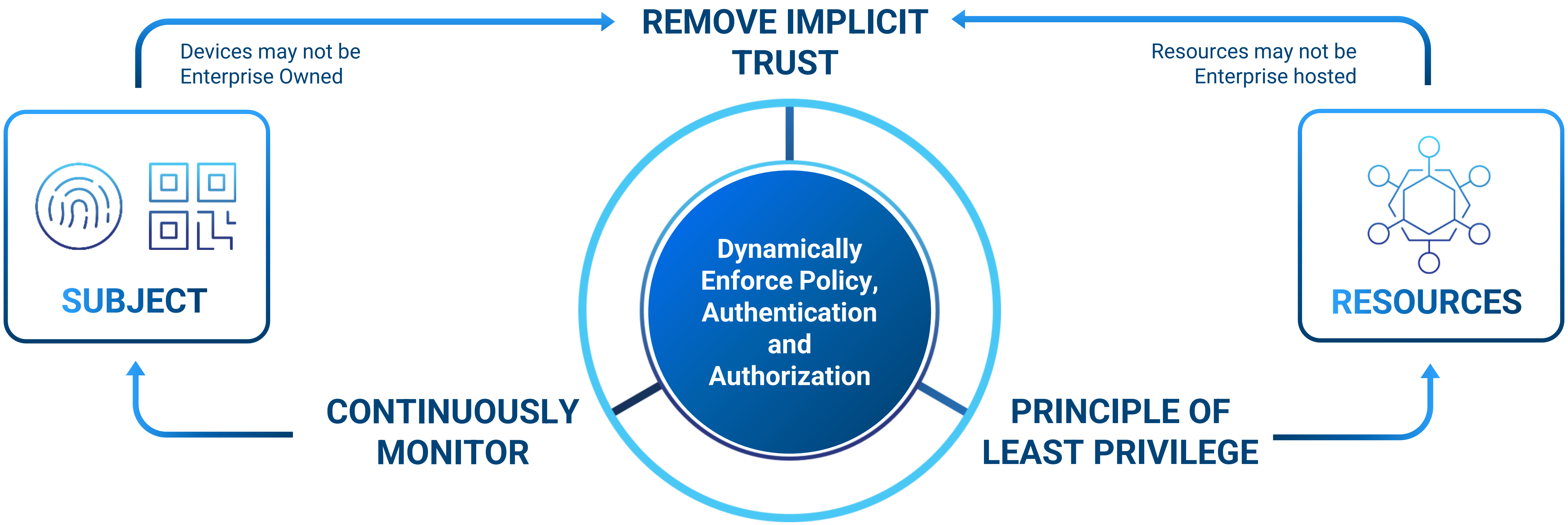
CYBERARK®

# Role of Identity Security in Zero Trust Model

Bartosz Kryński

Solutions Engineering Team Leader, CISSP

# Zero Trust Overview: *Adopt an Assume Breach Mindset*



REMOVE IMPLICIT TRUST

Devices may not be Enterprise Owned

Resources may not be Enterprise hosted

SUBJECT

RESOURCES

Dynamically Enforce Policy, Authentication and Authorization

CONTINUOUSLY MONITOR

PRINCIPLE OF LEAST PRIVILEGE

IDENTITY | DEVICES | NETWORK / ENVIRONMENT | APPLICATION WORKLOAD | DATA

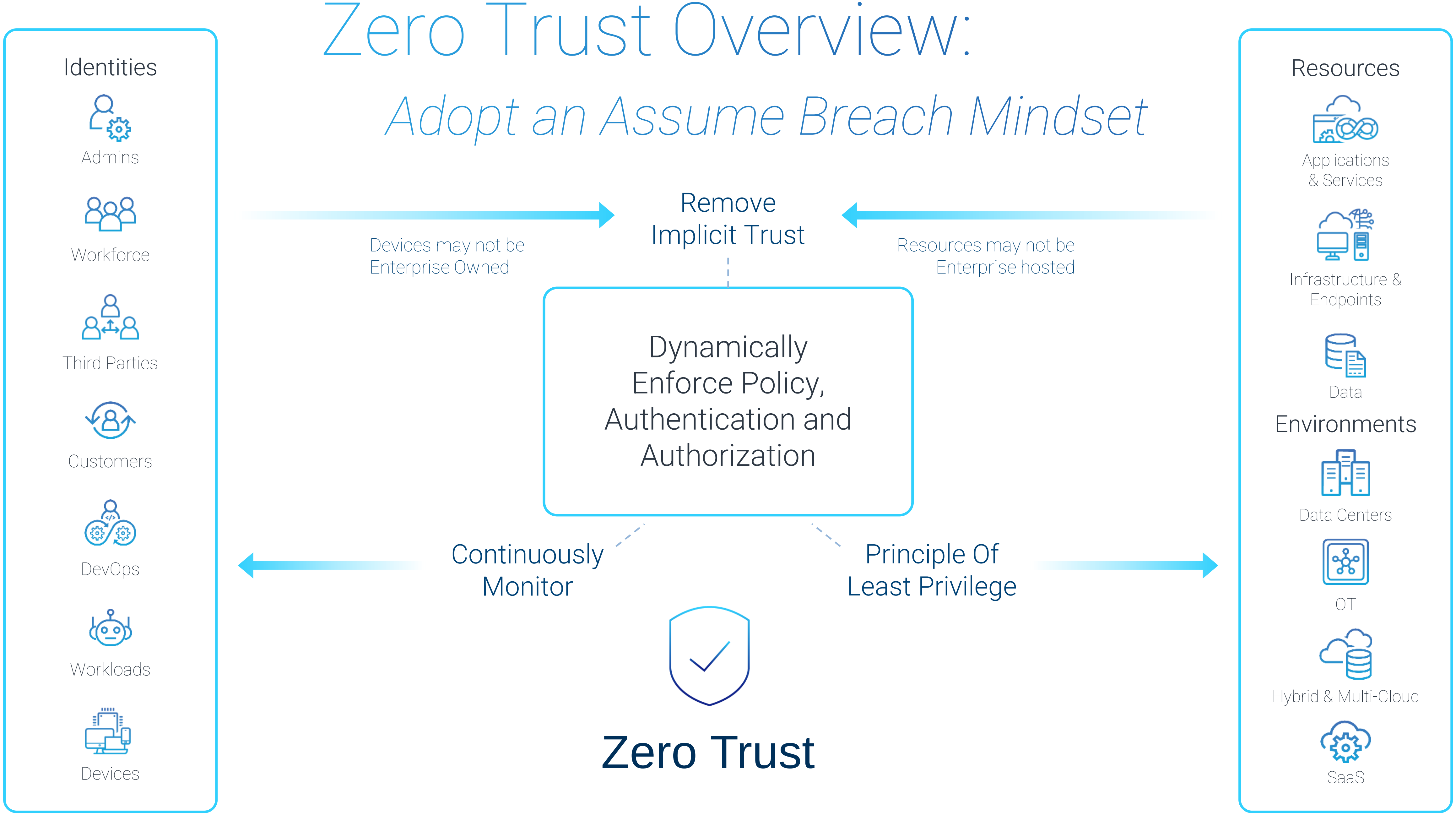
IMPLEMENTATION PILLARS

https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

# Zero Trust Overview:

## *Adopt an Assume Breach Mindset*



Identities

Admins

Workforce

Third Parties

Customers

DevOps

Workloads

Devices

Remove Implicit Trust

Devices may not be Enterprise Owned

Resources may not be Enterprise hosted

Dynamically Enforce Policy, Authentication and Authorization

Continuously Monitor

Principle Of Least Privilege

Zero Trust

Resources

Applications & Services

Infrastructure & Endpoints

Data

Environments

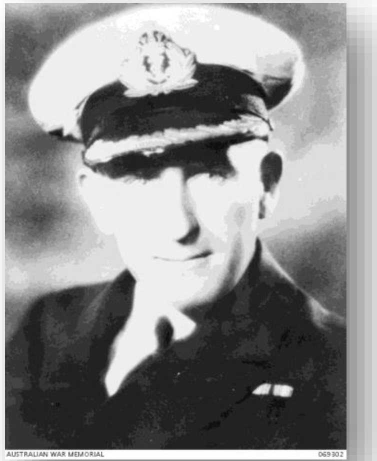
Data Centers

OT

Hybrid & Multi-Cloud

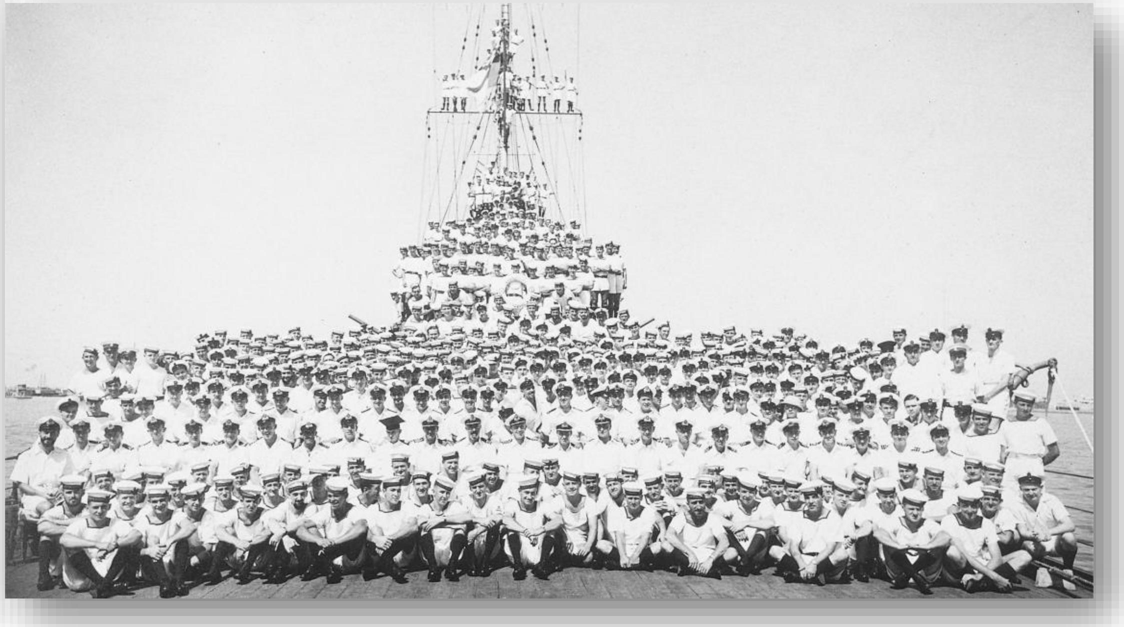
SaaS

# The Story of HMAS Sydney



HMAS Sydney
(Her Majesty Australian Ship)
The Royal Australian Navy

- Launch 1934
- Participated in the Italy-Ethiopia war 1935
- World War II – part of the British Fleet 1939 – 1941
- February 1941 – return to Australian water
- November 1941 - **lost**



# The Battle between HMAS Sydney and HSK Kormoran

## NO TRACE OF H.M.A.S. SYDNEY AFTER SINKING RAIDER

### No Survivors Located

CANBERRA, Sunday.—H.M.A.S. Sydney, pride of the Royal Australian Navy, is missing after an engagement with a heavily-armed enemy merchant raider.

No survivors from the cruiser's complement of 645 officers and ratings have been located.

This news was released to-night by the Prime Minister (Mr. Curtin) after consultation with the Australian Naval Board: "The Government regrets to say that it must be presumed that the Sydney has been lost," said Mr. Curtin. "The Sydney disappeared after a successful action with a raider, which she sank by gunfire."

First news of the action was given by survivors from the enemy vessel who had been picked up. Mr. Curtin gave an assurance that an extensive search was being made by air and surface units for survivors of the Sydney.

The location of the action has not been disclosed, but an official statement on the war record of the Sydney makes the disclosure that the cruiser, after returning from the Mediterranean, "remained on duty on the Australia station."

The action took place a few days ago, but the Government withheld the announcement until to-night, mainly for reasons of strategy.

No details of the fight between the Sydney and the heavily-armed raider are yet available.

Mr. Curtin revealed that no communication had been received from the Sydney. After days of waiting for a wireless message from the cruiser, naval authorities have been obliged to presume that she has been lost.

Naval authorities informed next-of-kin of the Sydney's complement last Wednesday. This provoked a flood of speculation, and newspaper offices and Government officials have been inundated with demands for information.

Explaining the decision to withhold official information, Mr. Curtin said to-night that "for strategical reasons, including the safety of other

received, and were appreciative of the cooperation of the Press in withholding publication.

"While regretting the loss of a fine ship and her gallant complement," said Mr. Curtin, "the people of Australia will be proud that she and they upheld the traditions of the Royal Australian Navy and completed a glorious career in a successful action against the enemy."

### May Replace Sydney

SYDNEY, Sunday.—Commenting on the sinking of H.M.A.S. Sydney, the Lord Mayor of Sydney (Ald. Crick) said to-night that he regarded the sinking as the real tragedy of this war.

"There is a suggestion afoot that we replace the Sydney," he added. "We may be able to replace its personnel, and if I, as Lord Mayor of

### November: 1914-1941

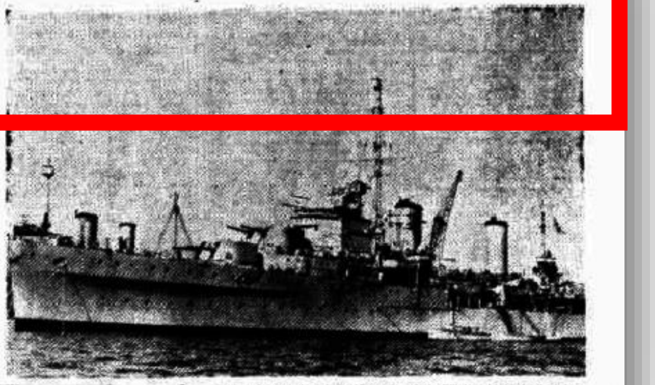
IT WAS 27 years to the month since the illustrious Sydney—from which the new Sydney took her name—destroyed the German raider Emden.

On November 10, 1914, the Admiralty officially announced the capture and destruction of the cruiser Emden at Keeling (Cocos) Islands, in the Indian Ocean, by the Sydney.

### *Was Our Fifth Biggest Warship*

H.M.A.S. SYDNEY was the fifth biggest ship in the Royal Australian Navy. Of the modified Leander class—the same as H.M.A.S. Hobart and H.M.A.S. Perth—the Sydney had a displacement of 6830 tons.

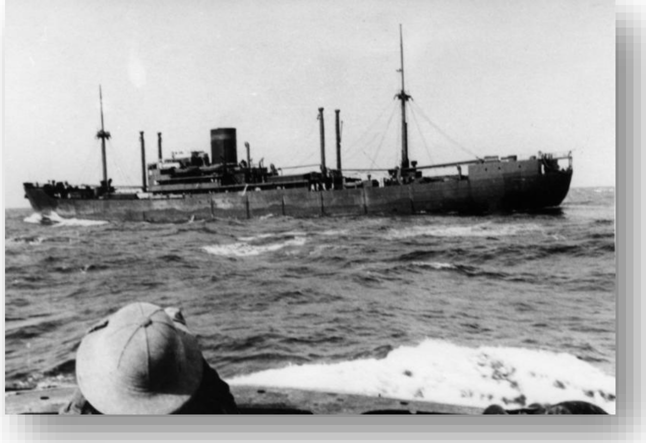
The personnel of the Sydney was made up as follows—Officers, 41; ratings, 594; R.A.A.F. officer, 1; R.A.A.F. ratings, 7; canteen personnel, 4.



This photograph of H.M.A.S. Sydney was taken when the cruiser returned to Sydney early this year.

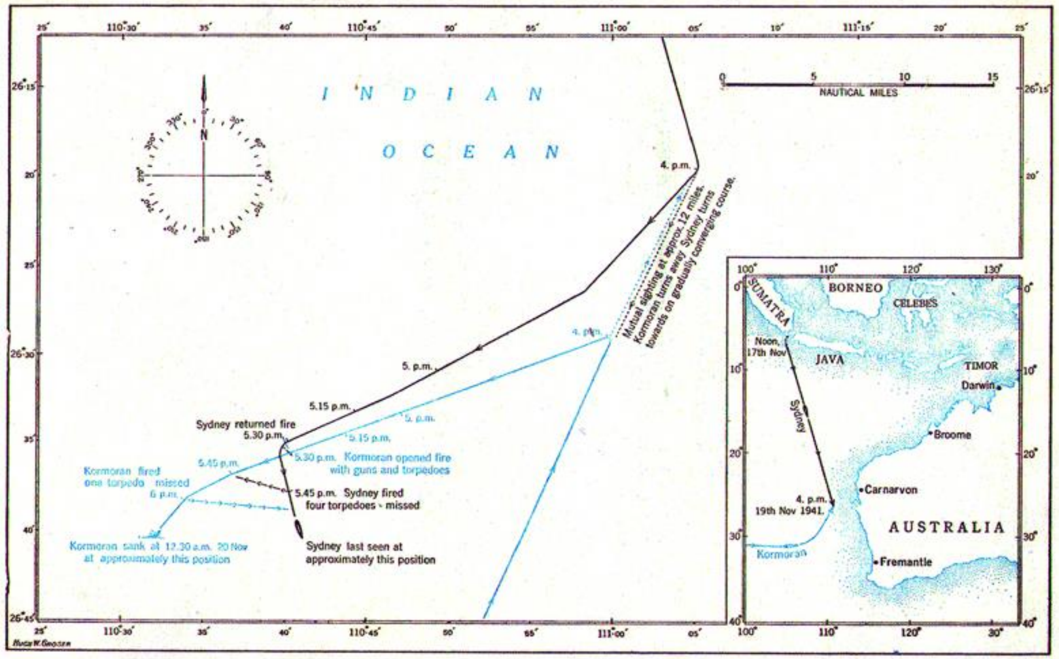
CAPTAIN JOSEPH BURNETT, Commanding Officer of the Sydney.

(Illustration)



HSK Kormoran

(German Auxiliary Cruiser - Kriegsmarine merchant raider)



INDIAN OCEAN
N
110°30′
35′
40′
110°45′
50′
55′
111°00′
05′
10′
111°15′
20′
25′
26°15′
20′
25′
26°30′
35′
40′
26°45′
0
5
10
15
NAUTICAL MILES
4. p.m.
Mutual sighting at approx. 12 miles. Kormoran turns away Sydney turns towards on gradually converging course.
4. p.m.
5. p.m.
5.15 p.m.
Sydney returned fire 5.30 p.m.
5. p.m.
5.15 p.m.
5.30 p.m. Kormoran opened fire with guns and torpedoes
5.45 p.m.
Kormoran fired one torpedo missed 6 p.m.
5.45 p.m. Sydney fired four torpedoes - missed
Kormoran sank at 12.30 a.m. 20 Nov at approximately this position
Sydney last seen at approximately this position
100°
110°
120°
130°
0°
10°
20°
30°
40°
SUMATRA
BORNEO
CELEBES
JAVA
TIMOR
Darwin
Broome
Carnarvon
AUSTRALIA
Fremantle
Noon, 17th Nov
Sydney
4. p.m. 19th Nov 1941.
Kormoran
Hugh W. Gibson

*Sydney-Kormoran* Action

HMAS Sydney

(Her Majesty Australian Ship)

The Royal Australian Navy

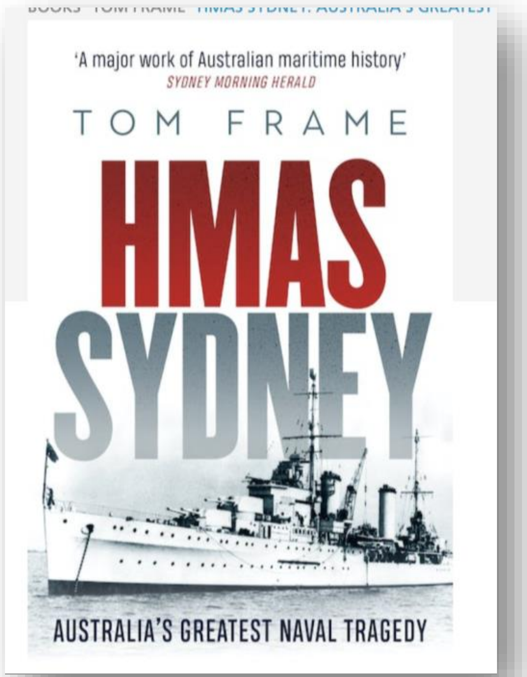
Captain **Joseph Burnett**

(26 December 1899 – 19 November 1941)

Captain Theodor Detmers

Source: Australian War Memorial by G. Hermonm Gill

# The Aftermath


BOOKS TOM FRAME HMAS SYDNEY: AUSTRALIA'S GREATEST

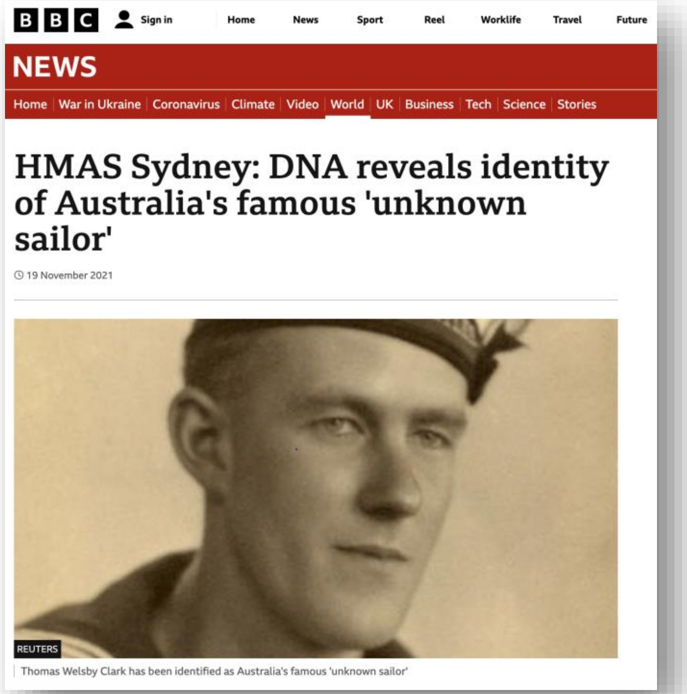
'A major work of Australian maritime history'
SYDNEY MORNING HERALD

TOM FRAME

HMAS SYDNEY

AUSTRALIA'S GREATEST NAVAL TRAGEDY

HMAS Sydney Wreck
(C) 2010 by Thomas Schmid, 3DHistory.de

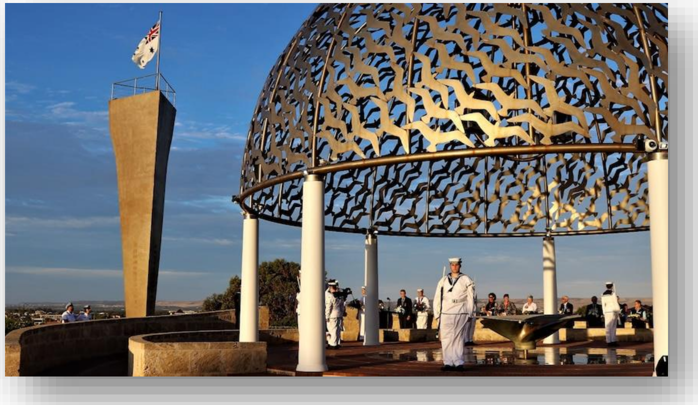

BBC
Sign in
Home
News
Sport
Reel
Worklife
Travel
Future
NEWS
Home | War in Ukraine | Coronavirus | Climate | Video | World | UK | Business | Tech | Science | Stories
REUTERS

## HMAS Sydney: DNA reveals identity of Australia's famous 'unknown sailor'

19 November 2021

Thomas Welsby Clark has been identified as Australia's famous 'unknown sailor'

645 Australian sailors went missing on 1941, wreckage has been found on 2008, only one body has been identified in 2007



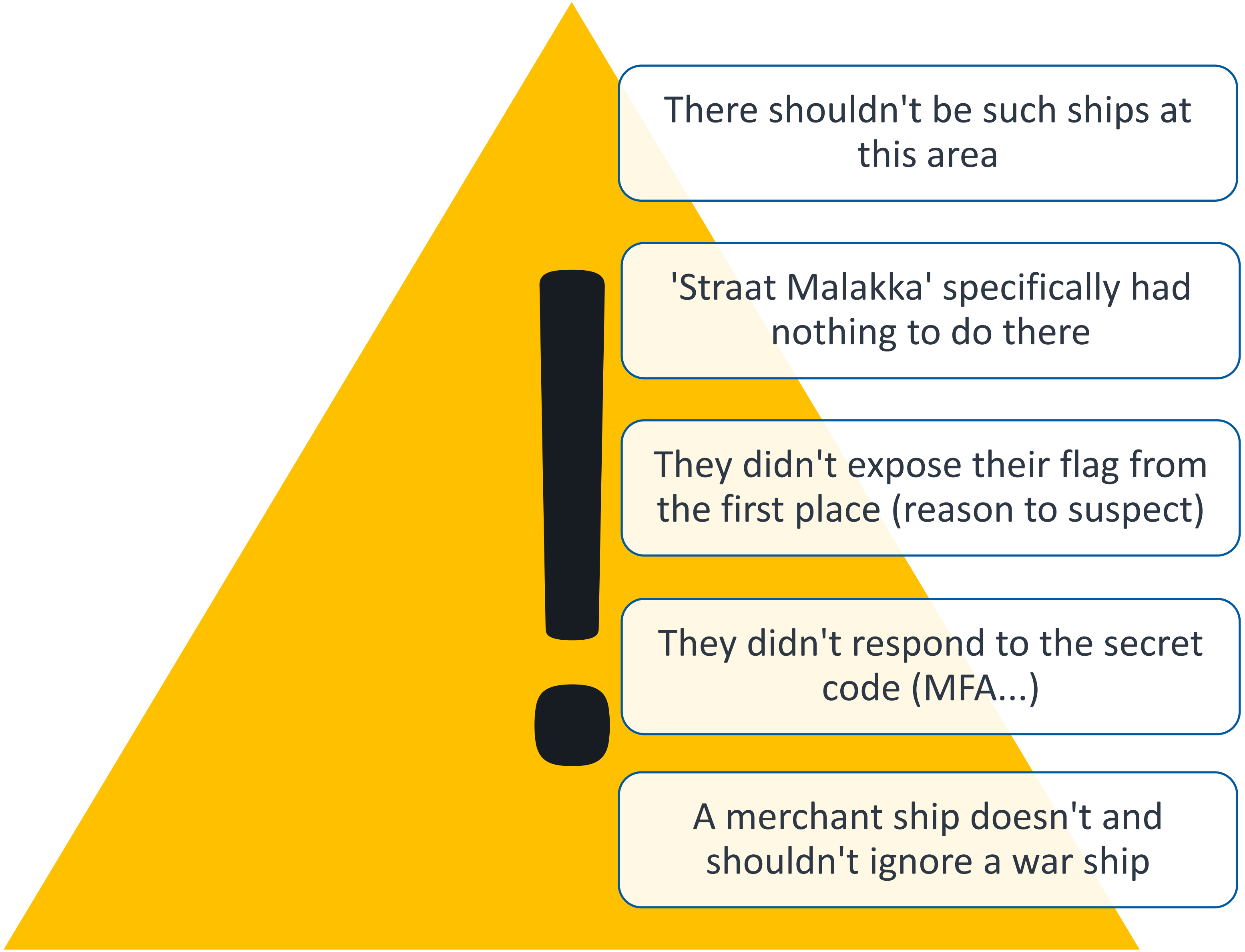
# What went wrong?

These were **NOT** implemented:

ZERO TRUST

IAAAA

(Identity Authentication, Authorization, Auditing, and Accounting)



There shouldn't be such ships at this area

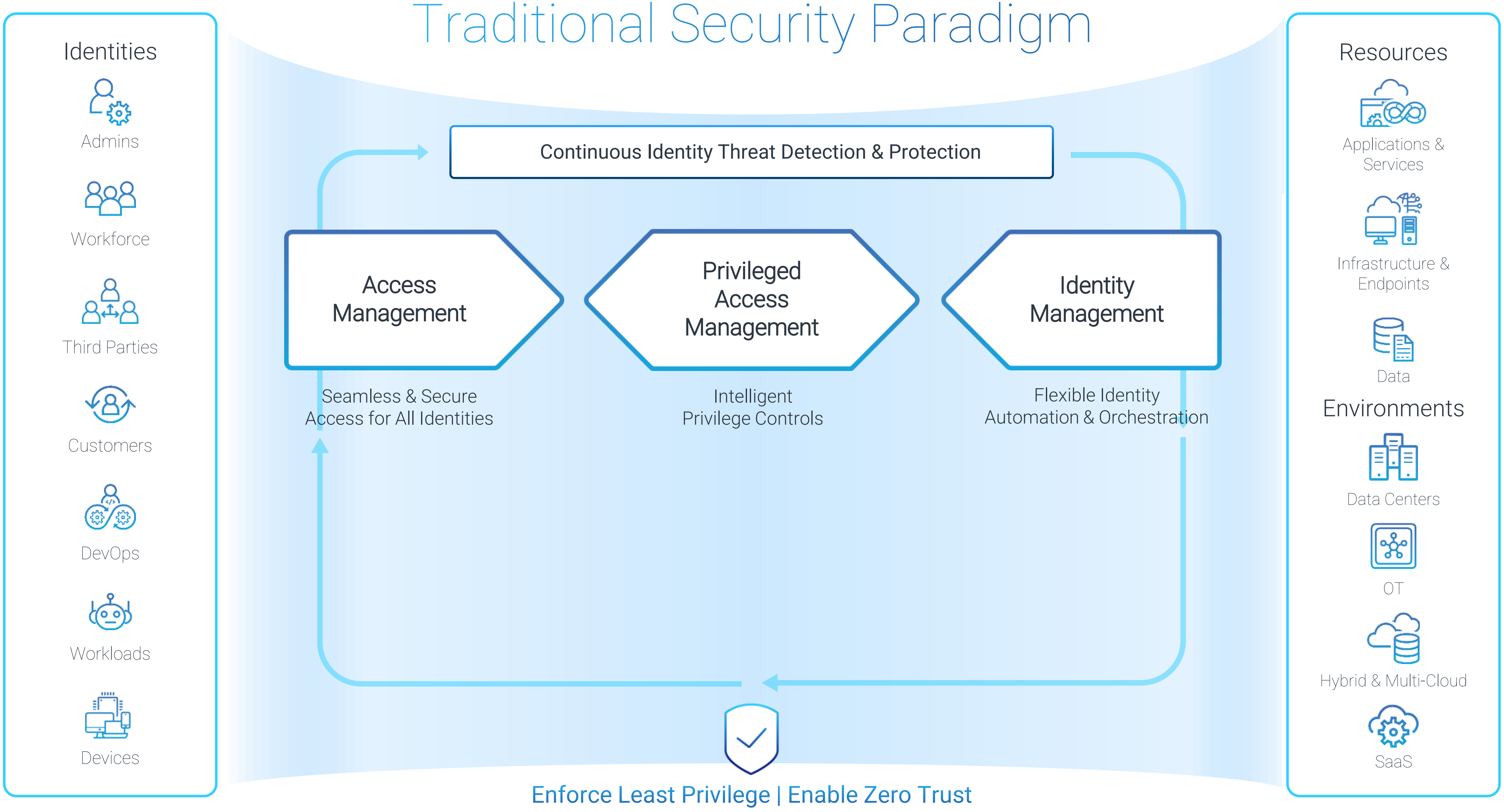
'Straat Malakka' specifically had nothing to do there

They didn't expose their flag from the first place (reason to suspect)

They didn't respond to the secret code (MFA...)

A merchant ship doesn't and shouldn't ignore a war ship

# Traditional Security Paradigm



Identities

Admins

Workforce

Third Parties

Customers

DevOps

Workloads

Devices

Continuous Identity Threat Detection & Protection

Access Management

Seamless & Secure Access for All Identities

Privileged Access Management

Intelligent Privilege Controls

Identity Management

Flexible Identity Automation & Orchestration

Enforce Least Privilege | Enable Zero Trust

Resources

Applications & Services

Infrastructure & Endpoints

Data

Environments

Data Centers

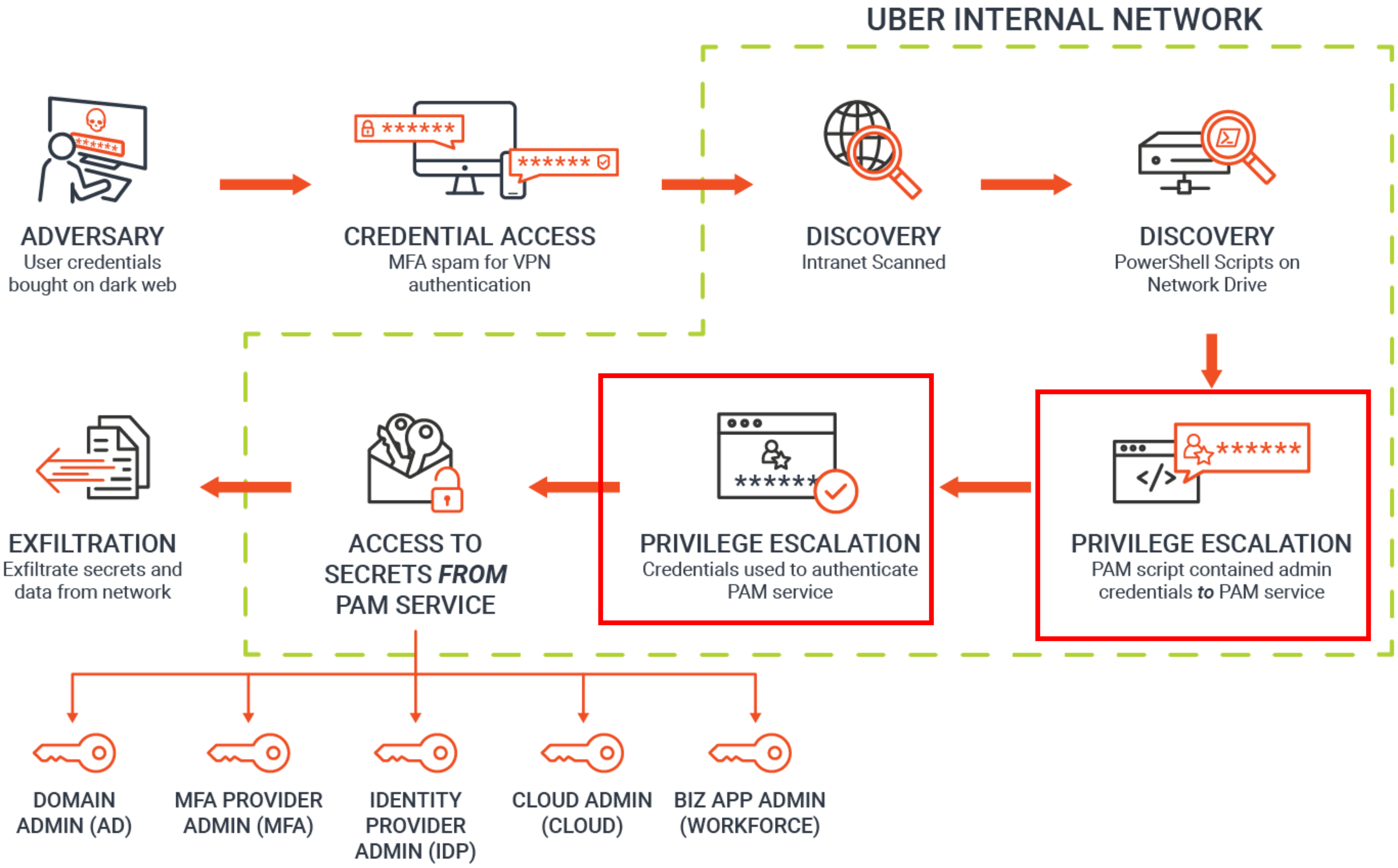
OT

Hybrid & Multi-Cloud

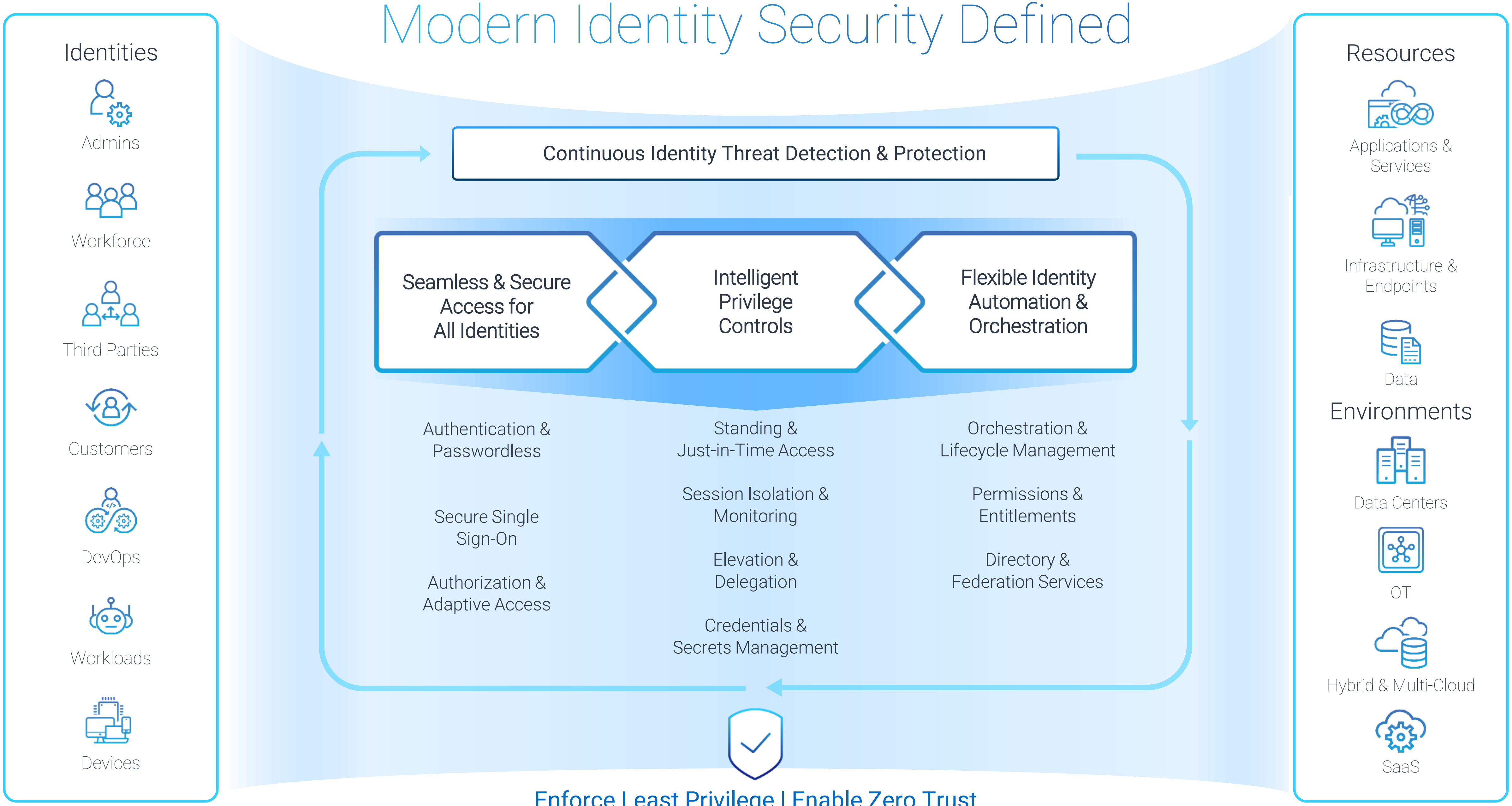
SaaS

# Latest Example – UBER Breach

- Social engineering and multiple MFA attack vectors
- Harvesting credentials for a PAM solution that allowed the attacker to gain high-level access, escalate privileges and exfiltrate.


UBER INTERNAL NETWORK
ADVERSARY
User credentials bought on dark web
CREDENTIAL ACCESS
MFA spam for VPN authentication
DISCOVERY
Intranet Scanned
DISCOVERY
PowerShell Scripts on Network Drive
PRIVILEGE ESCALATION
PAM script contained admin credentials *to* PAM service
PRIVILEGE ESCALATION
Credentials used to authenticate PAM service
ACCESS TO SECRETS *FROM* PAM SERVICE
EXFILTRATION
Exfiltrate secrets and data from network
DOMAIN ADMIN (AD)
MFA PROVIDER ADMIN (MFA)
IDENTITY PROVIDER ADMIN (IDP)
CLOUD ADMIN (CLOUD)
BIZ APP ADMIN (WORKFORCE)

# Modern Identity Security Defined



Identities

- Admins
- Workforce
- Third Parties
- Customers
- DevOps
- Workloads
- Devices

Continuous Identity Threat Detection & Protection

**Seamless & Secure Access for All Identities**

- Authentication & Passwordless
- Secure Single Sign-On
- Authorization & Adaptive Access

**Intelligent Privilege Controls**

- Standing & Just-in-Time Access
- Session Isolation & Monitoring
- Elevation & Delegation
- Credentials & Secrets Management

**Flexible Identity Automation & Orchestration**

- Orchestration & Lifecycle Management
- Permissions & Entitlements
- Directory & Federation Services

Resources

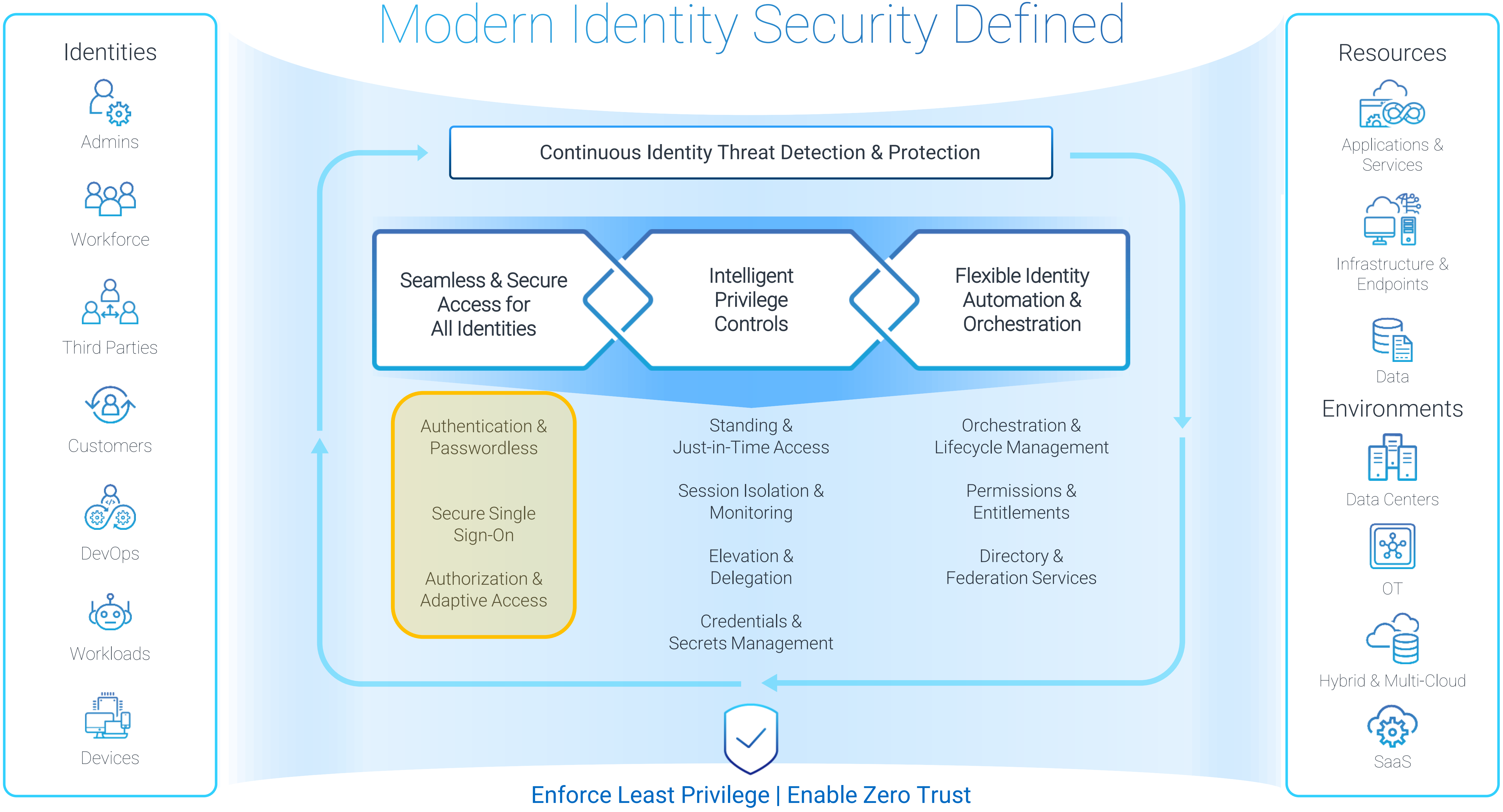
- Applications & Services
- Infrastructure & Endpoints
- Data

Environments

- Data Centers
- OT
- Hybrid & Multi-Cloud
- SaaS

Enforce Least Privilege | Enable Zero Trust

# Modern Identity Security Defined



## Identities

Admins

Workforce

Third Parties

Customers

DevOps

Workloads

Devices

## Resources

Applications & Services

Infrastructure & Endpoints

Data

## Environments

Data Centers

OT

Hybrid & Multi-Cloud

SaaS

Continuous Identity Threat Detection & Protection

### Seamless & Secure Access for All Identities

- Authentication & Passwordless
- Secure Single Sign-On
- Authorization & Adaptive Access

### Intelligent Privilege Controls

- Standing & Just-in-Time Access
- Session Isolation & Monitoring
- Elevation & Delegation
- Credentials & Secrets Management

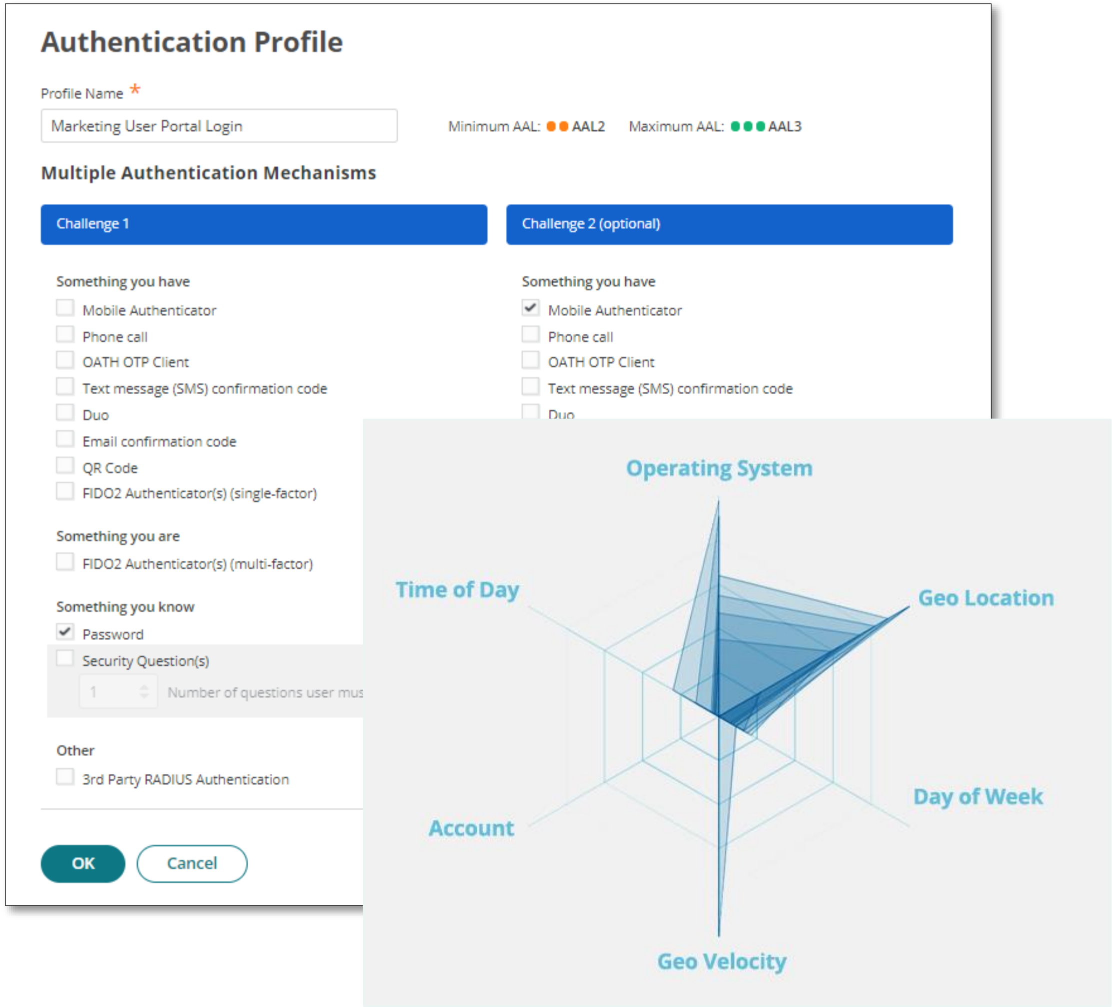
### Flexible Identity Automation & Orchestration

- Orchestration & Lifecycle Management
- Permissions & Entitlements
- Directory & Federation Services

Enforce Least Privilege | Enable Zero Trust

# Adaptive Multi-factor Authentication

Strengthen security through high authentication assurance, drive superior MFA user experience



## Authentication Profile

Profile Name *

Marketing User Portal Login

Minimum AAL: ●● AAL2 Maximum AAL: ●●● AAL3

**Multiple Authentication Mechanisms**

| Challenge 1 | Challenge 2 (optional) |
|---|---|
| Something you have | Something you have |
| □ Mobile Authenticator | ☑ Mobile Authenticator |
| □ Phone call | □ Phone call |
| □ OATH OTP Client | □ OATH OTP Client |
| □ Text message (SMS) confirmation code | □ Text message (SMS) confirmation code |
| □ Duo | □ Duo |
| □ Email confirmation code | |
| □ QR Code | |
| □ FIDO2 Authenticator(s) (single-factor) | |
| Something you are | |
| □ FIDO2 Authenticator(s) (multi-factor) | |
| Something you know | |
| ☑ Password | |
| □ Security Question(s) | |
| 1 Number of questions user mus | |
| Other | |
| □ 3rd Party RADIUS Authentication | |

OK Cancel

## Add an Extra Layer of Protection

before granting access to corporate applications

### MFA EVERYWHERE

Protect a broad range of use cases and resources

### STANDARDS BASED BROAD AUTHENTICATION

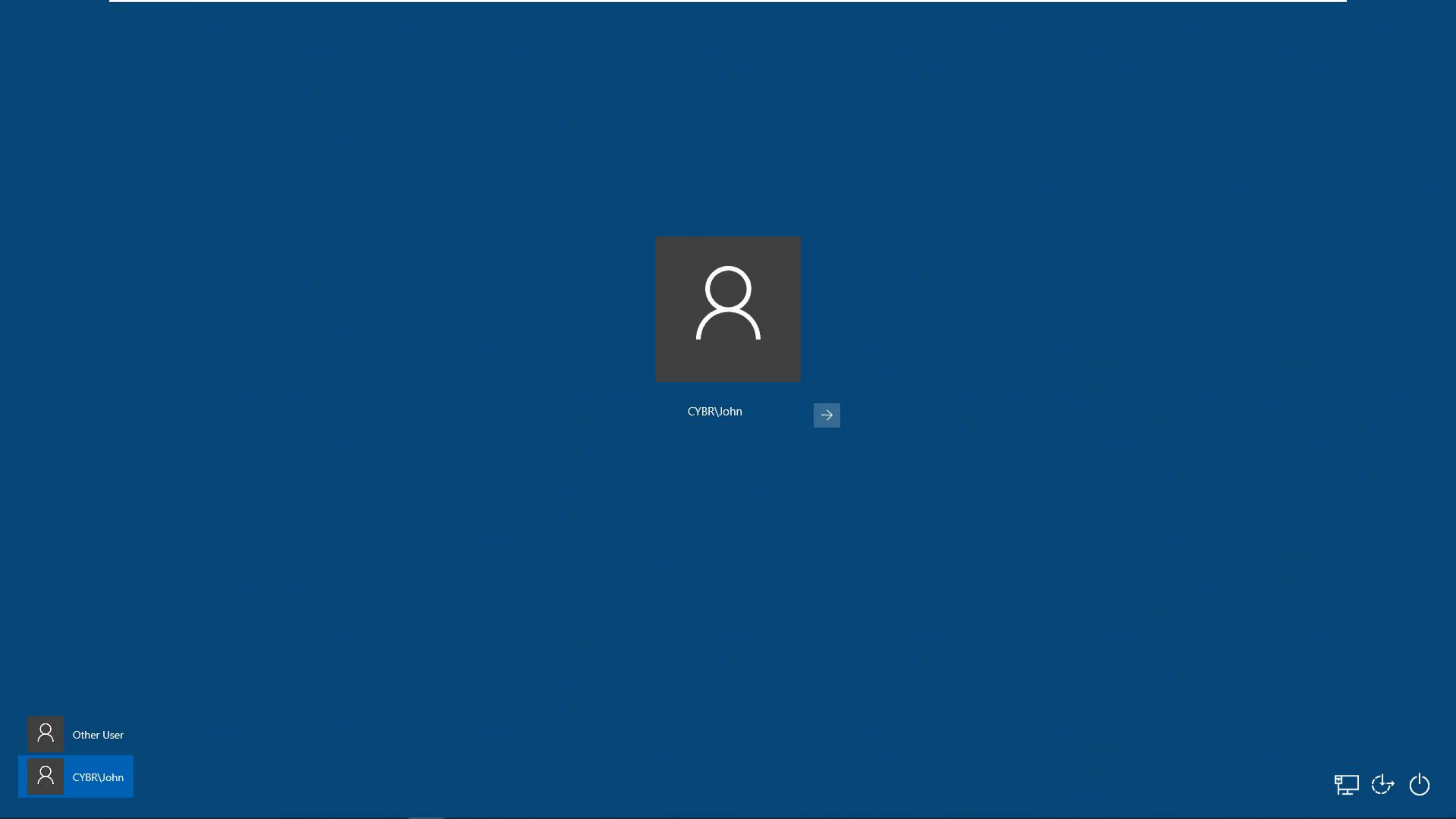
Broadest choice of authentication factors, including **Passwordless** factors. Support for FIDO, OATH, RADIUS

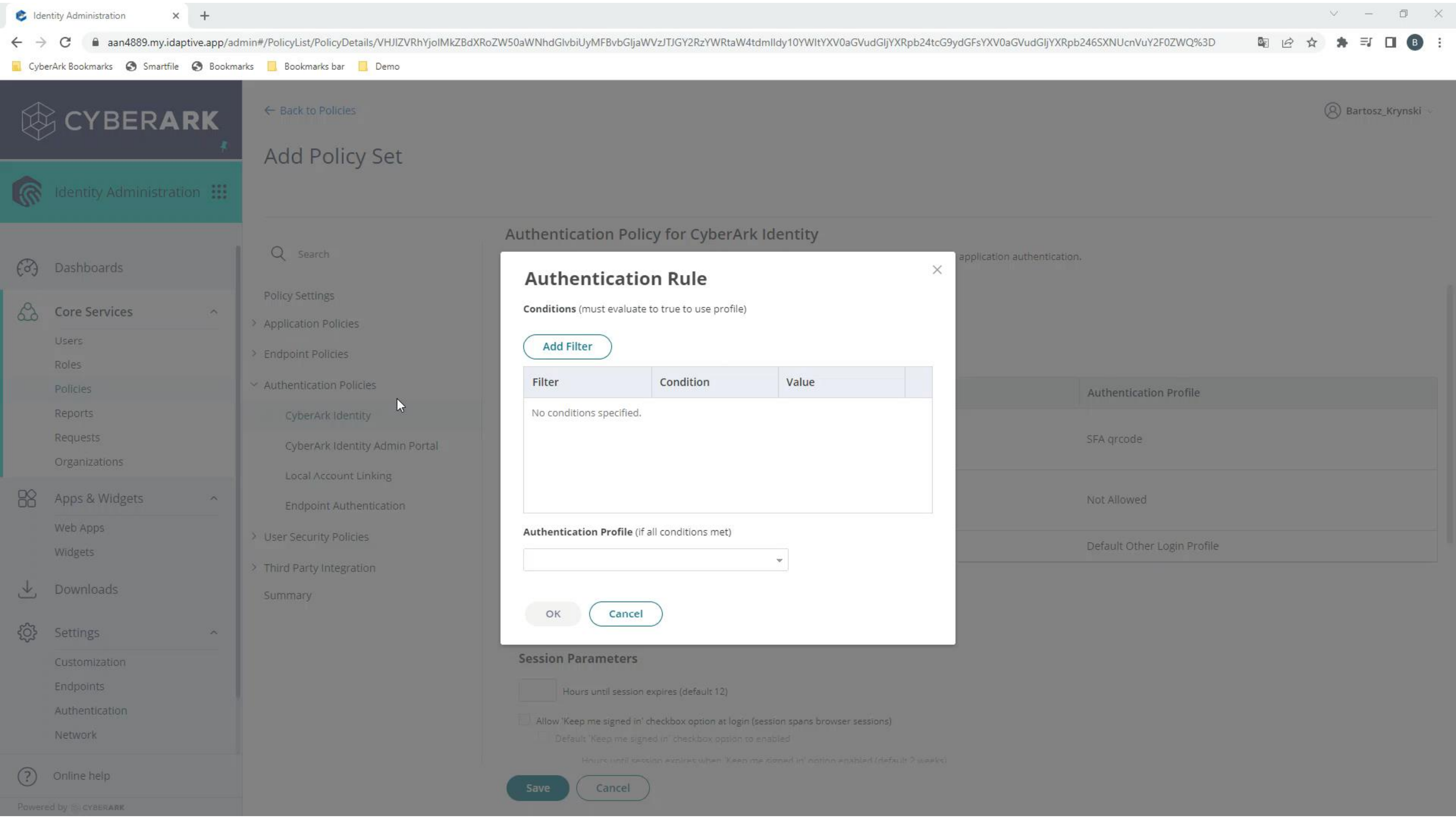
### MULTI-CONTEXT RISK-AWARE

Leverage machine learning for behavior-based MFA

### COMPLIANCE REPORTING AND VISIBILITY

Visibility into MFA adoption across the entire Organization based on best practices such as NIST


CYBR\John
Other User
CYBR\John



Add Policy Set

Authentication Policy for CyberArk Identity

application authentication.

| Authentication Profile |
|---|
| SFA qrcode |
| Not Allowed |
| Default Other Login Profile |

## Authentication Rule

**Conditions** (must evaluate to true to use profile)

| Filter | Condition | Value |
|---|---|---|
| No conditions specified. | | |

**Authentication Profile** (if all conditions met)

Session Parameters

Hours until session expires (default 12)

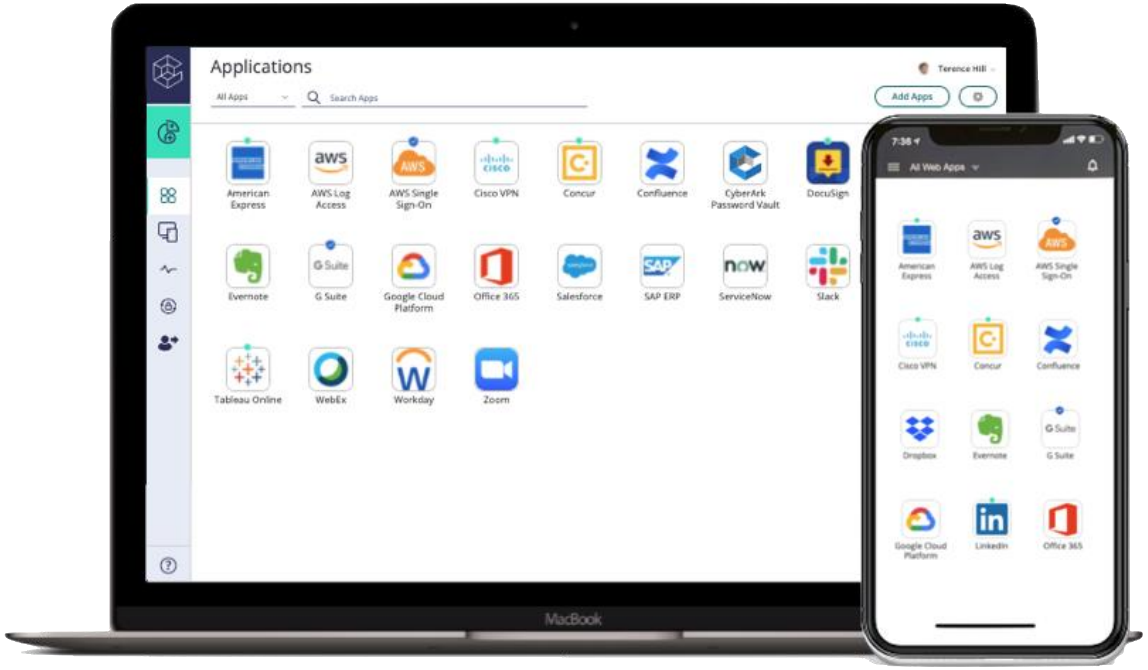
□ Allow 'Keep me signed in' checkbox option at login (session spans browser sessions)

□ Default 'Keep me signed in' checkbox option to enabled

Hours until session expires when 'Keep me signed in' option enabled (default 2 weeks)

# Centralized Access Management

Ease App Onboarding and drive productivity with anytime, anywhere access



## Enable one-click secure access to your cloud, mobile, and legacy apps from any device

### SINGLE SIGN-ON

A single identity to login to all cloud and on-prem apps leveraging SSO standards

### CENTRALIZED PASSWORD MGMT

Single console to federate with IDPs, define security policies and generate security and compliance reports

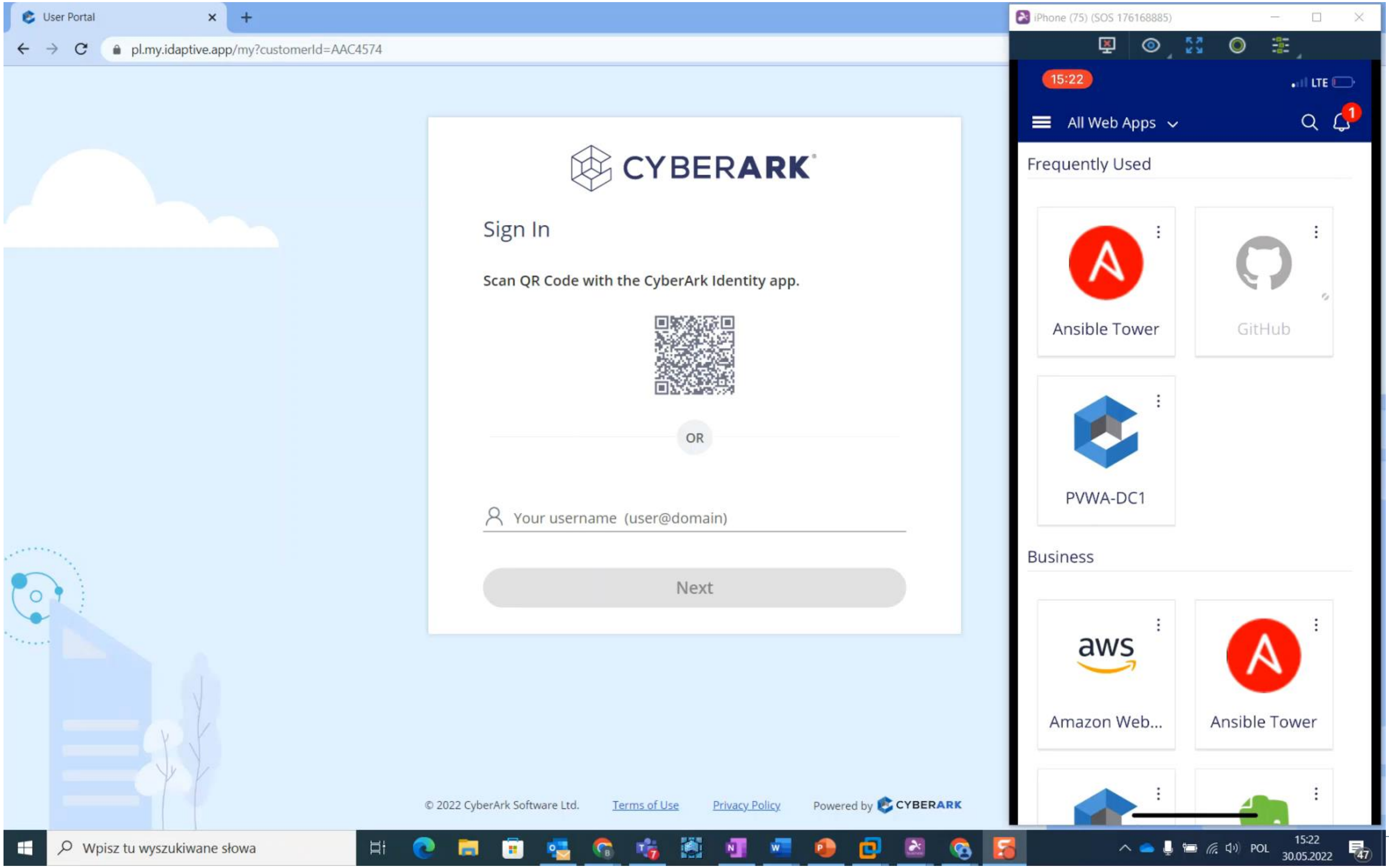
### SESSION PROTECTION

Business sessions recording, continuous user authentication, session protection

### CIAM - Customer Identity Mgt

Widgets, APIs and SDKs for every aspect of integrating identity and access management into your apps

# Single Sign-On demo



User Portal

pl.my.idaptive.app/my?customerId=AAC4574

CYBERARK

Sign In

Scan QR Code with the CyberArk Identity app.

OR

Your username (user@domain)

Next

© 2022 CyberArk Software Ltd. Terms of Use Privacy Policy Powered by CYBERARK

iPhone (75) (SOS 176168885)

15:22

All Web Apps

Frequently Used

Ansible Tower

GitHub

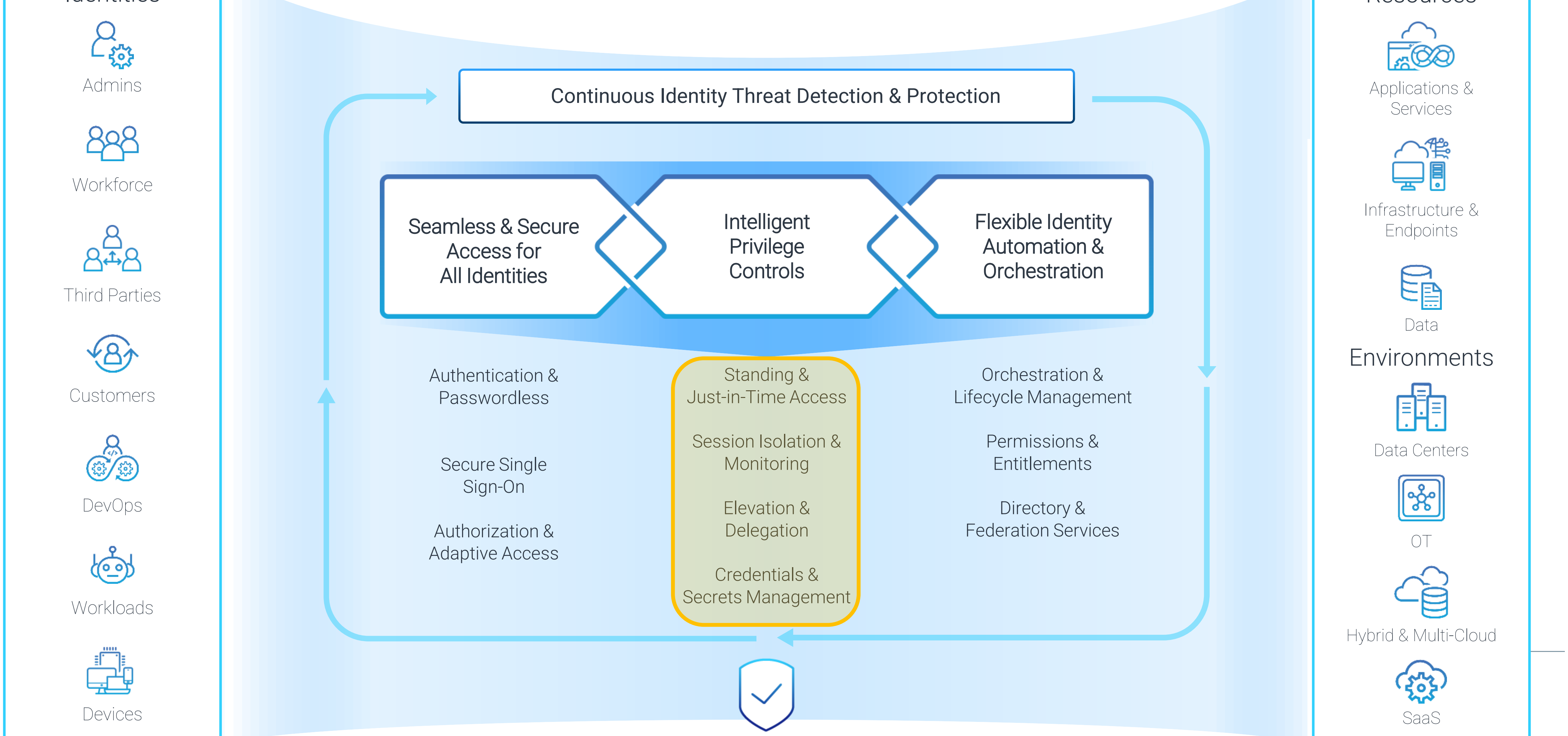
PWVA-DC1

Business

Amazon Web...

Ansible Tower

# Modern Identity Security Defined



## Identities

- Admins
- Workforce
- Third Parties
- Customers
- DevOps
- Workloads
- Devices

Continuous Identity Threat Detection & Protection

**Seamless & Secure Access for All Identities**

Authentication & Passwordless

Secure Single Sign-On

Authorization & Adaptive Access

**Intelligent Privilege Controls**

Standing & Just-in-Time Access

Session Isolation & Monitoring

Elevation & Delegation

Credentials & Secrets Management

**Flexible Identity Automation & Orchestration**

Orchestration & Lifecycle Management

Permissions & Entitlements

Directory & Federation Services

## Resources

- Applications & Services
- Infrastructure & Endpoints
- Data

## Environments

- Data Centers
- OT
- Hybrid & Multi-Cloud
- SaaS

Enforce Least Privilege | Enable Zero Trust

# Account Type Overview

## SYSTEM ACCOUNTS

Accounts with built-in passwords that must be vaulted and used in break-glass scenarios

INTERACTIVE

## OPERATIONAL ACCOUNTS

Accounts created with the purpose to provide operational, administrative access

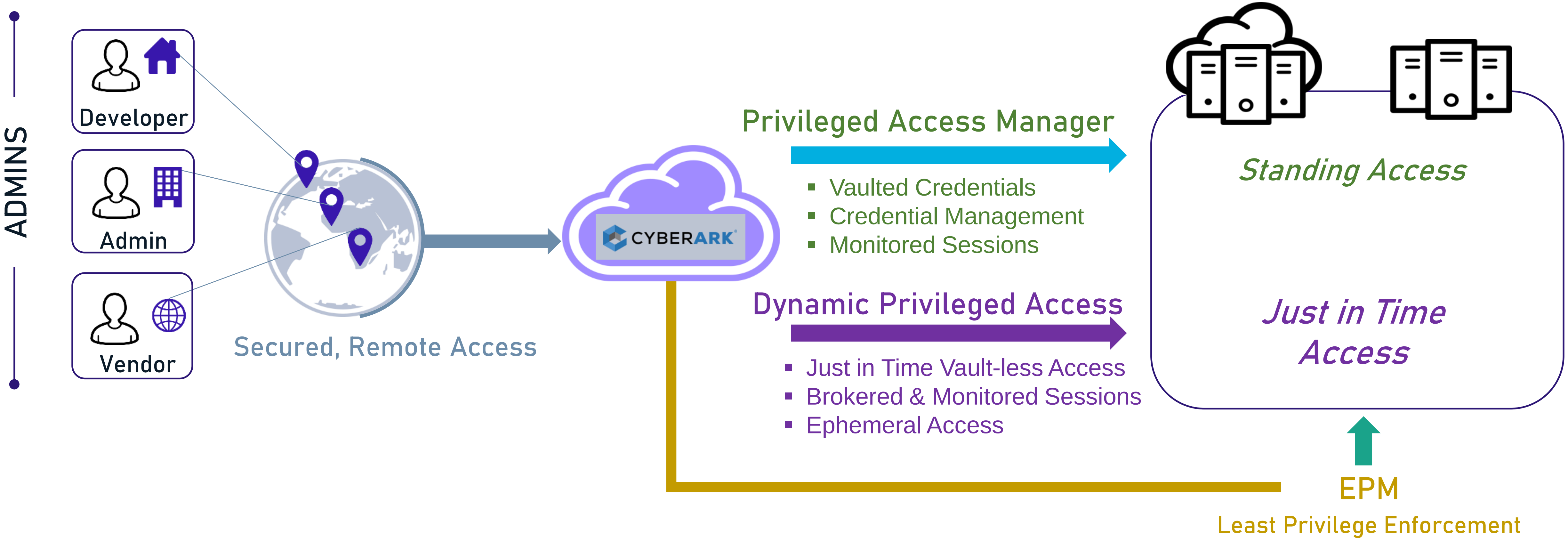
INTERACTIVE

## APPLICATION ACCOUNTS

Accounts created for the use within / by automated processes and applications

NON-INTERACTIVE

# Comprehensive PAM platform



Privileged Access Manager

- Vaulted Credentials
- Credential Management
- Monitored Sessions

Dynamic Privileged Access

- Just in Time Vault-less Access
- Brokered & Monitored Sessions
- Ephemeral Access

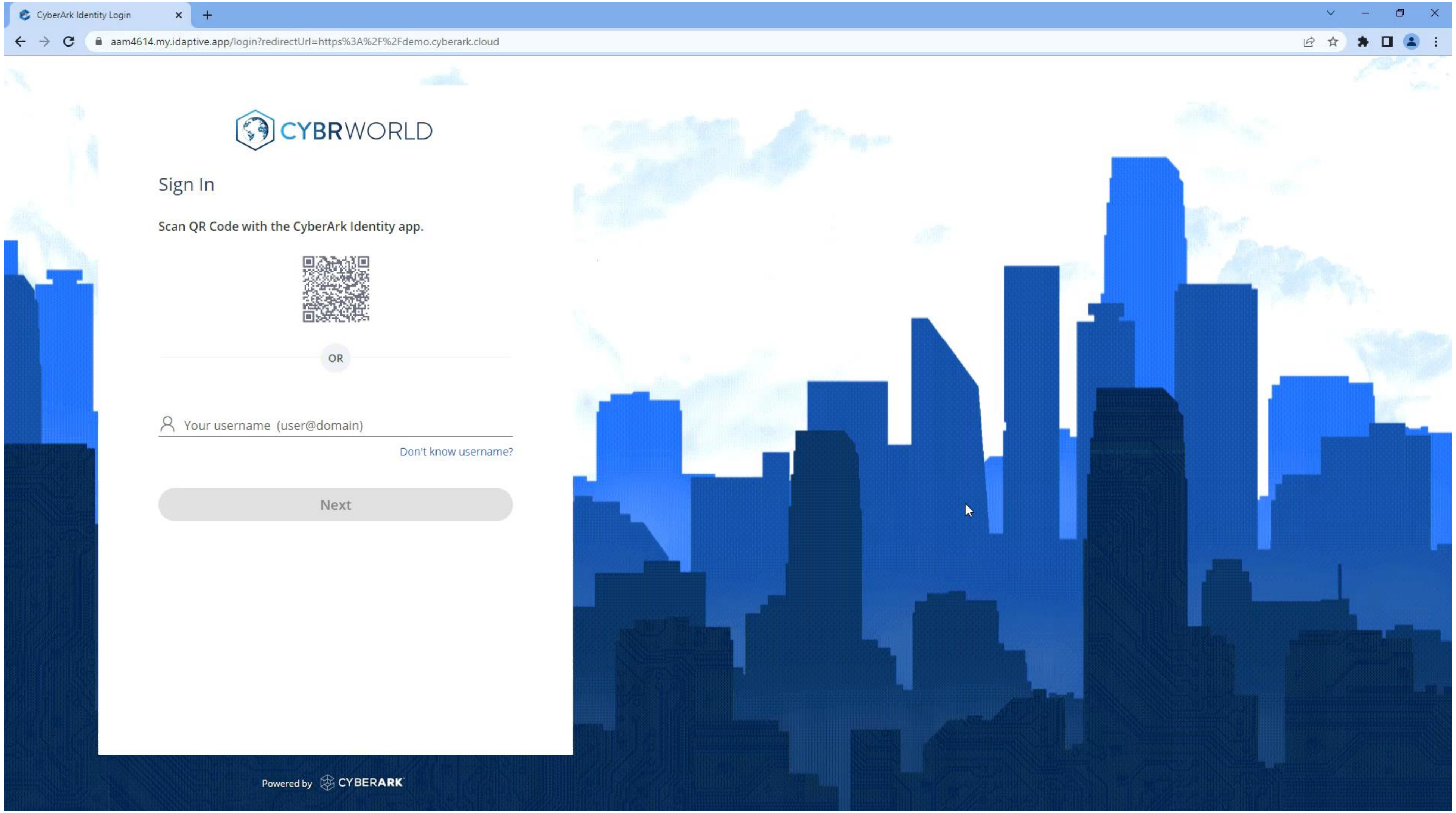
*Standing Access*

*Just in Time Access*

EPM

Least Privilege Enforcement

# Dynamic access example



CyberArk Identity Login

aam4614.my.idaptive.app/login?redirectUrl=https%3A%2F%2Fdemo.cyberark.cloud

CYBRWORLD

Sign In

Scan QR Code with the CyberArk Identity app.

OR

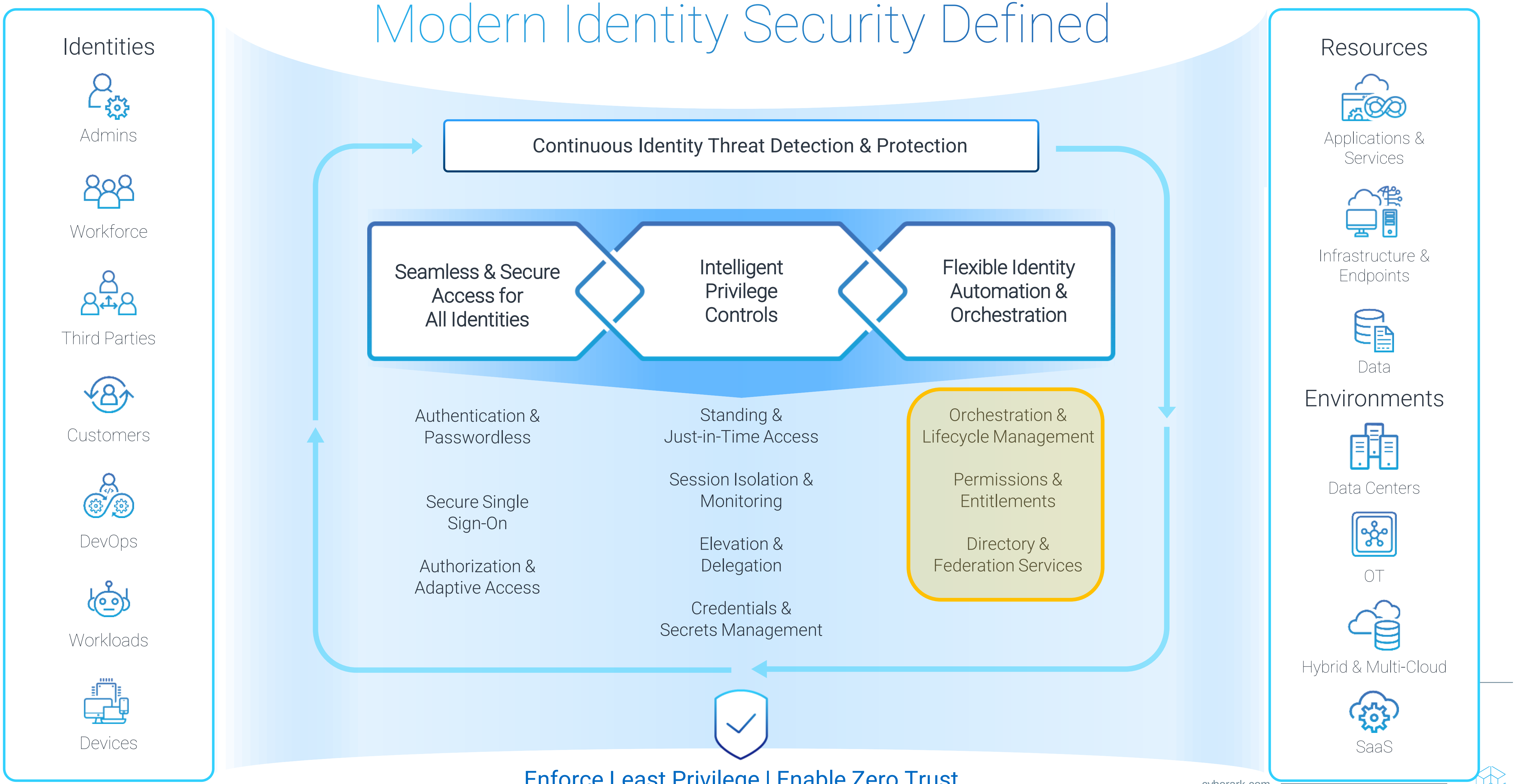
Your username (user@domain)

Don't know username?

Next

Powered by CYBERARK

# Modern Identity Security Defined



## Identities

Admins

Workforce

Third Parties

Customers

DevOps

Workloads

Devices

Continuous Identity Threat Detection & Protection

**Seamless & Secure Access for All Identities**

- Authentication & Passwordless
- Secure Single Sign-On
- Authorization & Adaptive Access

**Intelligent Privilege Controls**

- Standing & Just-in-Time Access
- Session Isolation & Monitoring
- Elevation & Delegation
- Credentials & Secrets Management

**Flexible Identity Automation & Orchestration**

- Orchestration & Lifecycle Management
- Permissions & Entitlements
- Directory & Federation Services

## Resources

Applications & Services

Infrastructure & Endpoints

Data

## Environments

Data Centers

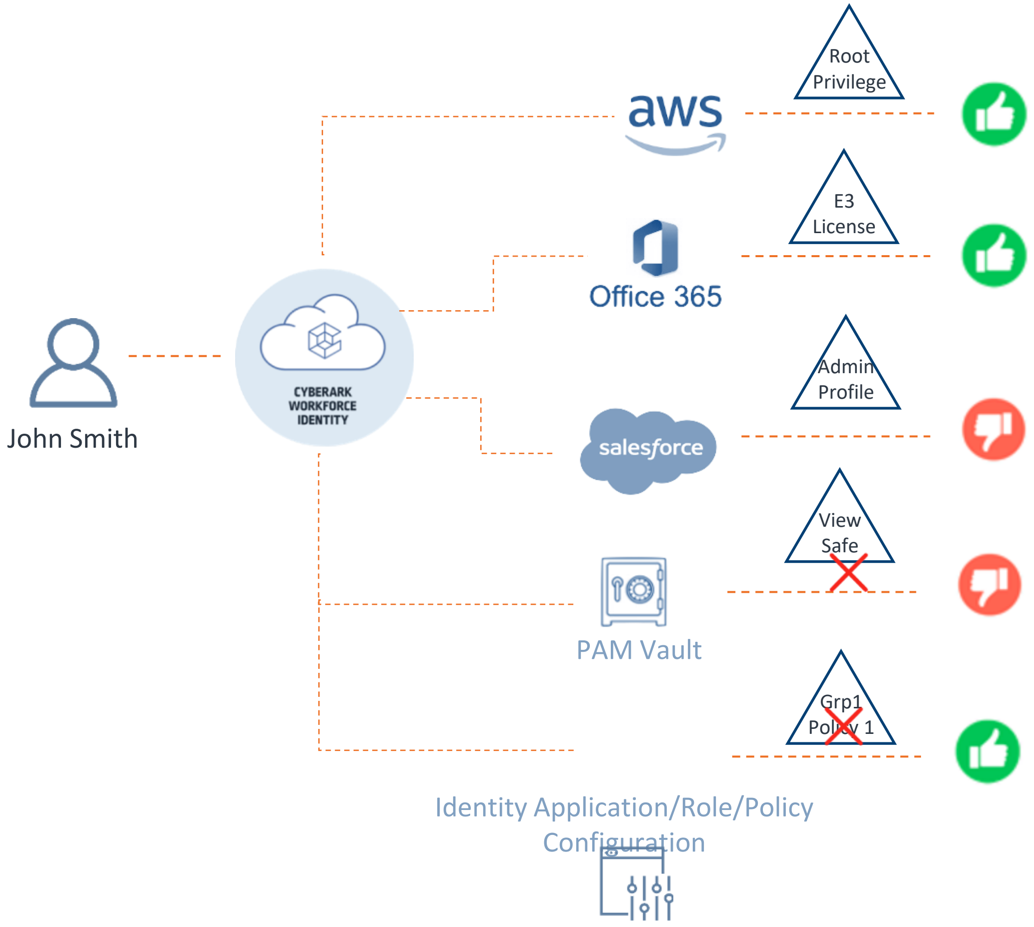
OT

Hybrid & Multi-Cloud

SaaS

**Enforce Least Privilege | Enable Zero Trust**

# CyberArk Identity Compliance



## Key Features

### DISCOVER ACCESS

Find all access and entitlements associated with users.

### CERTIFY ACCESS

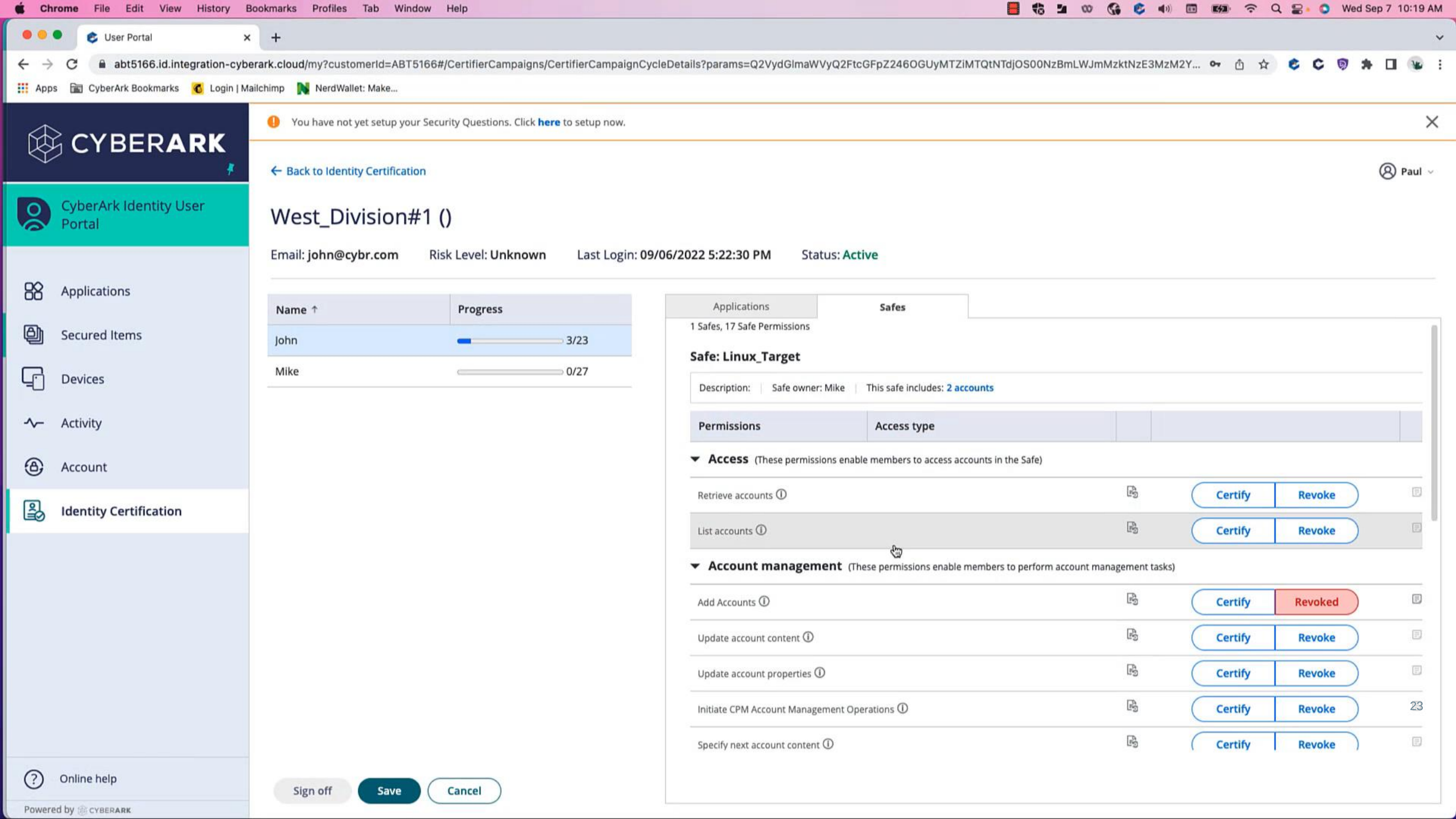
Continuously review and approve access based on risk.

### APPLICATION, ROLE, POLICY COMPLIANCE

Automate  onboarding and manage roles and policies.

### CONTINUOUS COMPLIANCE

Workflows, analytics, reports and dashboards.



You have not yet setup your Security Questions. Click here to setup now.

← Back to Identity Certification

West_Division#1 ()

Email: **john@cybr.com** Risk Level: **Unknown** Last Login: **09/06/2022 5:22:30 PM** Status: **Active**

| Name ↑ | Progress |
|---|---|
| John | 3/23 |
| Mike | 0/27 |

Applications | **Safes**

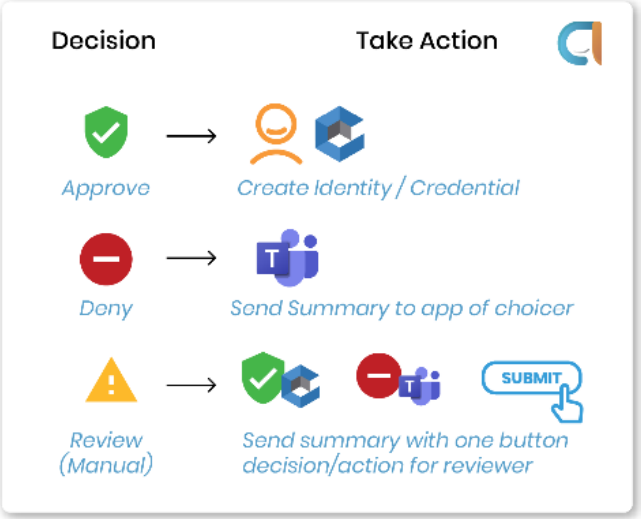
1 Safes, 17 Safe Permissions

**Safe: Linux_Target**

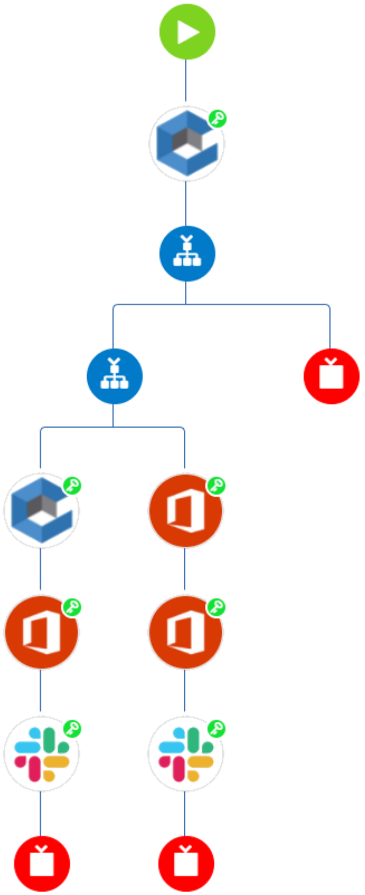
Description: | Safe owner: Mike | This safe includes: 2 accounts

| Permissions | Access type | | |
|---|---|---|---|
| **Access** (These permissions enable members to access accounts in the Safe) | | | |
| Retrieve accounts ⓘ | | | Certify Revoke |
| List accounts ⓘ | | | Certify Revoke |
| **Account management** (These permissions enable members to perform account management tasks) | | | |
| Add Accounts ⓘ | | | Certify Revoked |
| Update account content ⓘ | | | Certify Revoke |
| Update account properties ⓘ | | | Certify Revoke |
| Initiate CPM Account Management Operations ⓘ | | | Certify Revoke |
| Specify next account content ⓘ | | | Certify Revoke |

# CyberArk Identity Flows



| Decision | Take Action |
|---|---|
| Approve | Create Identity / Credential |
| Deny | Send Summary to app of choicer |
| Review (Manual) | Send summary with one button decision/action for reviewer |



## Key Features

### ACCESS CONTROL

Provision granular access to applications and provide advanced authorizations to access app data

### CONFIGURABLE WORKFLOWS

Easily create complex workflows to get any data into any app or take actions based on specific triggers

### GATHER AND TRANSFORM ANY DATA

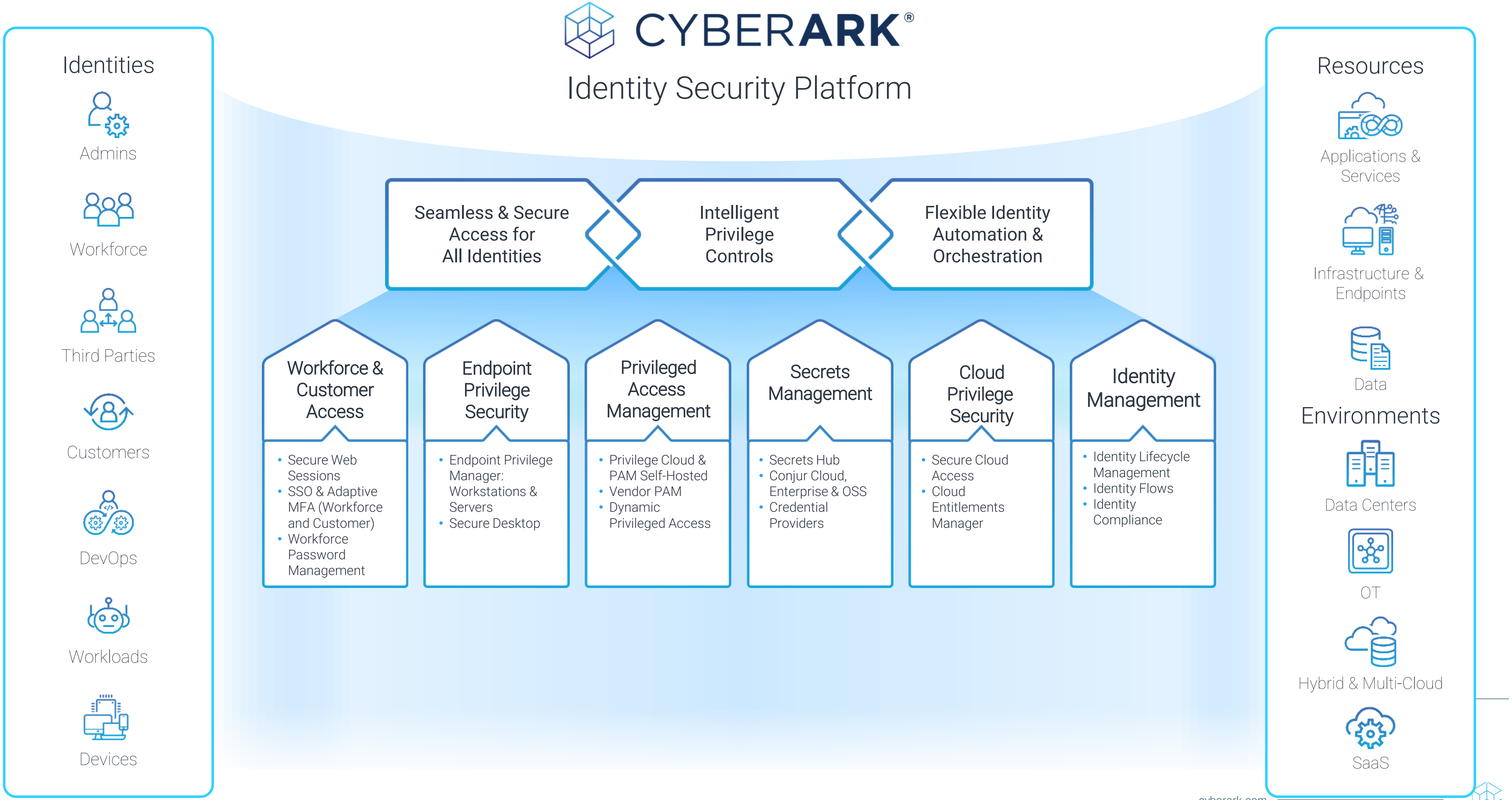
Use structured or unstructured data in ANY app(s) with 3000+ connectors and built-in logic

### NO-CODE INTEGRATION

Integrate and automate any combination of apps with any identity

# CYBERARK®

## Identity Security Platform



### Identities

- Admins
- Workforce
- Third Parties
- Customers
- DevOps
- Workloads
- Devices

### Seamless & Secure Access for All Identities

### Intelligent Privilege Controls

### Flexible Identity Automation & Orchestration

#### Workforce & Customer Access

- Secure Web Sessions
- SSO & Adaptive MFA (Workforce and Customer)
- Workforce Password Management

#### Endpoint Privilege Security

- Endpoint Privilege Manager: Workstations & Servers
- Secure Desktop

#### Privileged Access Management

- Privilege Cloud & PAM Self-Hosted
- Vendor PAM
- Dynamic Privileged Access

#### Secrets Management

- Secrets Hub
- Conjur Cloud, Enterprise & OSS
- Credential Providers

#### Cloud Privilege Security

- Secure Cloud Access
- Cloud Entitlements Manager

#### Identity Management

- Identity Lifecycle Management
- Identity Flows
- Identity Compliance

### Resources

- Applications & Services
- Infrastructure & Endpoints
- Data

### Environments

- Data Centers
- OT
- Hybrid & Multi-Cloud
- SaaS

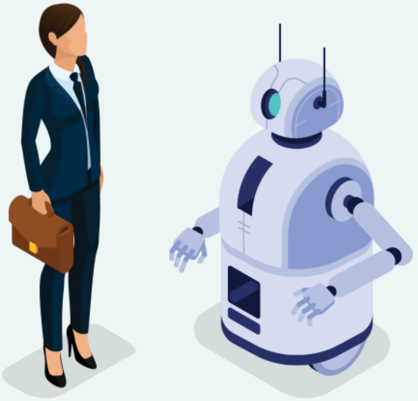
# Where to start?

## Build your plan with Blueprint

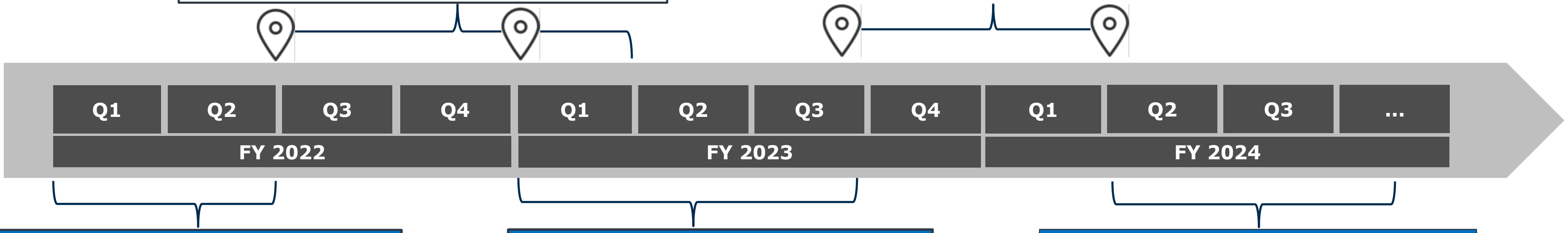
Identity Security Program Framework

Measurably Reduce Risk

Lessons Learned in Battle



Full Scope of Identities



## Stage 1 (Sprint)

- Windows Server Local Admins
- Hypervisor Admins
- Domain Admins
- Cloud Admins (TOP)
- MFA, SSO for Privileged users
- HSM, SIEM Integration
- IaaS Cloud admins
- 3rd Party Security Tools (ie. Vulnerability Scanners, discovery tools) & RPA
- MFA, SSO for Business users - Pilot
- Password storage for business users - Pilot

## Stage 2

- Privileged AD Users
- Windows Workstation Local Admins
- CI/CD Consoles
- *NIX root accounts & SSH Keys
- Privileged Remote Access – Admins
- Privileged Remote Access – 3r Party Vendors
- Cloud Admins (ALL)
- IT Admin, Developer workstations
- Dynamic apps - CI/CD & K8s – (TOP)
- Static Apps (J2EE) an admin scripts (TOP)
- MFA & SSO for critical saas apps
- Lifecycle Mgt – Pilot
- Business session monitoring
- Password storage for business users

## Stage 3

- Database Built-In Admins
- Out of Band Access
- Critical Windows Services
- Windows servers
- Business user workstations
- Dynamic apps - CI/CD Pipelines (ALL)
- MFA, SSO & Lifecycle Mgt for (ALL)

## Stage 4

- Named DBA
- Network & Infra Admins (ALL)
- Client-Server apps (TOP)
- ITSM Integration
- All Workstations
- Static Apps (ALL)
- Administrative Scripts (ALL)

## Stage 5

- Client-Server apps (ALL)
- Windows Services
- *NIX Servers

**Legend**

📍 Strategy Refresh Point
🟦 Remote Access & PAM
🟥 Least privilege
🟩 Secrets Management
🟧 Workforce Identity

*   To be finished
** To be verified with business units

cyberark.is/identity-security