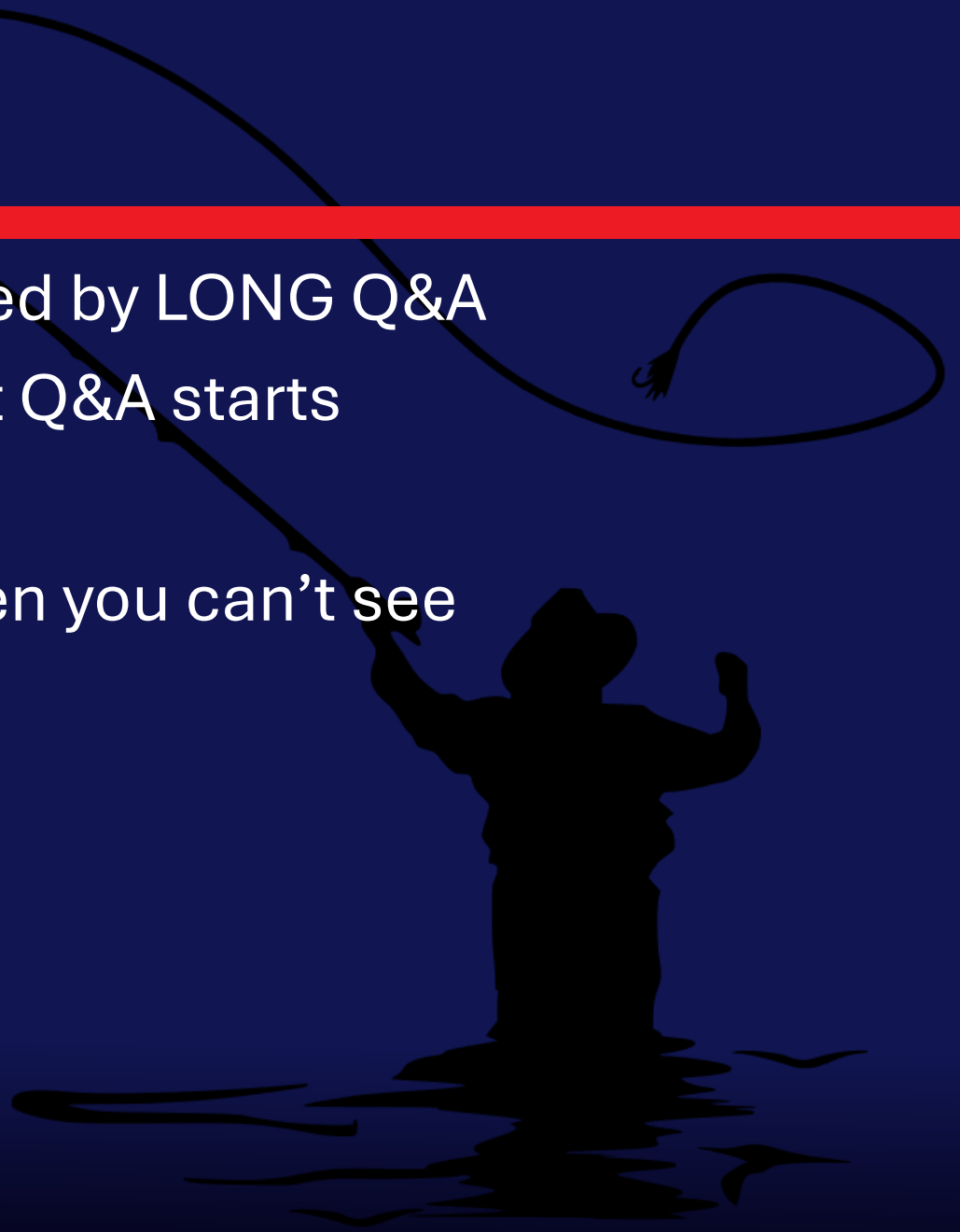
Hello Passkey, Bye Password: Phishing-Resistant MFA Made Simple

Attention

- MMS sessions are 60-75 minutes followed by LONG Q&A
- Please hold detailed questions until that Q&A starts
- Feel free to ask clarification questions
- Remind the speakers to use Zoom It when you can’t see



Speakers

Lee Schlipphak

Consultant

leeschl

in/leeschl

Jan Ketil Skanke

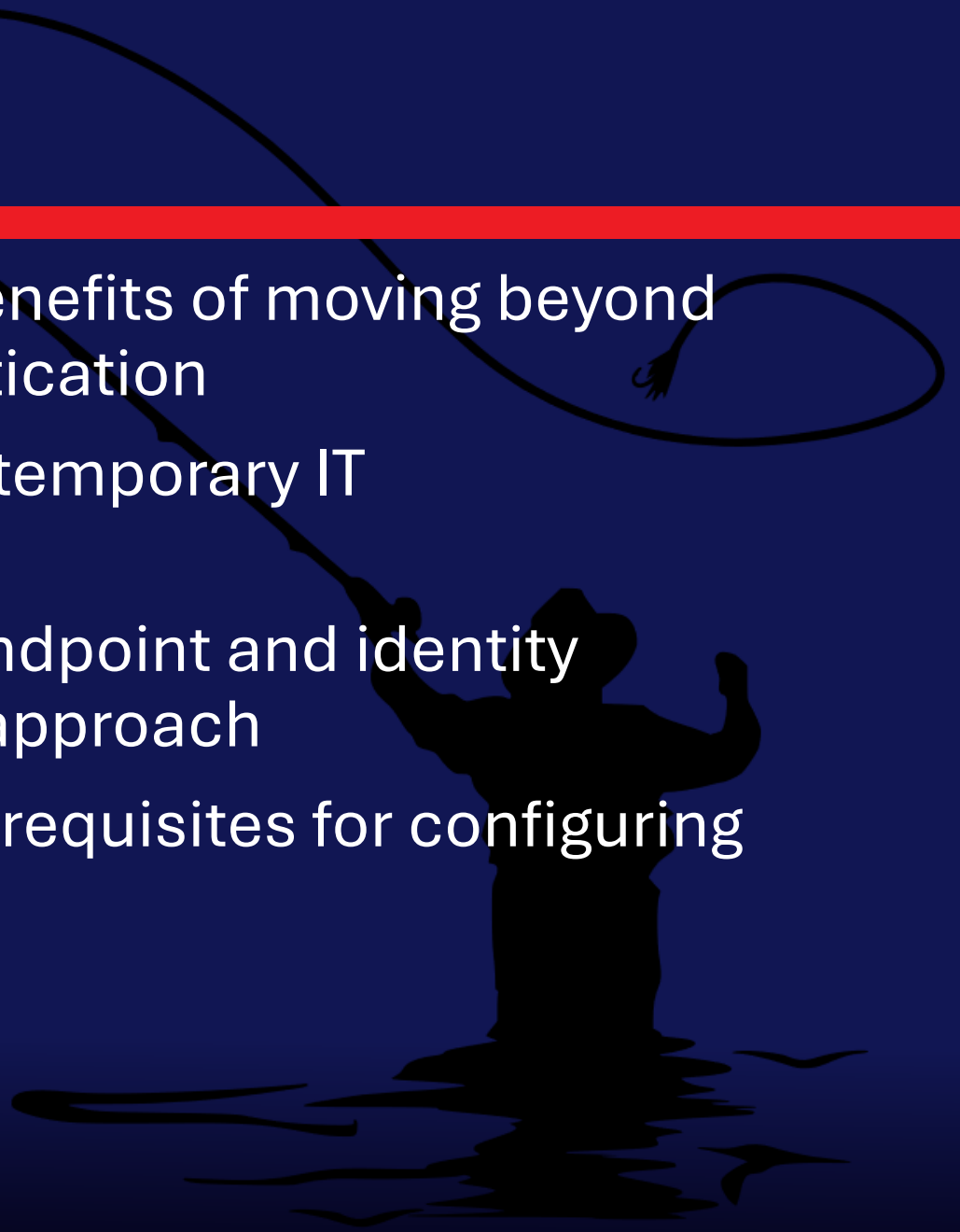
Principal Cloud Architect

in/JankeSkanke

Can’t see our slides? Can’t hear? Need to repeat the question? Call us out!

Session Takeaways

- Understand the security and usability benefits of moving beyond passwords to phishing-resistant authentication
- Master the management of WHfB in contemporary IT environments for enhanced security
- Explore the integration of WHfB within endpoint and identity management for a seamless Zero Trust approach
- Gain insights into best practices and prerequisites for configuring WHfB alongside Microsoft Intune



MMS

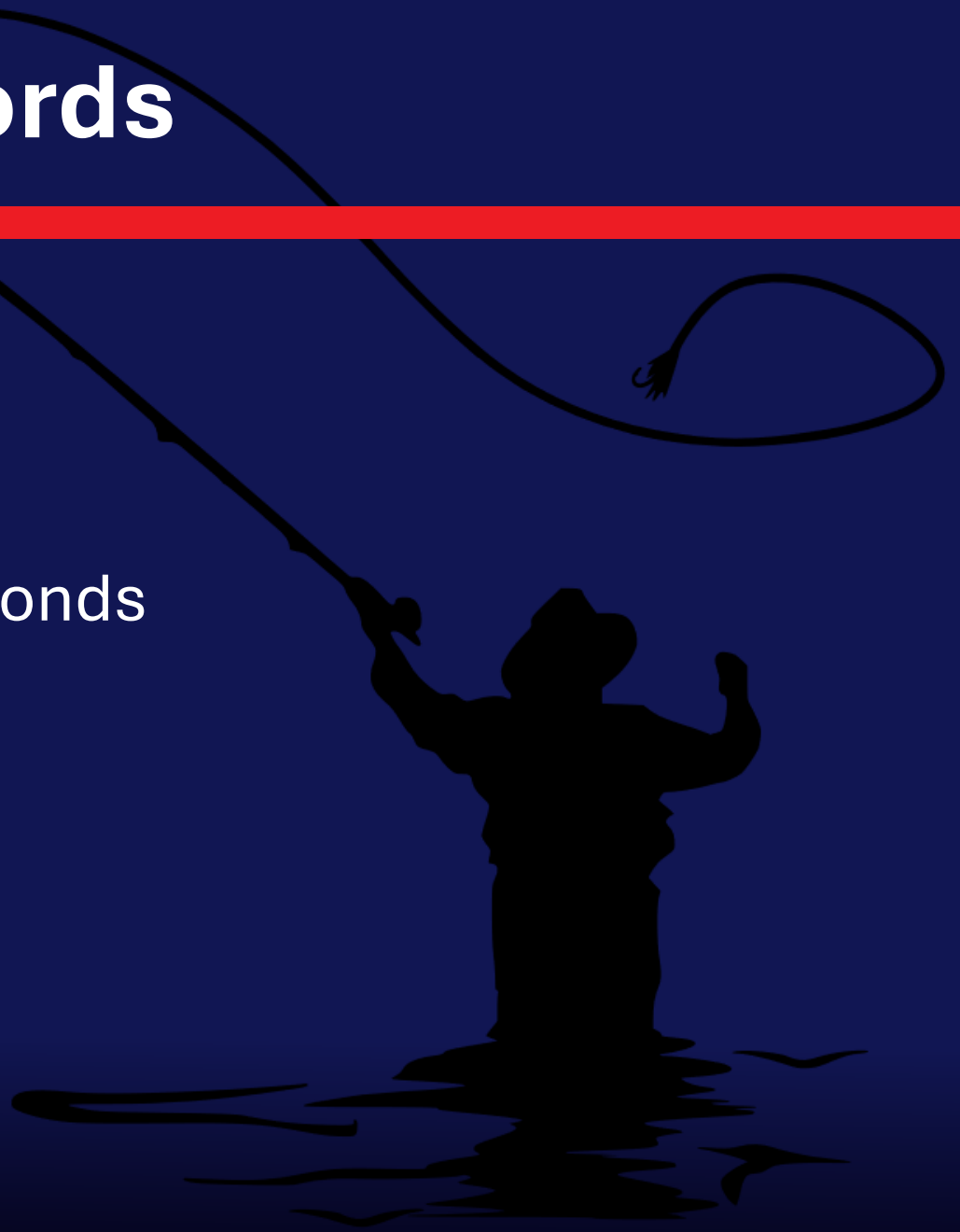
The Problem with Passwords

... are the passwords

The Problem with Passwords

The Problem with Passwords

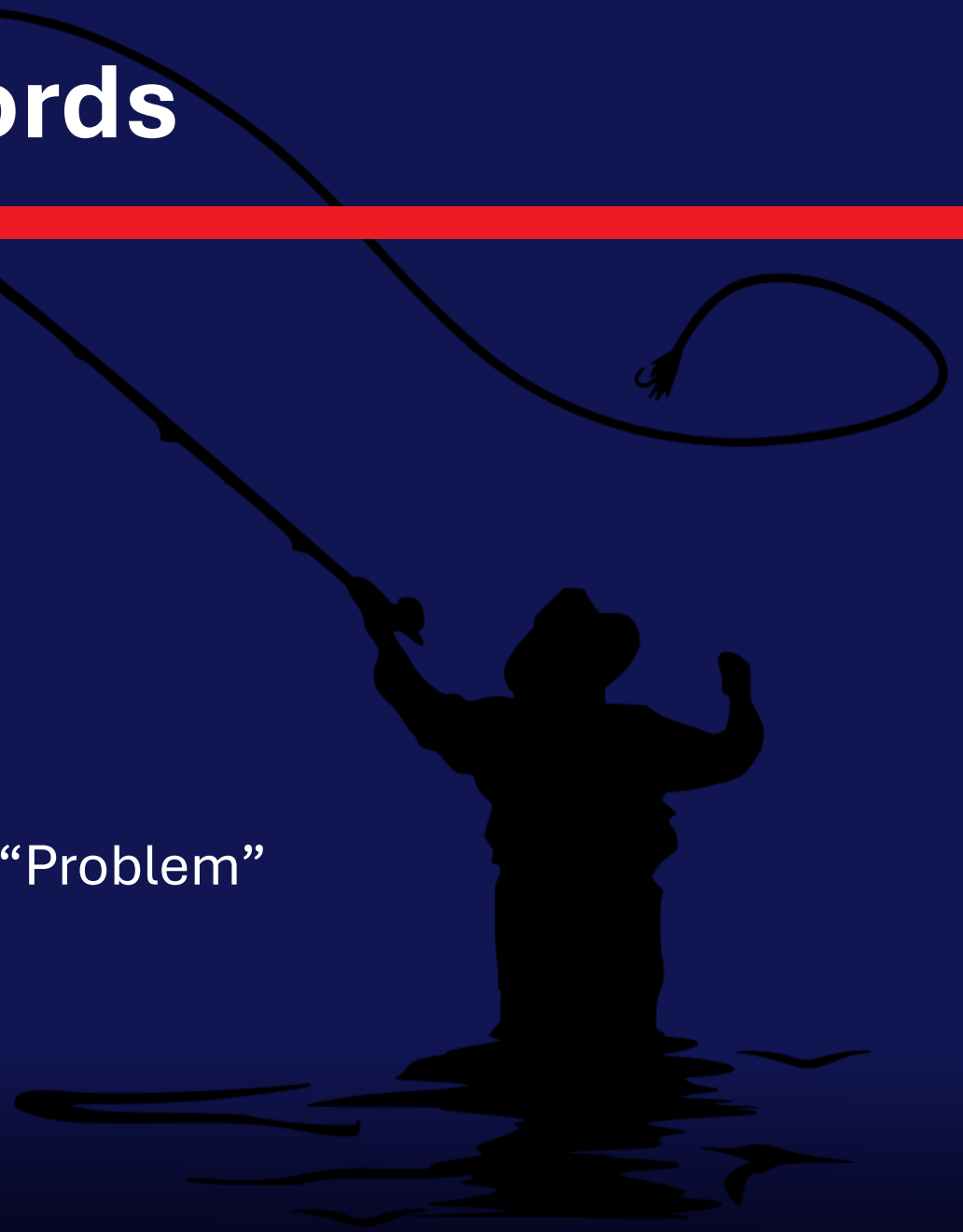
- Too complex for users
- Users forget them all the time
- Users recycle passwords
- Passwords could be hacked in a few seconds



The Problem with Passwords

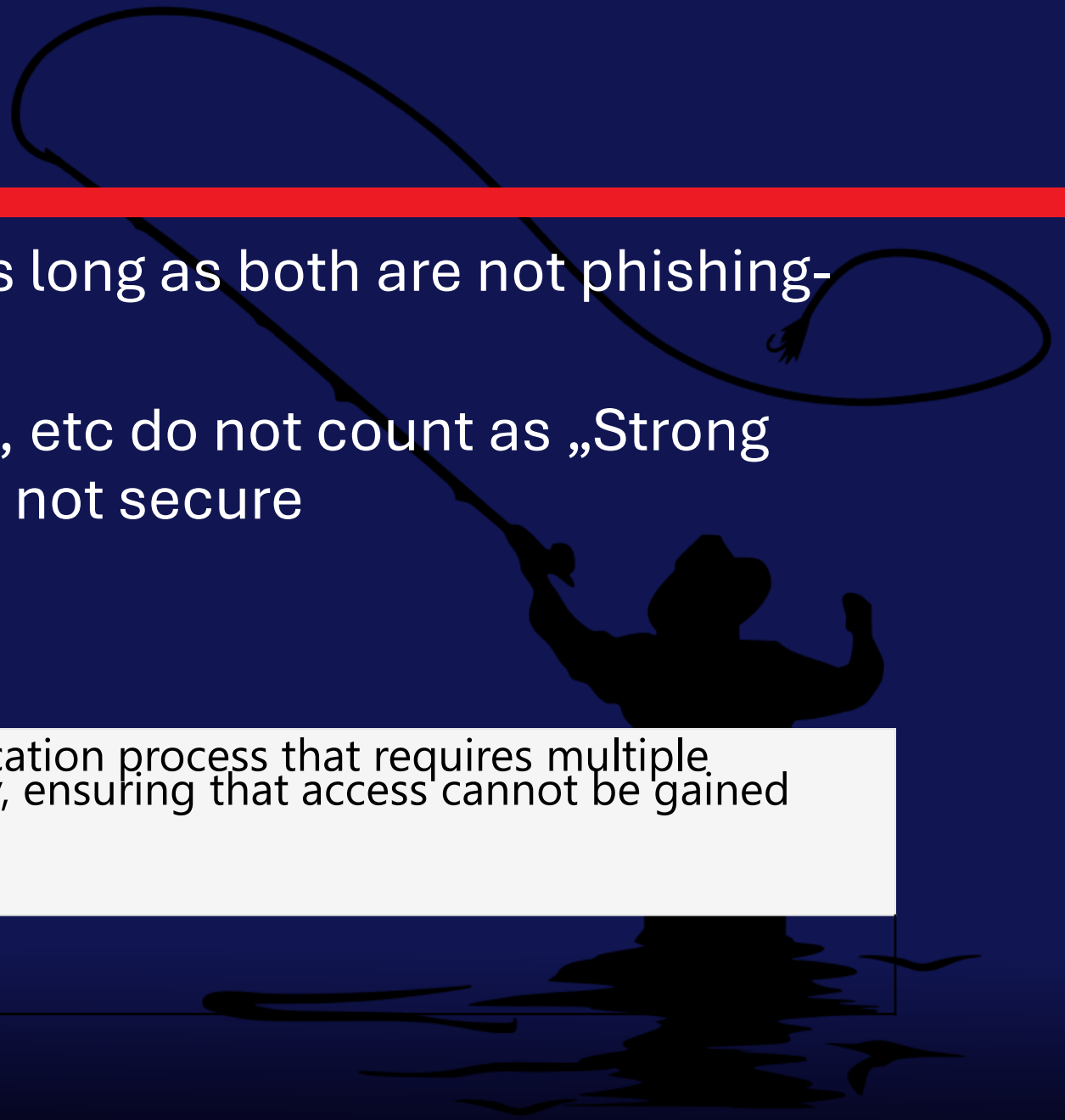
- Passwords are easy to steal
  - Phishing
  - Social Engineering
- User are not sensible
  - Phishing Simulations are not enough

=> Passwords + human component build the “Problem”



MFA

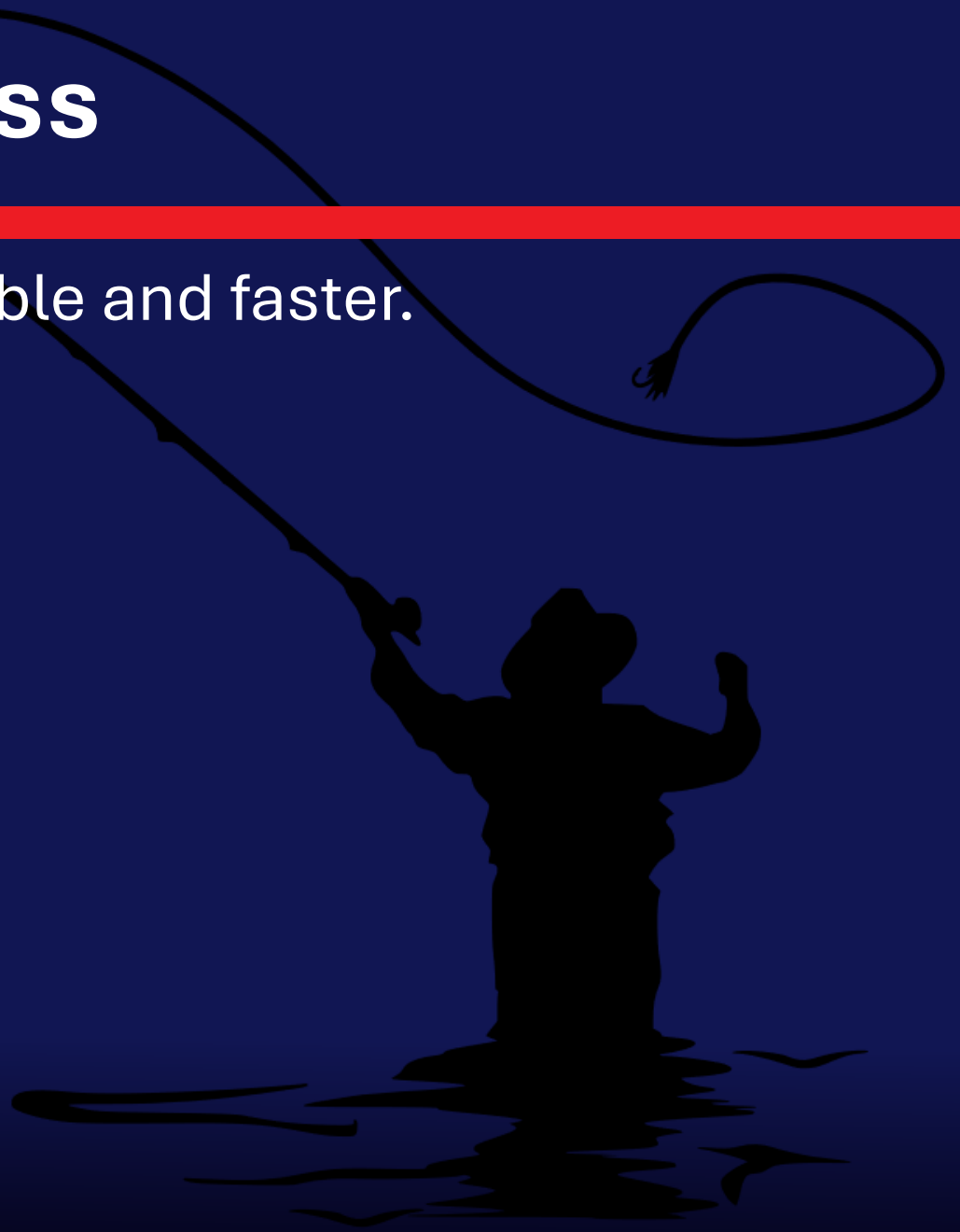
- Password + MFA –ne Secure => as long as both are not phishing-resistant
- SMS, E-Mail Codes, App Prompts, etc do not count as „Strong authentication methods“ and are not secure



Strong authentication refers to an authentication process that requires multiple independent factors to verify a user's identity, ensuring that access cannot be gained through a single compromised credential.

The Future is passwordless

- The user experience is improved, enjoyable and faster.
- Authentication with Passkeys is secure
- Phishing resistant by design
- Passkeys are unique (per service)



MMS

Passkeys

- Passwordless
- Authentication via biometrics or PIN
- Authentication is based on Asymmetric-Kryptography - FIDO2
- Private Key stays on the device – Security Key, Smartphone

Password vs. Passkey Authentication Flow

Password

- Login: Username + PW
- App send the PW to the Identity Provider for validation
- Identity Provider compares PW-Hash and provides Access Token
- Shared Secrets are susceptible to compromise
- Only Zero Trust compatible with phishing resistant MFA

Passkey/WHfB

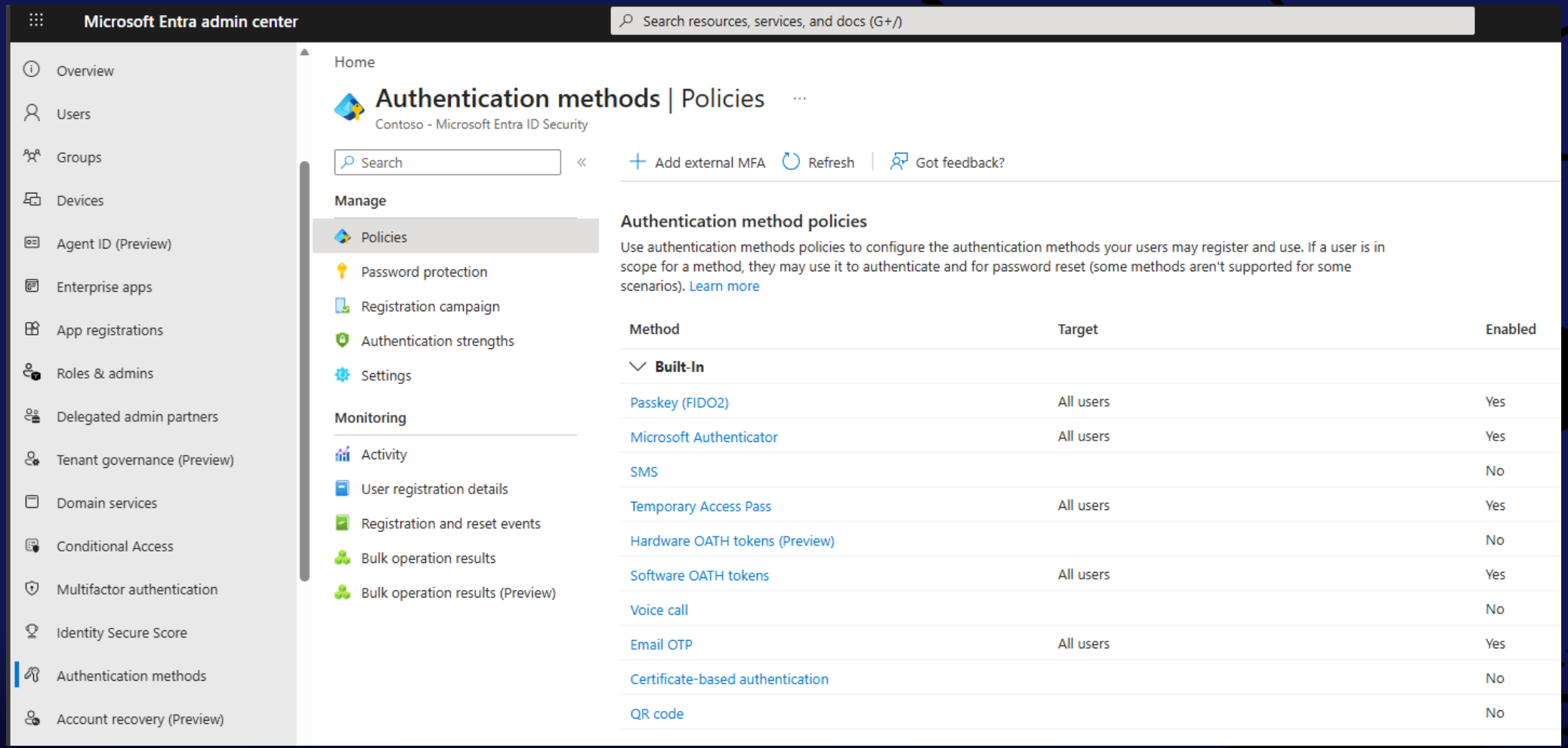
- Login: Bio or PIN encrypts private Key in TPM
- Private key is device bounded and the Identity Provider uses public keys for validation
- Device signs Nonce with private key -> Entra ID validates it using the public key > Issues a Primary Refresh Token (PRT) > TPM protects session key
- Asymmetric cryptography. Private Keys stays on device
- Passkeys/ WHfB is phishing-resistant

How Windows Hello for Business authentication works | Microsoft Learn

DEMO

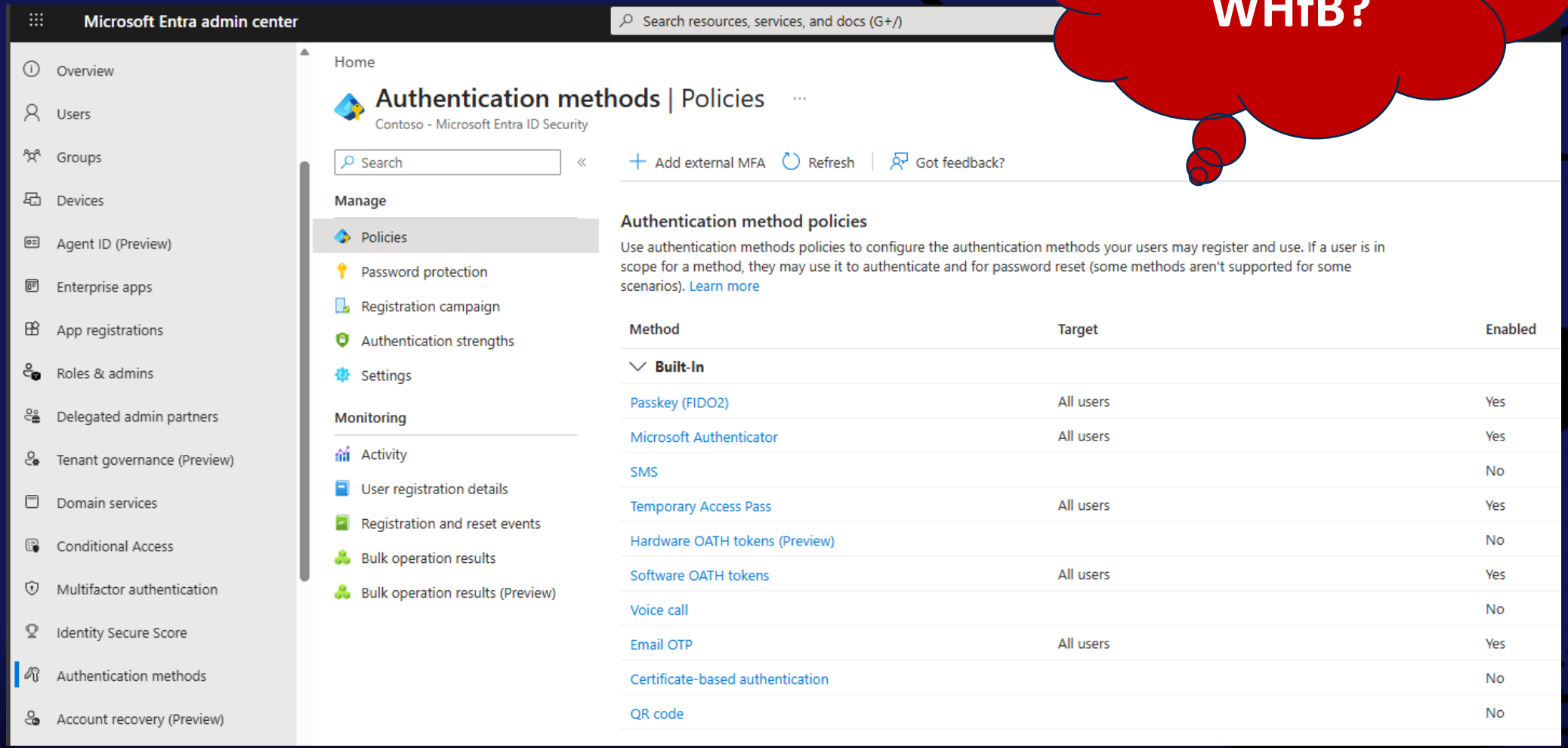
Entra Auth Methods

Entra Authentication Methods



Entra Authentication

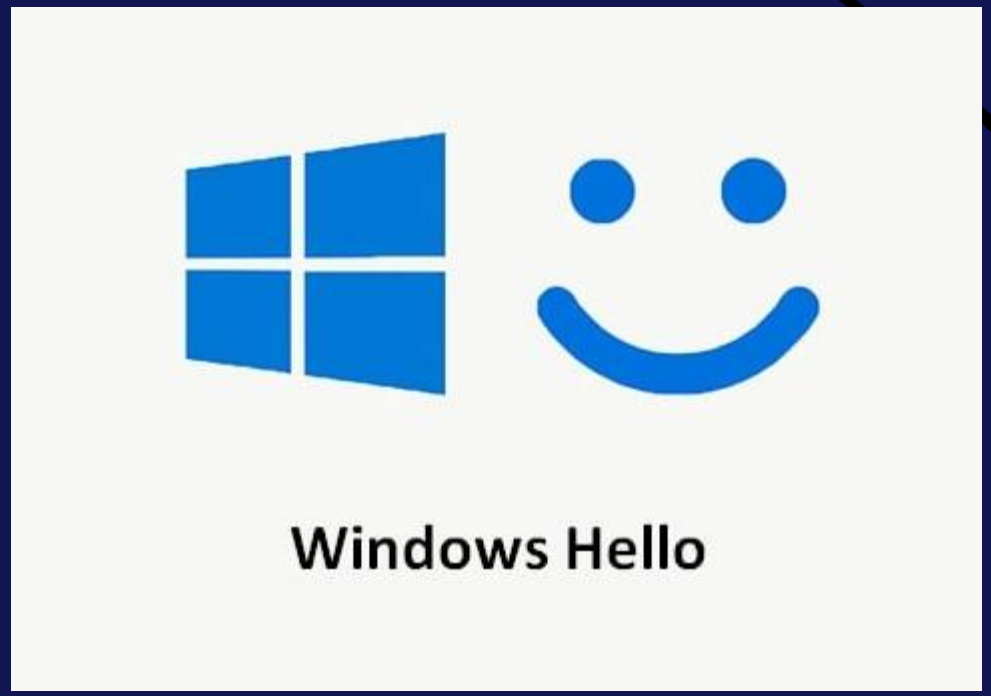
Where is WHfB?



Windows Hello for Business

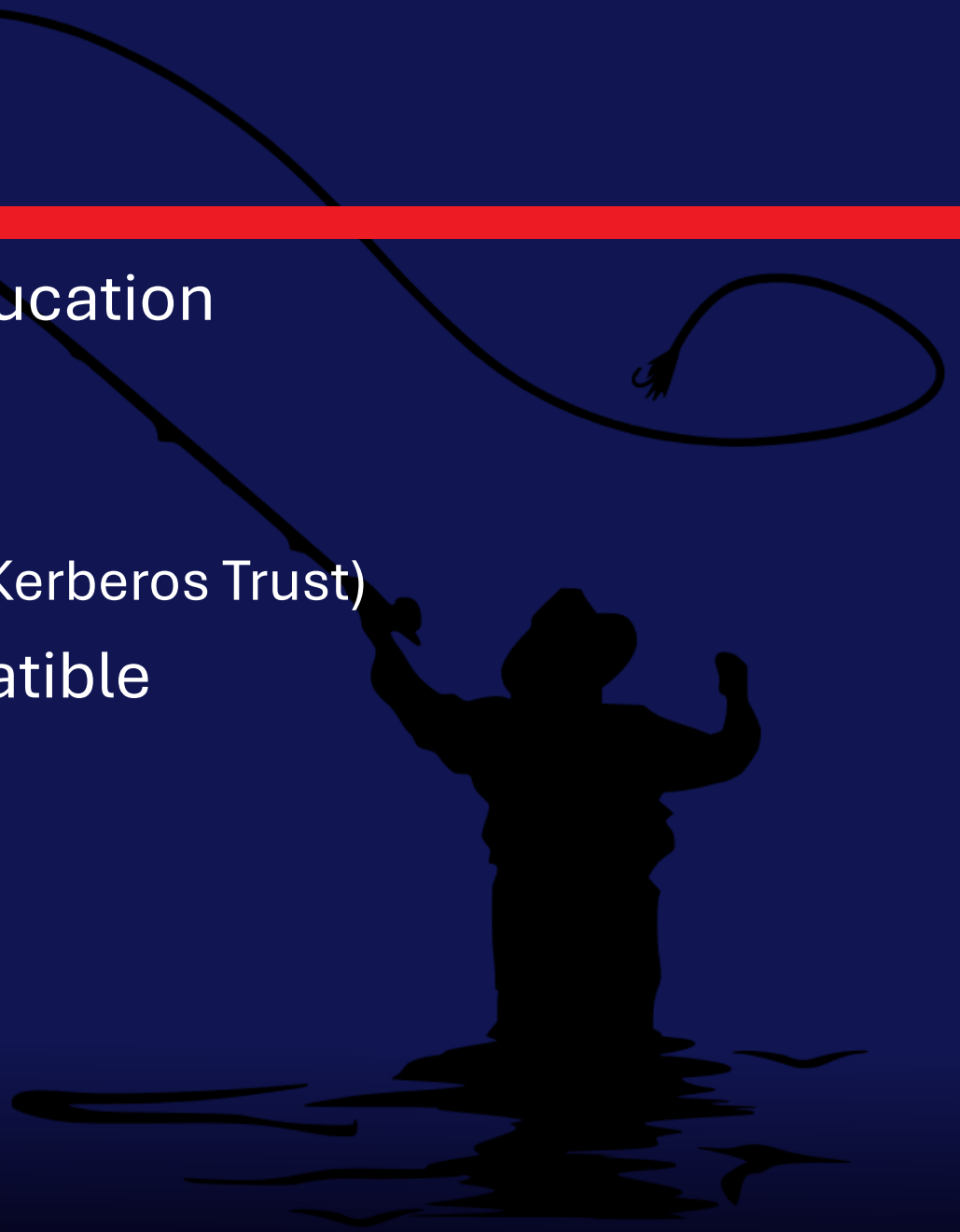
Deep Dive

Windows Hello for Business



WHfB Prerequisites

- Windows 11 Professional/Enterprise/Education
- TPM 2.0 preferred for improved security
- Entra ID Account (Hybrid/Cloud-Native)
  - Hybrid requires additional setup (ex Cloud Kerberos Trust)
- Biometric sensors, that are WHfB compatible



Biometric sensors

- All of the sensors must include anti-spoofing measures
- Performance rate is defined by False Accept Rate (FAR) and False Reject Rate (FRR)
- FAR > FRR
- Ratio: 1 in 100.000

Acceptable performance range for small to large size touch sensors:

- False Accept Rate (FAR): <0.001 - 0.002%
- Effective, real world FRR with Anti-spoofing or liveness detection: <10%

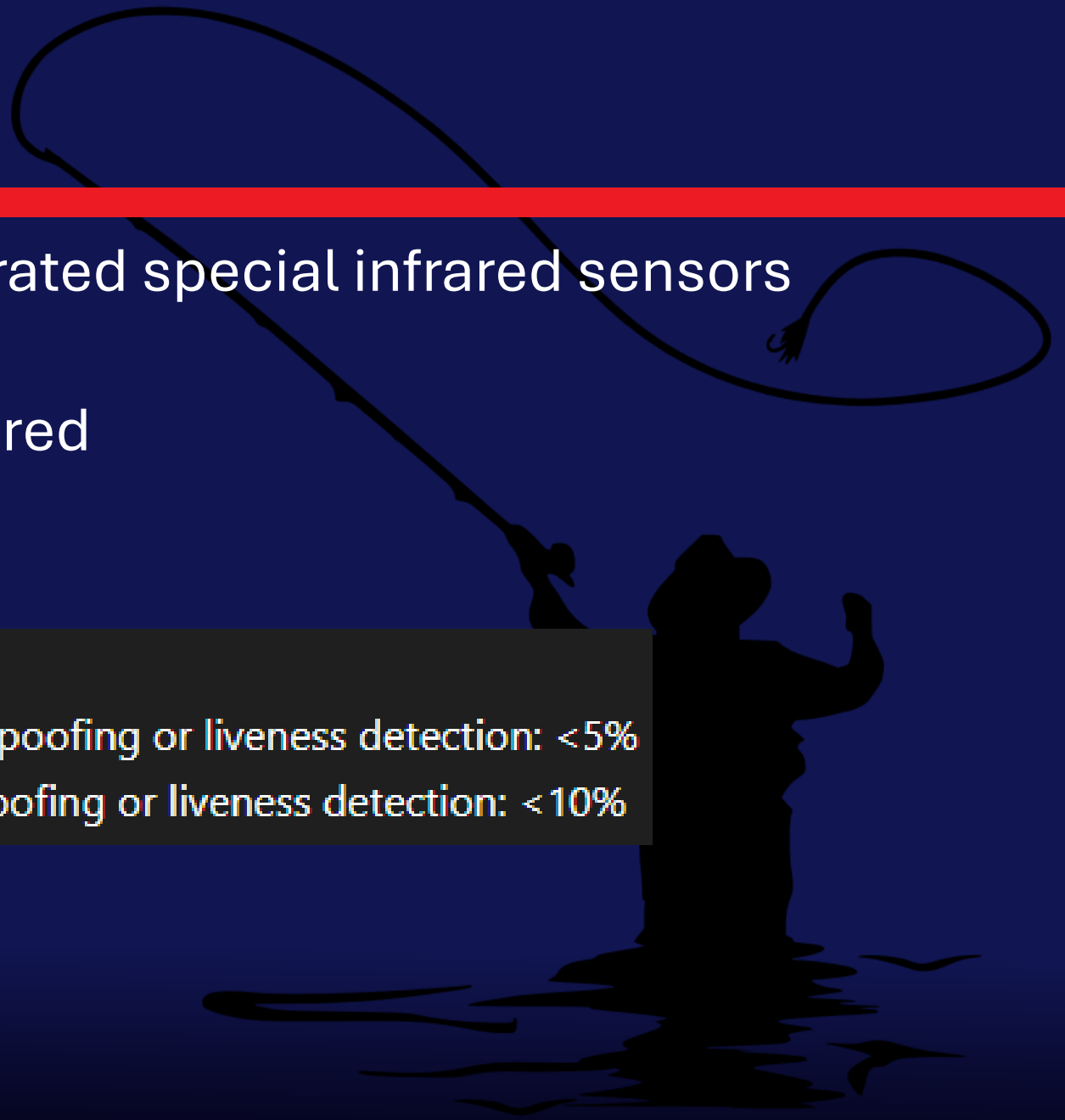
Acceptable performance range for swipe sensors:

- False Accept Rate (FAR): <0.002%
- Effective, real world FRR with Anti-spoofing or liveness detection: <10%

Biometric sensors

- Facial Recognition requires integrated special infrared sensors and software
- Anti-spoofing measures are required

- False Accept Rate (FAR): <0.001%
- False Reject Rate (FRR) without Anti-spoofing or liveness detection: <5%
- Effective, real world FRR with Anti-spoofing or liveness detection: <10%



WHfB licence requirements

The following table lists the Windows editions that support Windows Hello for Business:

Expand table

Windows Pro	Windows Enterprise	Windows Pro Education/SE	Windows Education
Yes	Yes	Yes	Yes

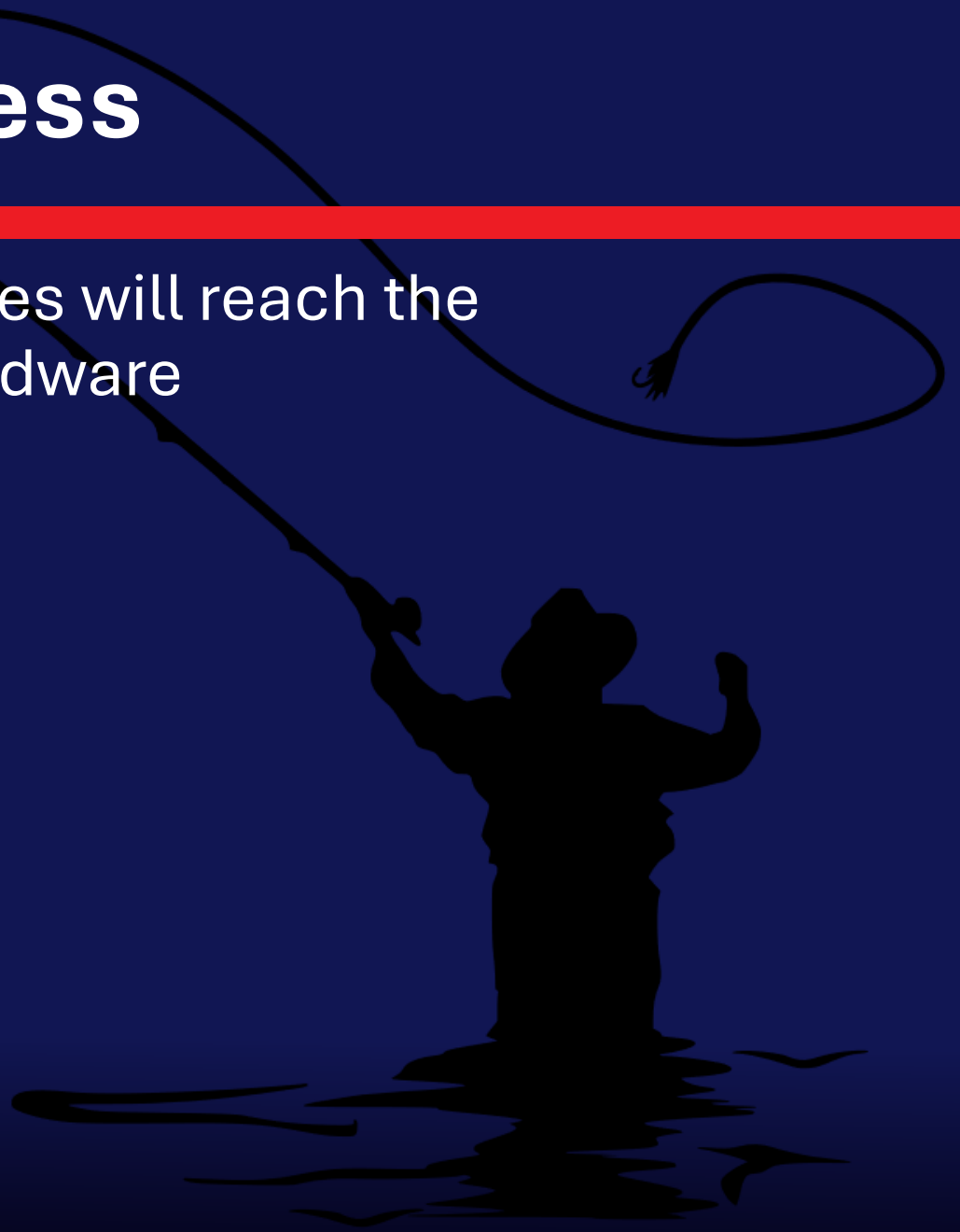
Windows Hello for Business license entitlements are granted by the following licenses:

Expand table

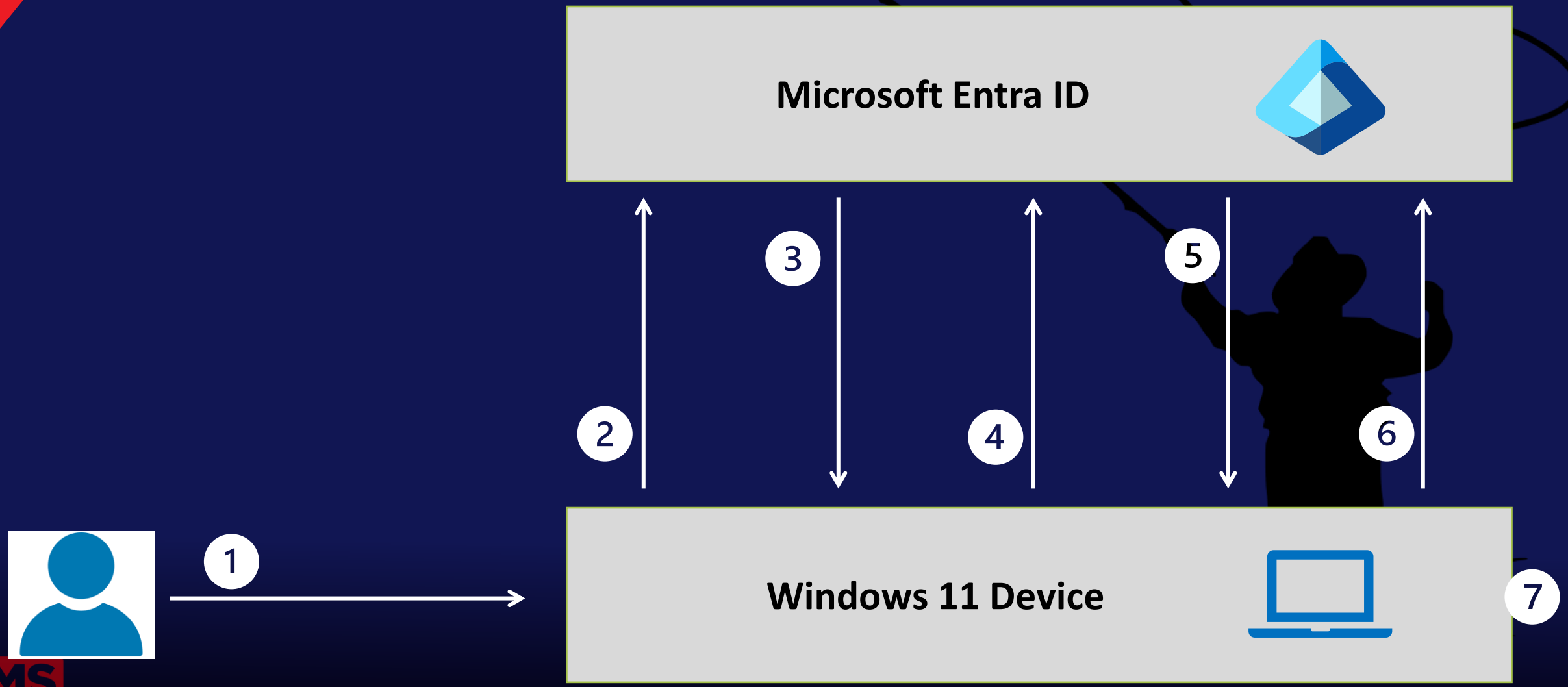
Windows Pro/Pro Education/SE	Windows Enterprise E3	Windows Enterprise E5	Windows Education A3	Windows Education A5
Yes	Yes	Yes	Yes	Yes

Windows Hello for Business

- No additional costs, because your devices will reach the requirements in most cases with the hardware
- No external hardware necessary
- Low maintanance
- Improves User experience
- Quick and easy implemented



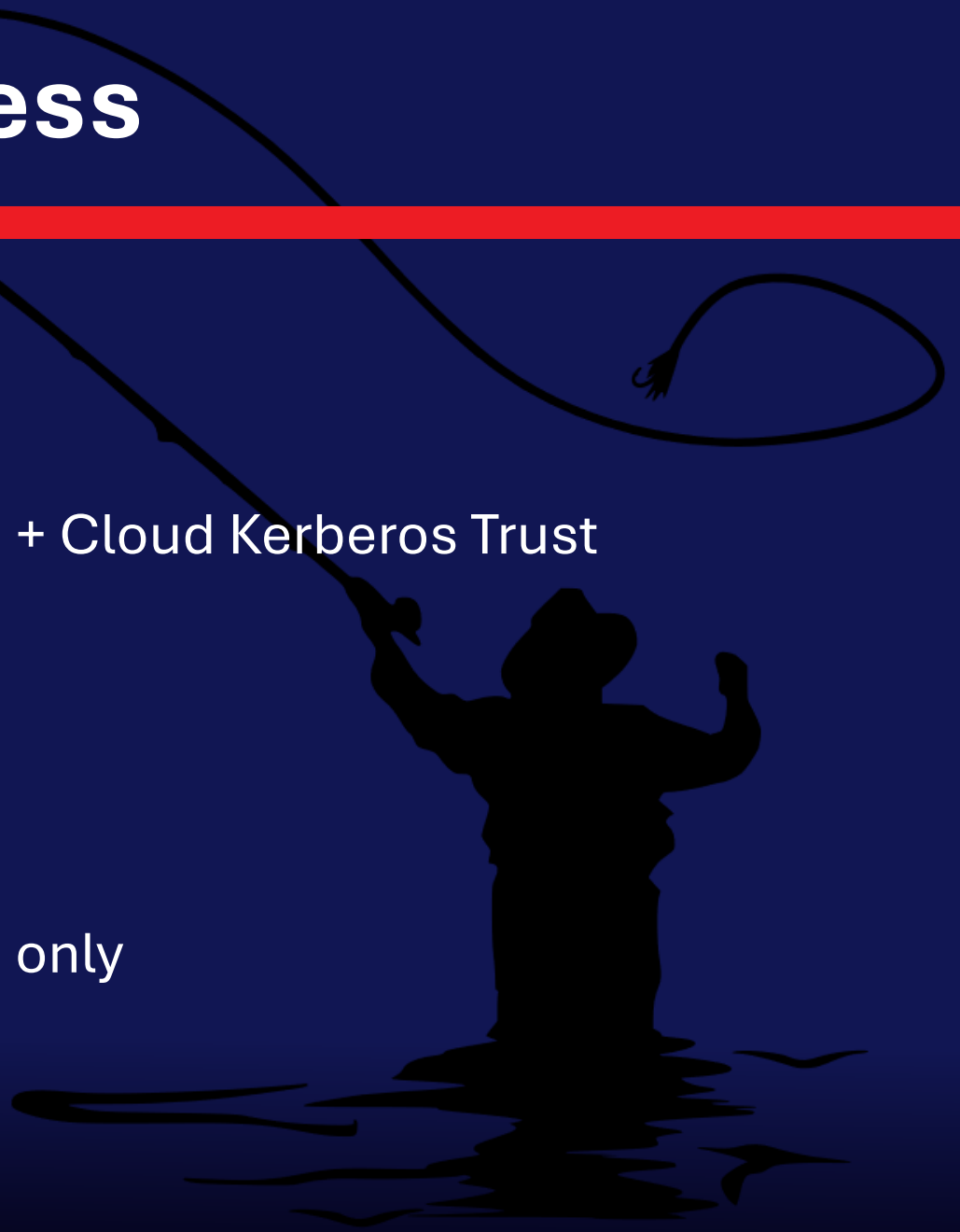
Windows Hello for Business



Windows Hello for Business

- Hybrid Infrastructure
  - Devices Cloud Only
  - Users hybrid
  - Implemention in Microsoft Entra and Intune + Cloud Kerberos Trust configuration Onprem

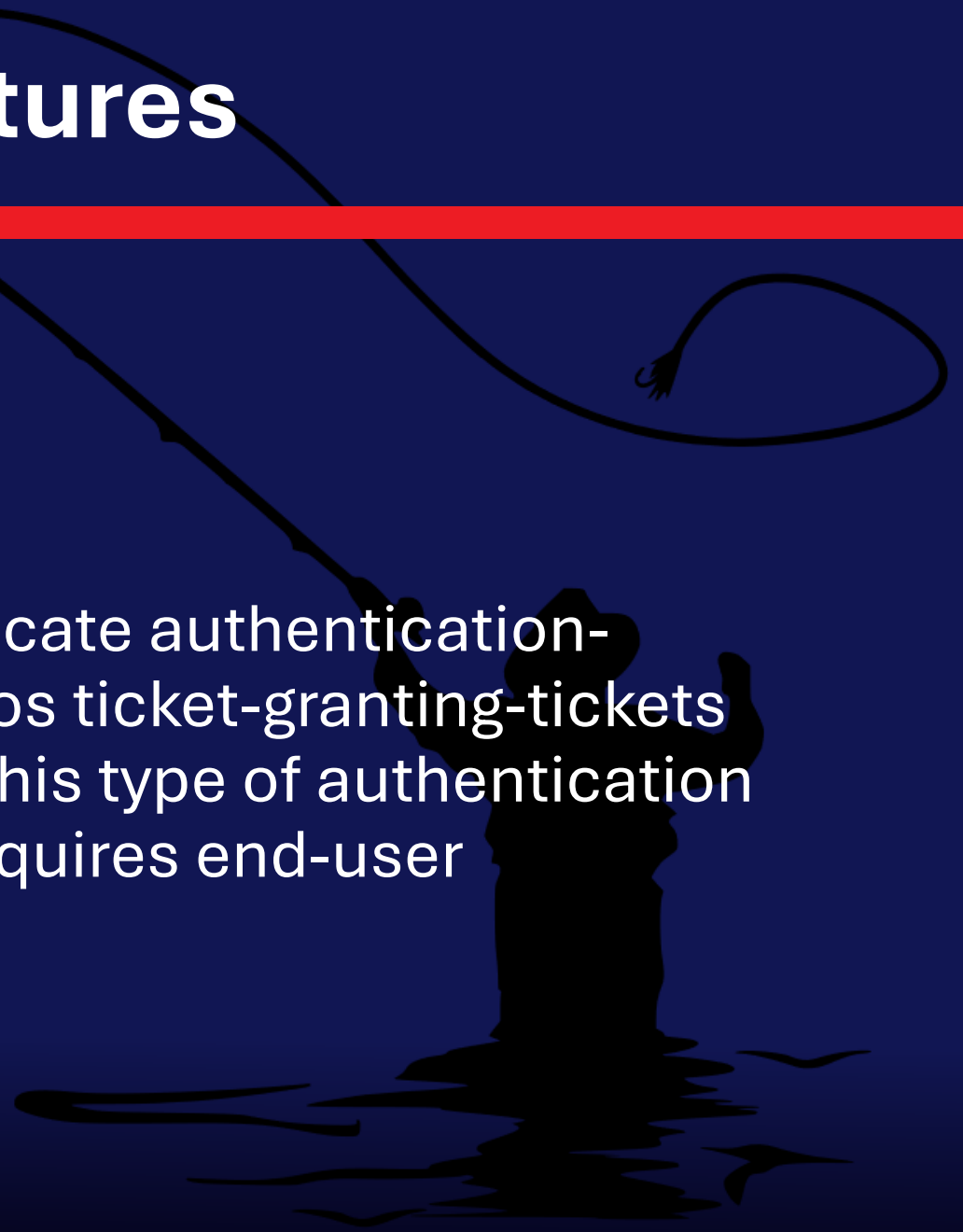
- Cloud Only Infrastructure
  - Users & Devices Cloud only
  - Implemention in Microsoft Entra and Intune only



WHfB – Hybrid Infrastructures

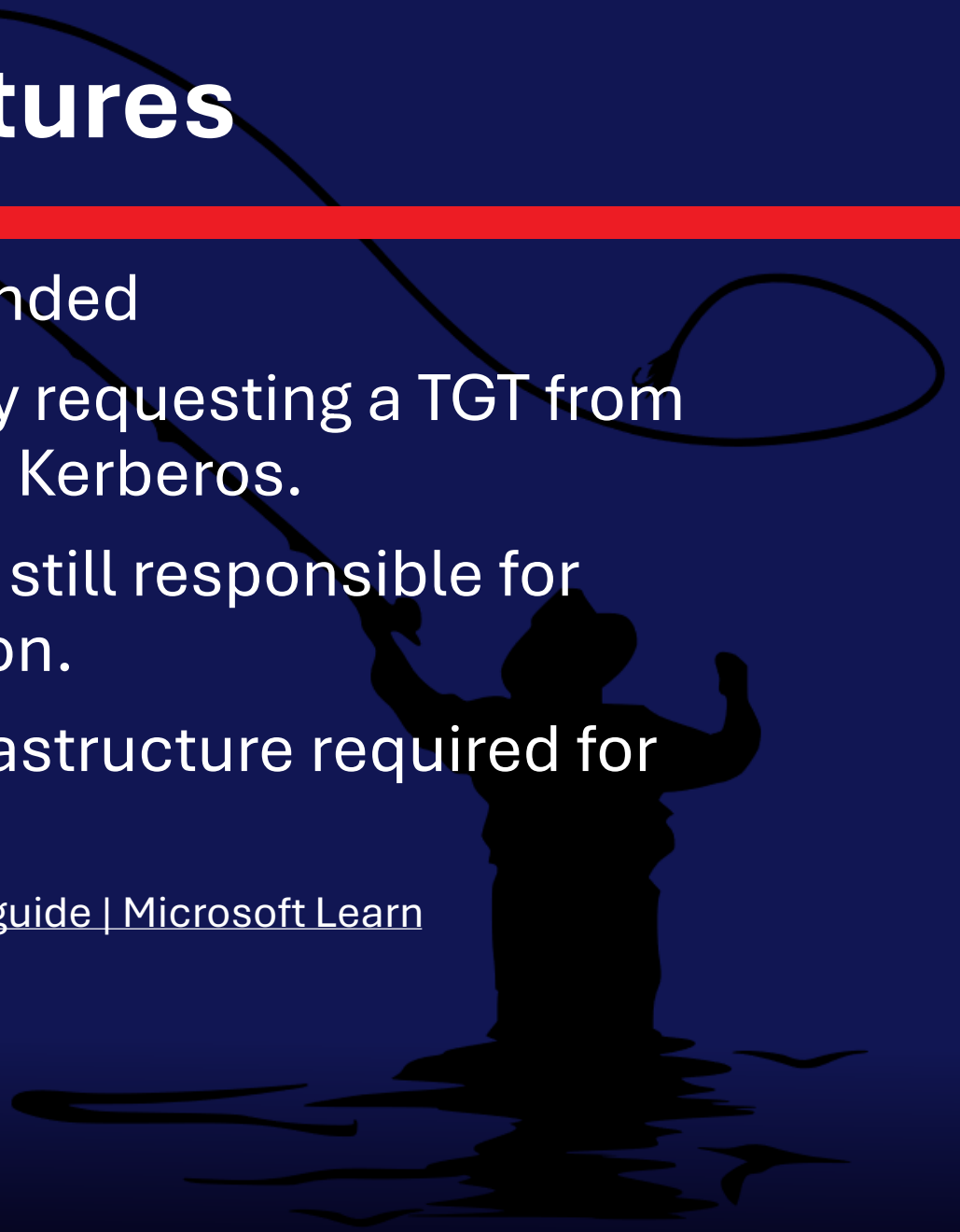
- Trust types:
  - Key
  - Certificate
  - Cloud Kerberos
- “*Key trust* and *certificate trust* use certificate authentication-based Kerberos when requesting kerberos ticket-granting-tickets (TGTs) for on-premises authentication. This type of authentication requires a PKI for DC certificates, and requires end-user certificates for certificate trust.”

Plan a Windows Hello for Business Deployment | Microsoft Learn



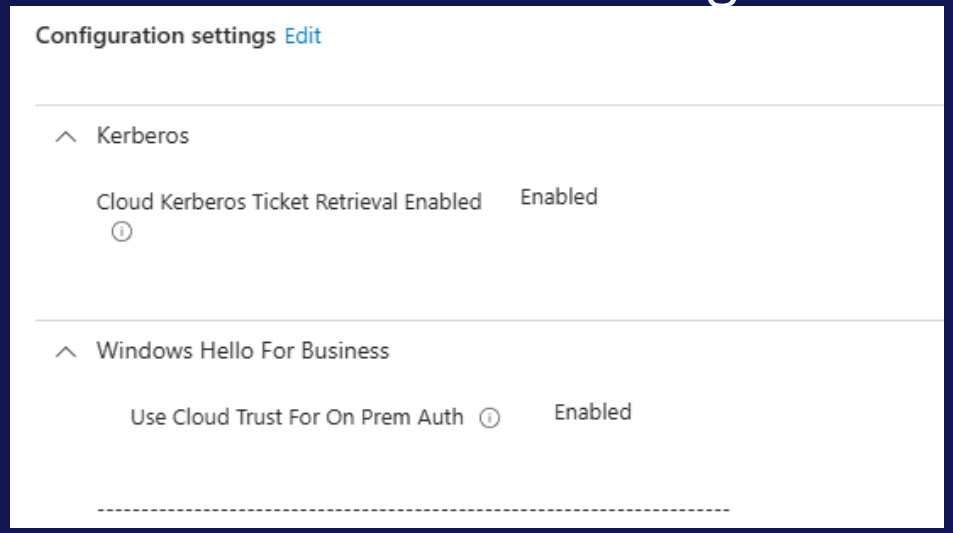
WHfB – Hybrid Infrastructures

- Cloud Kerberos Trust is highly recommended
- Users authenticate to Active Directory by requesting a TGT from Microsoft Entra ID, using Microsoft Entra Kerberos.
- The on-premises domain controllers are still responsible for Kerberos service tickets and authorization.
- Cloud Kerberos trust uses the same infrastructure required for FIDO2 security key sign-in
- Windows Hello for Business cloud Kerberos trust deployment guide | Microsoft Learn



WHfB – Hybrid Infrastructures

- Cloud Kerberos Trust implementation is very easy
  - Create a RODC
  - Passwordless security key sign-in to on-premises resources - Microsoft Entra ID | Microsoft Learn
  - Intune Config additional to the WHfB Configuration



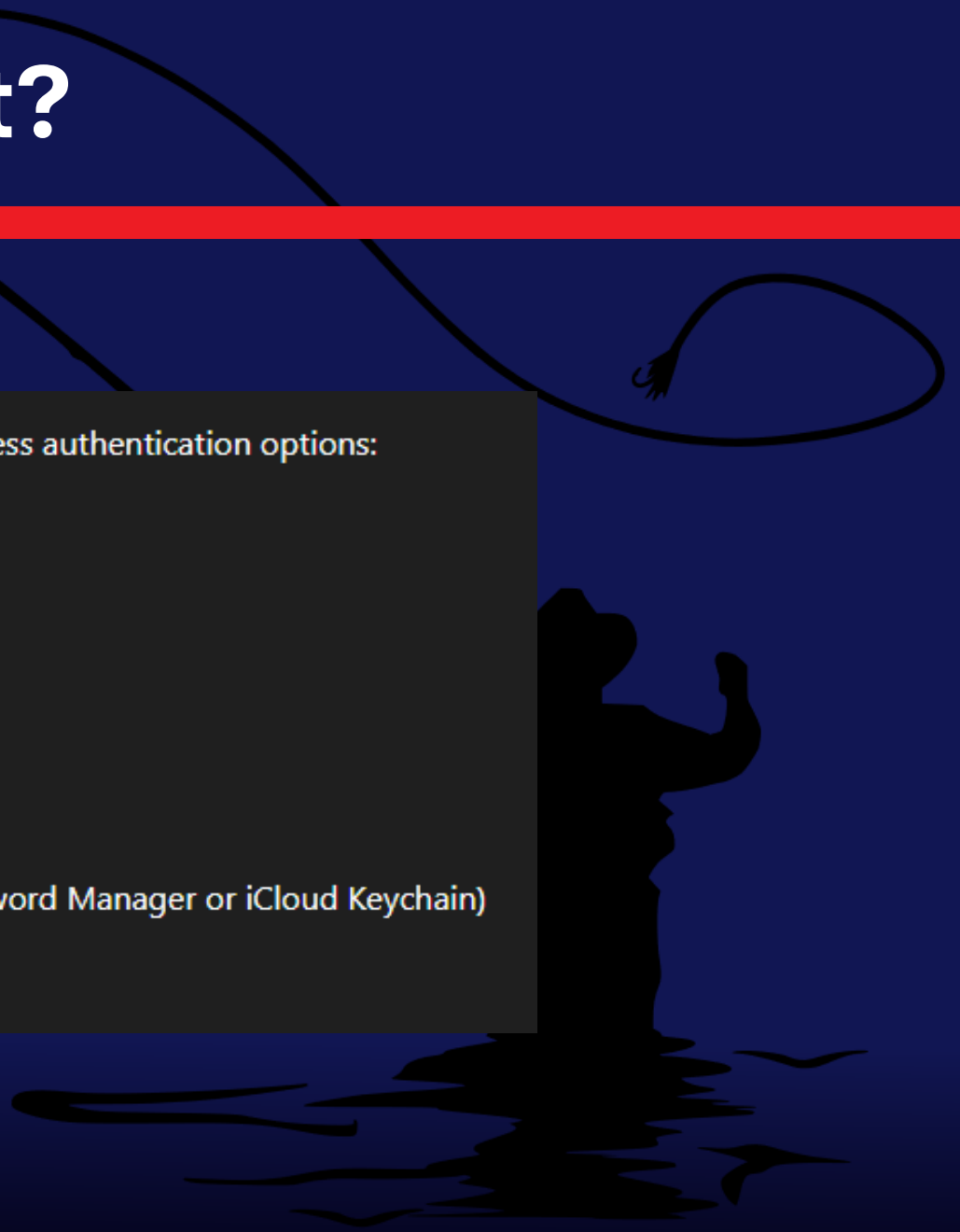
  - Windows Hello for Business cloud Kerberos trust deployment guide | Microsoft Learn

WHfB = Phishingresistant?

- Microsoft says YES!

Microsoft Entra ID offers the following phishing-resistant passwordless authentication options:

- Passkeys (FIDO2)
  - Windows Hello for Business
  - Microsoft Entra passkey on Windows (preview)
  - Platform credential for macOS (preview)
  - Entra Passkey on Windows
  - Microsoft Authenticator app passkeys
  - FIDO2 security keys
  - Synced passkeys (synced via providers such as Google Password Manager or iCloud Keychain)
- Certificate-based authentication/smart cards



WHfB = Phishingresistant!

But...

It's only **attack resistant** with enabled Enhanced Sign-In Security (ESS)!

ESS is a security mechanism in Windows that ensures that:

WHfB credentials may only be used if the Windows session system and the sign-in process are cryptographically bound to a trusted, unaltered system environment.

PIN & biometrics, device security and the use of the WHfB Key are tightly coupled to the protected Windows sign-in path.

WHfB = Phishingresistant + Attackresistant

Without ESS

- Key is secure, but
  - LogonUI
  - Credential Broker
  - User Session Context

are not bounded on cyptographical basis!

Attacker cannot extract the key, but may be able to manipulate the sign-in path.

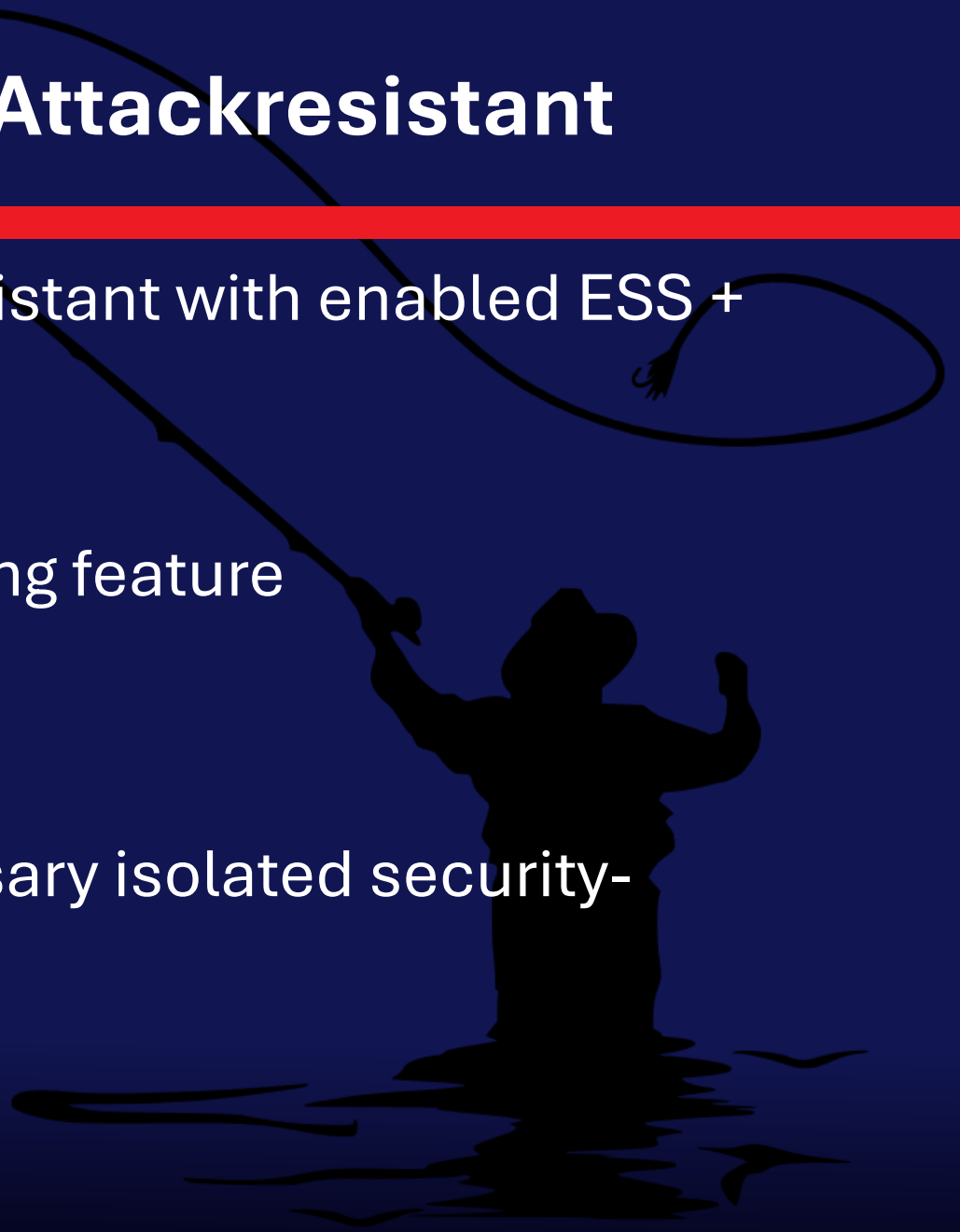
WHfB = Phishingresistant + Attackresistant

WHfB is phishingresistant AND Attack resistant with enabled ESS + Credential Guard!

Credential Guard is no additional hardening feature

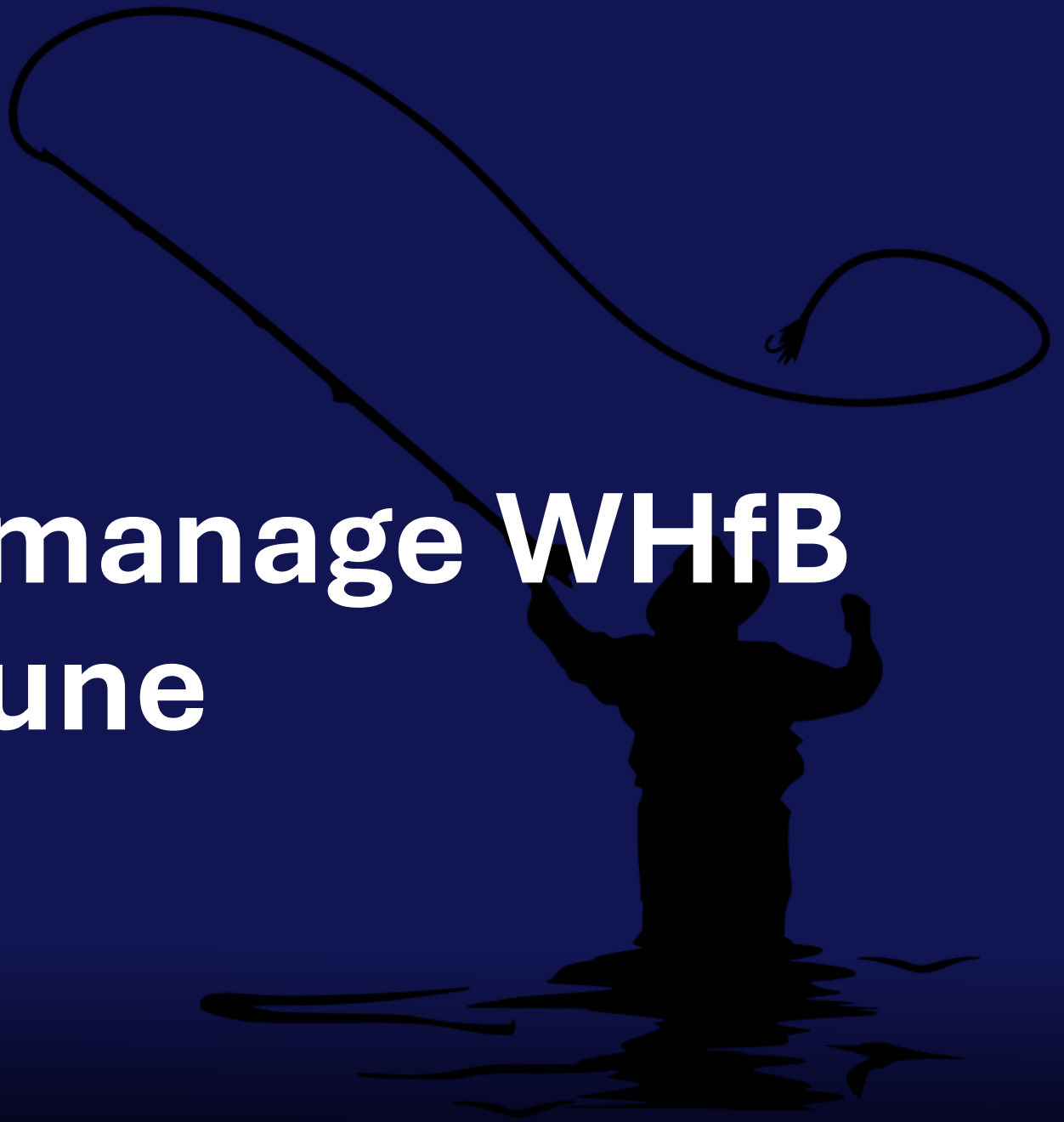
- It is a requirement for ESS!

The Credential Guard provides the necessary isolated security-context.



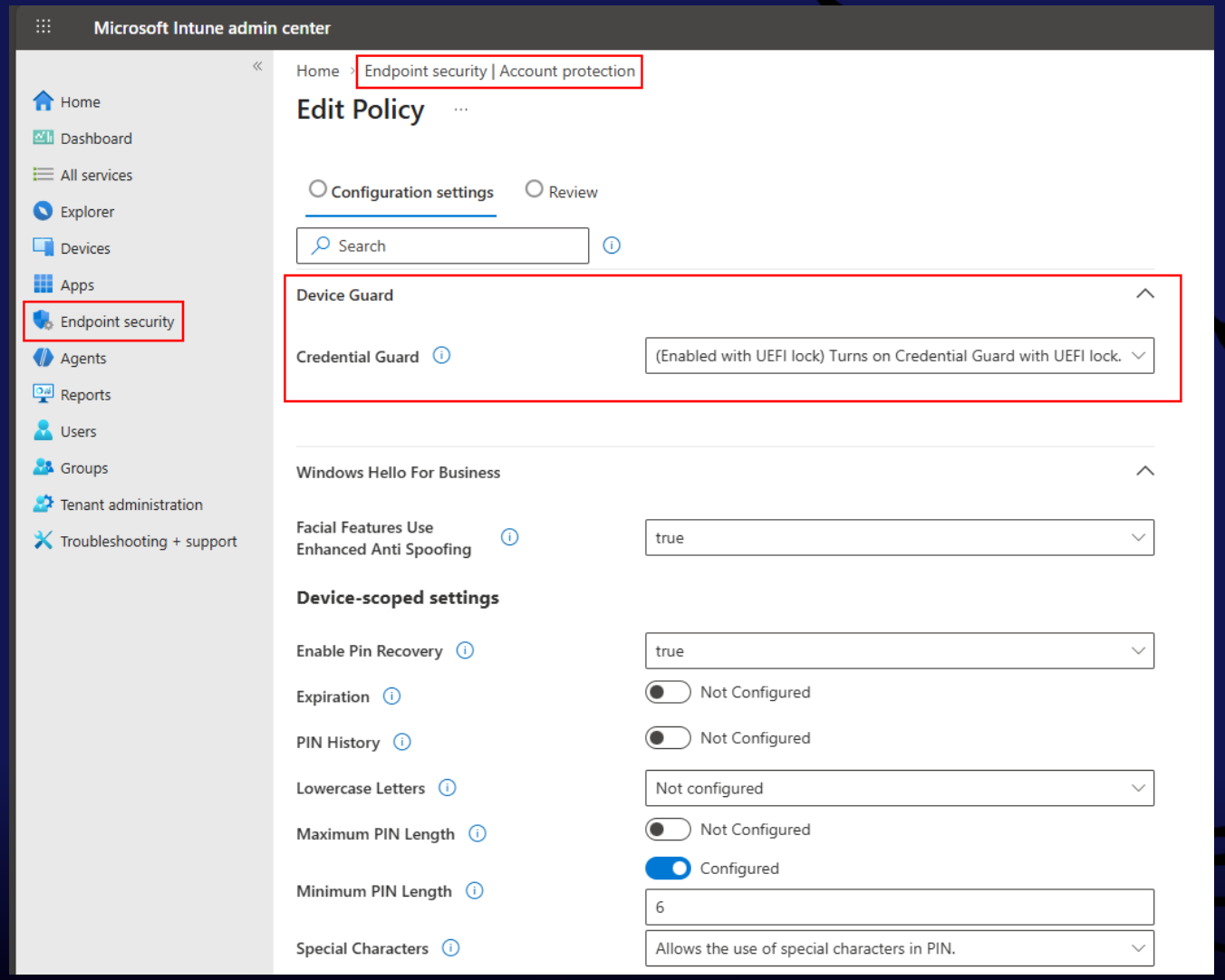
DEMO

How to manage WHfB with Intune

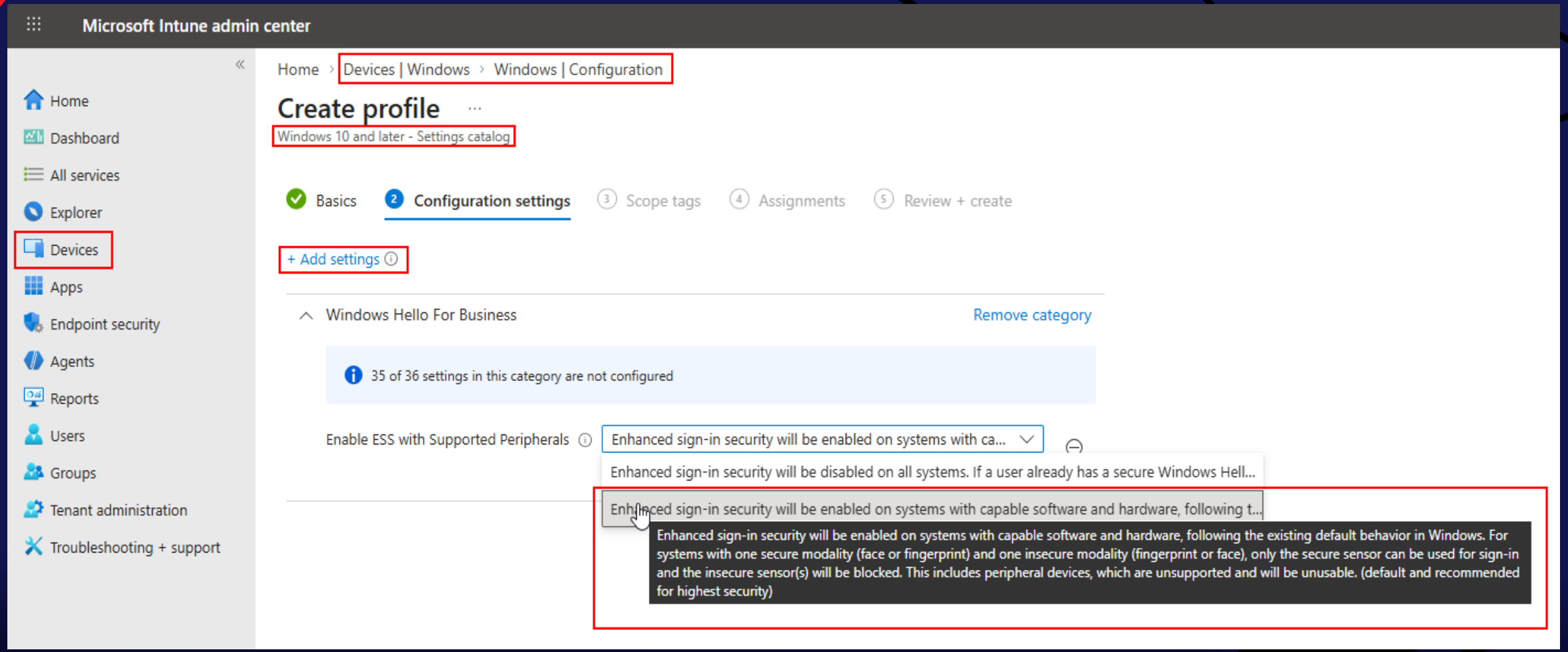


MMS

Enable Credential Guard



Enable ESS


Microsoft Intune admin center
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home › Devices | Windows › Windows | Configuration
Create profile
Windows 10 and later - Settings catalog
Basics
2 Configuration settings
3 Scope tags
4 Assignments
5 Review + create
+ Add settings
Windows Hello For Business
Remove category
35 of 36 settings in this category are not configured
Enable ESS with Supported Peripherals
Enhanced sign-in security will be enabled on systems with ca...
Enhanced sign-in security will be disabled on all systems. If a user already has a secure Windows Hell...
Enhanced sign-in security will be enabled on systems with capable software and hardware, following t...
Enhanced sign-in security will be enabled on systems with capable software and hardware, following the existing default behavior in Windows. For systems with one secure modality (face or fingerprint) and one insecure modality (fingerprint or face), only the secure sensor can be used for sign-in and the insecure sensor(s) will be blocked. This includes peripheral devices, which are unsupported and will be unusable. (default and recommended for highest security)

Contoso - Microsoft Entra admin | Contoso - Microsoft Intune admin

https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView/initialValue//tabId//recommendationResourceId//fromNav/Identity

InPrivate

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Copilot

admin@M365x4491345...
CONTOSO (M365X44913456.ON...

Home
Entra agents
Favorites
Entra ID
Overview
Users
Groups
Devices
Agent ID (Preview)
Enterprise apps
App registrations
Roles & admins
Delegated admin partners
Tenant governance (Preview)
Domain services
Conditional Access
Multifactor authentication
Identity Secure Score
Authentication methods
Account recovery (Preview)
Password reset

Home > Authentication methods | Bulk operation results (Preview) > Account Recovery (Preview) > Credentials > Settings > Overview > Security | Authentication methods

Contoso

Add | Manage tenants | What's new | Preview features | Got feedback?

To improve your experience, we're experimenting with your Home page. Click "Got feedback?" to tell us what you think.

Overview | Monitoring | Properties | Recommendations | Setup guides

Search your tenant

Basic information

Name	Contoso	Users	34
Tenant ID	2a5d0dd4-fea5-41fc-96f2-95f4978ea922	Groups	36
Primary domain	M365x44913456.onmicrosoft.com	Applications	6
License	Microsoft Entra ID P2	Devices	0

Alerts

Global Administrators
8
Microsoft recommends fewer than 5 Global Administrators.
View privileged role assignments

Migrate to the converged Authentication methods policy
Please migrate your authentication methods off the legacy MFA and SSPR policies by September 2025 to avoid any service impact
Learn more

My feed

MA
MOD Administrator
6b0885d3-29f6-48f7-a571-6794731c0b52
Global Administrator
View role information

Microsoft Entra Connect
Not enabled
Sync has never run

View Authentication Strength - Mi | Contoso - Microsoft Intune admin

https://intune.microsoft.com/#home

InPrivate

Microsoft Intune admin center

Copilot

admin@M365x4491345...
CONTOSO (M365X44913456.ON...

- Home
- Dashboard
- All services
- Explorer
- Devices
- Apps
- Endpoint security
- Agents
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Contoso

Update firewall configurations for new Intune network service endpoints. Learn more about Intune network service endpoints

Mehrfachgenehmigung durch Administratoren wird empfohlen. Schützen Sie sensible Aktionen mit zusätzlicher Genehmigung. Weitere Informationen zur Multi-Admin-Genehmigung

Erste Schritte

Securely manage devices, access, and apps with Intune

Maximize productivity and simplify administration without compromising endpoint management and security.

Status

Devices not in compliance
0

Connector errors
0

Configuration policies with errors or conflict
0

Service health
Healthy

Client app install failures
0

Account status
Active

Spotlight

Learn more about Intune Suite solutions

The unified solution includes Remote Help, Endpoint Privilege Management, AI-powered advanced analytics, and more.

Explore

Increase productivity with Cloud PCs

Easily provision Windows 365 Cloud PCs and manage them alongside your physical devices.

Explore

View Authentication Strength - Mi | Create a profile - Microsoft Intune

https://intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/DevicesWindowsMenu/~/configuration

InPrivate

Microsoft Intune admin center

Copilot

admin@M365x4491345...
CONTOSO (M365X44913456.ON...

Home > Devices | Windows > Windows

Windows | Configuration

Search

- Home
- Dashboard
- All services
- Explorer
- Devices
- Apps
- Endpoint security
- Agents
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

- Windows devices
- Monitor
- Device onboarding
  - Windows 365
  - Enrollment
- Manage devices
  - Configuration
  - Compliance
  - Scripts and remediations
  - Group Policy analytics
  - eSIM cellular profiles (preview)
- Manage updates
  - Windows updates
- Organize devices
  - Device clean-up rules
  - Assignment filters

Policies | Import ADMX

+ Create | Refresh | Export | Columns

Search | Add filters

Policy name	Platform	Policy type
Win10-DeviceConfig-Restrictions	Windows 10 and later	Device restriction

Add or remove favorites by pressing Ctrl+Shift+F

Create a profile

Platform

Select platform

Profile type

Select profile type

Create

Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Endpoint security | Account protection

Search
Overview
Overview
All devices
Security baselines
Security tasks
Manage
Antivirus
Disk encryption
Firewall
Endpoint Privilege Management
Endpoint detection and response
App Control for Business
Attack surface reduction
Account protection
Device compliance
Conditional access
Monitor
Assignment failures
Setup
Microsoft Defender for Endpoint
Help and support
Help and support

Add or remove favorites by pressing Ctrl+Shift+F

Create Policy | Refresh | Export

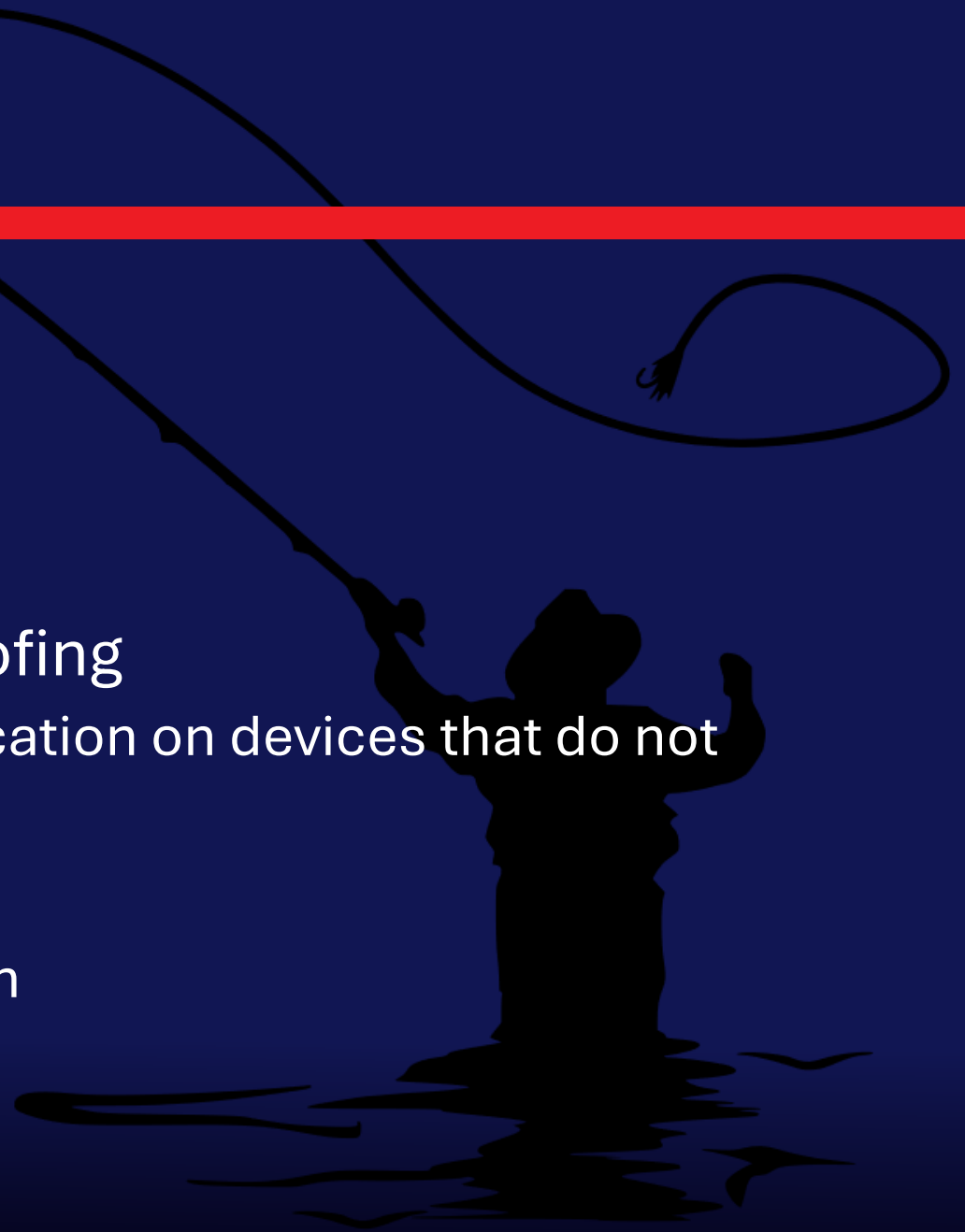
Search by profile name

Policy name	Policy type	Assigned	Platform	Target	Last modified
No results					

More learning bites

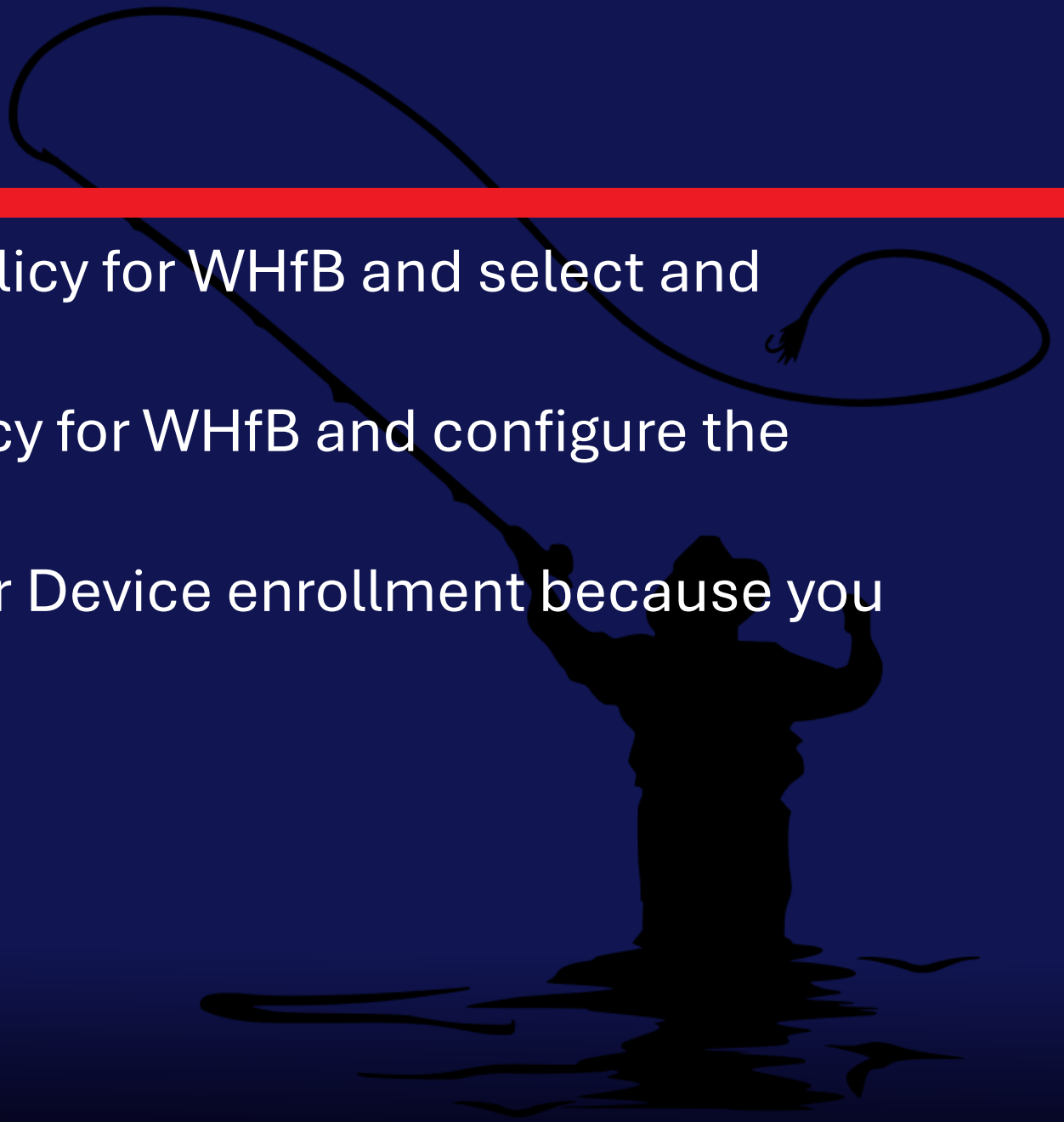
Configuration Musts!

- Credential Guard with UEFI lock
  - Security feature
  - Prerequisite for Enhanced Sign-In Security
- Enable ESS with supported Peripherals
- Facial Features Use Enhanced Anti Spoofing
  - This disables Windows Hello face authentication on devices that do not support enhanced anti-spoofing.
- Require Security Device
  - TPM becomes a must for this authentication
- PIN complexity settings



Best Practices

- Create a Device Configuration Policy for WHfB and select and configure your prefered settings
- Create a Account Protection Policy for WHfB and configure the settings you prefer
- Do not use the WHfB Policy under Device enrollment because you can not do exceptions

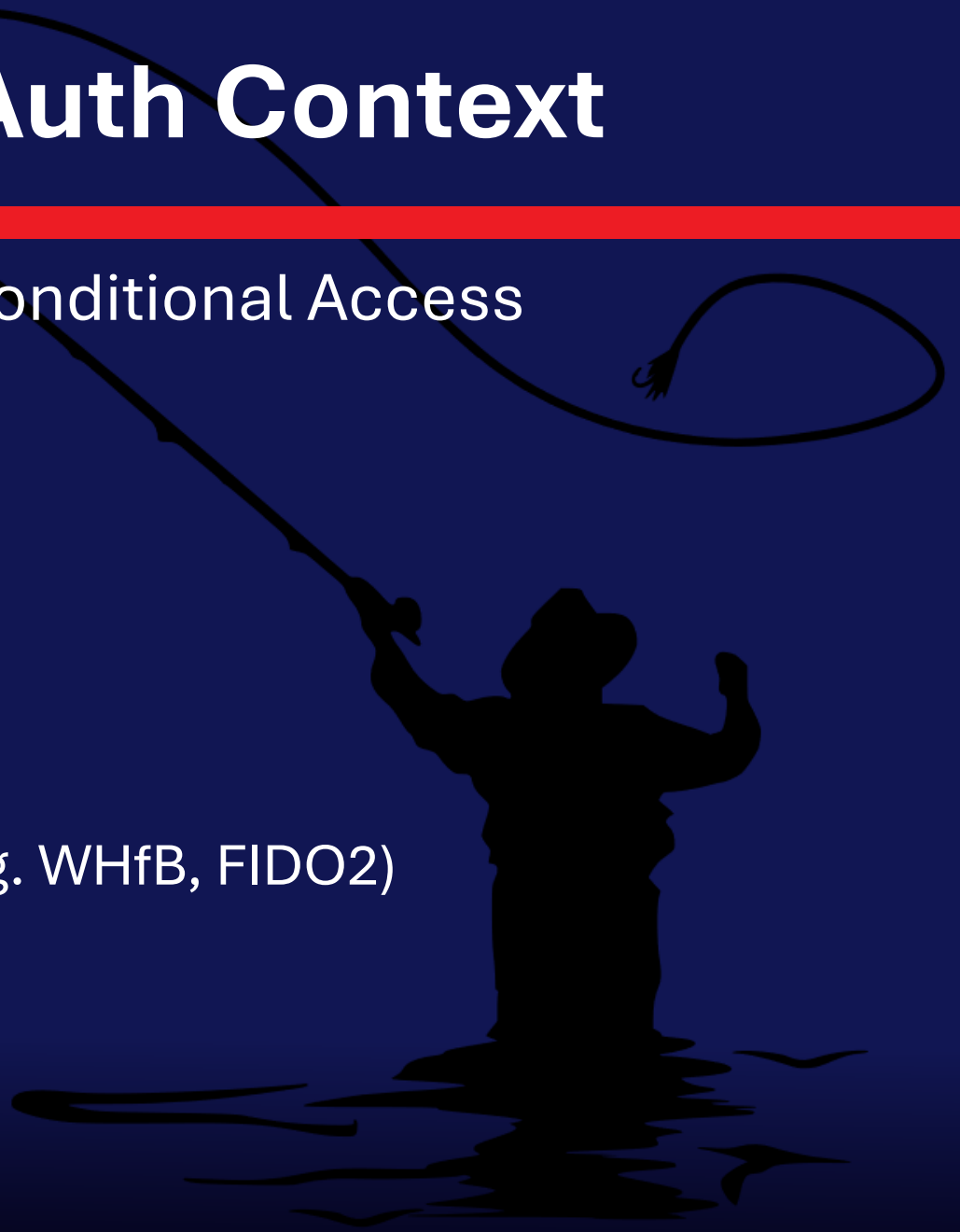


Putting the pieces together

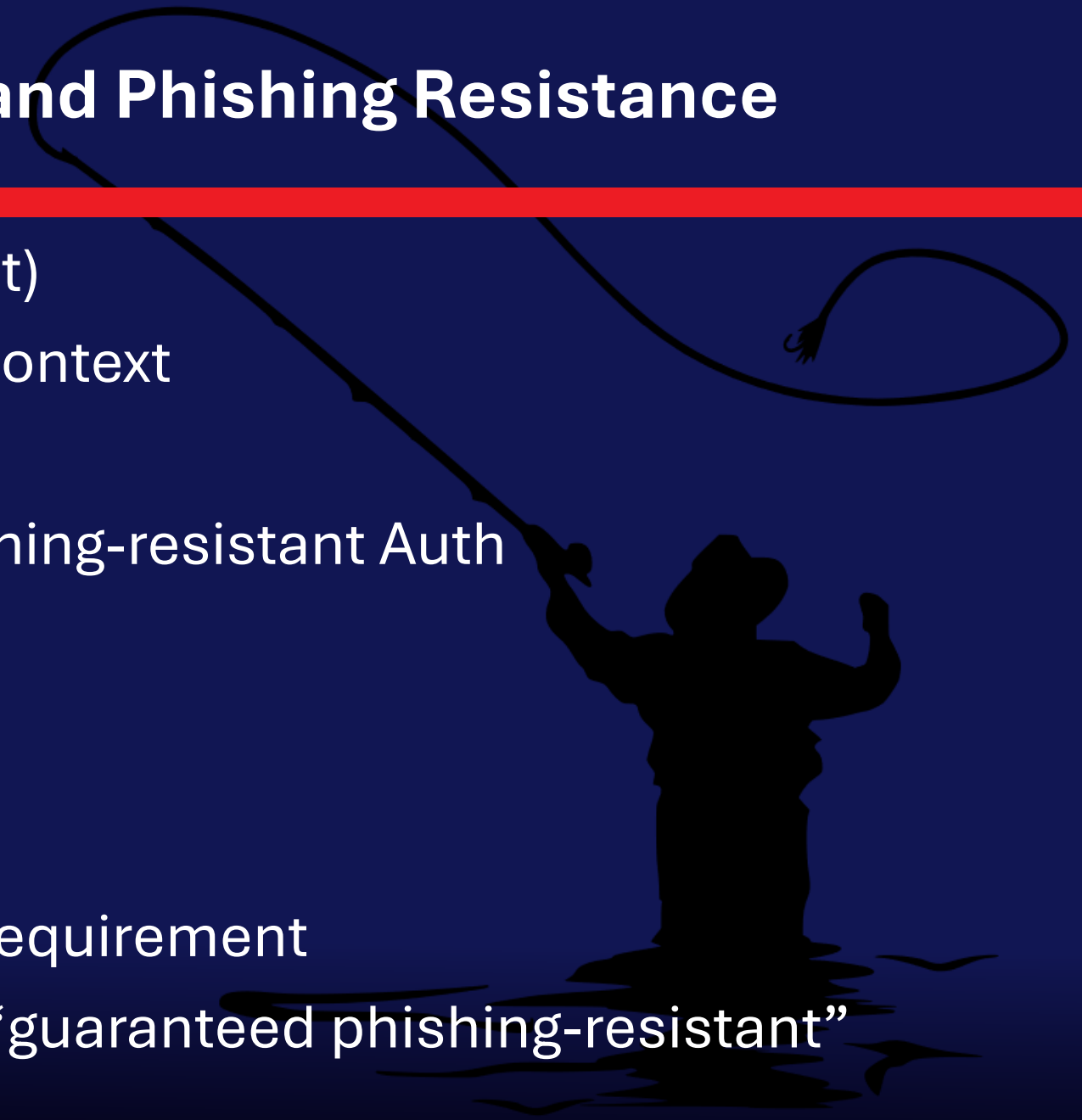
Conditional Access and Auth Context

- Phishing-resistant Auth is enforced by Conditional Access
  - Using Authentication Strength

- What do we get with CA + Auth Context
  - The app requests an authentication context
  - Conditional Access matches that context
  - CA enforces an Authentication Strength
  - Only specific auth methods are allowed (e.g. WHfB, FIDO2)



Why this matters for WHFB and Phishing Resistance



✅ Correct flow (phishing-resistant)

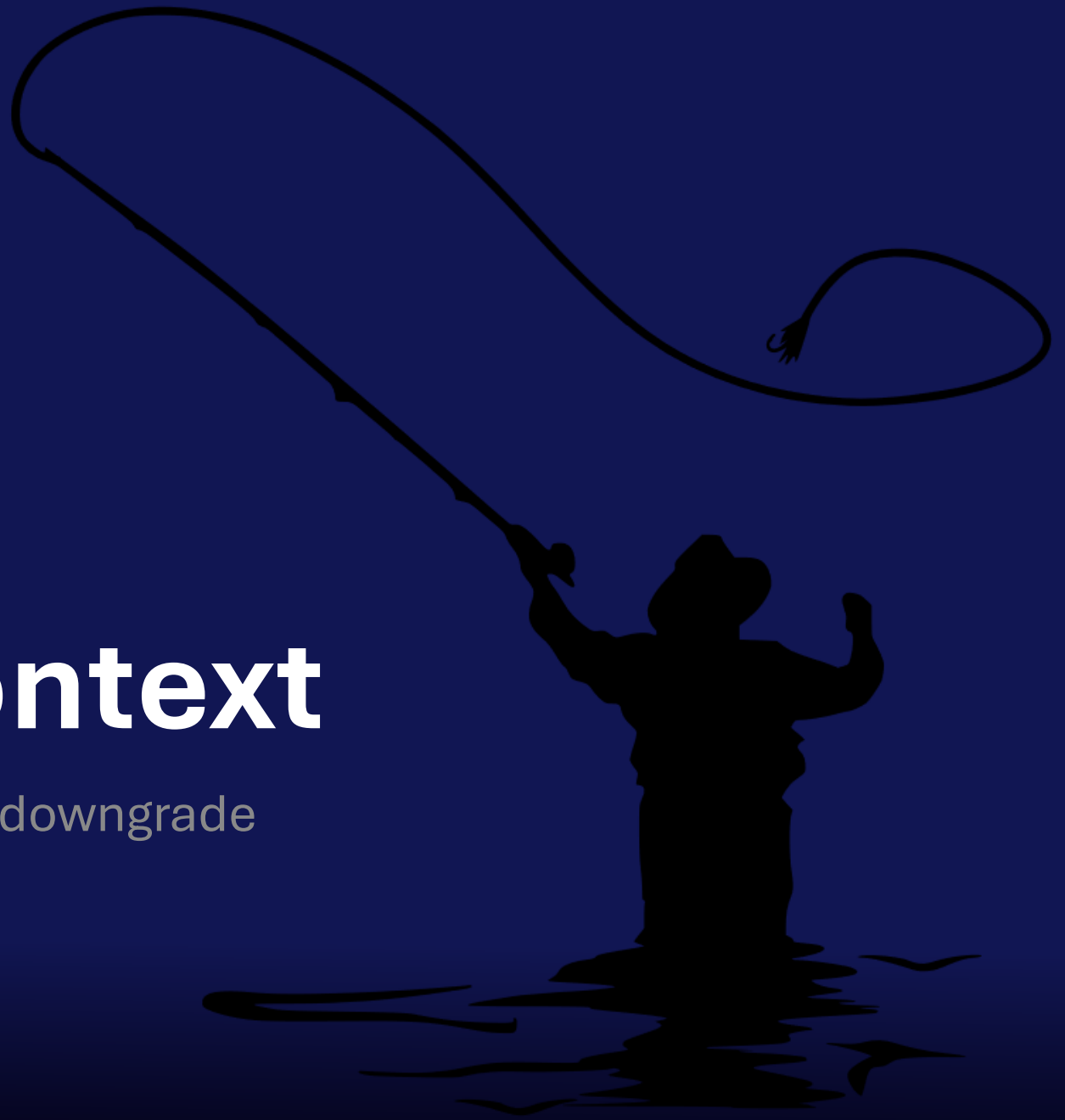
1. App requests Authentication Context
2. Conditional Access triggers
3. Authentication Strength = Phishing-resistant Auth
4. Allowed methods:
   - Windows Hello for Business
   - FIDO2
   - Hardware-bound certs
5. Passwords cannot satisfy the requirement

➡️ This is where WHfB becomes “guaranteed phishing-resistant”

DEMO

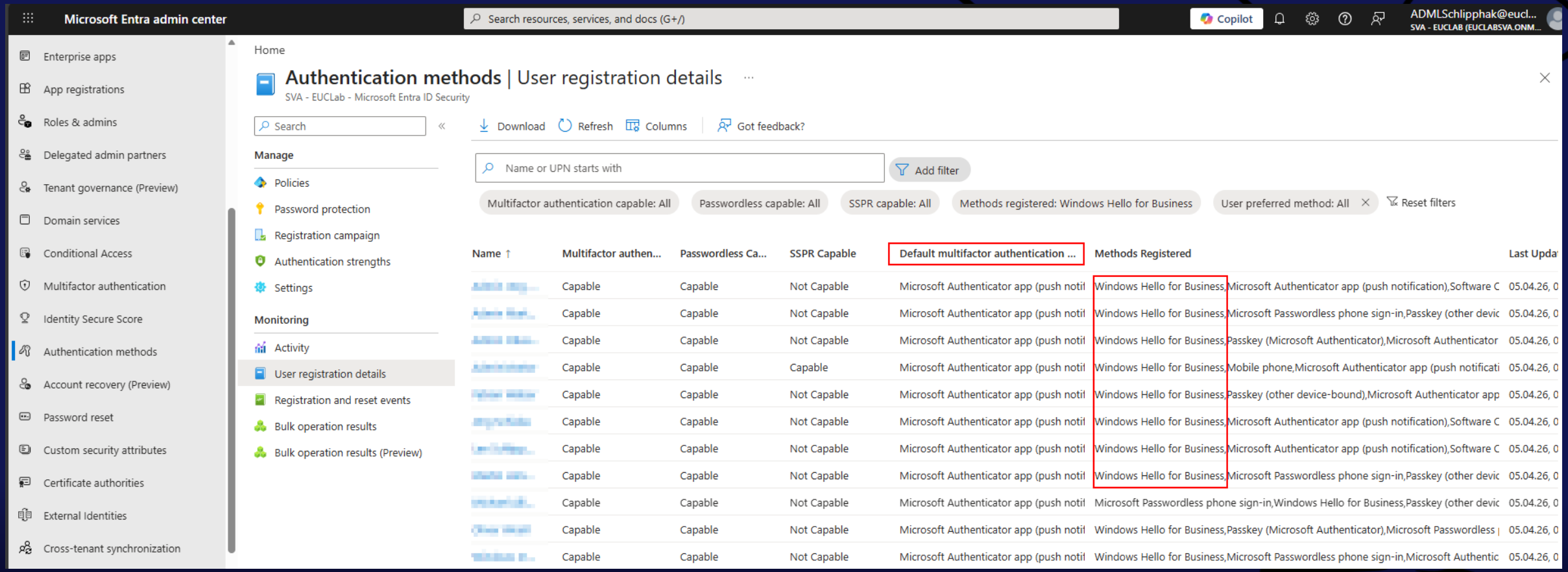
Auth Context

Protect against auth downgrade



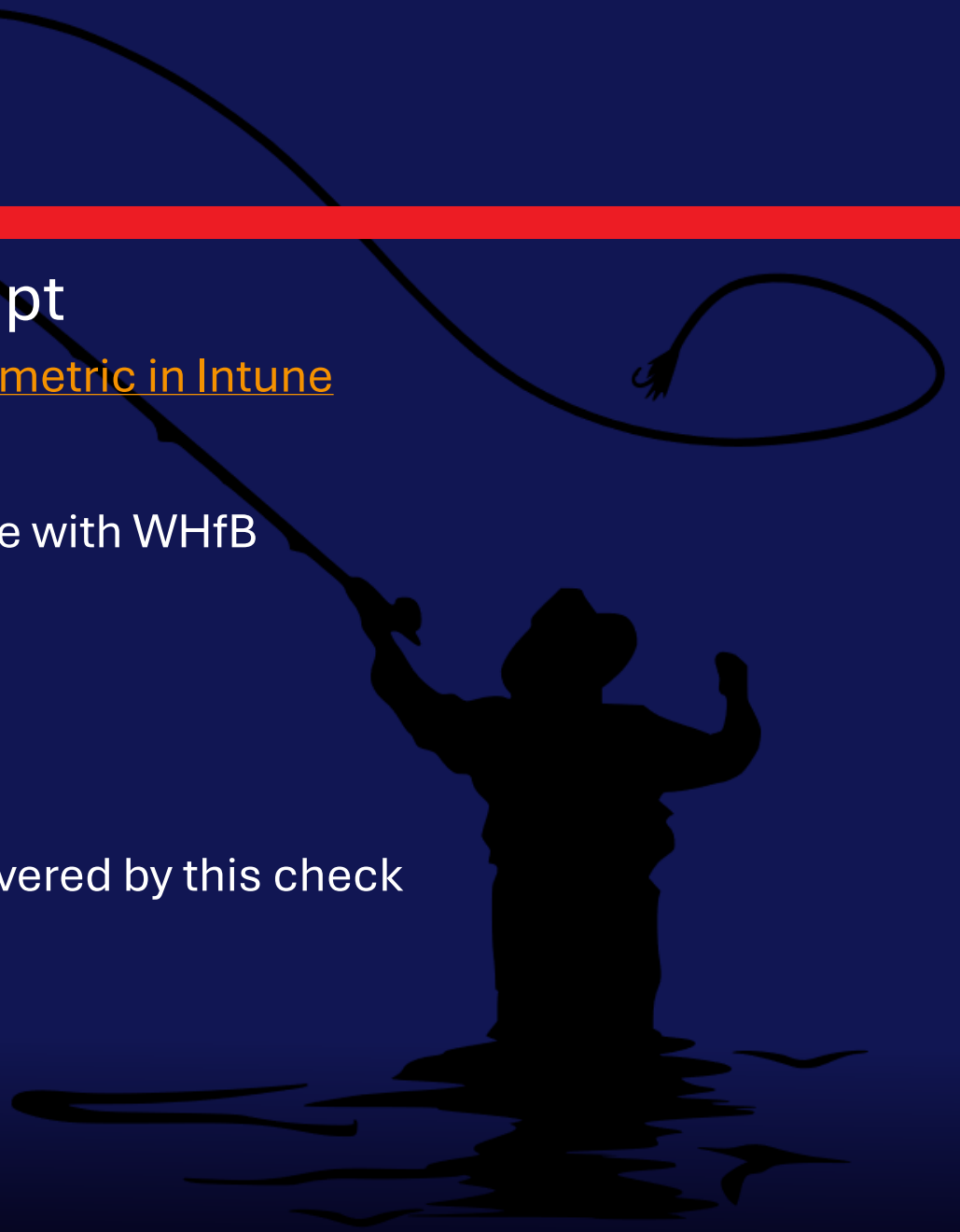
MMS

Reporting


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
ADMLSchlipphak@eucl...
SVA - EUCLAB (EUCLABSVA.ONM...
Enterprise apps
App registrations
Roles & admins
Delegated admin partners
Tenant governance (Preview)
Domain services
Conditional Access
Multifactor authentication
Identity Secure Score
Authentication methods
Account recovery (Preview)
Password reset
Custom security attributes
Certificate authorities
External Identities
Cross-tenant synchronization
Home
Authentication methods | User registration details
SVA - EUCLab - Microsoft Entra ID Security
Search
Manage
Policies
Password protection
Registration campaign
Authentication strengths
Settings
Monitoring
Activity
User registration details
Registration and reset events
Bulk operation results
Bulk operation results (Preview)
Download
Refresh
Columns
Got feedback?
Name or UPN starts with
Add filter
Multifactor authentication capable: All
Passwordless capable: All
SSPR capable: All
Methods registered: Windows Hello for Business
User preferred method: All
Reset filters
Name
Multifactor authen...
Passwordless Ca...
SSPR Capable
Default multifactor authentication ...
Methods Registered
Last Upda
Capable Capable Not Capable Microsoft Authenticator app (push notif Windows Hello for Business,Microsoft Authenticator app (push notification),Software C 05.04.26, 0
Capable Capable Not Capable Microsoft Authenticator app (push notif Windows Hello for Business,Microsoft Passwordless phone sign-in,Passkey (other devic 05.04.26, 0
Capable Capable Not Capable Microsoft Authenticator app (push notif Windows Hello for Business,Passkey (Microsoft Authenticator),Microsoft Authenticator 05.04.26, 0
Capable Capable Capable Microsoft Authenticator app (push notif Windows Hello for Business,Mobile phone,Microsoft Authenticator app (push notificati 05.04.26, 0
Capable Capable Not Capable Microsoft Authenticator app (push notif Windows Hello for Business,Passkey (other device-bound),Microsoft Authenticator app 05.04.26, 0
Capable Capable Not Capable Microsoft Authenticator app (push notif Windows Hello for Business,Microsoft Authenticator app (push notification),Software C 05.04.26, 0
Capable Capable Not Capable Microsoft Authenticator app (push notif Windows Hello for Business,Microsoft Authenticator app (push notification),Software C 05.04.26, 0
Capable Capable Not Capable Microsoft Authenticator app (push notif Windows Hello for Business,Microsoft Passwordless phone sign-in,Passkey (other devic 05.04.26, 0
Capable Capable Not Capable Microsoft Authenticator app (push notif Microsoft Passwordless phone sign-in,Windows Hello for Business,Passkey (other devic 05.04.26, 0
Capable Capable Not Capable Microsoft Authenticator app (push notif Windows Hello for Business,Passkey (Microsoft Authenticator),Microsoft Passwordless 05.04.26, 0
Capable Capable Not Capable Microsoft Authenticator app (push notif Windows Hello for Business,Microsoft Passwordless phone sign-in,Microsoft Authentic 05.04.26, 0

Report for preparation

- Check prerequisites via remediation script
  - Generate a Report for Devices capable of WHFB/Biometric in Intune
- Dsregcmd /Status
  - Helps identify if the device is mandatorily compatible with WHfB
    - AzureADJoined/ DomainJoined
    - TPM
    - NgcPrerequisites
    - DeviceAuthStatus
    - AzureAdPrt
  - User prerequisites and biometric sensors are not covered by this check



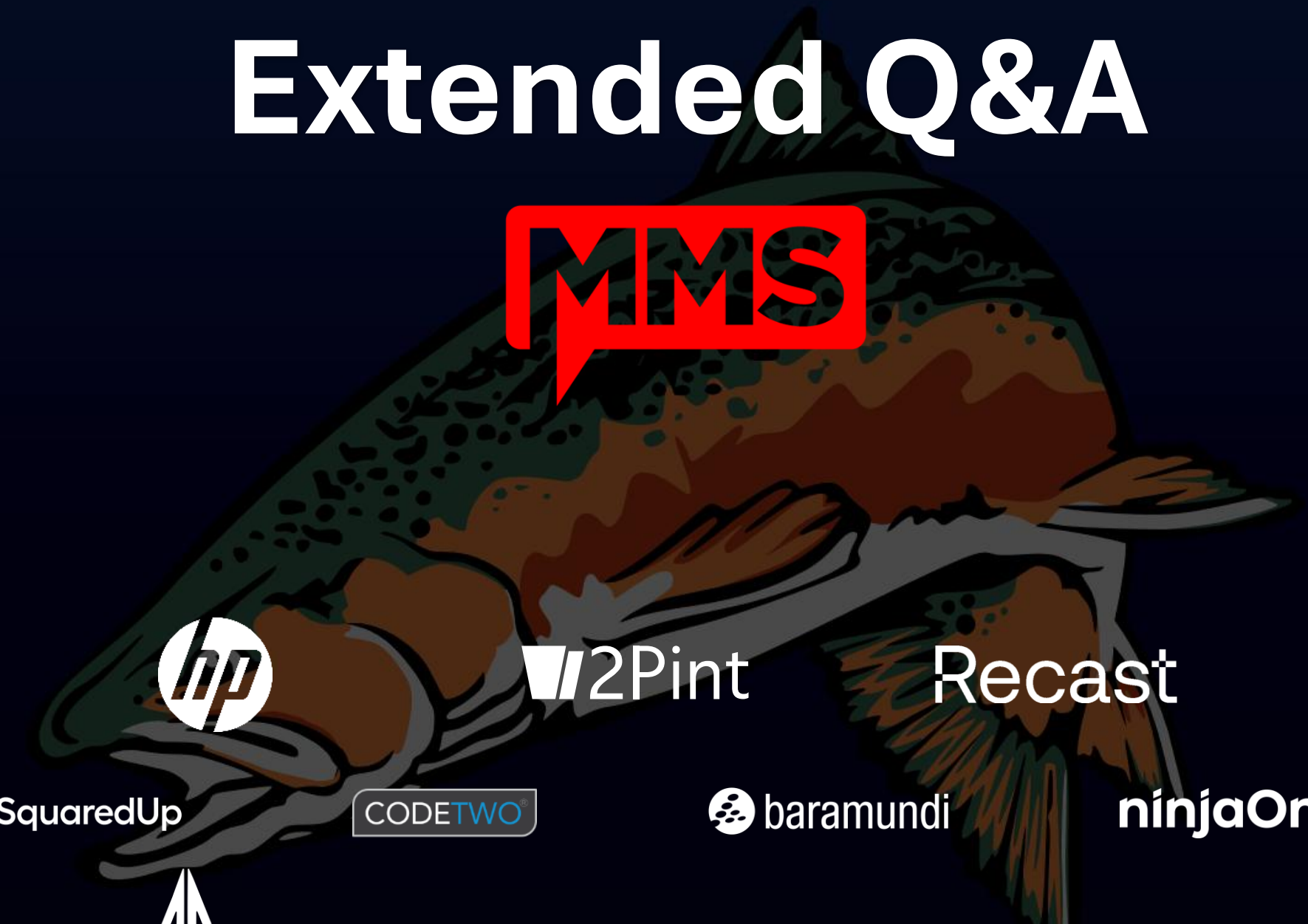
SAVE THE DATES

Oct 25-28, 2026

May 2-6, 2027

Oct 10-13, 2027

Extended Q&A



MMS

PATCH MY PC

hp

2Pint

Recast

robopack
empowered by SOFTWARE CENTRAL

SquaredUp

CODETWO

baramundi

ninjaOne

Rimo3

App Control

TeamViewer

numecent

aiden