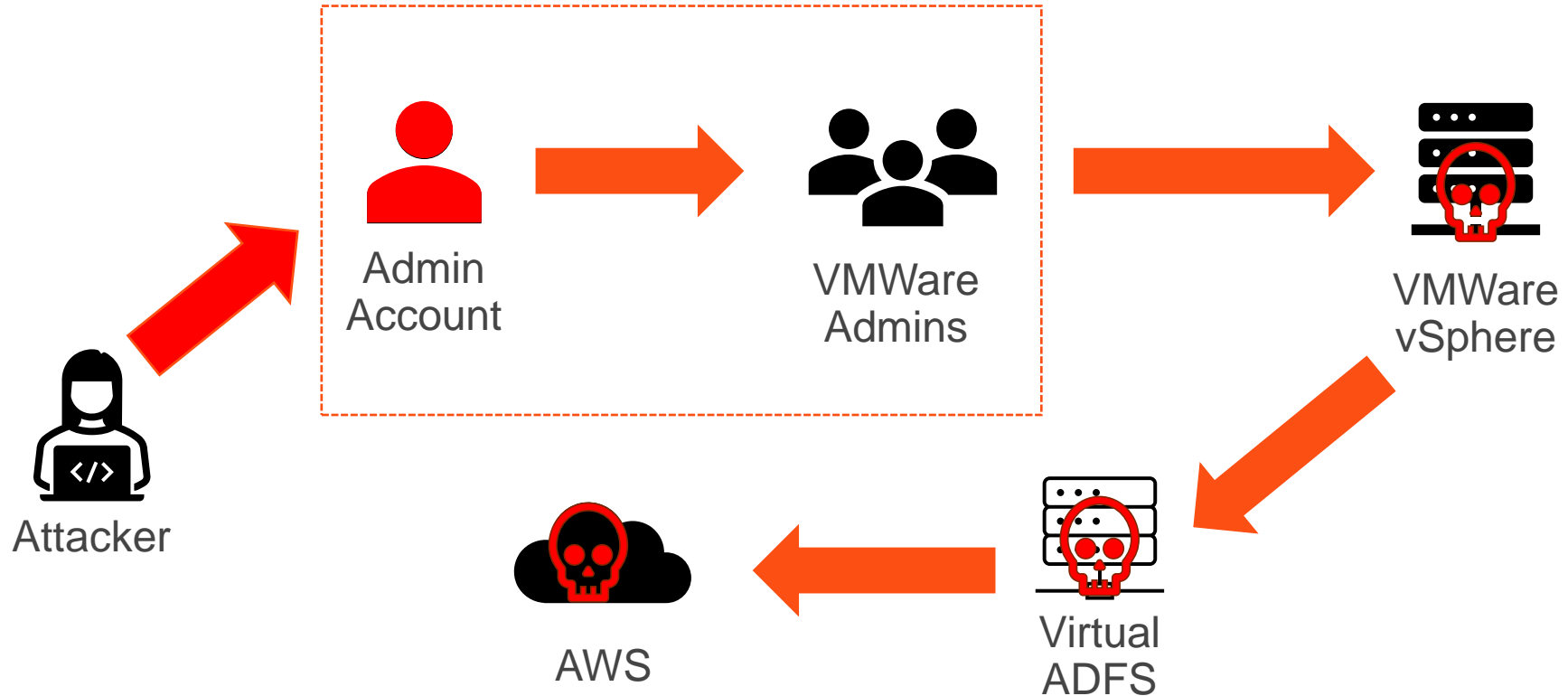
# Attack Scenario: VMware to ADFS to Azure AD



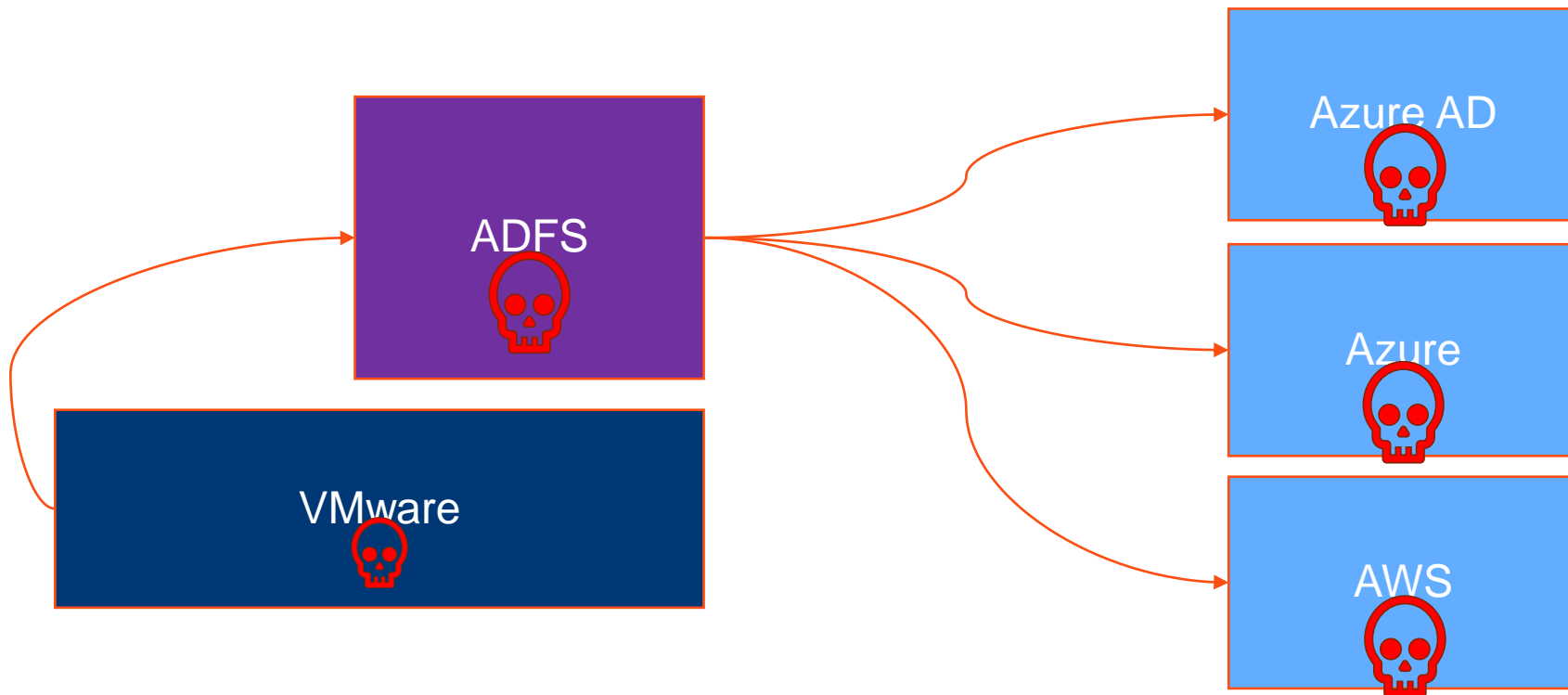
# Attack Scenario: VMware to ADFS to Azure



# Attack Scenario: VMware to ADFS to AWS



# Attack Scenario: VMware -> ADFS -> Azure AD



*Compromise Azure AD (& ADFS & VMware & Azure & AWS) by getting admin rights on the ADFS server*

# Attack Scenario Key Takeaways

- Most VMware environments aren't properly secured.
- Most on-prem systems are hosted on VMware so the security of the virtual infrastructure is paramount.
- Compromise of VMware could result in the compromise of every server and associated system hosted on the platform.

# Attack Scenario Key Mitigation

- VMware platform security is critical to the security of most of the systems in many organizations.
- Ensure VMware administration is well protected.
- Restrict VMware admin rights only to the accounts that require them.
- Ensure only admin accounts are used to manage VMware.

# Attack Scenario

---

1. Password Vaults
2. VMware & AD
3. VMware & Azure AD
4. From Azure AD to AD
5. ADFS
6. Azure AD Connect
7. IPMI
8. Red Forest

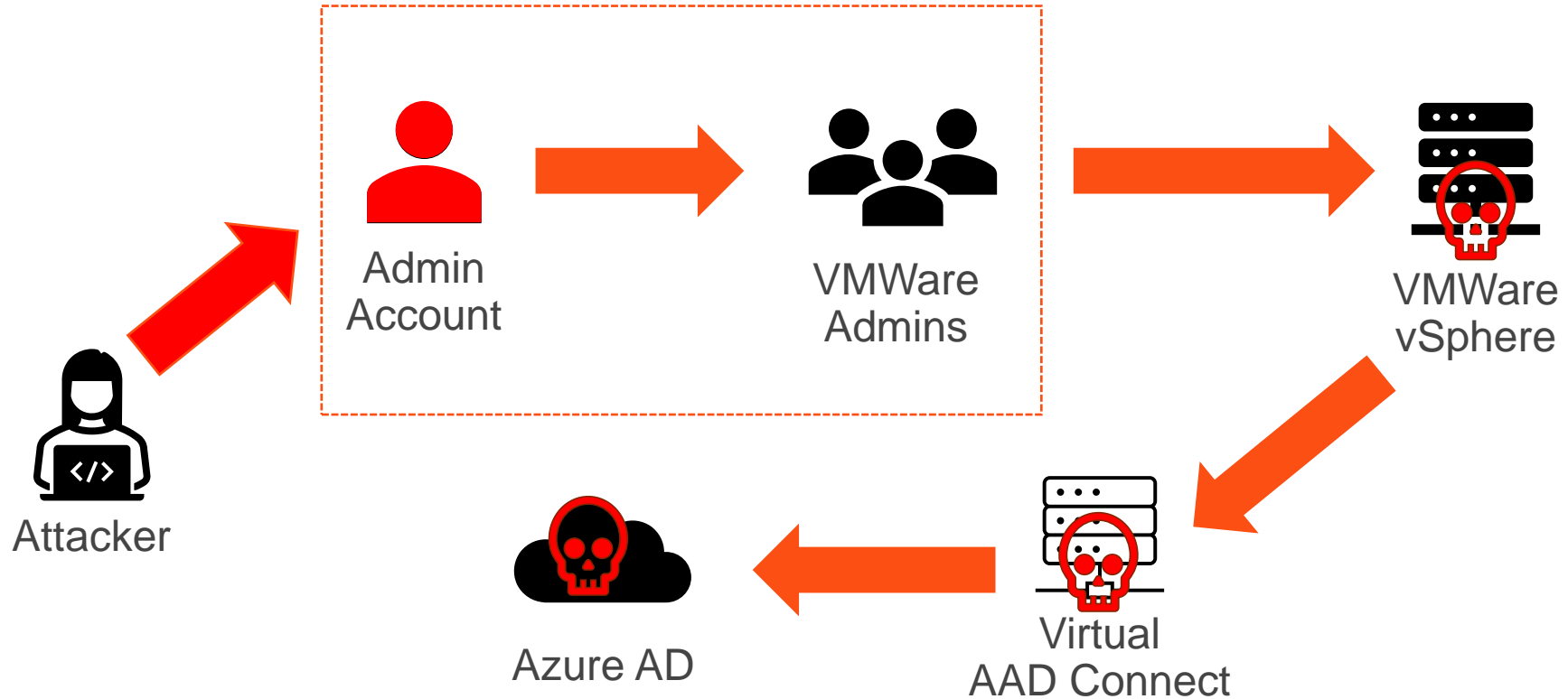
**TEC**

**The Experts  
Conference**

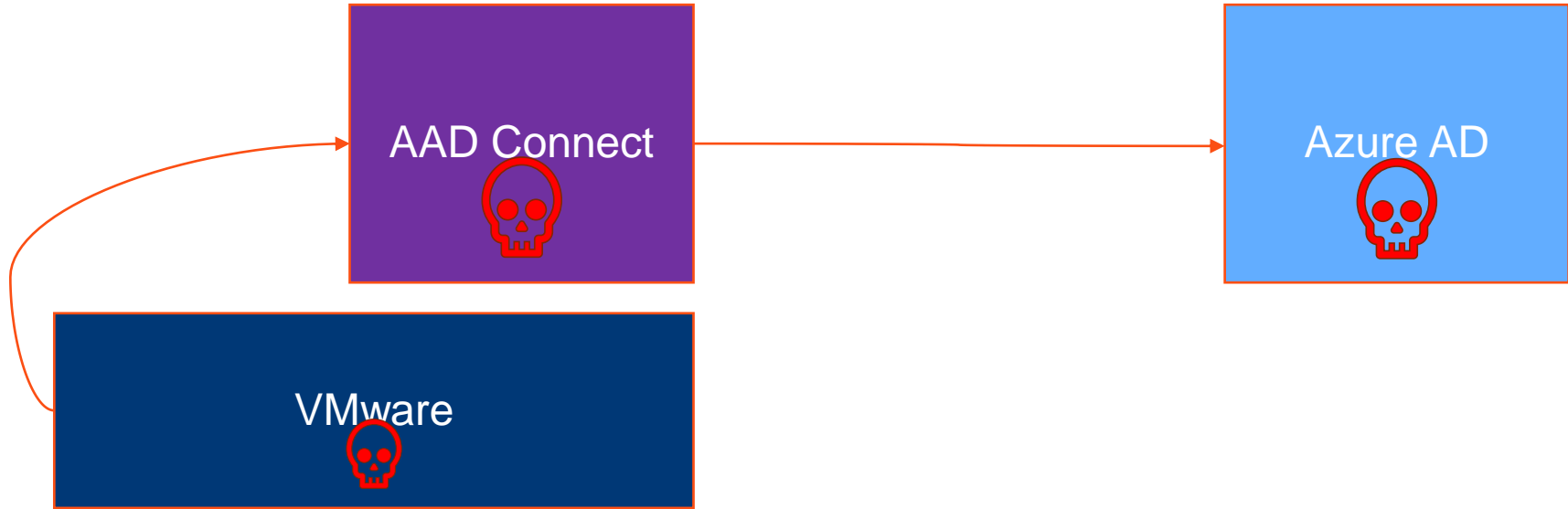
*Sponsored by Quest®*



# Attack Scenario: VMware to AAD Connect to Azure AD



# Attack Scenario: VMware -> AAD Connect -> Azure AD



*Compromise Azure AD (& AAD Connect & VMware) by getting admin rights on the AAD Connect server*

# Attack Scenario Key Takeaways

- Most VMware environments aren't properly secured.
- Most on-prem systems are hosted on VMware so the security of the virtual infrastructure is paramount.
- Compromise of VMware could result in the compromise of every server and associated system hosted on the platform.

# Attack Scenario Key Mitigation

- VMware platform security is critical to the security of most of the systems in many organizations.
- Ensure VMware administration is well protected.
- Restrict VMware admin rights only to the accounts that require them.
- Ensure only admin accounts are used to manage VMware.

# Attack Scenario

---

Intelligent Platform  
Management Interface (IPMI)

1. Password Vaults
2. VMware & AD
3. VMware & Azure AD
4. From Azure AD to AD
5. ADFS
6. Azure AD Connect
7. IPMI
8. Red Forest

**TEC**

**The Experts  
Conference**

*Sponsored by Quest®*

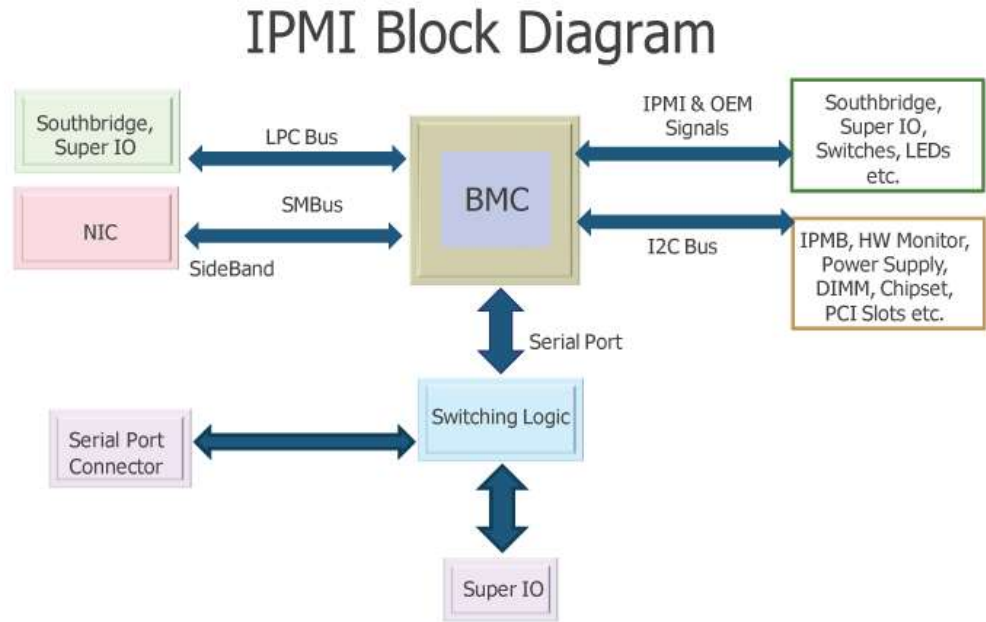
# Background: IPMI

The Intelligent Platform Management Interface (IPMI) is a set of computer interface specifications for an autonomous computer subsystem that provides management and monitoring capabilities independently of the host system's CPU, firmware (BIOS or UEFI) and operating system.

## Implementations

- **HP Integrated Lights-Out**, HP's implementation of IPMI
- **Dell DRAC**, Dell's implementation of IPMI
- **IBM Remote Supervisor Adapter**, IBM's out-of-band management products, including IPMI implementations
- **MegaRAC**, AMI's out-of-band management product and OEM IPMI firmware used in e.g. **ASUS**, **Tyan** and **Supermicro** motherboards
- **Avocent MergePoint Embedded Management Software**, an OEM IPMI firmware used in e.g. **Gigabyte** and **Dell** motherboards

[https://en.wikipedia.org/wiki/Intelligent\\_Platform\\_Management\\_Interface](https://en.wikipedia.org/wiki/Intelligent_Platform_Management_Interface)



**YO DAWG I HEARD YOU LIKE COMPUTERS**

**SO I PUT A COMPUTER IN YOUR  
COMPUTER SO YOU CAN COMPUTER YOUR COMPUTER**

# Background: IPMI

- HP ILO
  - 59 CVEs
  - Integrated Lights-Out 5 (iLO 5) firmware version: 11 CVEs
- Dell DRAC
  - Dell Idrac9 Firmware: 15 CVEs
  - Dell Idrac8 Firmware: 7 CVEs



## Alert (TA13-207A)

[View Alerts](#)

### Risks of Using the Intelligent Platform Management Interface (IPMI)

Original release date: July 29, 2013 | Last revised: October 07, 2016

[Add IPMI](#) [Twitter](#) [Facebook](#) [LinkedIn](#)

#### Systems Affected

Any system connected to the internet running the Intelligent Platform Management Interface (IPMI) may be affected. IPMI is resident on many server platforms, and provides low-level access to a system that can override operating system controls.

#### Overview

Attackers can easily identify and access systems that run IPMI and are connected to the internet. It is important to restrict IPMI access to specific management IP addresses within an organization and preferably separated into a separate LAN segment.

#### Description

##### What is the Intelligent Platform Management Interface (IPMI)?

IPMI is a low level interface specification that has been adopted by many hardware vendors. It allows a system administrator to remotely manage servers at the hardware level. IPMI runs on the Baseboard Management Controller (BMC) and provides access to the BIOS, disks, and other hardware. It also supports remote booting from a CD or through the network; and monitoring of the server environment. The BMC itself also runs a limited set of network services to facilitate management and communications amongst systems.

##### What is the Risk?

Attackers can use IPMI to essentially gain physical-level access to the server. An attacker can reboot the system, install a new operating system, or compromise data, bypassing any operating system controls. Some issues identified by [Dan Farmer](#):

- Passwords for IPMI authentication are saved in clear text.
- Knowledge of one IPMI password gives you the password for all computers in the IPMI managed group.
- Root access on an IPMI system grants complete control over hardware, software, firmware on the system.
- BMCs often run excess and older network services that may be vulnerable.
- IPMI access may also grant remote console access to the system, resulting in access to the BIOS.
- There are few, if any, monitoring tools available to detect if the BMC is compromised.
- Certain types of traffic to and from the BMC are not encrypted.
- Unclear documentation on how to sanitize IPMI passwords without destruction of the motherboard.

Attackers can easily search and identify internet-connected target systems, and IPMI is no exception.

## Alert (TA13-207A)

[View Alerts](#)

### Risks of Using the Intelligent Platform Management Interface (IPMI)

Original release date: July 29, 2013 | Last revised: October 07, 2016

Attackers can use IPMI to essentially gain physical-level access to the server. An attacker can reboot the system, install operating system, and bypassing any operating system controls. Some issues identified by [Dan Farmer](#):

- Passwords for IPMI authentication are saved in clear text.
- Knowledge of one IPMI password gives you the password for all computers in the IPMI managed group.
- Root access on an IPMI system grants complete control over hardware, software, firmware on the system.
- BMCs often run excess and older network services that may be vulnerable.
- IPMI access may also grant remote console access to the system, resulting in access to the BIOS.
- There are few, if any, monitoring tools available to detect if the BMC is compromised.
- Certain types of traffic to and from the BMC are not encrypted.
- Unclear documentation on how to sanitize IPMI passwords without destruction of the motherboard.

- There are few, if any, monitoring tools available to detect if the BMC is compromised.
- Certain types of traffic to and from the BMC are not encrypted.
- Unclear documentation on how to sanitize IPMI passwords without destruction of the motherboard.

Attackers can easily search and identify internet-connected target systems, and IPMI is no exception.

# HP iLO Vulnerability CVE-2017-12542

HP released patches for CVE-2017-12542 in iLO 4 firmware version 2.54.

The vulnerability affects all HP iLO 4 servers running firmware version 2.53 and before. Other iLO generations, like iLO 5, iLO 3, and more are not affected.

<https://www.bleepingcomputer.com/news/security/you-can-bypass-authentication-on-hpe-ilo4-servers-with-29-a-characters/>



```
curl -H "Connection: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
```

[https://airbus-seclab.github.io/ilo/SSTIC2018-Article-subverting\\_your\\_server\\_through\\_its\\_bmc\\_the\\_hpe\\_ilo4\\_case-gazet\\_perigaud\\_czarny.pdf](https://airbus-seclab.github.io/ilo/SSTIC2018-Article-subverting_your_server_through_its_bmc_the_hpe_ilo4_case-gazet_perigaud_czarny.pdf)

# DSA-2020-063: iDRAC Buffer Overflow Vulnerability

Summary: Dell EMC iDRAC has been updated to address a vulnerability which may potentially be exploited to compromise the affected systems.

ARTICLE  
CONTENT

Article Content

---

LEGAL  
INFORMATION

Impact  
High

ARTICLE  
PROPERTIES

Details

RATE THIS  
ARTICLE

- Buffer Overflow Vulnerability

CVE-2020-5344

Dell EMC iDRAC7, iDRAC8 and iDRAC9 versions prior to 2.65.65.65, 2.70.70.70, 4.00.00.00 contain a stack-based buffer overflow vulnerability. An unauthenticated remote attacker may exploit this vulnerability to crash the affected process or execute arbitrary code on the system by sending specially crafted input data.

CVSS v3.1 Base Score: 7.0 ([CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:H](#))

Dell Technologies recommends all customers consider both the CVSS base score and any relevant temporal and environmental scores that may impact the potential severity associated with a particular security vulnerability.

# Dell EMC iDRAC Multiple Vulnerabilities (CVE-2018-15774 and CVE-2018-15776)

Summary: Dell EMC guidance to mitigate risk and resolution for the iDRAC multiple vulnerabilities. For specific information on affected iDRAC versions and next steps to apply the updates, refer [See more](#)

ARTICLE  
CONTENT

ARTICLE  
PROPERTIES

RATE THIS  
ARTICLE

This article may have been automatically translated. If you have any feedback regarding its quality, please let us know using the form at the bottom of this page.

## Article Content

### Symptoms

CVE Identifier: CVE-2018-15774, CVE-2018-15776

Severity: Medium

### Affected products:

- Dell EMC iDRAC7/iDRAC8 versions prior to 2.61.60.60 (CVE-2018-15774 and CVE-2018-15776)
- Dell EMC iDRAC9 versions prior to 3.20.21.20, 3.21.24.22, 3.21.26.22 and 3.23.23.23 (CVE-2018-15774)

### Summary:

Dell EMC iDRAC has been updated to address multiple vulnerabilities which may potentially be exploited to compromise the affected systems.

### Details:

- Privilege Escalation Vulnerability (CVE-2018-15774)

Dell EMC iDRAC7/iDRAC8 versions prior to 2.61.60.60 and iDRAC9 versions prior to 3.20.21.20, 3.21.24.22, 3.21.26.22, and 3.23.23.23 contain a privilege escalation vulnerability. An authenticated malicious iDRAC user with operator privileges could potentially exploit a permissions check flaw in the Redfish interface to gain administrator access.

# IPMI Network Check

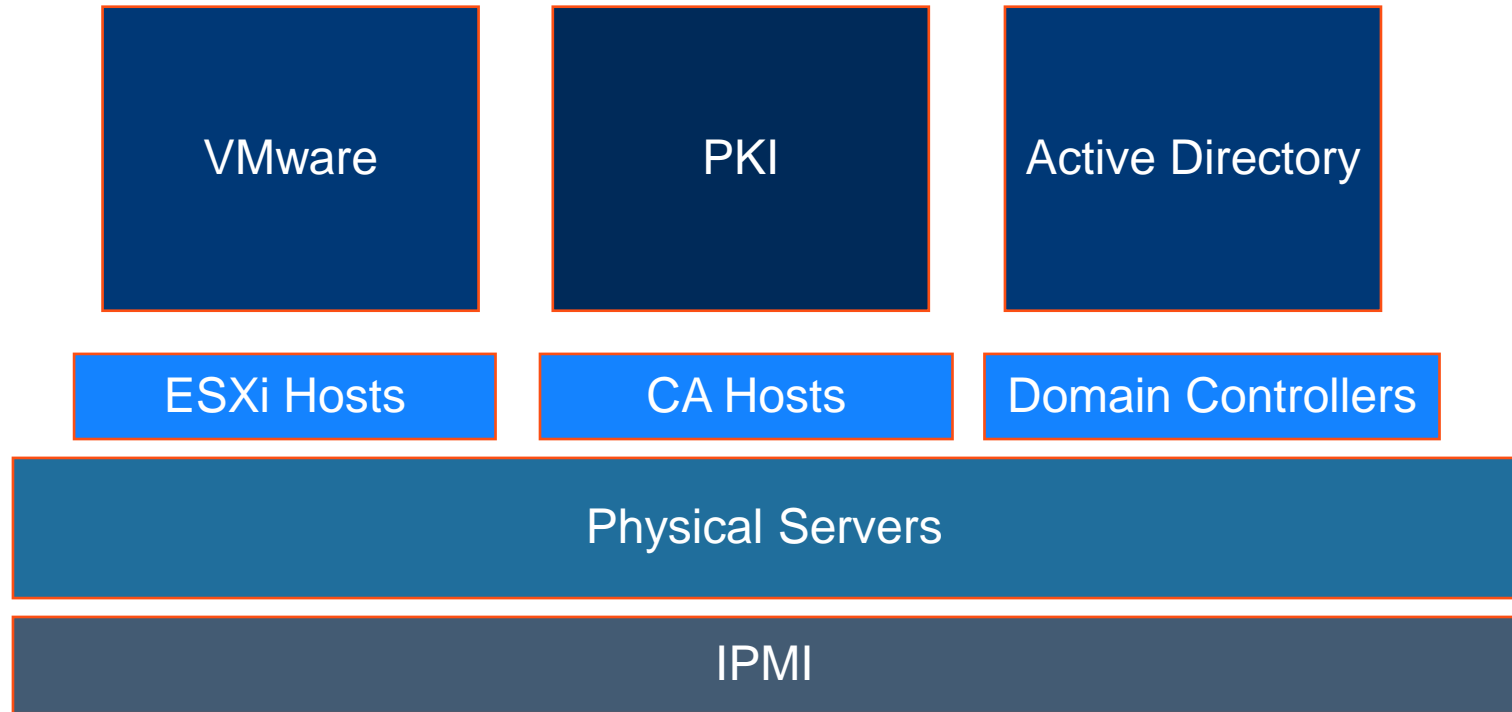
- iDRAC: TCP port 5696 or 5353
- ILO: TCP port 2381
- Port response on the production network = very bad

*Test-NetConnection \$IPAddress -Port 2381*

```
PS C:\> test-netconnection 172.16.101.11 -port 2381

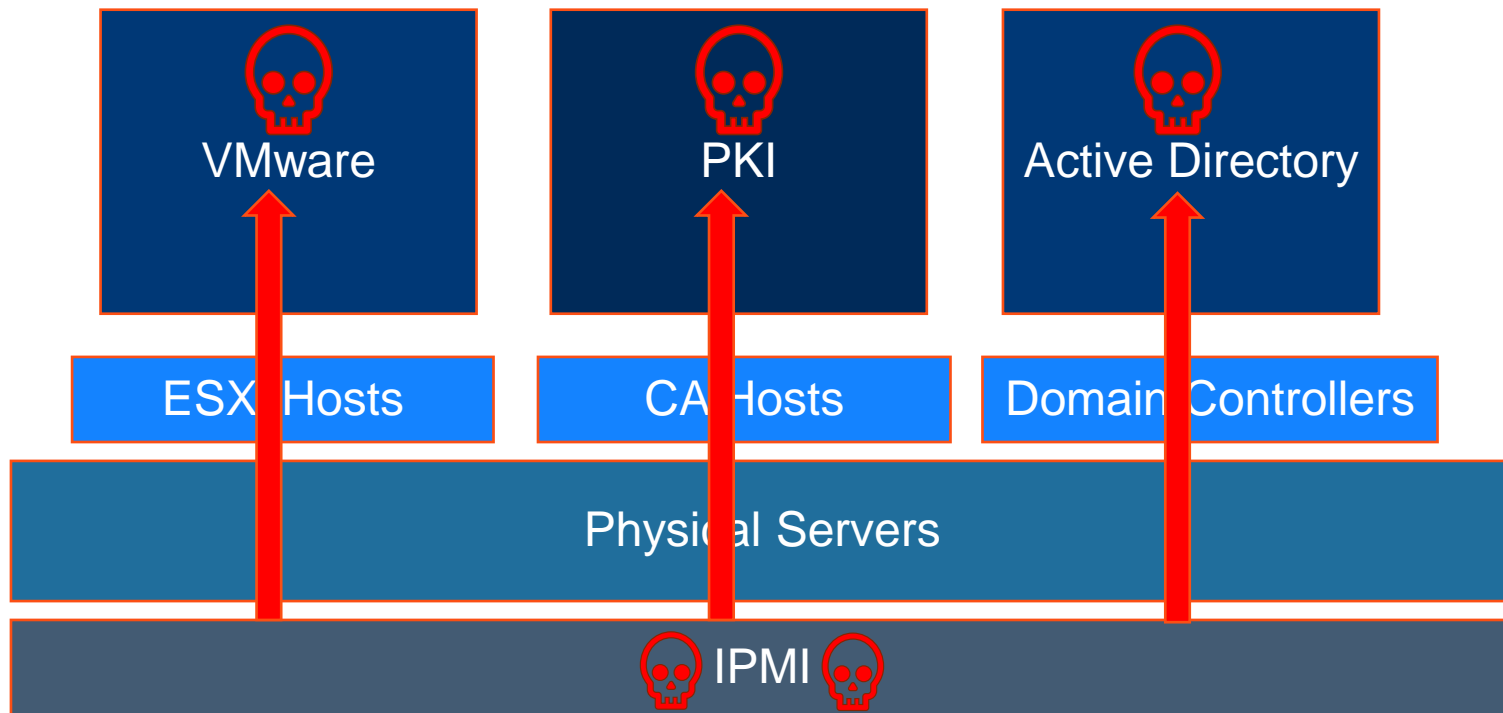
ComputerName      : 172.16.101.11
RemoteAddress     : 172.16.101.11
RemotePort        : 2381
InterfaceAlias    : Wi-Fi
SourceAddress     : 172.16.250.109
TcpTestSucceeded  : True
```

# Attack Scenario: IPMI





# Attack Scenario: IPMI





# Attack Scenario Key Takeaways

- IPMI such as ILO and iDRAC is typically enabled by default on physical servers and often connected to the primary production network.
- IPMI access on the primary network provides attackers the ability to compromise the physical server to then compromise the services running on the server.
- IPMI access on the network puts all systems hosted by physical servers at risk (which is everything).

# Attack Scenario Key Mitigations

- Ensure IPMI systems (iDRAC, ILO, etc.) are on a separate out of band (OOB) network instead of the production corporate network.
- If IPMI can't be separated on a different network, ensure there are network controls to restrict access to these systems.
- Keep physical server hardware firmware updated.
  - HPE iLO Amplifier Pack is a free tool that helps with this:  
<https://buy.hpe.com/us/en/software/server-management-software/server-ilo-management/ilo-management-engine/ilo-amplifier-pack/p/1009838729>

# Firmware Issues



<https://eclipsium.com/2022/08/31/august-firmware-threat-report/>

# More on this coming out soon

- Watch the News....



# Attack Scenario

---

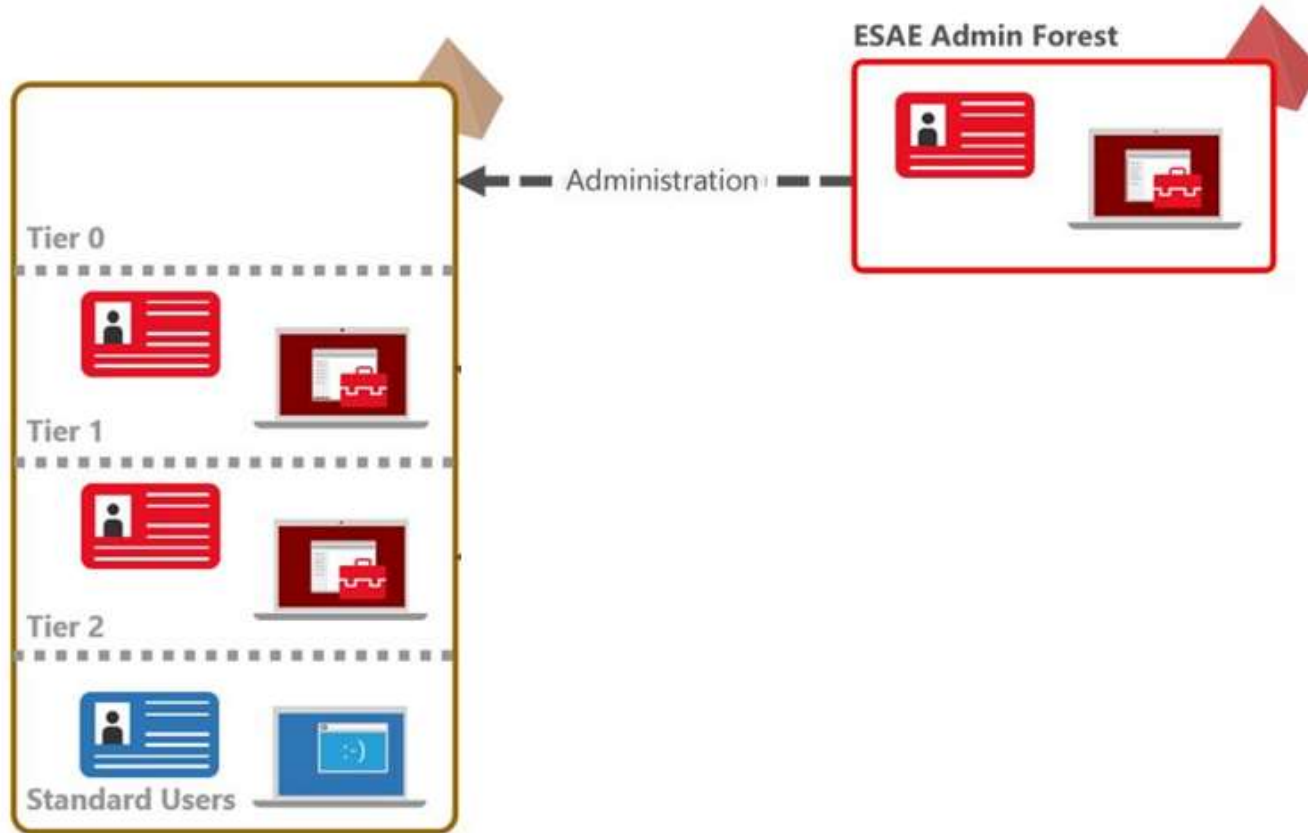
1. Password Vaults
2. VMware & AD
3. VMware & Azure AD
4. From Azure AD to AD
5. ADFS
6. Azure AD Connect
7. IPMI
8. Admin Forest /  
Red Forest

**TEC**

**The Experts  
Conference**

*Sponsored by Quest®*

# Background: Admin Forest

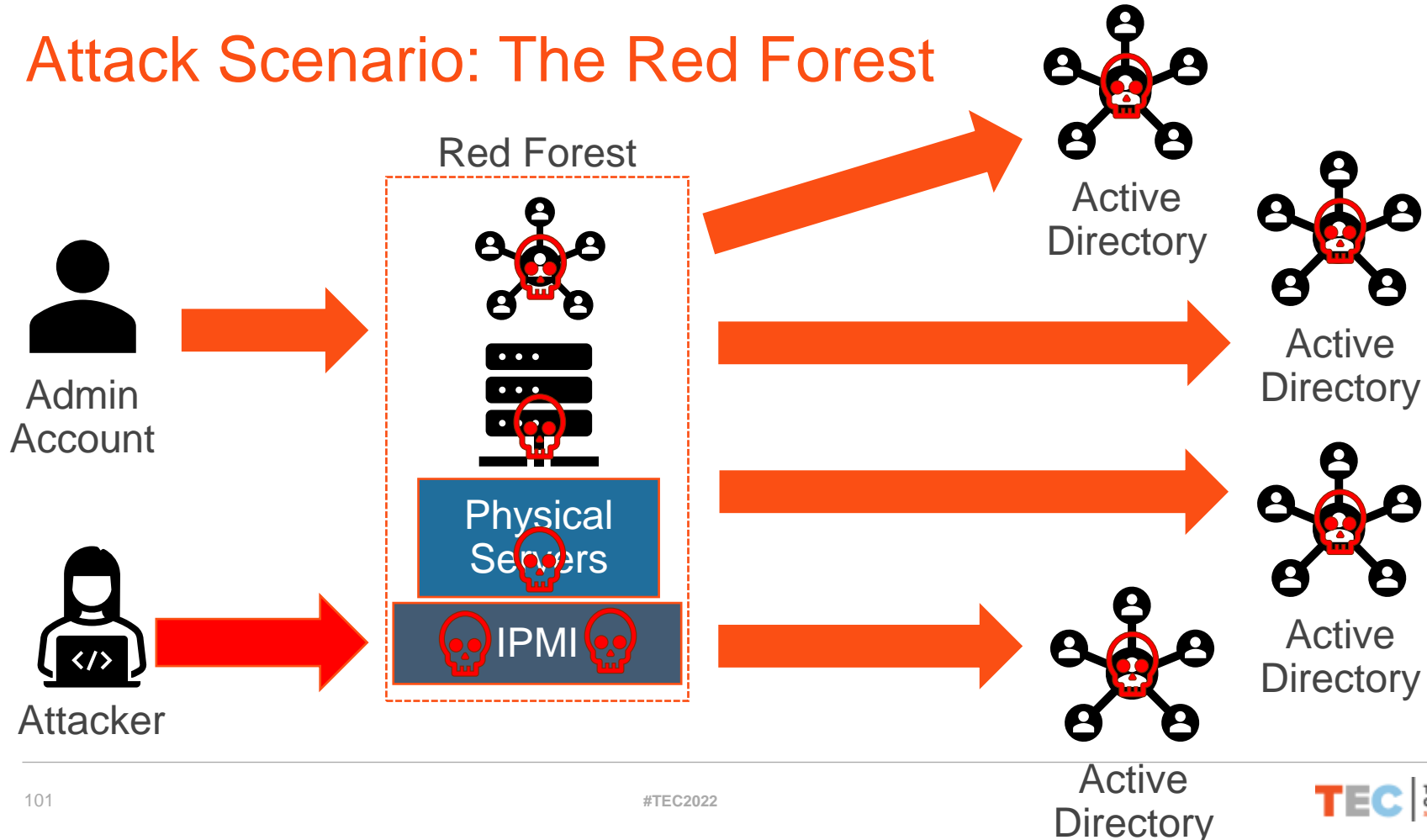


# Background: Admin Forest

- Red Forest, aka Admin Forest, aka Enhanced Security Administrative Environment (ESAE).
- ESAE forest is isolated from the production network with strong network controls and only allows encrypted communication to production DCs & select AD Admin systems.
- 1-way trust with Selective Authentication (production AD forest trusts ESAE).
- Production AD admin groups are empty, except group for ESAE admin groups.
- No production AD admin groups/accounts in ESAE have admin rights to ESAE.
- All systems run current/recent versions of Windows.
- Auto-patching by ESAE management/patching system.
- Production AD admin accounts in ESAE should not retain full-time Production AD admin group membership and require MFA for authentication.
- ESAE should be carefully monitored for anomalous activity.

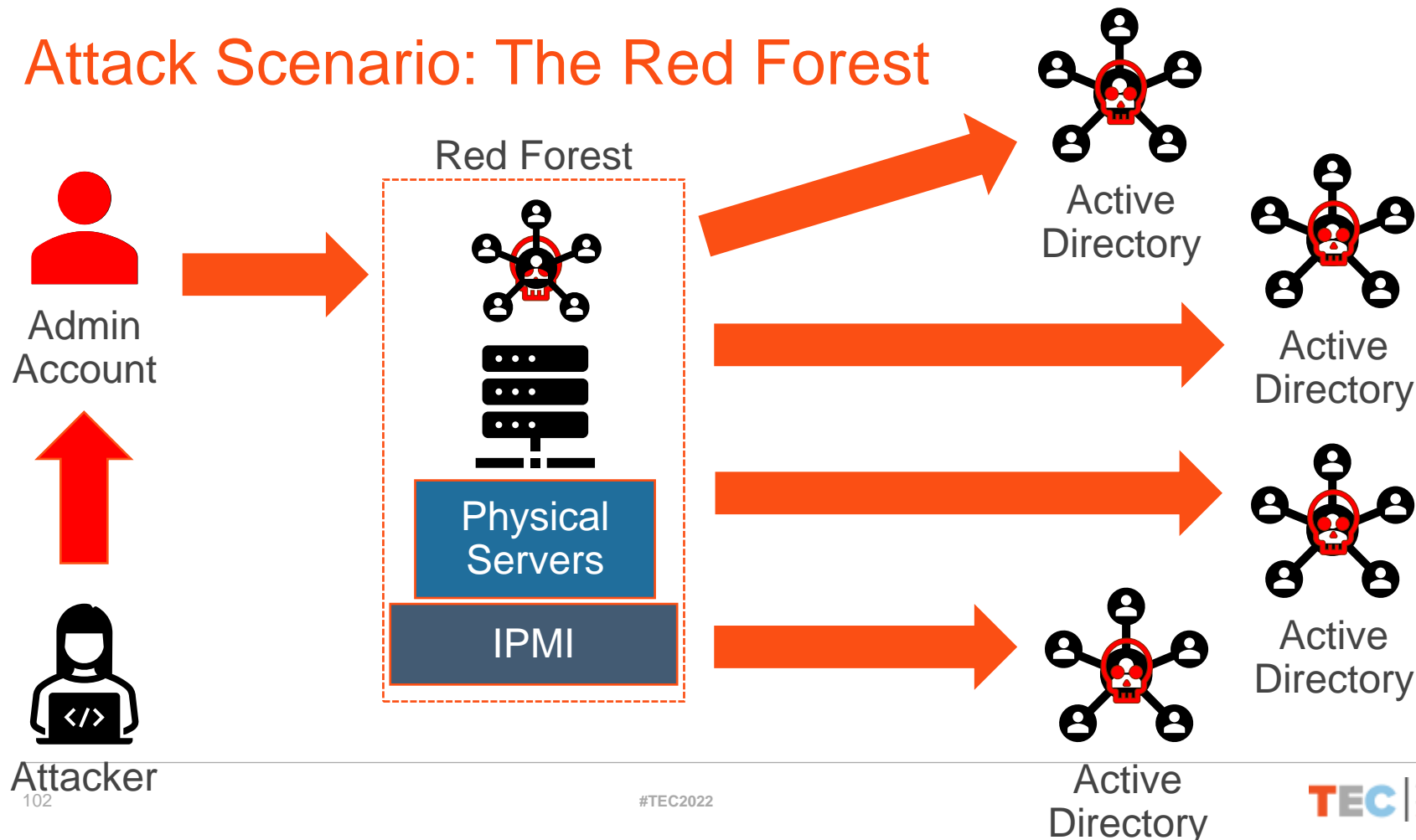


# Attack Scenario: The Red Forest





# Attack Scenario: The Red Forest



# Attack Scenario Key Takeaways

- The Red Forest (aka Admin Forest) is deployed to enable administration of multiple Active Directory forests in many companies.
- The compromise of the Red Forest would result in compromise of all managed AD forests.
- Accessible IPMI is a big risk to many Red Forests.
- If the admin accounts and systems aren't secured appropriately, then the entire admin environment is potentially at risk.
- Red Forest can be challenging to get 100% right.

# Attack Scenario Key Mitigations

- Secure IPMI configuration.
- Restrict access to the Admin/Red Forest only to AD admins.
- Ensure that only Tier 0 systems have access/control to this environment.
- Trust configuration between the Admin Forest & managed forests is a forest trust, not external.



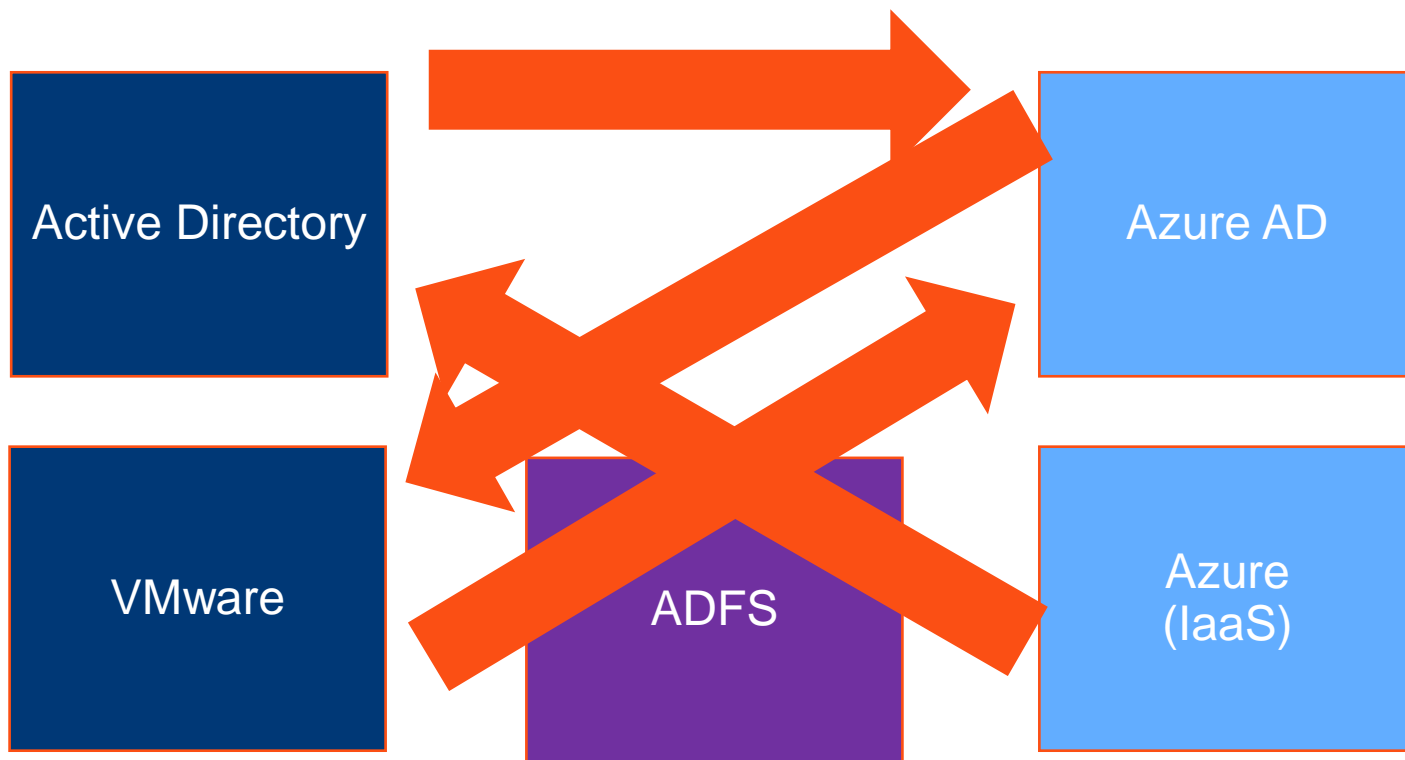
# Attack Scenario: Ransomware

**TEC**

**The Experts  
Conference**

*Sponsored by Quest®*

# Ransomware





# Mitigations

# Mitigation

- The best way to mitigate these issues is a combination of:
  - Security Assessments
  - System hardening
  - Authentication flow identification
  - Secure Cloud integration components

# Active Directory Security Recommendations

#TEC2022

**TEC**

**The Experts  
Conference**

*Sponsored by Quest®*



# Securing AD: Level 1

- Randomize computer local Administrator account passwords. (Microsoft LAPS)
- Minimize groups (& users) with DC admin/logon rights.
- Separate user & admin accounts.
- No user accounts in any admin groups.
- Admin accounts set to “sensitive & cannot be delegated”.
- All AD Admin accounts added to “Protected Users” group.
- Long, complex (>30 characters) passwords for Service Accounts.
- Ensure that supported Windows versions are running on DCs and that they are appropriately patched.
- Ensure Authenticated Users can't join computers to AD (Remove from DC-linked GPO setting “Add workstations to domain”).
- Configure GPO to prevent local accounts from connecting over network to computers.

# Securing AD: Level 2

- ADAs should only logon to a DC (or admin workstation or admin server).
- Service Accounts (SAs):
  - Leverage “(Group) Managed Service Accounts”.
  - Implement Fine-Grained Password Policies (DFL >2008).
  - Limit SAs to systems of the same security level, not shared between workstations & servers (for example).
  - Ensure passwords are >25 characters.
- Ensure all computers are talking NTLMv2 & Kerberos, deny LM/NTLMv1.
- Disable all SMBv1.
- Separate Admin workstations for administrators (locked-down & no internet).
- No Domain Admin service accounts on non-Tier0 systems.
- Limit management protocol access on DCs to admin subnets (RDP, WMI, WinRM, etc).

# Securing AD: Level 3

- Complete separation of administration
- ADAs never logon to other security tiers.
- Restrict workstation to workstation communication with host firewalls
  - AD clients don't need special rules, default block All inbound works.
- Implement network segmentation.

# Protect Admin Creds

- Ensure all admins only log onto approved admin workstations & servers.
- Add all admin accounts to Protected Users group (requires Windows 2012 R2 DCs).
- Admin workstations & servers:
  - Control & limit access to admin workstations & servers.
  - Remove NetBIOS over TCP/IP
  - Disable LLMNR.
  - Disable WPAD.

# Additional Mitigations

- Enable NTLM Auditing on DCs.
- Enable SMB Auditing on DCs & file servers.
- Enable PowerShell logging everywhere & send to SIEM.
- Monitor scheduled tasks on sensitive systems (DCs, etc).
- Block internet access to DCs & servers.
- Change the KRBTGT account password (twice) every year & when an AD admin leaves.
- Configure LDAP Signing & Channel Binding.
- Use PingCastle (<https://pingcastle.com/>) and Bloodhound (<https://github.com/BloodHoundAD>) to help identify problematic AD configurations.

# VMware Security Recommendations

**TEC**

**The Experts  
Conference**

*Sponsored by Quest®*

# VMware Security Recommendations

- Update all ESXi hosts to current supported version.
- Update all VMware Tools to current supported version on all VMs.
- Enable Lockdown mode.
- Physically secure servers.
- Identify and secure IPMI out of band systems (ILO, DRAC, etc.).
- Ensure VMware admin groups are well secured in Active Directory.
- Tier 0 VMs (AD/PKI/AADC/etc) should be hosted in a separate Tier 0 vCenter/Hyper-V instance.
- At a minimum, use RBAC in vCenter so that server admins can't access Tier 0 assets like virtual DCs, PKI, AAD Connect, etc.
- Encrypt the virtual DCs (and other T0 assets) with vSphere Virtual Machine Encryption, or if you can't do that, at least use FDE on the virtual DCs with BitLocker TPM so that low tier VM admins can't easily access ntds.dit from vmdks, snapshots, backup files, etc.

# Azure AD Security Recommendations

#TEC2022

**TEC**

**The Experts  
Conference**

*Sponsored by Quest®*



# Azure AD Security Recommendations

- Ensure admin accounts sourced in Azure AD (onmicrosoft accounts) are the only members in Azure AD roles, not regular user accounts.
- Leverage PIM for controlling Azure AD role membership and ensure all people accounts are Eligible and not Permanent members.
- Use Azure AD MFA with Microsoft Authenticator (preferably with number matching).
- Review highly privileged application permissions (such as Directory.ReadWrite.All).
- If there are highly privileged application permissions, ensure there's additional protections for the Application Administrator & Cloud Application Administrator roles.

# Azure (IaaS) Security Recommendations

**TEC**

**The Experts  
Conference**

*Sponsored by Quest®*

# Azure (IaaS) Security Recommendations

- Restrict Azure AD Global Administrator role membership.
- Minimize Admin and Owner roles on the root as well as Subscriptions with sensitive systems.
- If there are Domain Controllers in Azure, all Azure admin roles become Tier 0.
- Configure security policies.
- Enable Network Security Groups on subnets or virtual machines.
- Restrict access through Internet facing endpoint

# Mitigation Summary from all Attack Scenarios

**TEC**

**The Experts  
Conference**

*Sponsored by Quest®*

# On-prem AD & Password Vaults

- Ensure only admin accounts are used for administration and that admin accounts are well protected.
- Ensure only Tier 0 admin accounts are members of password vault admin groups.
- Restrict password vault access to the system and related computers.
- Admins should only connect to a password vault from an admin system (workstation or server) specific to administration.
- Admins should only connect to a password vault with credentials other than regular user or admin credentials. We refer to this as a “transition account.”
- Ensure credentials are not stored in files or scripts on network shares or personal storage.

# Azure AD / Microsoft Office 365 & Azure

- Severely restrict membership in Global Admins.
- Ensure only admin accounts are used for administration and that they are well protected.
- Preferably use PIM (eligible) for all Azure AD roles.
- Require MFA for all Azure AD admins.
- Do not synchronize on-prem admin accounts to Azure AD.  
(simpler if properly separated in top-level admin OU)
- If write-back is configured, think through potential issues.
- Closely monitor membership of the “User Access Administrator” Azure role (root level).
- Place Domain Controllers and other sensitive systems in another Azure tenant.

# VMware vSphere

- Ensure only admin accounts are used to manage VMware.
- Ensure VMware administration is well protected (Tier 0).
- Restrict VMware admin rights only to the accounts that require them.
- Protect VMware Admin groups to protect VMware.
- Don't use AD groups for VMware administration if the group and associated accounts can't be securely managed and used.
- VMware platform security is critical to the security of most of the systems in many organizations.

# IPMI & Admin/Red Forest

- Ensure IPMI systems (iDRAC, ILO, etc.) are on a separate out of band (OOB) network instead of the production corporate network.
- If IPMI can't be separated on a different network, ensure there are network controls to restrict access to these systems.
- Keep physical server hardware firmware updated.
- HPE iLO Amplifier Pack is a free tool that helps with this:  
<https://buy.hpe.com/us/en/software/server-management-software/server-ilo-management/ilo-management-engine/ilo-amplifier-pack/p/1009838729>
- Restrict access to the Admin/Red Forest only to AD admins.
- Ensure that only Tier 0 systems have access/control to the Admin/Red Forest environment.
- Ensure trust configuration between the Admin Forest & managed forests is a forest trust, not external.



# Conclusion



Interconnections between multiple systems provide attack opportunity.

Identification of these connections and hardening systems is critical for security.

Review configuration to discover potential security issues.



Slides, Video & Security Articles: [Hub.TrimarcSecurity.com](https://Hub.TrimarcSecurity.com)

# References

- Microsoft Graph Permissions Reference

<https://learn.microsoft.com/en-us/graph/permissions-reference>

- Role Assignable Groups

<https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept>

- Azure AD Roles

<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

- From Azure AD to AD via Azure – An Unanticipated Attack Path

<https://www.hub.trimarcsecurity.com/post/from-azure-ad-to-active-directory-via-azure-an-unanticipated-attack-path>

- HPE iLO Amplifier Pack

<https://buy.hpe.com/us/en/software/server-management-software/server-ilo-management/ilo-management-engine/ilo-amplifier-pack/p/1009838729>

# References

- Airbus Security – ILO  
[https://github.com/airbus-seclab/ilo4\\_toolbox](https://github.com/airbus-seclab/ilo4_toolbox)
- Microsoft PTA  
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta>
- Attacking Microsoft PTA & Azure AD Connect  
<https://blog.xpnsec.com/azuread-connect-for-redteam/>
- Azure AD Seamless SSO  
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso>
- Attacking Azure AD Seamless SSO  
<https://www.dsinternals.com/en/impersonating-office-365-users-mimikatz/>
- Introducing ROADtools - The Azure AD exploration framework  
<https://dirkjanm.io/introducing-roadtools-and-roadrecon-azure-ad-exploration-framework/>
- Dirk-jan Mollema's talks  
<https://dirkjanm.io/talks/>

# Similar Talks

- Trimarc Webcast: Top 10 Ways to Improve Active Directory Security Quickly
  - [Slides](#)
  - [YouTube Video](#)
- BSlides Charm Presentation: AD CS Means 'Active Directory is Cheese (Swiss)'
  - [Slides](#)
  - [YouTube Video](#)
- TEC Presentation: Hardening Azure AD in the Face of Emerging Threats
  - [On Demand Video](#)
- DEFCON Presentation: Hacking the Hybrid Cloud
  - [Slides](#)
  - [YouTube Video](#)
- Trimarc Webcast: Performing Your Own AD Security Review
  - [Slides](#)
  - [YouTube Video](#)



# Questions?

# Thank you!