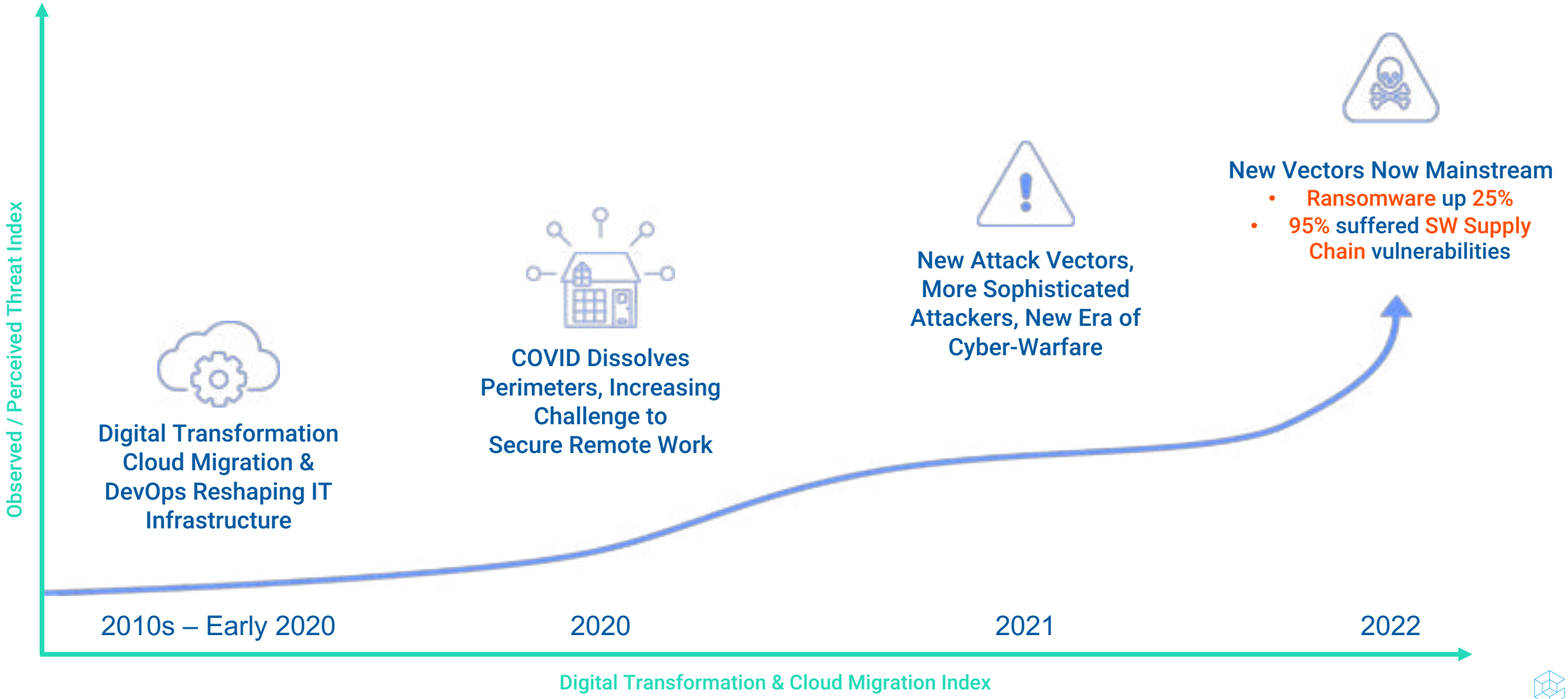
CYBERARK®

Privileged Access Manager
- Overview -

19th April 2023
TECH MORNINGS / DGS Event

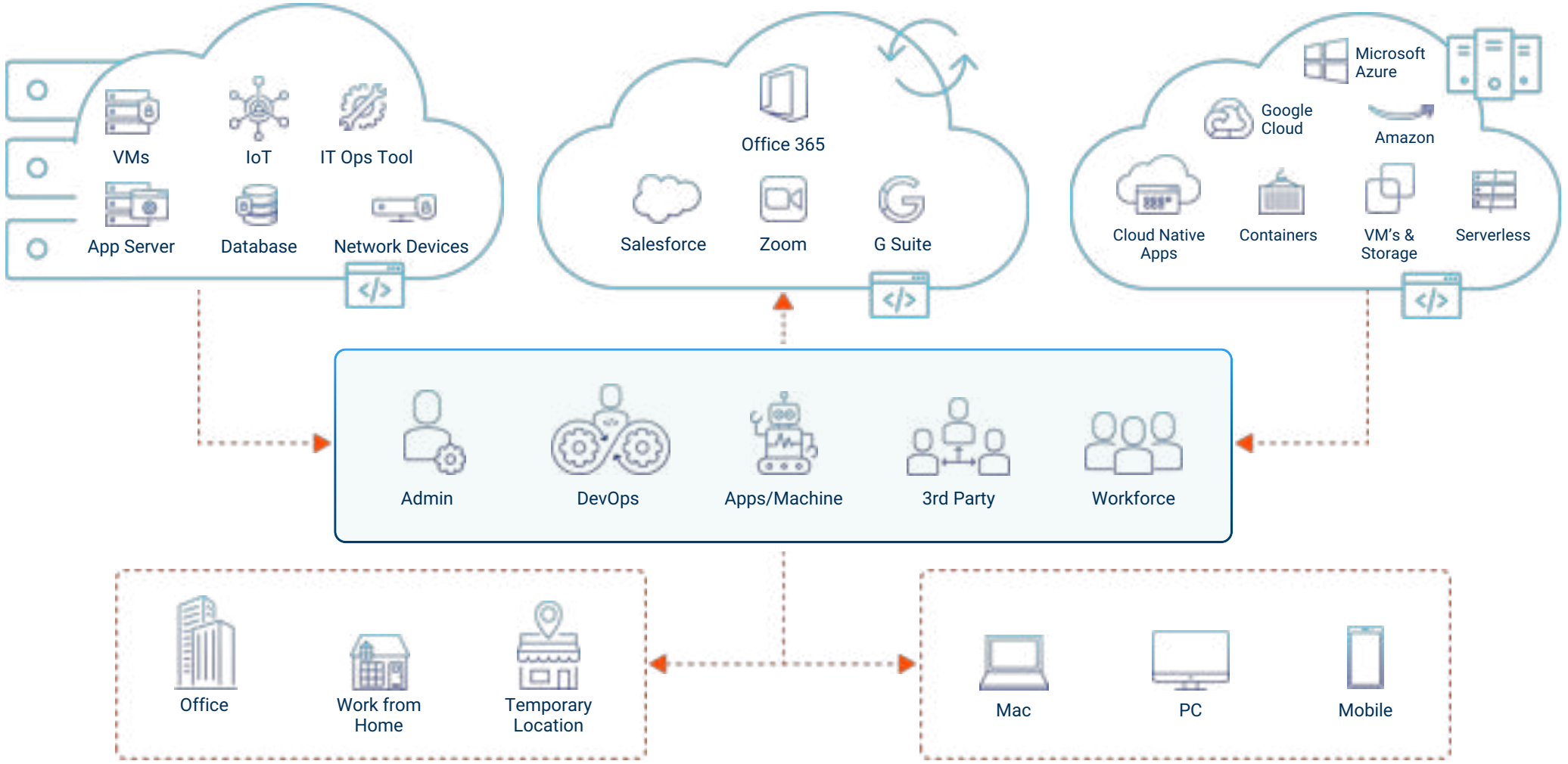
cyberark.is/identity-security

Cybersecurity Global Trends Keep Evolving

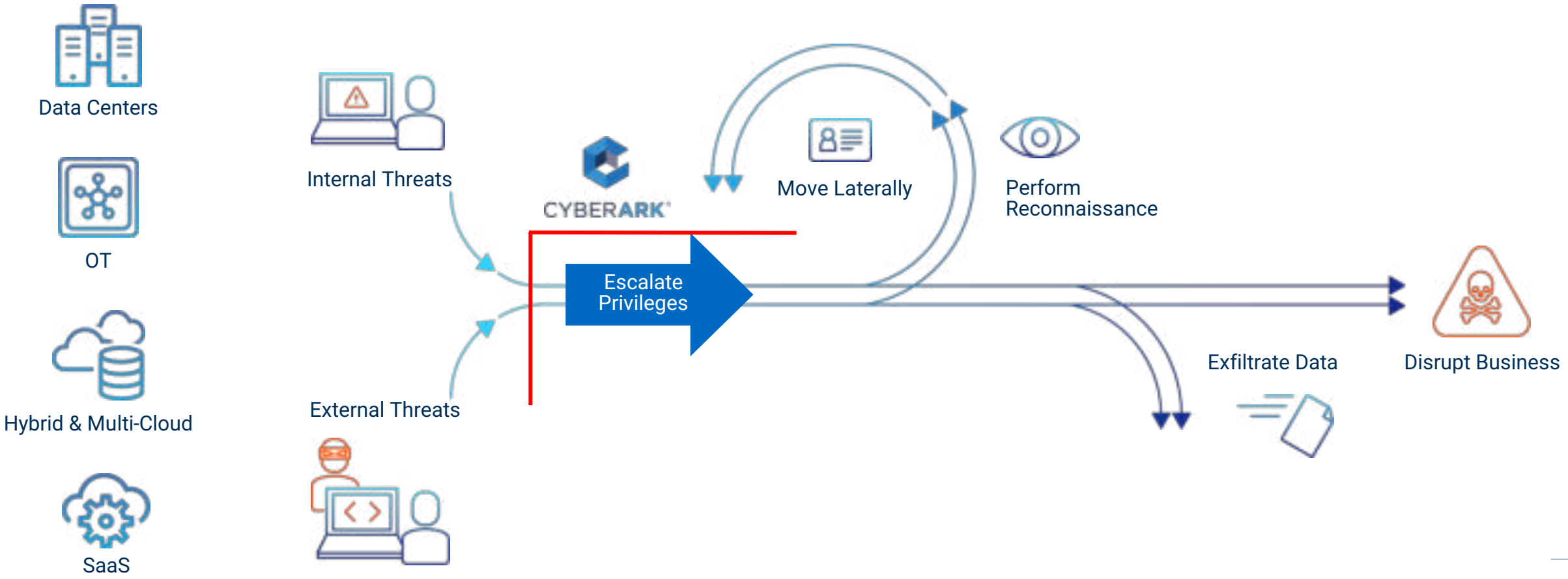


2022 Data Breach Investigation Report (DBIR) from Verizon

Privilege is everywhere. All identities can become privileged under certain conditions.



Your Environment Evolves, Attack Paths Don't



Securing Identities is Critical for Zero Trust

Identities

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

Devices may not be Enterprise Owned

Remove Implicit Trust

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

CyberArk Defines Identity Security as

Centered on intelligent **privilege controls,**

Identity Security

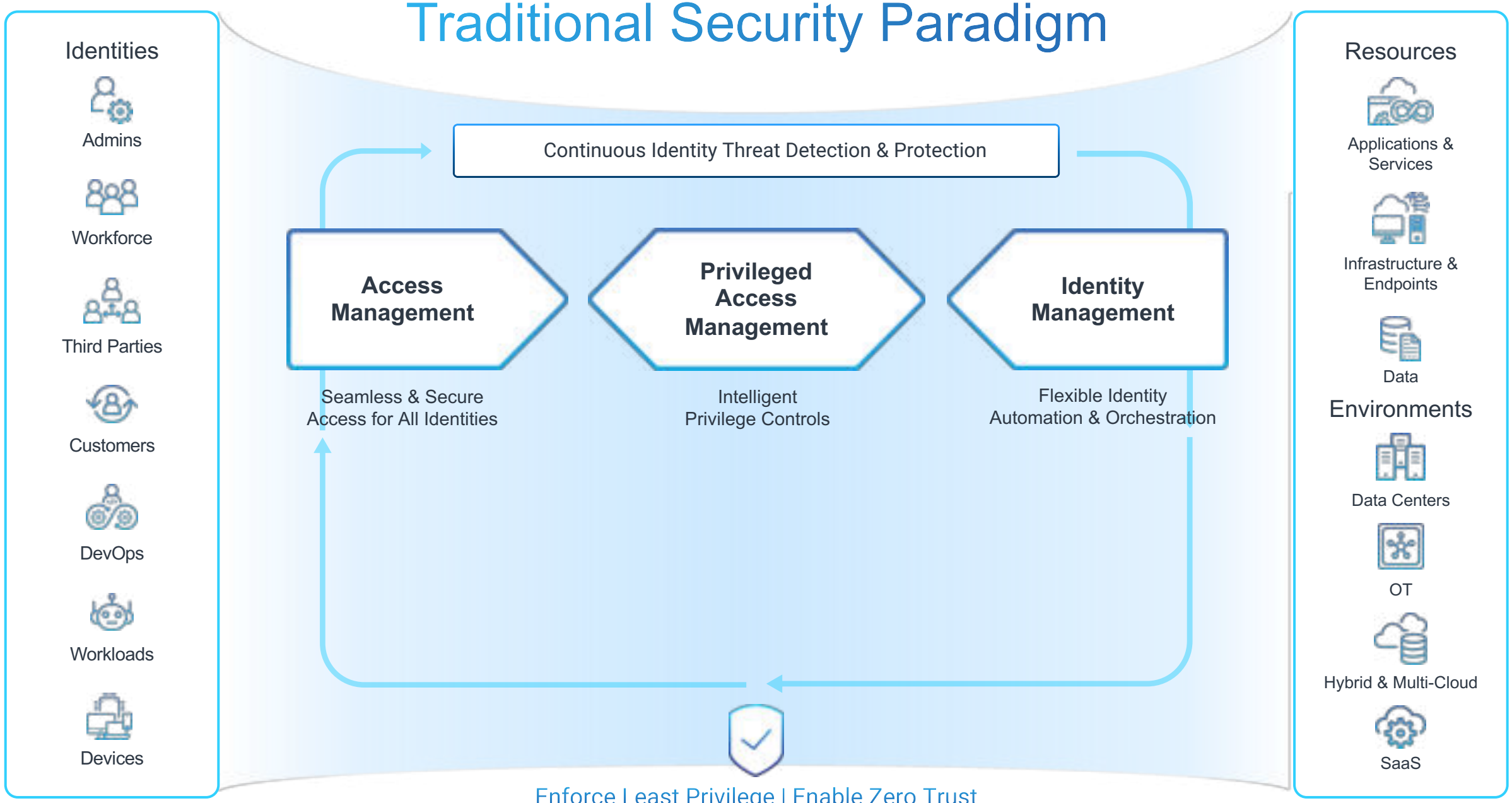
seamlessly **secures human and machine identities**

accessing workloads from **hybrid to multi-cloud,** and

flexibly **automates the identity lifecycle -**

all with **a unified approach**.

Traditional Security Paradigm



Modern Identity Security Defined

Identities

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

Continuous Identity Threat Detection & Protection

Seamless & Secure Access for All Identities	Intelligent Privilege Controls	Flexible Identity Automation & Orchestration
Secure Single Sign-On	Standing & Just-in-Time Access	Orchestration & Lifecycle Management
Authentication & Passwordless	Session Isolation & Monitoring	Permissions & Entitlements
Authorization & Adaptive Access	Elevation & Delegation	Directory & Federation Services
	Credentials & Secrets Management	

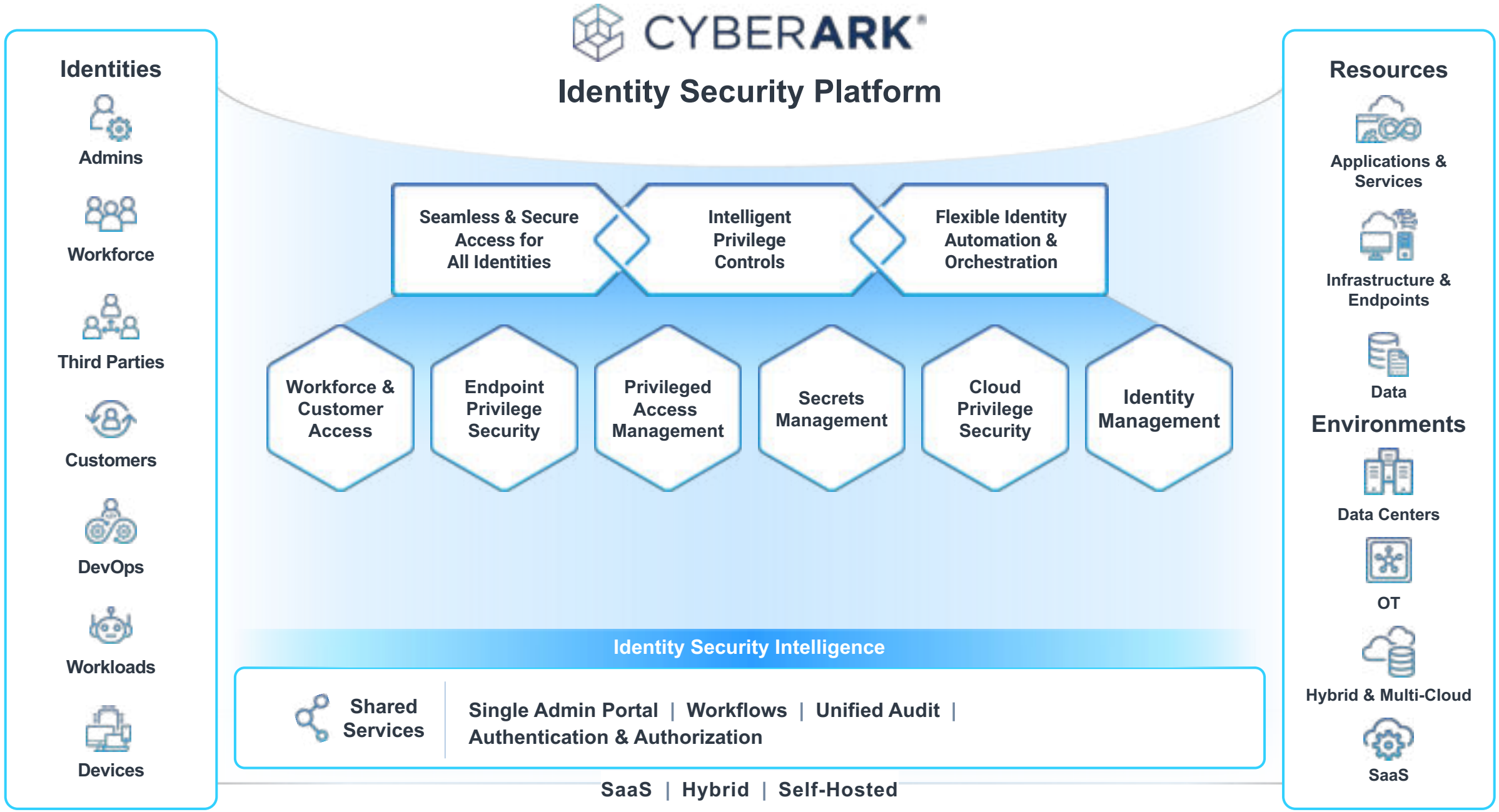
Enforce Least Privilege | Enable Zero Trust

Resources

- Applications & Services
- Infrastructure & Endpoints
- Data

Environments

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


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
Endpoint Privilege Security
Privileged Access Management
Secrets Management
Cloud Privilege Security
Identity Management
Identity Security Intelligence
Shared Services
Single Admin Portal | Workflows | Unified Audit |
Authentication & Authorization
SaaS | Hybrid | Self-Hosted
Resources
Applications & Services
Infrastructure & Endpoints
Data
Environments
Data Centers
OT
Hybrid & Multi-Cloud
SaaS

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

Identity Security Intelligence

Shared Services

Single Admin Portal | Workflows | Unified Audit | Authentication & Authorization

SaaS | Hybrid | Self-Hosted

Resources

- Applications & Services
- Infrastructure & Endpoints
- Data

Environments

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

CYBERARK®

C³ Alliance

200+ Certified Partners

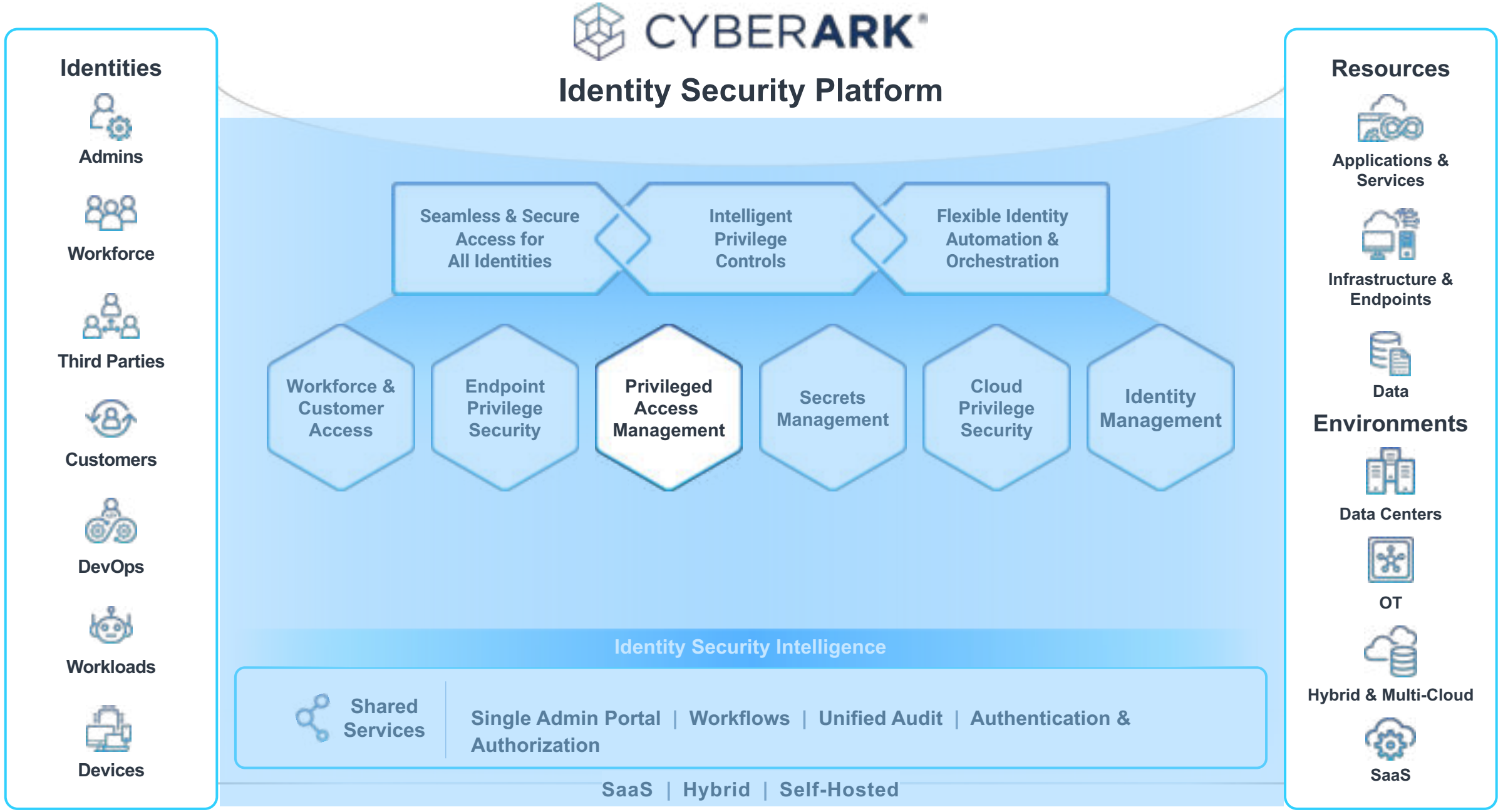
300+ Certified Joint Solutions

- Analytics
- ICS
- Identity & Access Management
- Authentication
- ITSM
- Detection
- Orchestration & Response
- DevOps
- Robotic Process Automation
- Discovery
- SIEM
- Governance
- HSM
- Vulnerability Management

200+ Plug-ins

- CPM Plug-ins
- PSM Plug-ins

Privileged Access Management


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
Endpoint Privilege Security
Privileged Access Management
Secrets Management
Cloud Privilege Security
Identity Management
Identity Security Intelligence
Shared Services
Single Admin Portal | Workflows | Unified Audit | Authentication & Authorization
SaaS | Hybrid | Self-Hosted
Resources
Applications & Services
Infrastructure & Endpoints
Data
Environments
Data Centers
OT
Hybrid & Multi-Cloud
SaaS

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

Privileged Identities – the PAM Solution

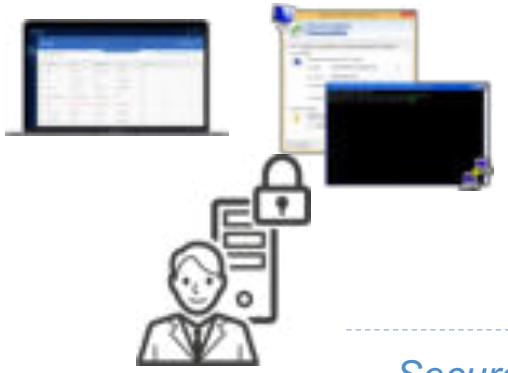
Secure Storage

Flexible Connection Methods

Analytics & Remediation

Password Rotation

Session Isolation & Monitoring



Privileged User

Secure connection to jump server

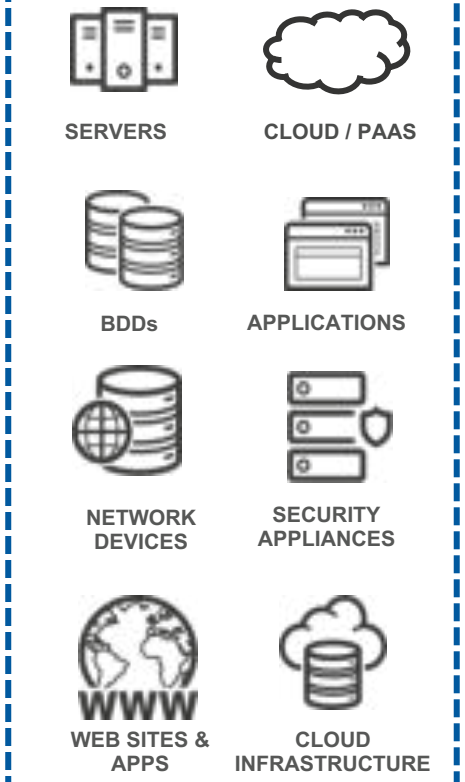
Password Rotation

Monitored Session to the target

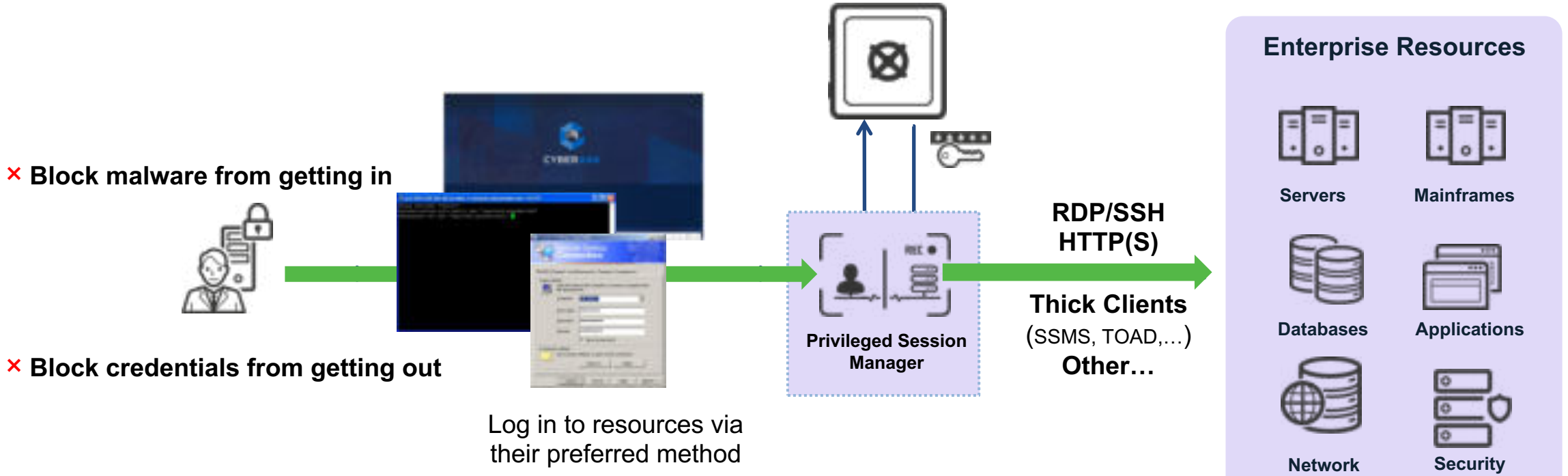
SIEM

Suspicious action
(ex: CyberArk bypass attempt)

ENTERPRISE RESOURCES



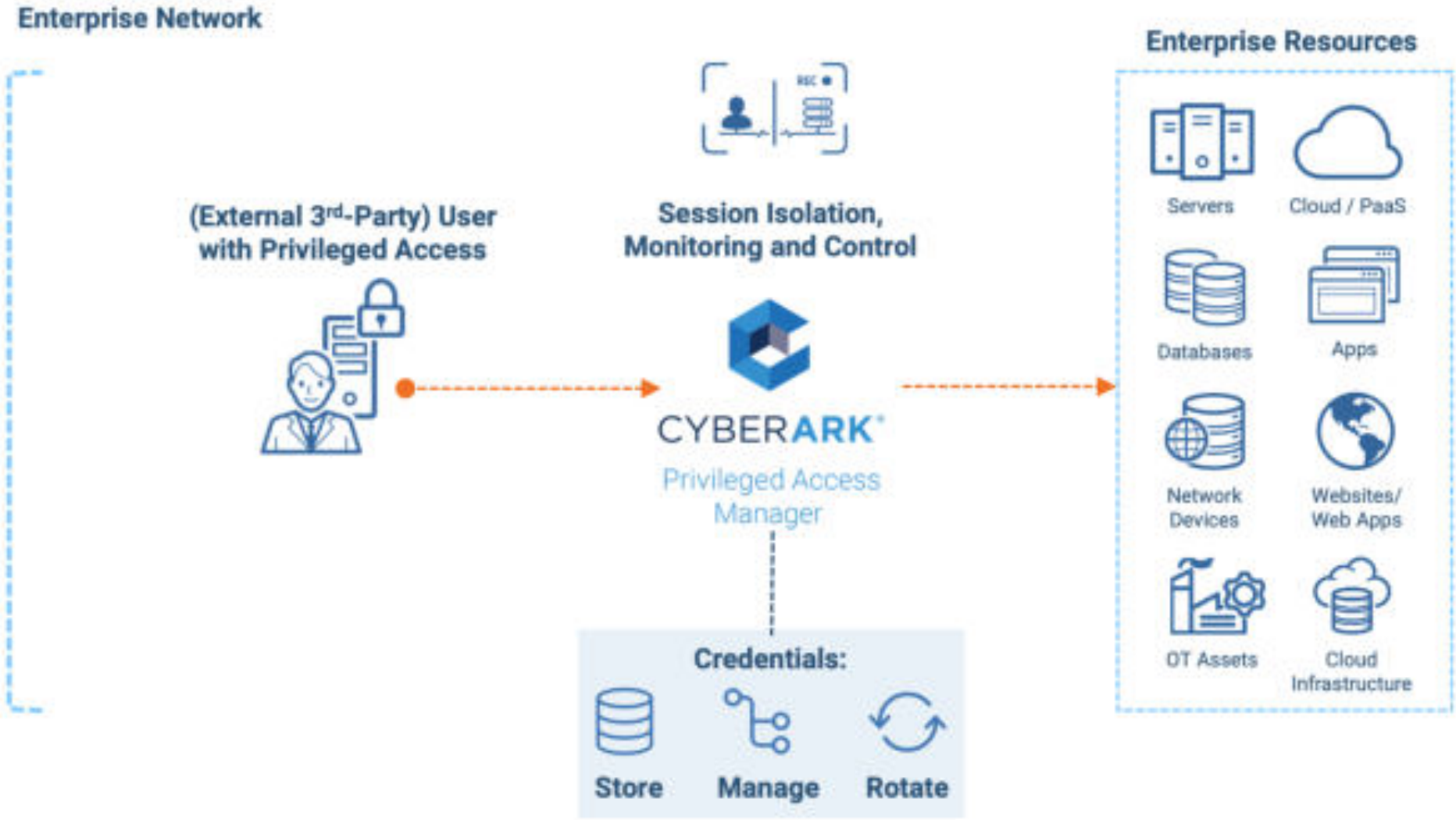
Session Isolation, Monitoring and Recording



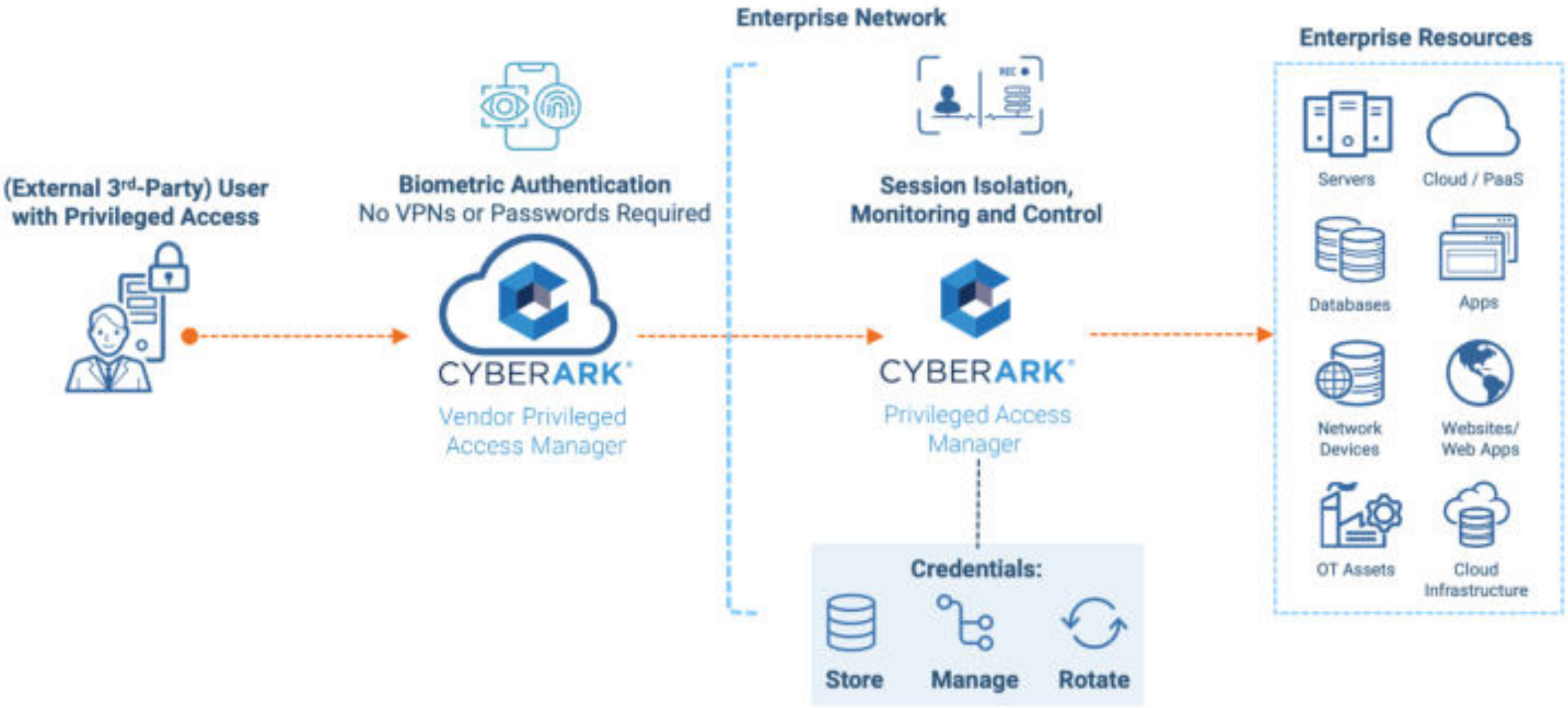
- Isolates sensitive assets from the rest of the infrastructure while still enabling necessary access
- Tracks and records user activity during privileged sessions
- Thwarts attacks by scoring and terminating sessions based on risk level

Remote Access (Vendor PAM)

Vendor PAM – How it Works



Vendor PAM – How it Works



Secrets Management

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
- Endpoint Privilege Security
- Privileged Access Management
- **Secrets Management**
- Cloud Privilege Security
- Identity Management

Identity Security Intelligence

Shared Services

Single Admin Portal | Workflows | Unified Audit | Authentication & Authorization

SaaS | Hybrid | Self-Hosted

Resources

- Applications & Services
- Infrastructure & Endpoints
- Data

Environments

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

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

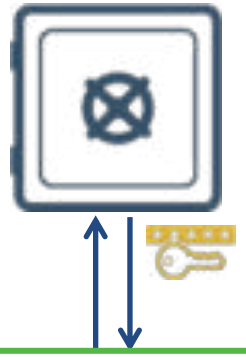
Accounts **created** for the use within / by automated processes and applications

NON-INTERACTIVE

Securing application secrets

Application Examples

Type	System
Application Servers	IBM, ORACLE WebLogic, Apache Tomcat, JBoss
CI/CD Tools Chains	Jenkins, Chef, Ansible, Terraform
Container Platforms /PaaS	OpenShift, kubernetes, Pivotal Cloud Foundry
SDKs & Dev. Libraries	Go, Java, Ruby, Python .NET, C/C++, CLI, REST
Multiple Platforms	Windows, *nix, zOS, Cloud
RPA	Automation Anywhere, WorkFusion, blueprism, UiPath
Security Tools	ForeScout, tenable, Qualys.
Other Third Party Applications	C3 alliance partners solution with built in AAM integration



AFTER:

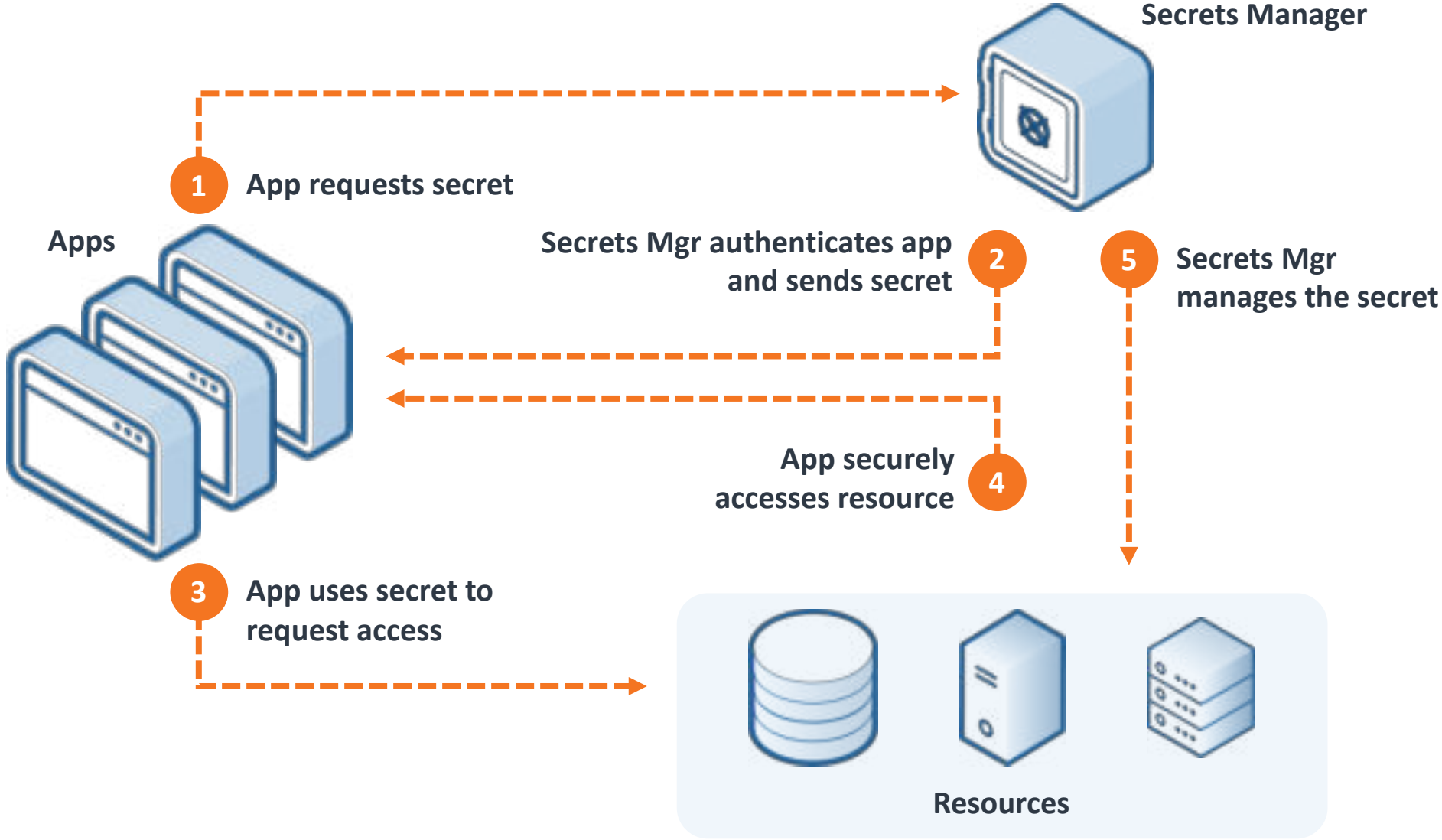
UserName = GetUserName()
Password = GetPassword()
Host = GetHost()
ConnectDatabase(Host, UserName, Password)

BEFORE:

UserName = "app"
Password = "y7qeF$1"
Host = "10.10.3.56"
ConnectDatabase(Host, UserName, Password)

What does “Securing an app” mean?

- COTS
- Containerized
- Serverless
- Microservice
- OS-Based
- Mainframe
- Scripts



Thank You