bakotech®

CYBERARK®

How to unify management and protection of all identities

Bartosz Kryński
Solutions Engineering Team Leader, CISSP

Dan

IT Administrator

Dan

IT Administrator

New Identities

New Environments

New Attacker Methods

bako tech®

How to move from audit compliance to comprehensive program?

Leading Insurance Company Strengthens Security, Boosts Regulatory Compliance And Delivers Digital Transformation

GOAL

Provide password rotation for selected databases, enforce standarization in privileged access with tiering model

SOLUTION

CyberArk Identity Security Platform to strengthen security and boost regulatory compliance as the business consolidates

RESULTS

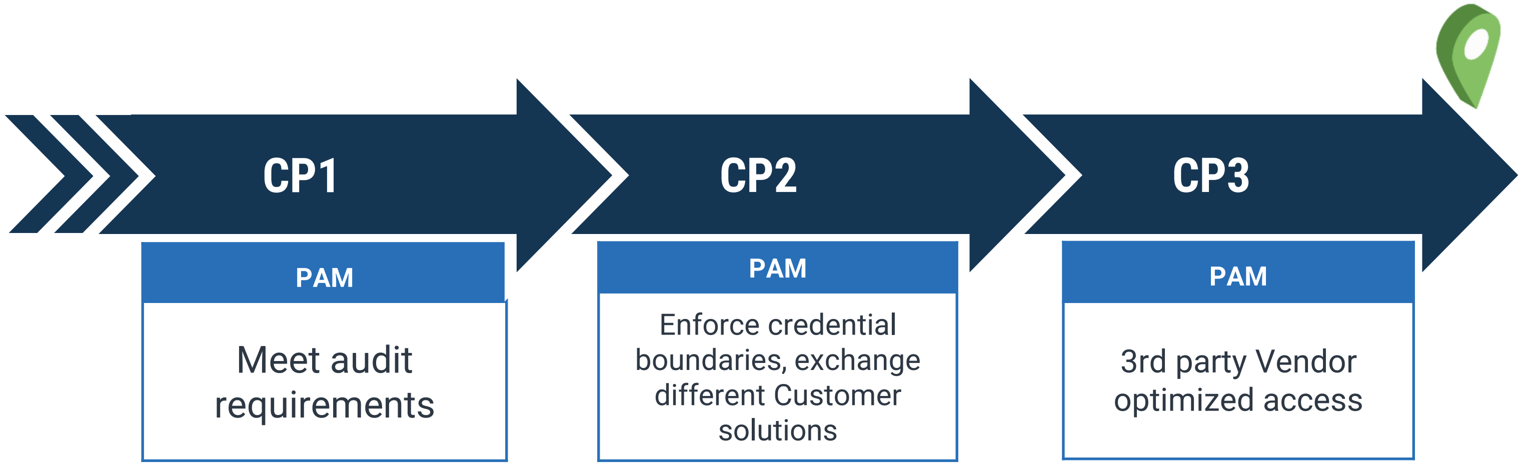
- Effective privileged access management strategy
- One solution for many use cases
- Unified identity security program for ZTA

Customer Case Study

Identity Security project plan

Legend

- 📍 Strategy Refresh
- 🟦 Access Controls
- 🟦 PAM Controls
- 🟩 Least Privilege Controls
- 🟥 Secrets Management Controls



CP1

PAM

Meet audit requirements

CP2

PAM

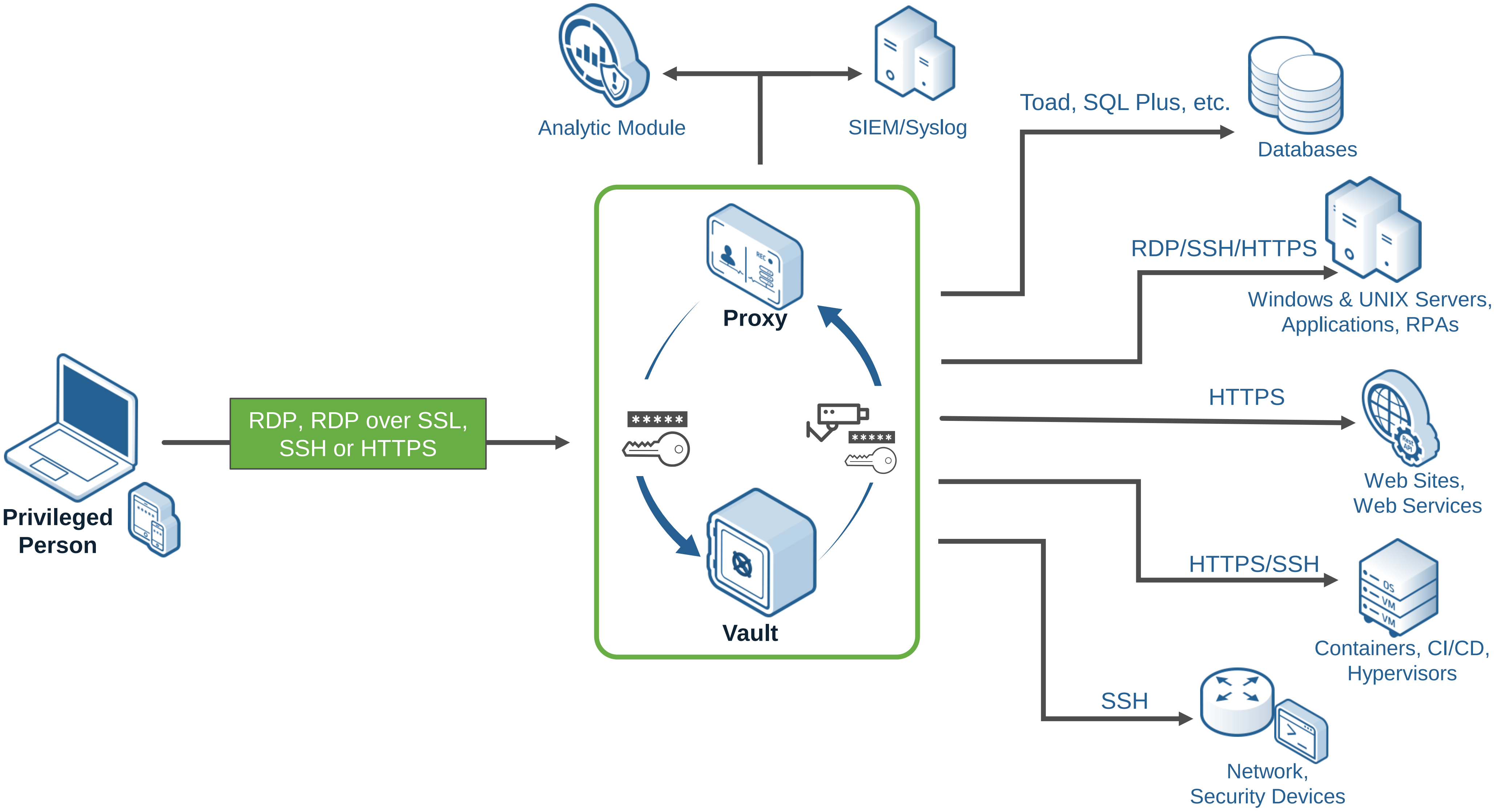
Enforce credential boundaries, exchange different Customer solutions

CP3

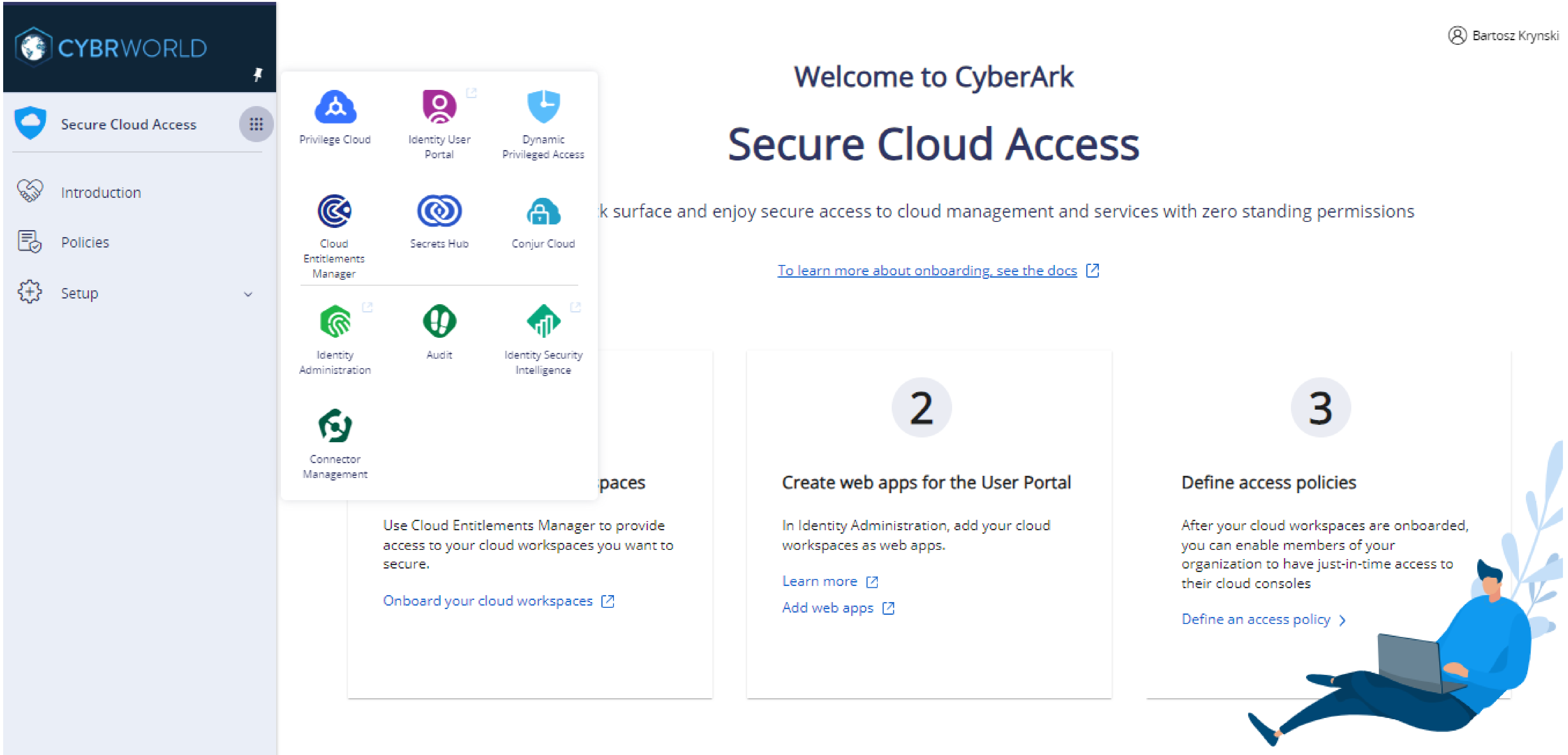
PAM

3rd party Vendor optimized access

Privileged access protection in details



CyberArk Identity Security Platform



Welcome to CyberArk

Secure Cloud Access

k surface and enjoy secure access to cloud management and services with zero standing permissions

To learn more about onboarding, see the docs

paces

Use Cloud Entitlements Manager to provide access to your cloud workspaces you want to secure.

Onboard your cloud workspaces

2

Create web apps for the User Portal

In Identity Administration, add your cloud workspaces as web apps.

Learn more

Add web apps

3

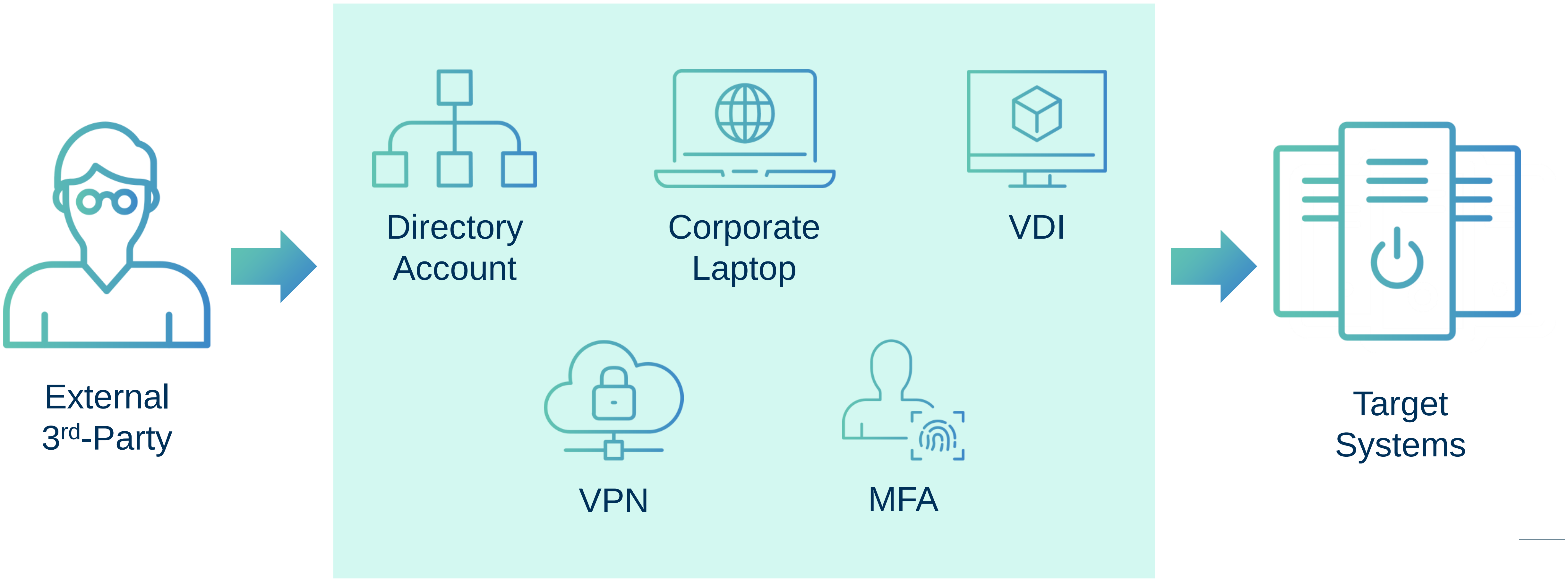
Define access policies

After your cloud workspaces are onboarded, you can enable members of your organization to have just-in-time access to their cloud consoles

Define an access policy

Common IDENTITY Issues with external vendors

Conventional Approaches



External
3rd-Party

Directory Account

Corporate Laptop

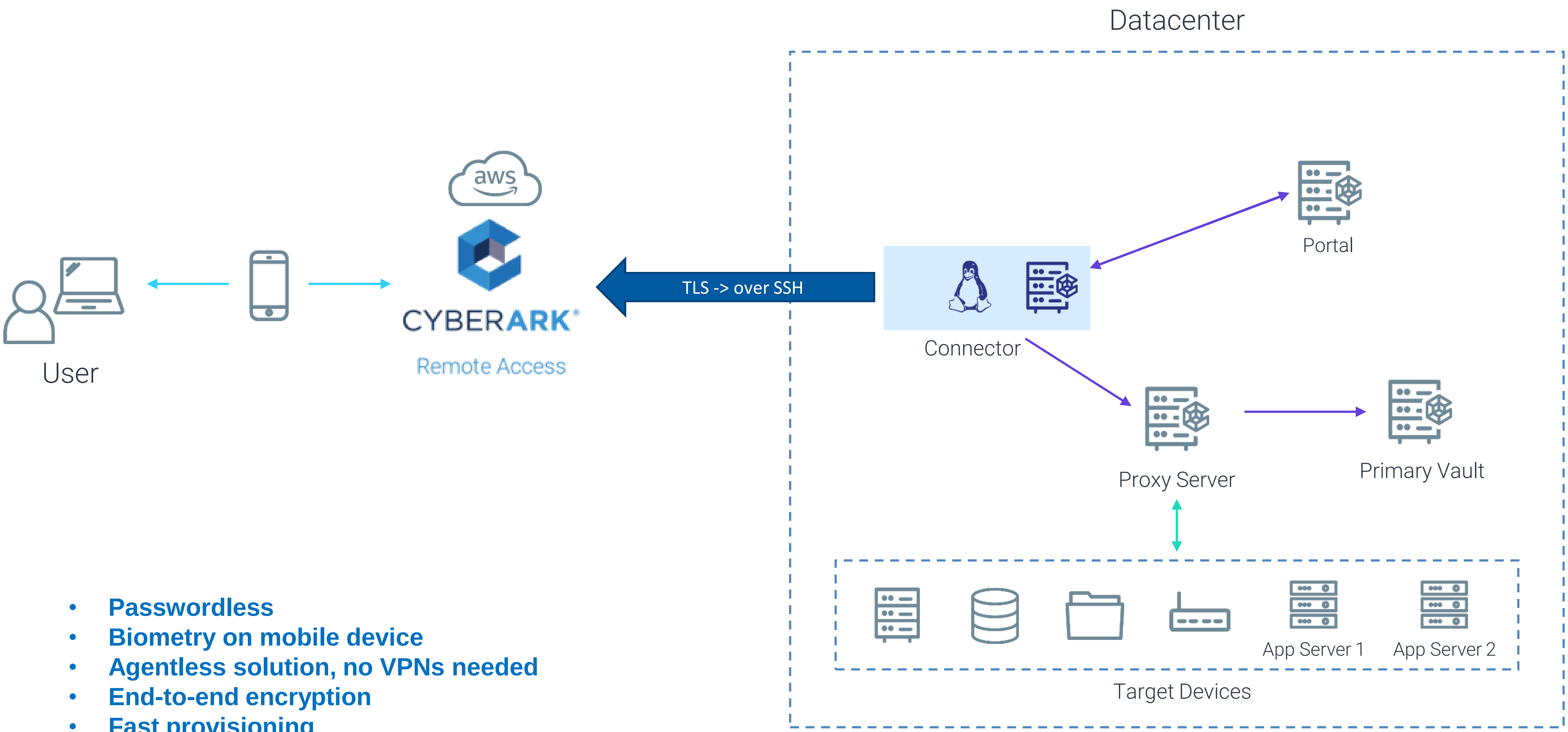
VDI

VPN

MFA

Target Systems

CyberArk Vendor PAM Architecture

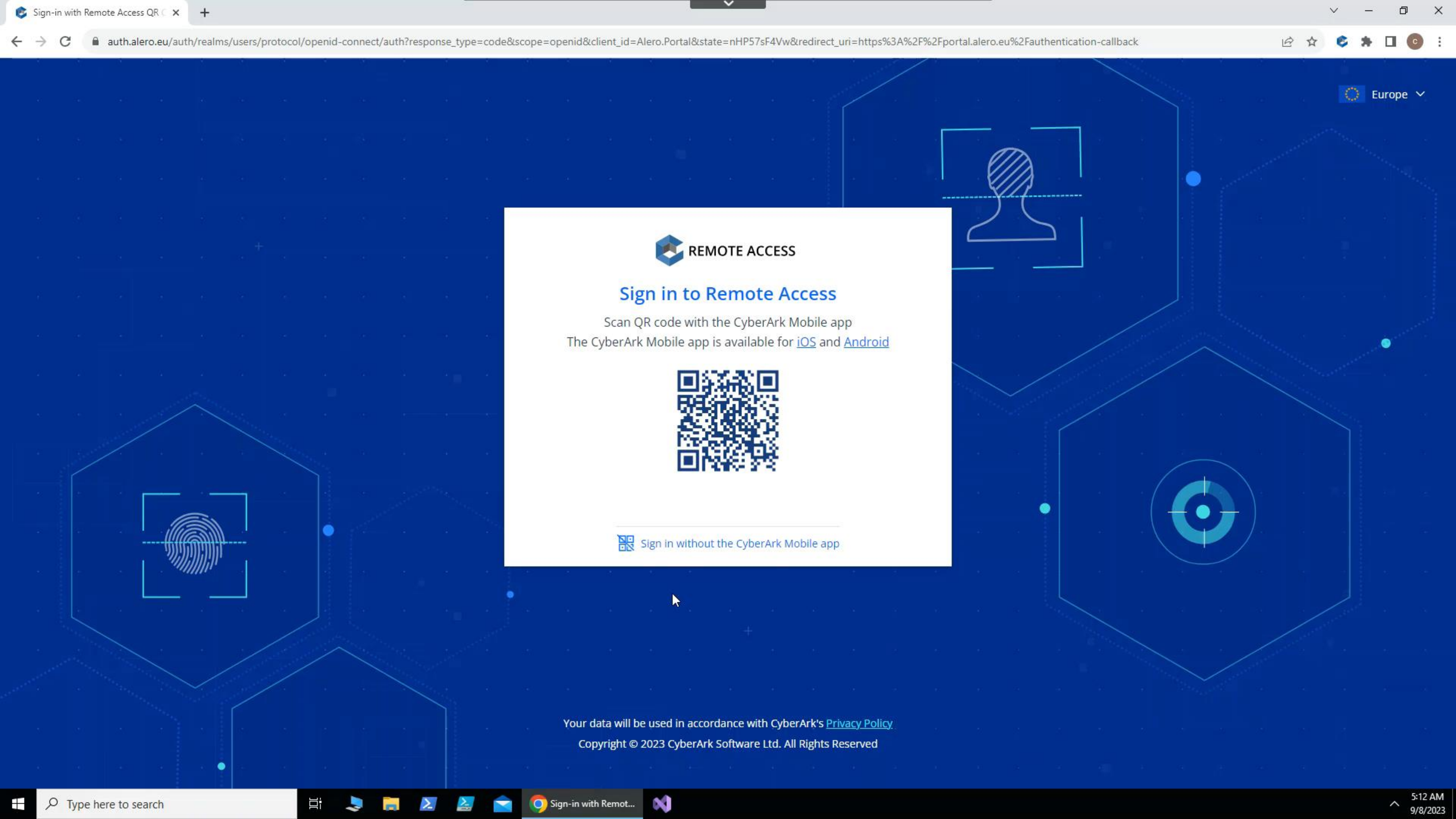


- **Passwordless**
- **Biometry on mobile device**
- **Agentless solution, no VPNs needed**
- **End-to-end encryption**
- **Fast provisioning**

It’s demo time!

Katarzyna
Business

Bartek
Security Admin



Sign-in with Remote Access QR C
auth.alero.eu/auth/realms/users/protocol/openid-connect/auth?response_type=code&scope=openid&client_id=Alero.Portal&state=nHP57sF4Vw&redirect_uri=https%3A%2F%2Fportal.alero.eu%2Fauthentication-callback
Europe
Type here to search
Sign-in with Remot...
5:12 AM
9/8/2023

REMOTE ACCESS

Sign in to Remote Access

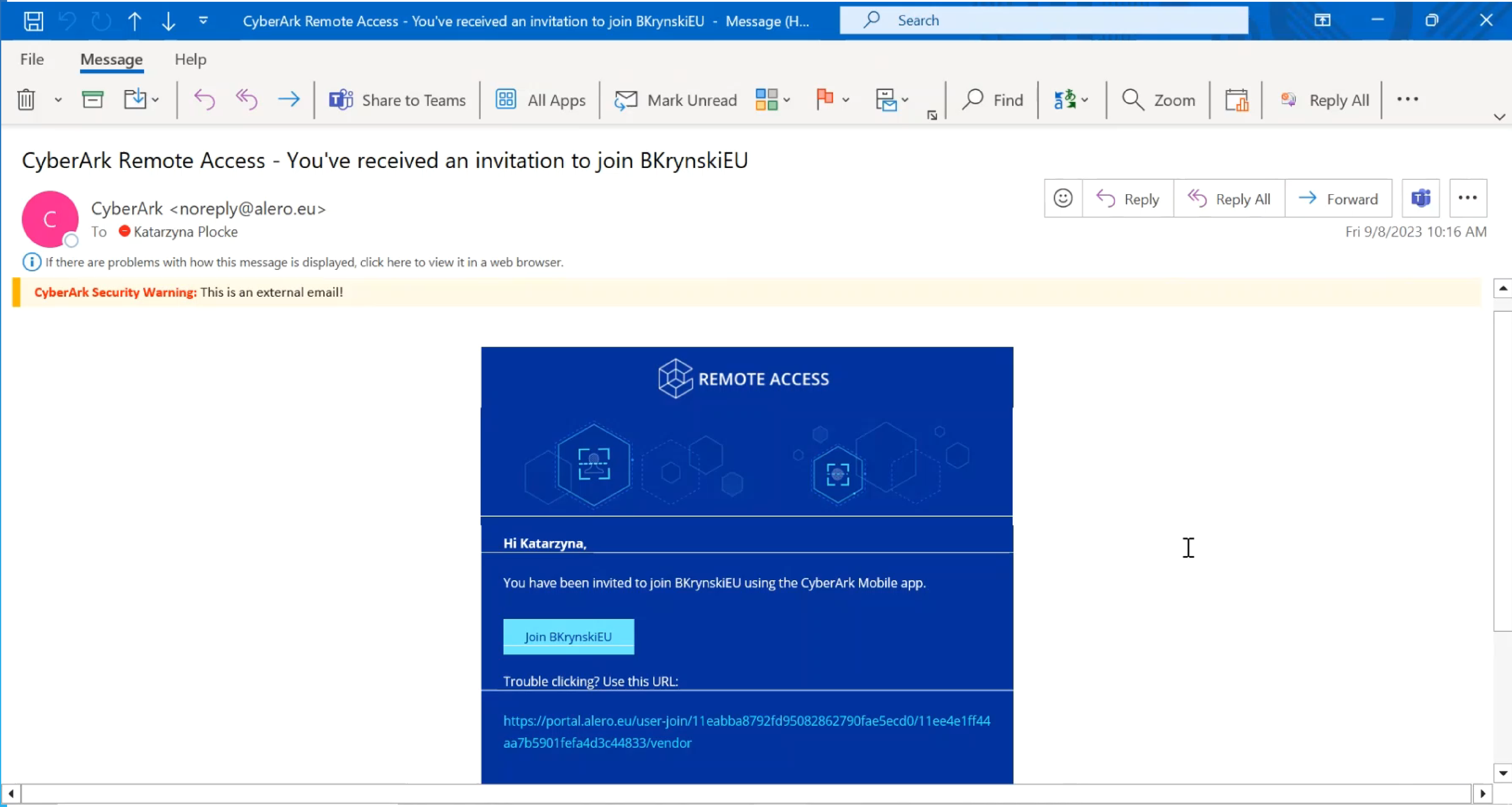
Scan QR code with the CyberArk Mobile app

The CyberArk Mobile app is available for iOS and Android

Sign in without the CyberArk Mobile app

Your data will be used in accordance with CyberArk's Privacy Policy

Copyright © 2023 CyberArk Software Ltd. All Rights Reserved



CyberArk Remote Access - You've received an invitation to join BKrynskiEU

CyberArk <noreply@alero.eu>
To Katarzyna Plocke

Fri 9/8/2023 10:16 AM

If there are problems with how this message is displayed, click here to view it in a web browser.

CyberArk Security Warning: This is an external email!

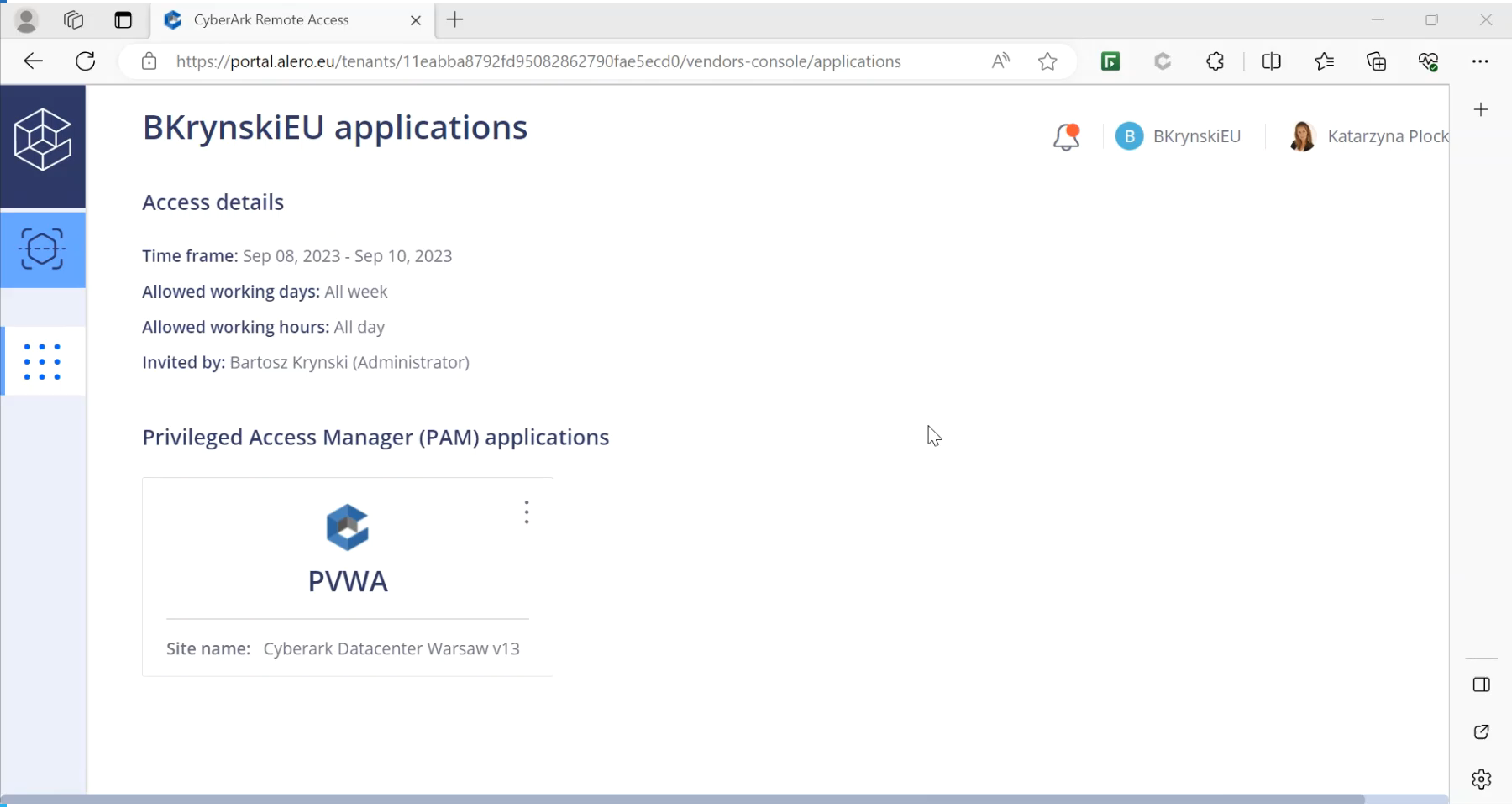
Hi Katarzyna,

You have been invited to join BKrynskiEU using the CyberArk Mobile app.

Join BKrynskiEU

Trouble clicking? Use this URL:

https://portal.alero.eu/user-join/11eabba8792fd95082862790fae5ecd0/11ee4e1ff44aa7b5901fefa4d3c44833/vendor


CyberArk Remote Access
https://portal.alero.eu/tenants/11eabba8792fd95082862790fae5ecd0/vendors-console/applications
B
BKrynskiEU
Katarzyna Plock

BKrynskiEU applications

Access details

Time frame: Sep 08, 2023 - Sep 10, 2023

Allowed working days: All week

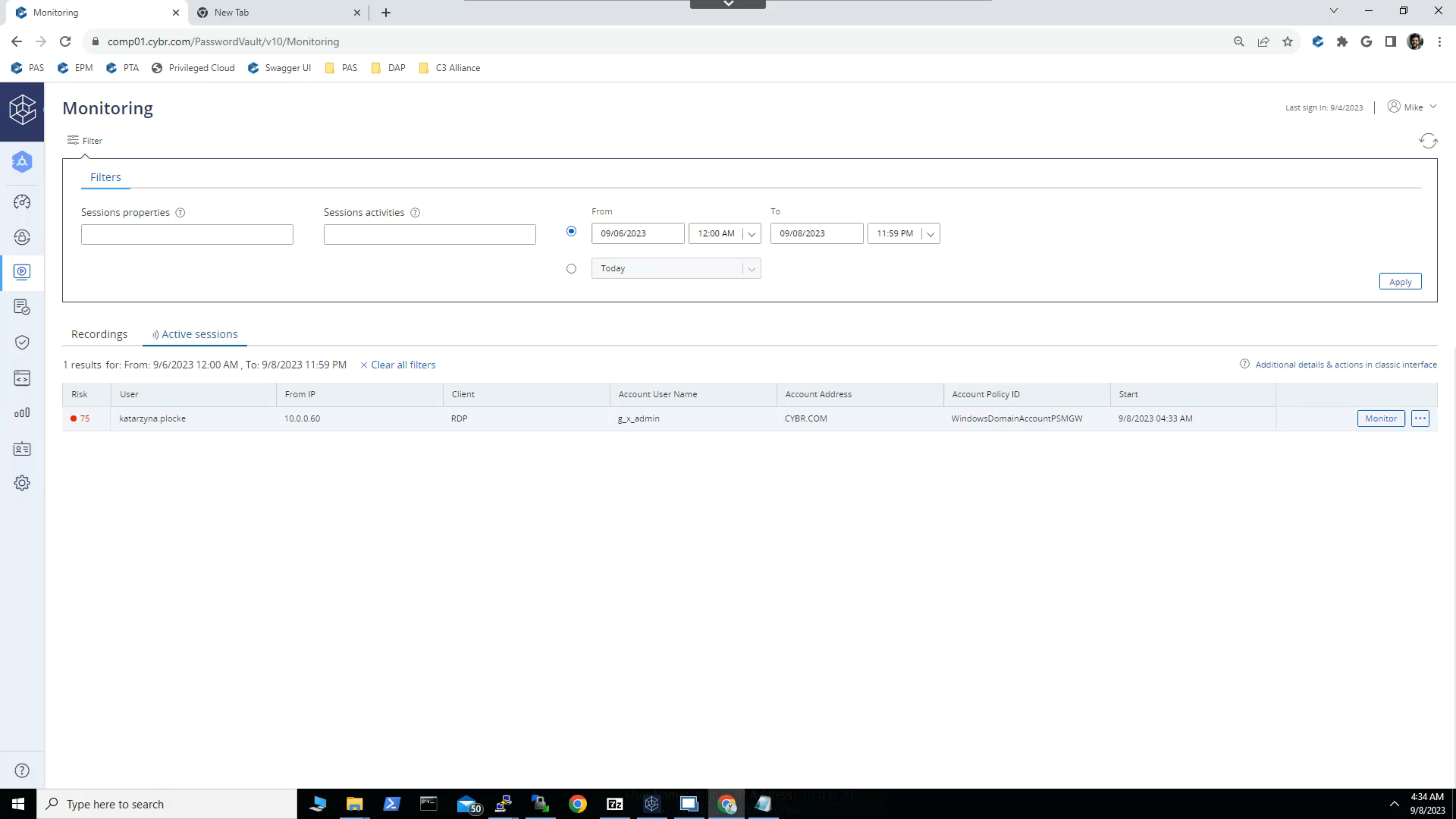
Allowed working hours: All day

Invited by: Bartosz Krynski (Administrator)

Privileged Access Manager (PAM) applications

PVWA

Site name: Cyberark Datacenter Warsaw v13



Monitoring

Sessions properties

Sessions activities

● From 09/06/2023 12:00 AM To 09/08/2023 11:59 PM

○ Today

1 results for: From: 9/6/2023 12:00 AM , To: 9/8/2023 11:59 PM ✕ Clear all filters

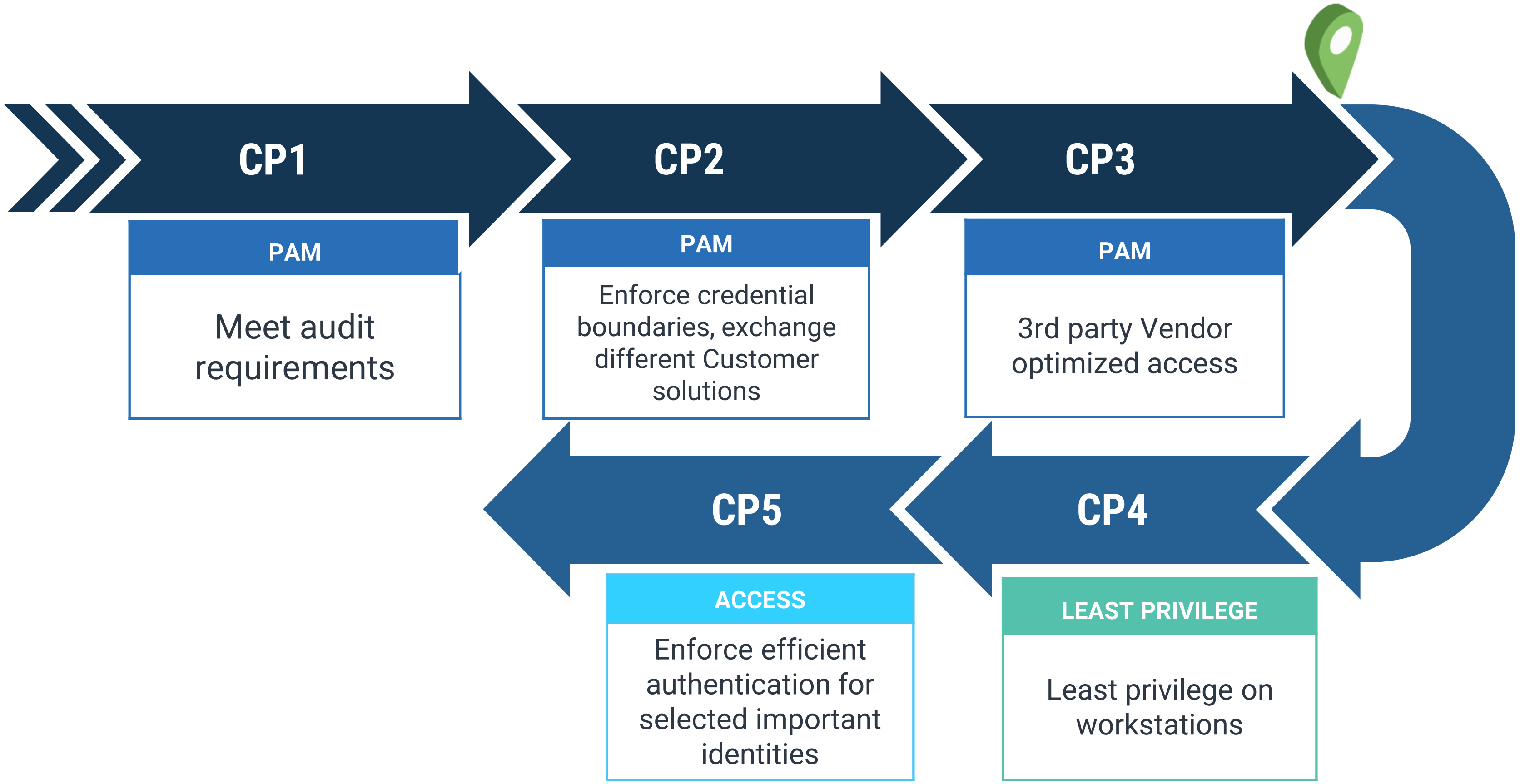
Additional details & actions in classic interface

Risk	User	From IP	Client	Account User Name	Account Address	Account Policy ID	Start
● 75	katarzyna.plocke	10.0.0.60	RDP	g_x_admin	CYBR.COM	WindowsDomainAccountPSMGW	9/8/2023 04:33 AM

Identity Security project plan

Legend

- 📍 Strategy Refresh
- 🟦 Access Controls
- 🟦 PAM Controls
- 🟩 Least Privilege Controls
- 🟥 Secrets Management Controls



CP1

PAM

Meet audit requirements

CP2

PAM

Enforce credential boundaries, exchange different Customer solutions

CP3

PAM

3rd party Vendor optimized access

CP4

LEAST PRIVILEGE

Least privilege on workstations

CP5

ACCESS

Enforce efficient authentication for selected important identities

Threat Mitigation Techniques

Leading authorities consistently rank these critical controls as priorities:

Control Admin Rights

Controlling or removing admin rights to prevent attackers from escalating privileges and moving laterally

Application Allowlist

Controlling applications allowed to execute

Application Patching

Patching applications against known vulnerabilities

OS Patching

Patching operating systems against known vulnerabilities

PSN Public Services Network

GCHQ

CBEST

USGCB

SANS

HIPAA

PCI DSS COMPLIANT

SOX Sarbanes-Oxley Compliance

…Detection technologies are much further down the list

ENFORCE LEAST PRIVILEGE AT THE ENDPOINT

Least Privilege

Remove local admin rights on Windows workstations, servers, and Macs.

Application control

Software inventory, application groups and policy-based start-up and privilege control

JIT elevation

Policy-based audited JIT sessions with MFA step-up

PROTECT FROM RANSOWMARE AND DEFEND CREDENTIALS

Credential defense

Active protection for Windows and browser credentials and credential stores

Ransomware protection

Multi-layered protection at every stage of attack

Privilege Deception

Deception components in the attack path.

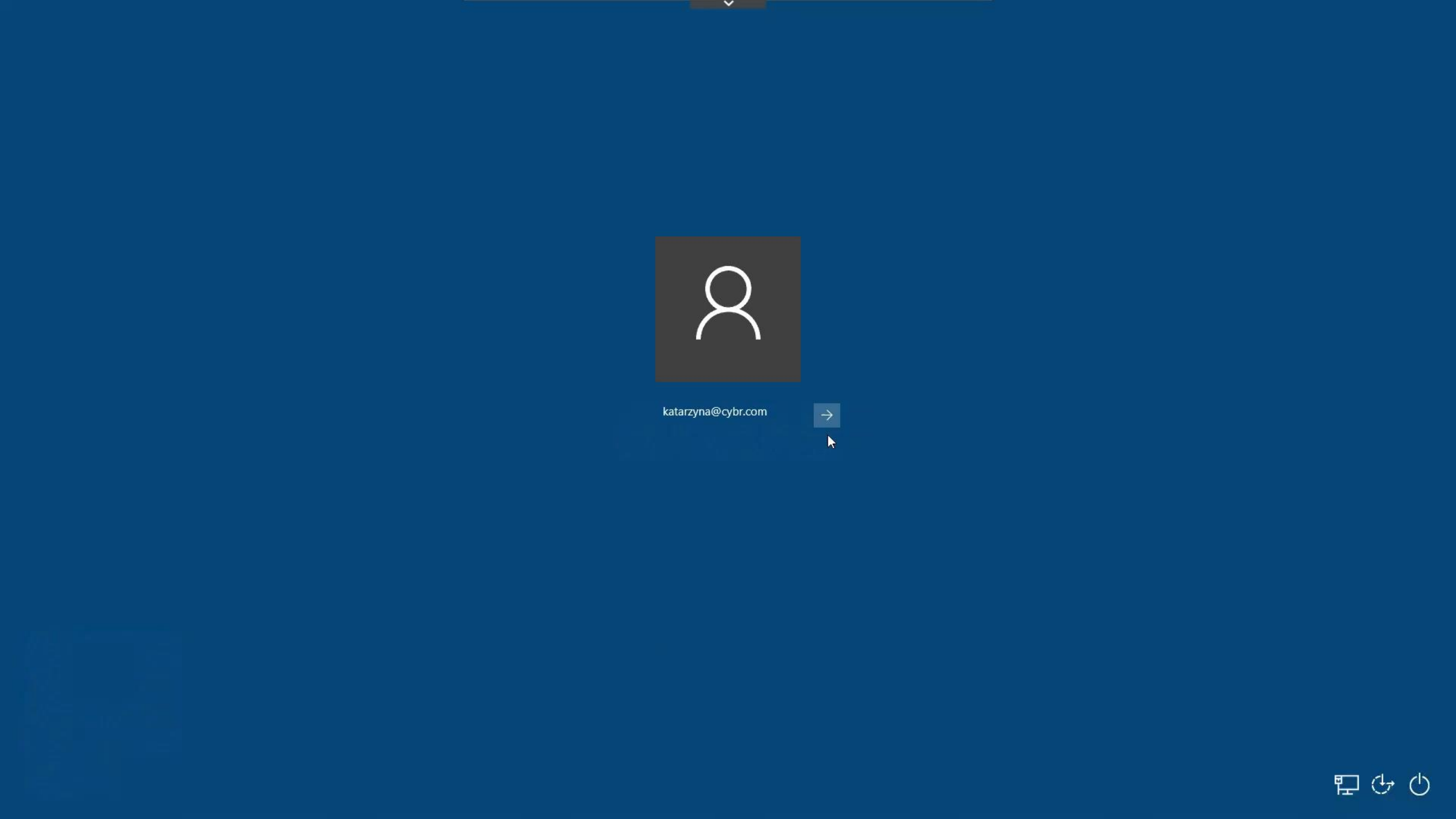
CyberArk Workforce Identity Portfolio

Core Capabilities

- Single Sign-On
- Adaptive Multi-Factor Authentication
- Lifecycle Management
- Directory Services
- Workforce Password Management
- User Behavior Analytics

Add-On Capabilities

- Secure Web Sessions
- Application Gateway
- Identity Flows
- Identity Compliance



katarzyna@cybr.com

Identity Security project plan

Legend

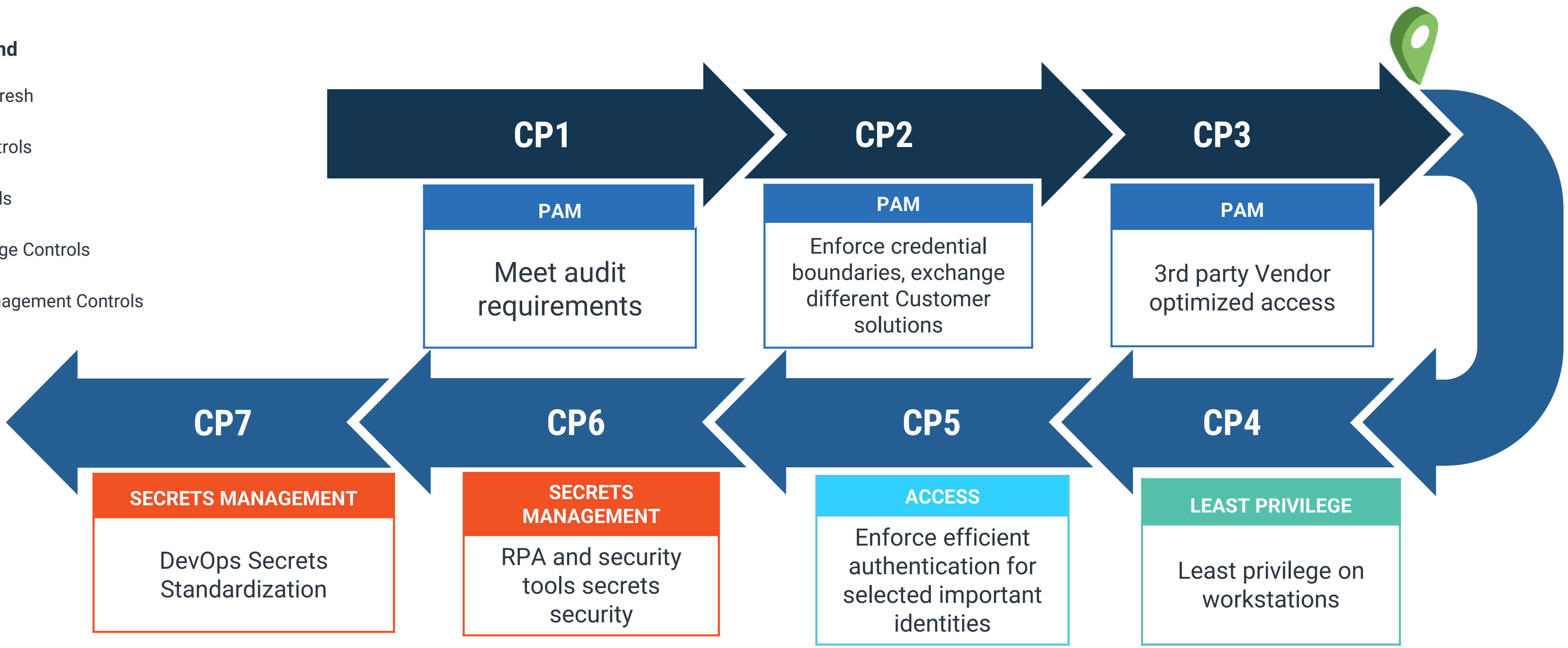
📍 Strategy Refresh

🟦 Access Controls

🟦 PAM Controls

🟩 Least Privilege Controls

🟥 Secrets Management Controls



CP1 – PAM: Meet audit requirements

CP2 – PAM: Enforce credential boundaries, exchange different Customer solutions

CP3 – PAM: 3rd party Vendor optimized access

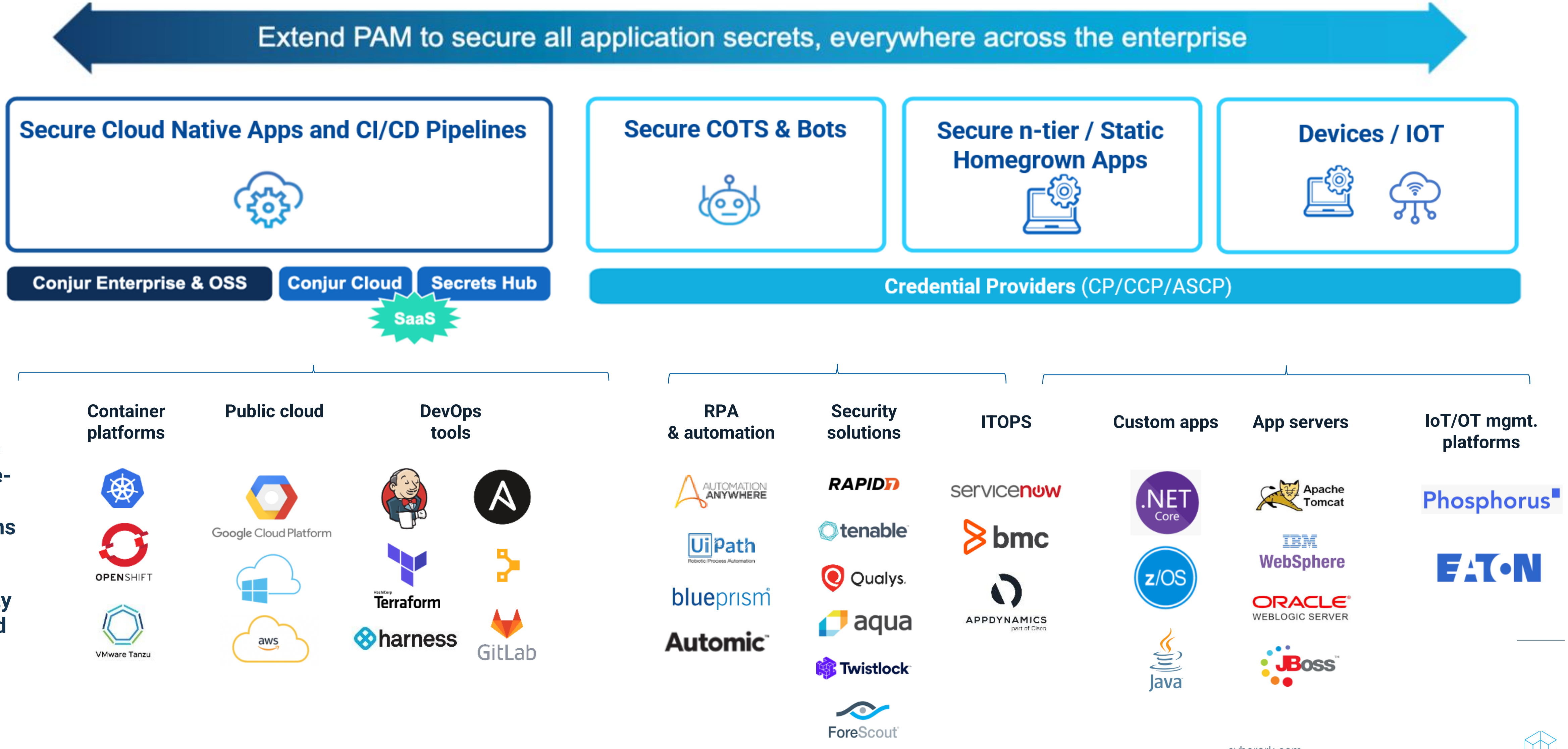
CP4 – LEAST PRIVILEGE: Least privilege on workstations

CP5 – ACCESS: Enforce efficient authentication for selected important identities

CP6 – SECRETS MANAGEMENT: RPA and security tools secrets security

CP7 – SECRETS MANAGEMENT: DevOps Secrets Standardization

CyberArk Secrets Management Solutions



Extend PAM to secure all application secrets, everywhere across the enterprise

- **Secure Cloud Native Apps and CI/CD Pipelines**: Conjur Enterprise & OSS | Conjur Cloud | Secrets Hub (SaaS)
- **Secure COTS & Bots**
- **Secure n-tier / Static Homegrown Apps**
- **Devices / IOT**

The last three areas: Credential Providers (CP/CCP/ASCP)

Over 200 out-of-the-box integrations

+

community supported

Container platforms
- OPENSHIFT
- VMware Tanzu

Public cloud
- Google Cloud Platform
- aws

DevOps tools
- HashiCorp Terraform
- harness
- GitLab

RPA & automation
- AUTOMATION ANYWHERE
- UiPath Robotic Process Automation
- blueprism
- Automic

Security solutions
- RAPID7
- tenable
- Qualys.
- aqua
- Twistlock
- ForeScout

ITOPS
- servicenow
- bmc
- APPDYNAMICS part of Cisco

Custom apps
- .NET Core
- z/OS
- Java

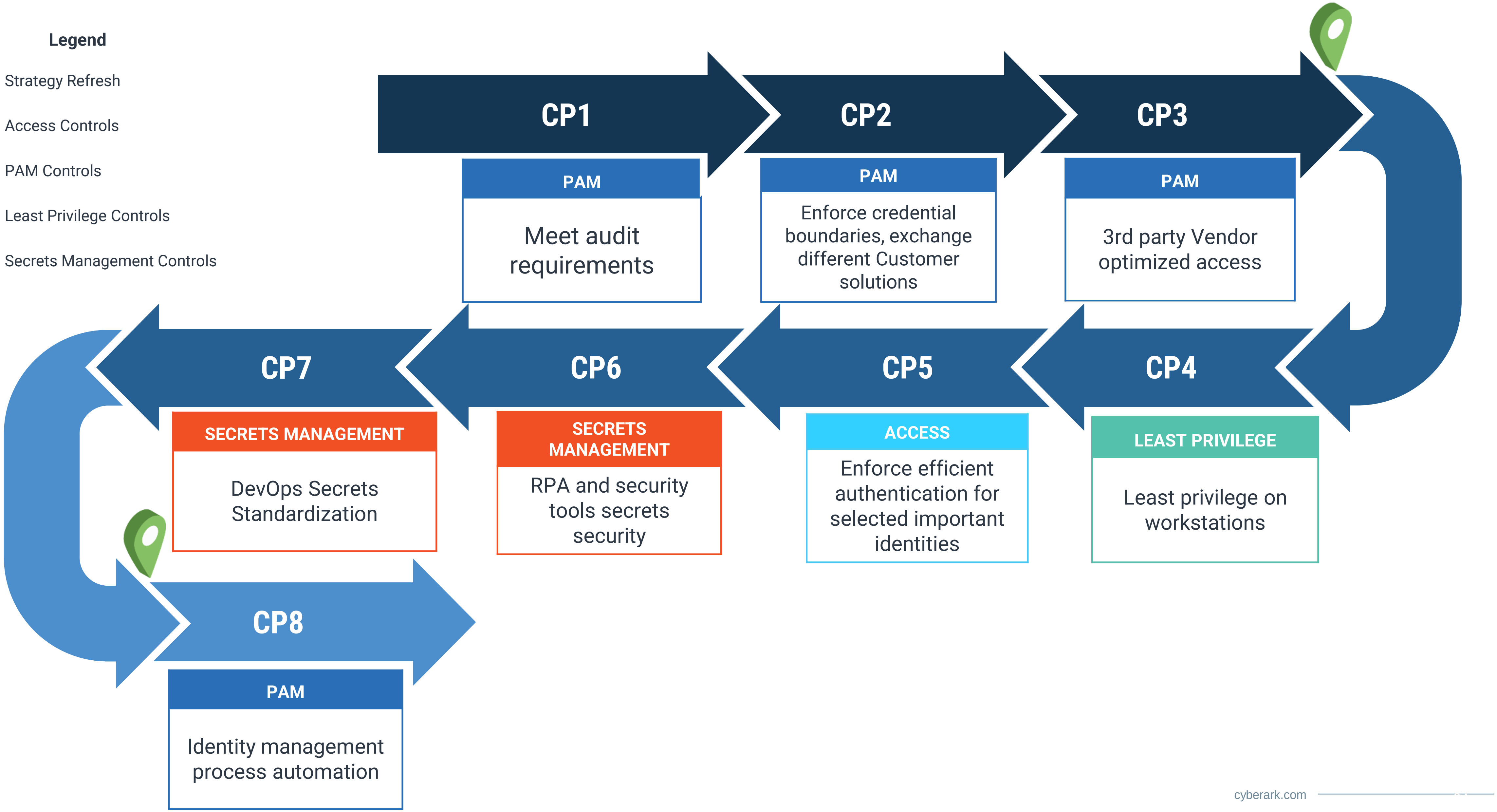
App servers
- Apache Tomcat
- IBM WebSphere
- ORACLE WEBLOGIC SERVER
- JBoss

IoT/OT mgmt. platforms
- Phosphorus
- EATON

Identity Security project plan

Legend

- 📍 Strategy Refresh
- 🟦 Access Controls
- 🟦 PAM Controls
- 🟩 Least Privilege Controls
- 🟥 Secrets Management Controls



CP1 — PAM: Meet audit requirements

CP2 — PAM: Enforce credential boundaries, exchange different Customer solutions

CP3 — PAM: 3rd party Vendor optimized access

CP4 — LEAST PRIVILEGE: Least privilege on workstations

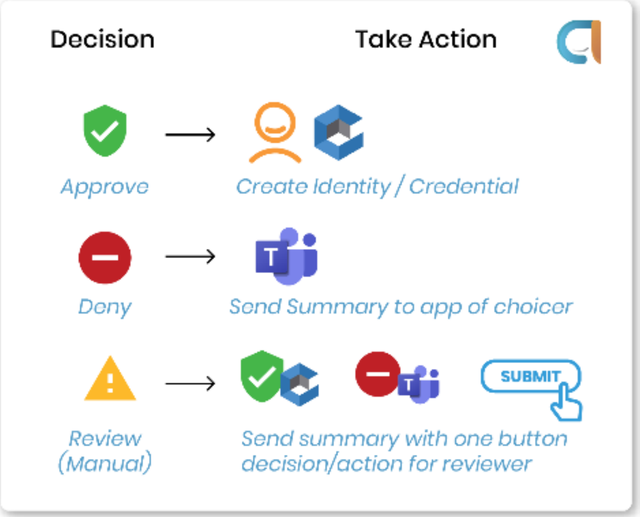
CP5 — ACCESS: Enforce efficient authentication for selected important identities

CP6 — SECRETS MANAGEMENT: RPA and security tools secrets security

CP7 — SECRETS MANAGEMENT: DevOps Secrets Standardization

CP8 — PAM: Identity management process automation

CyberArk Identity Flows



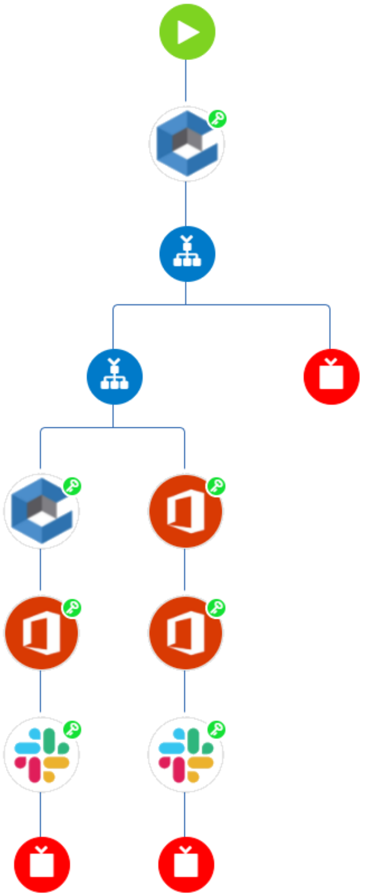
Decision

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

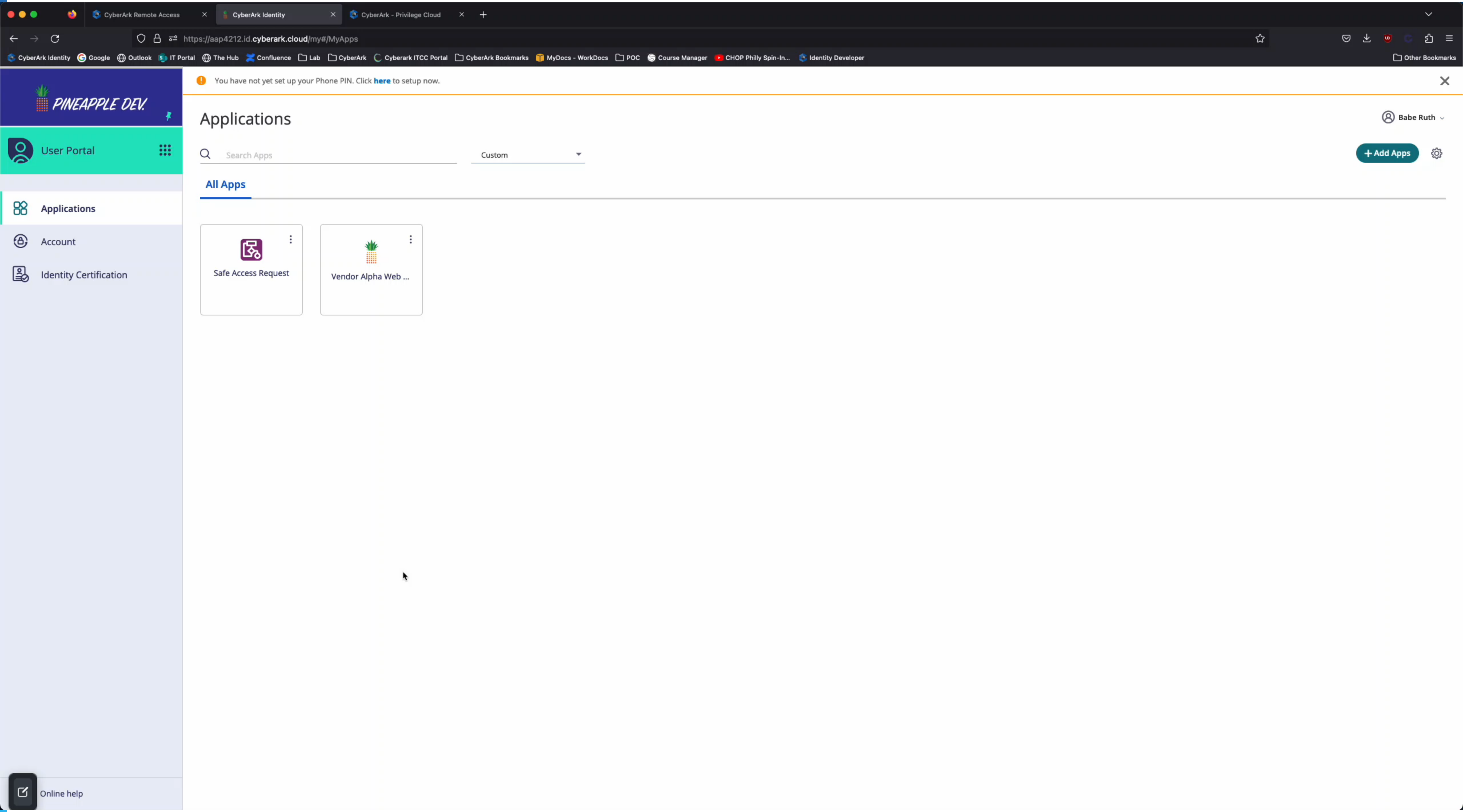
Easily create complex workflows to get any data into any app or take actions based on specific triggers

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

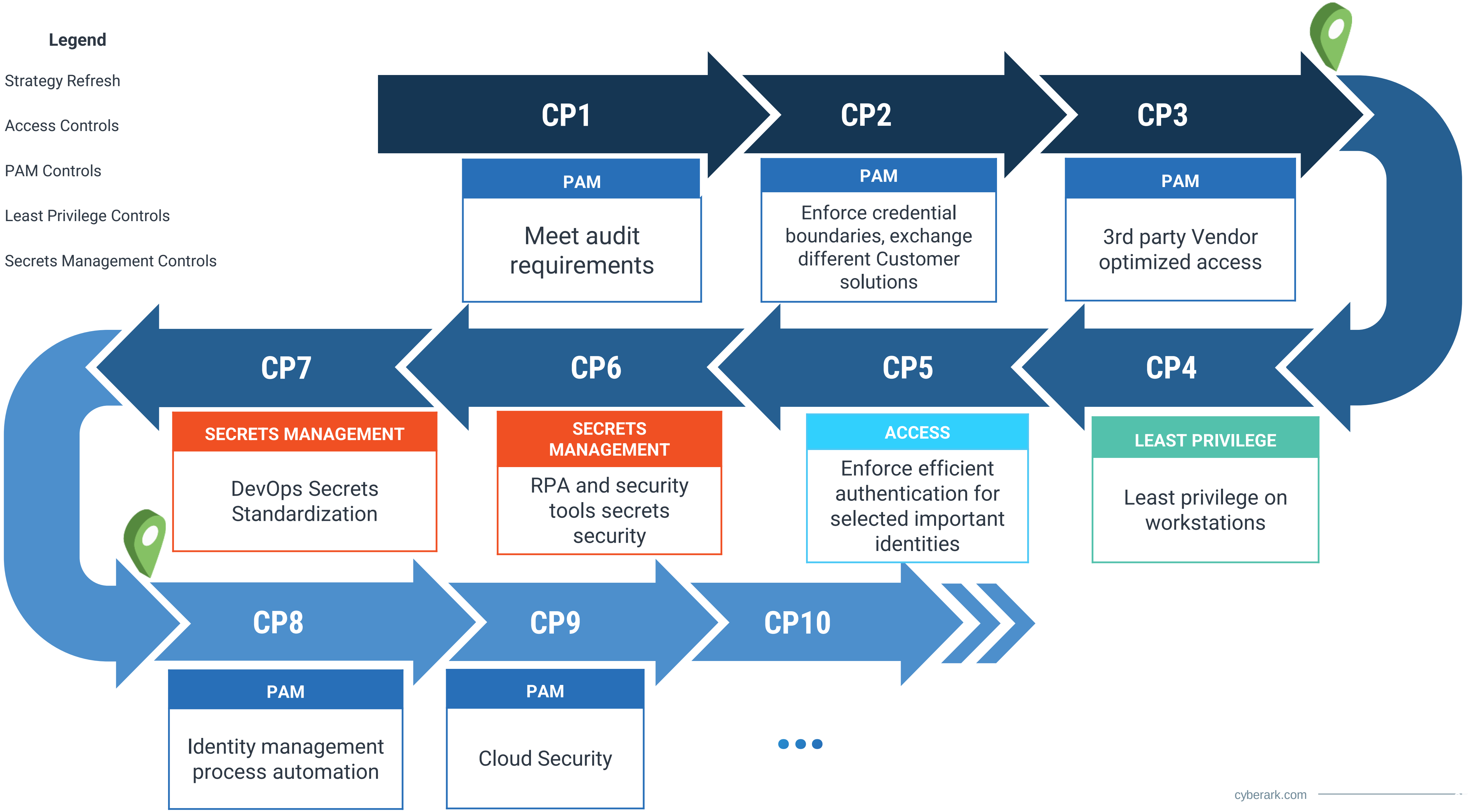


You have not yet set up your Phone PIN. Click here to setup now.

Identity Security project plan

Legend

- 📍 Strategy Refresh
- 🟦 Access Controls
- 🟦 PAM Controls
- 🟩 Least Privilege Controls
- 🟧 Secrets Management Controls



CP1

PAM

Meet audit requirements

CP2

PAM

Enforce credential boundaries, exchange different Customer solutions

CP3

PAM

3rd party Vendor optimized access

CP4

LEAST PRIVILEGE

Least privilege on workstations

CP5

ACCESS

Enforce efficient authentication for selected important identities

CP6

SECRETS MANAGEMENT

RPA and security tools secrets security

CP7

SECRETS MANAGEMENT

DevOps Secrets Standardization

CP8

PAM

Identity management process automation

CP9

PAM

Cloud Security

CP10

•••

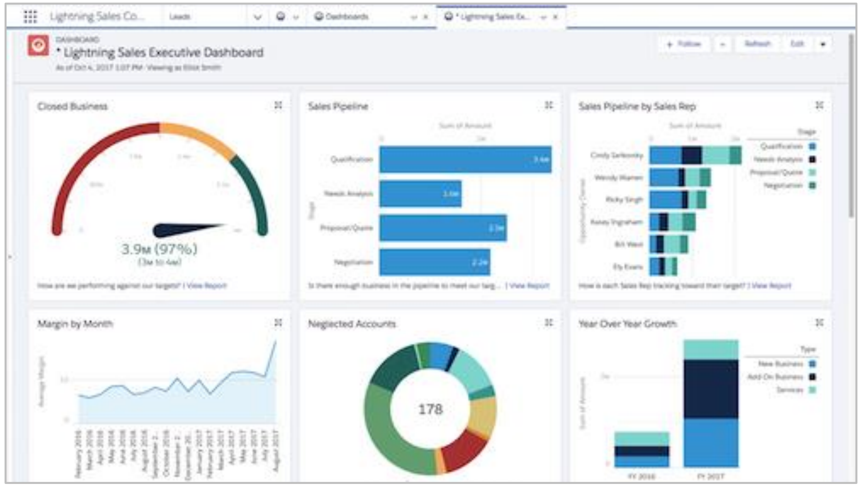
Different Environments Require Different Methods

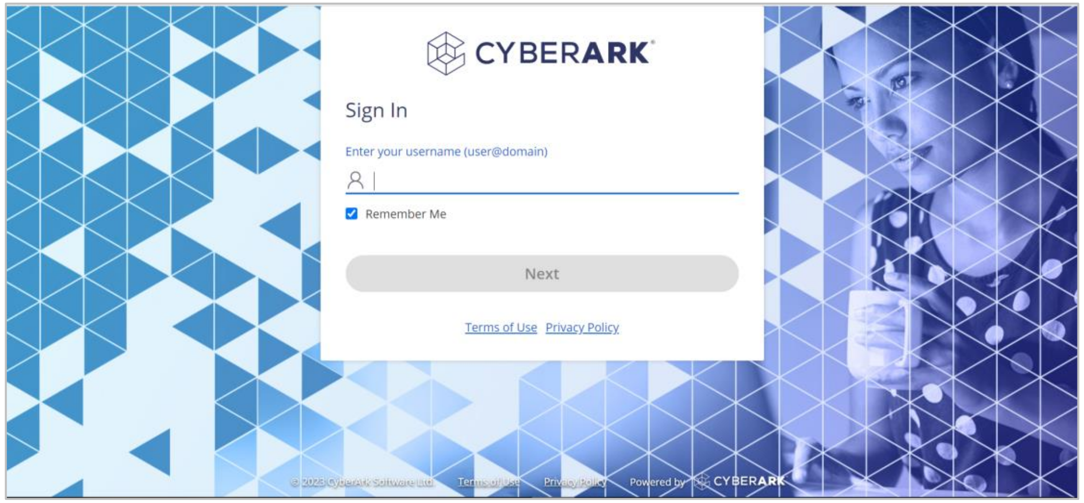
Secure access for ***human identities*** at every layer of your cloud estate.

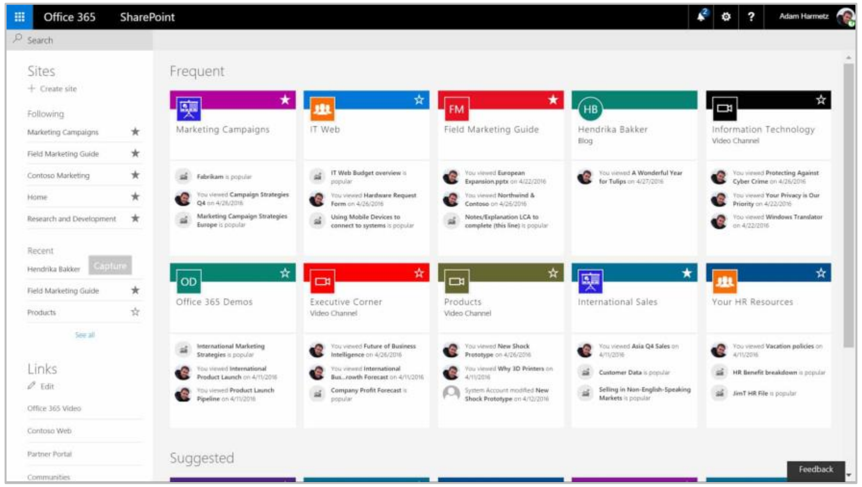
Use Case	Methods	Environments
Secure access to Third party **SaaS apps.**	Session protection + monitoring	salesforce workday. Epic zendesk DATADOG
Secure access to lift-and-shift workloads running **inside the VMs.**	Vaulted, Isolated access for standing accounts & system access	Microsoft SQL Server Windows Server Linux SAP servicenow CHECK POINT paloalto NETWORKS ORACLE
Secure access to workloads **ON** cloud Infrastructure (IaaS).	Dynamic, Just-In-Time access	Linux Windows Server kubernetes PostgreSQL redis docker
Secure access to CSP services **IN** the cloud.	Native, Zero Standing Privilege access	aws Azure Google Cloud

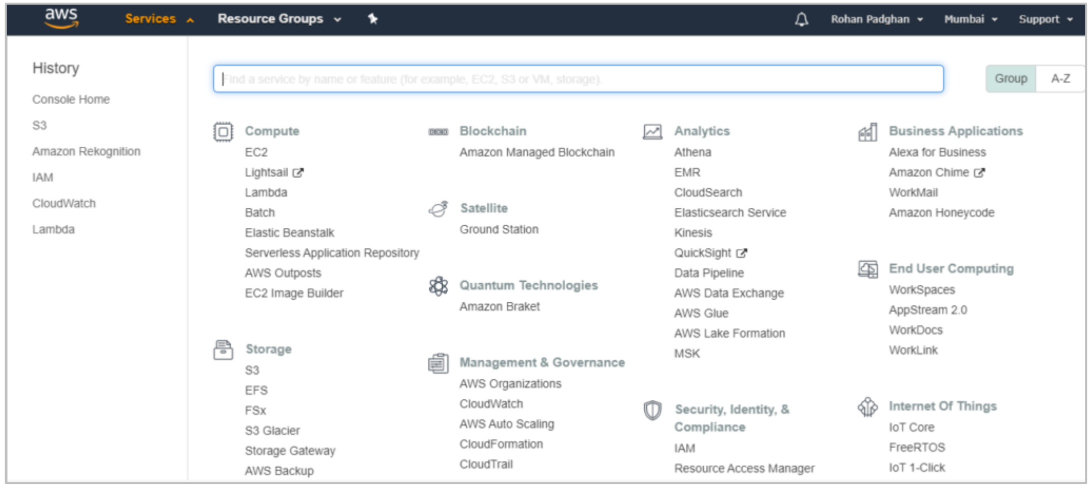
Copyright © 2023 CyberArk Software Ltd. All rights reserved

What’s In Common?





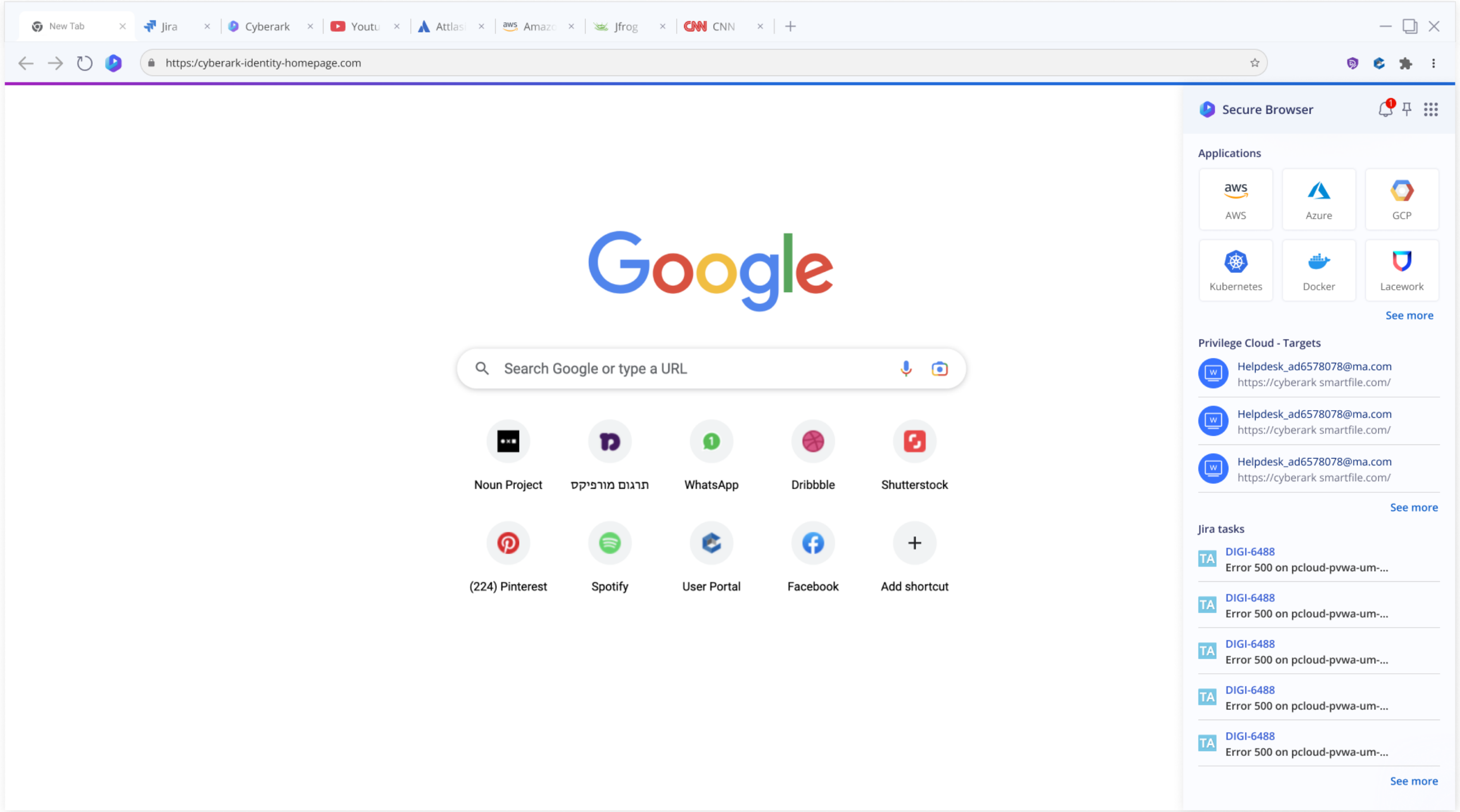




It’s a new attack vector, 50% increase in attacks targeting Chrome browser

*WatchGuard, "Internet Security Report, Q2 2022," 2022

Introducing CyberArk Secure Browser



Secure Browser

Applications

AWS | Azure | GCP | Kubernetes | Docker | Lacework

See more

Privilege Cloud - Targets

Helpdesk_ad6578078@ma.com
https://cyberark smartfile.com/

Helpdesk_ad6578078@ma.com
https://cyberark smartfile.com/

Helpdesk_ad6578078@ma.com
https://cyberark smartfile.com/

See more

Jira tasks

TA DIGI-6488
Error 500 on pcloud-pvwa-um-...

TA DIGI-6488
Error 500 on pcloud-pvwa-um-...

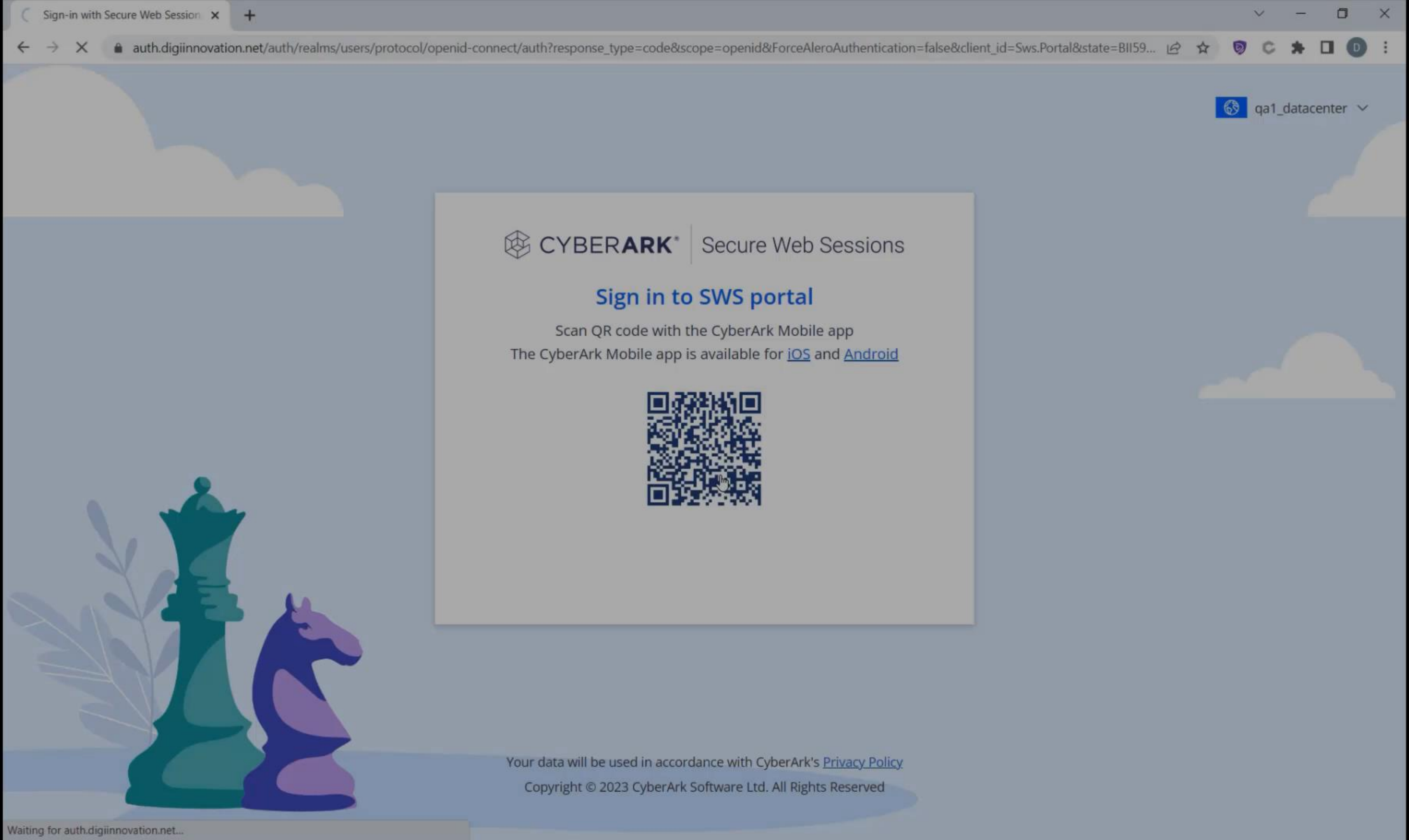
TA DIGI-6488
Error 500 on pcloud-pvwa-um-...

TA DIGI-6488
Error 500 on pcloud-pvwa-um-...

TA DIGI-6488
Error 500 on pcloud-pvwa-um-...

See more

Extend Identity Security controls to web browsing on managed and unmanaged devices



Sign-in with Secure Web Session
auth.digiinnovation.net/auth/realms/users/protocol/openid-connect/auth?response_type=code&scope=openid&ForceAleroAuthentication=false&client_id=Sws.Portal&state=BII59...
qa1_datacenter
CYBERARK
Secure Web Sessions

Sign in to SWS portal

Scan QR code with the CyberArk Mobile app

The CyberArk Mobile app is available for iOS and Android

Your data will be used in accordance with CyberArk's Privacy Policy

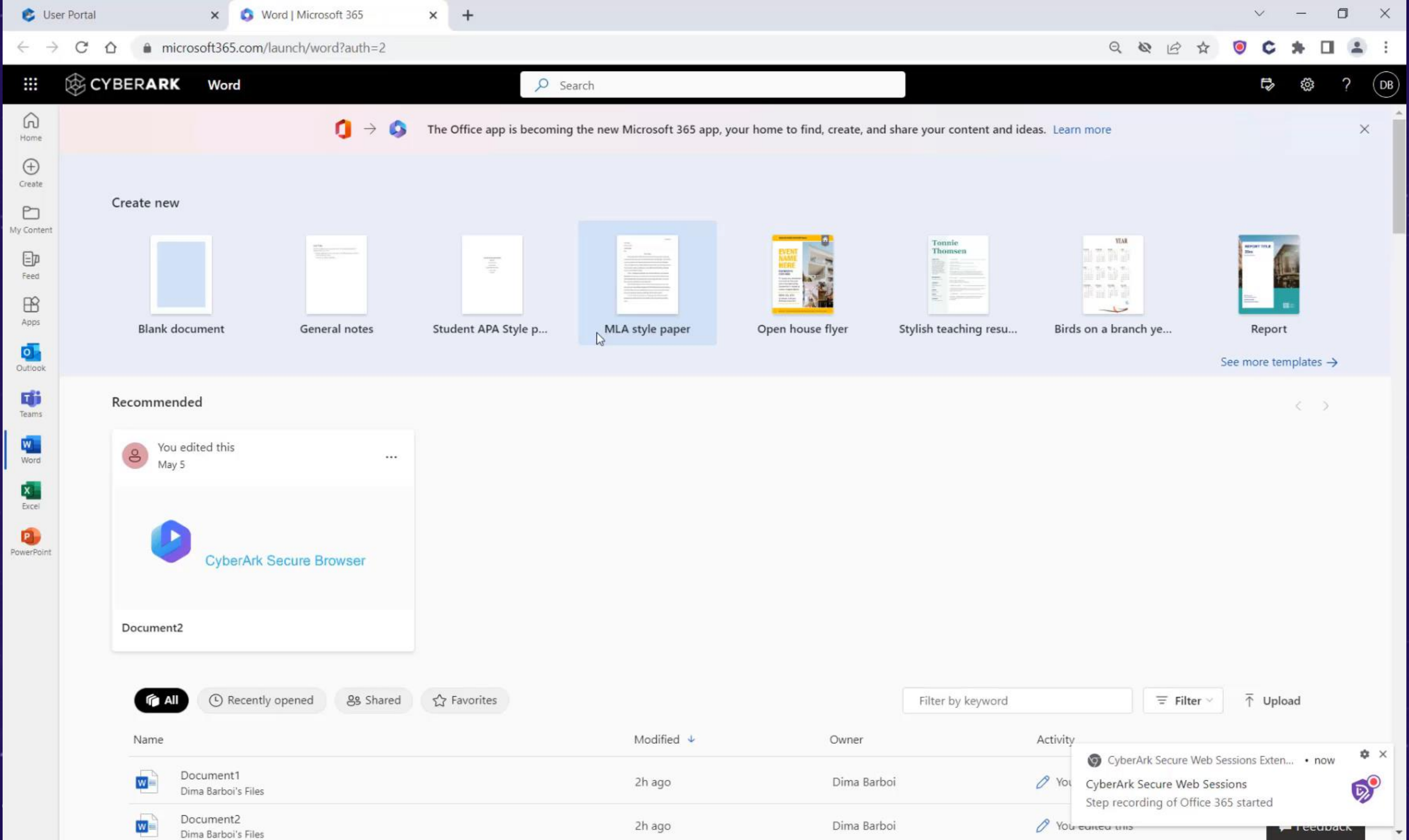
Copyright © 2023 CyberArk Software Ltd. All Rights Reserved

Waiting for auth.digiinnovation.net...

Recycle Bin
Google Chrome
RED TEAM

Cookieless Browsing

Copyright © 2023 CyberArk Software Ltd. All rights reserved



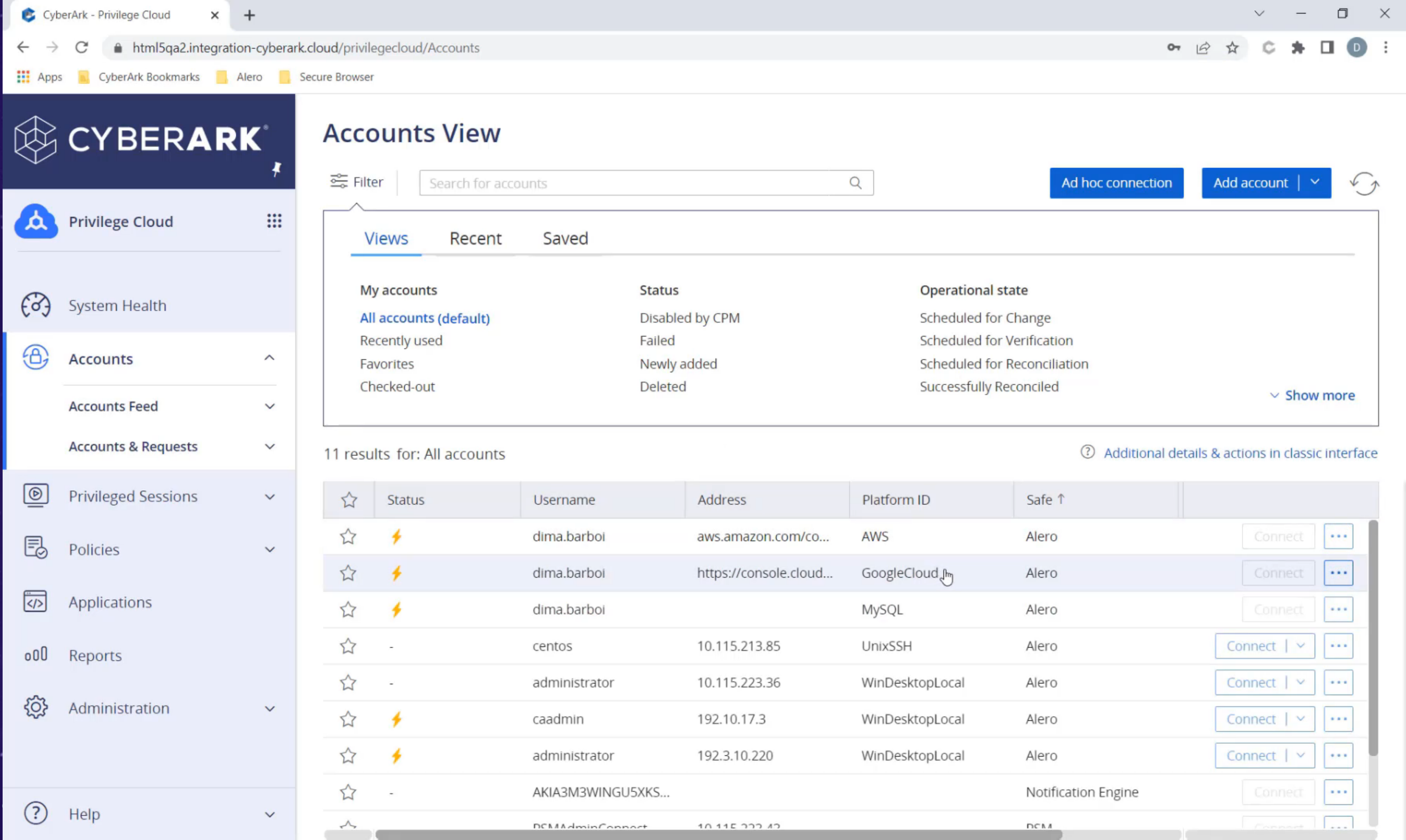
The Office app is becoming the new Microsoft 365 app, your home to find, create, and share your content and ideas.

Create new

You edited this
May 5
Document2

Name	Modified	Owner	Activity
Document1 Dima Barboi's Files	2h ago	Dima Barboi	You
Document2 Dima Barboi's Files	2h ago	Dima Barboi	You edited this

CyberArk Secure Web Sessions Exten... • now
CyberArk Secure Web Sessions
Step recording of Office 365 started



CyberArk - Privilege Cloud

html5qa2.integration-cyberark.cloud/privilegecloud/Accounts

Apps | CyberArk Bookmarks | Alero | Secure Browser

Accounts View

My accounts	Status	Operational state
All accounts (default)	Disabled by CPM	Scheduled for Change
Recently used	Failed	Scheduled for Verification
Favorites	Newly added	Scheduled for Reconciliation
Checked-out	Deleted	Successfully Reconciled

11 results for: All accounts

☆	Status	Username	Address	Platform ID	Safe ↑	
☆	⚡	dima.barboi	aws.amazon.com/co...	AWS	Alero	Connect ···
☆	⚡	dima.barboi	https://console.cloud...	GoogleCloud	Alero	Connect ···
☆	⚡	dima.barboi		MySQL	Alero	Connect ···
☆	-	centos	10.115.213.85	UnixSSH	Alero	Connect ···
☆	-	administrator	10.115.223.36	WinDesktopLocal	Alero	Connect ···
☆	⚡	caadmin	192.10.17.3	WinDesktopLocal	Alero	Connect ···
☆	⚡	administrator	192.3.10.220	WinDesktopLocal	Alero	Connect ···
☆	-	AKIA3M3WINGU5XKS...			Notification Engine	Connect ···
☆		PSMAdminConnect	10.115.223.42		PSM	

Recycle Bin
Google Chrome
CyberArk Secure Browser

Contact us if you have any questions!

Katarzyna.Plocke@cyberark.com

Armands.Alvaters@bakotech.com

Bartosz.Krynski@cyberark.com

bako tech®