QUELLO CHE (FORSE) NON SAPEVATE DEL SENSO DEL PRIVILEGE MANAGEMENT

2020.11.26

Massimo Carlotti – PreSales Team Leader Italy / CYBERARK

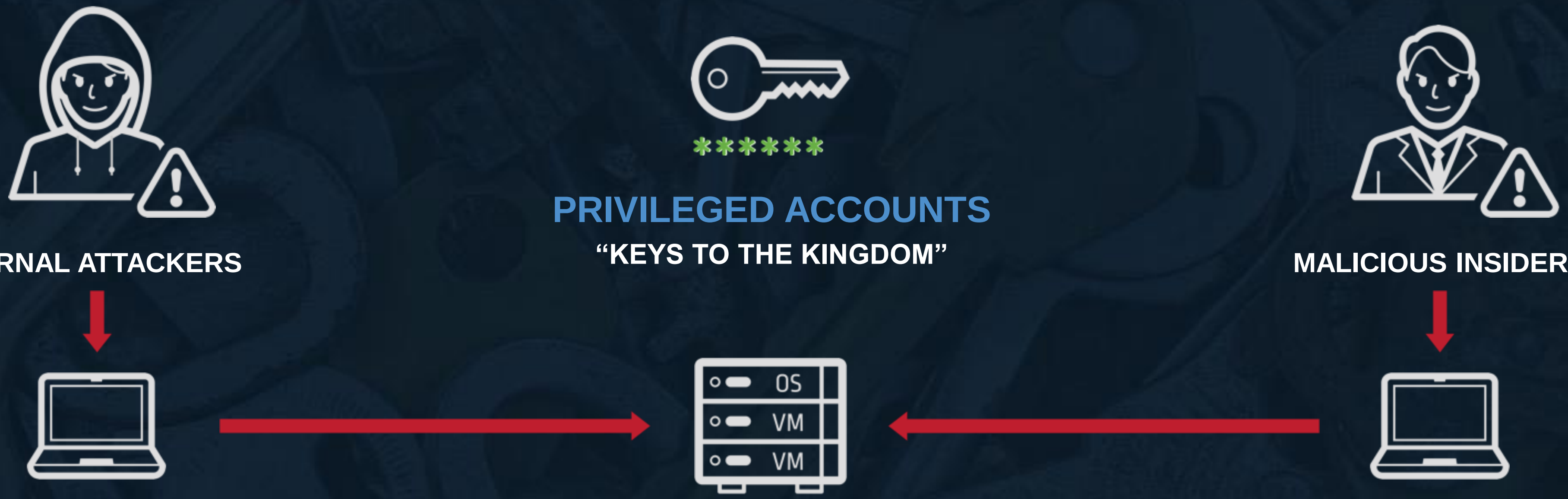
AGENDA – Privilege Management

- Why
- How
- What
- Q&A

AGENDA – Privilege Management

- **WHY**
- How
- What
- Q&A

WHY YOU SHOULD LISTEN



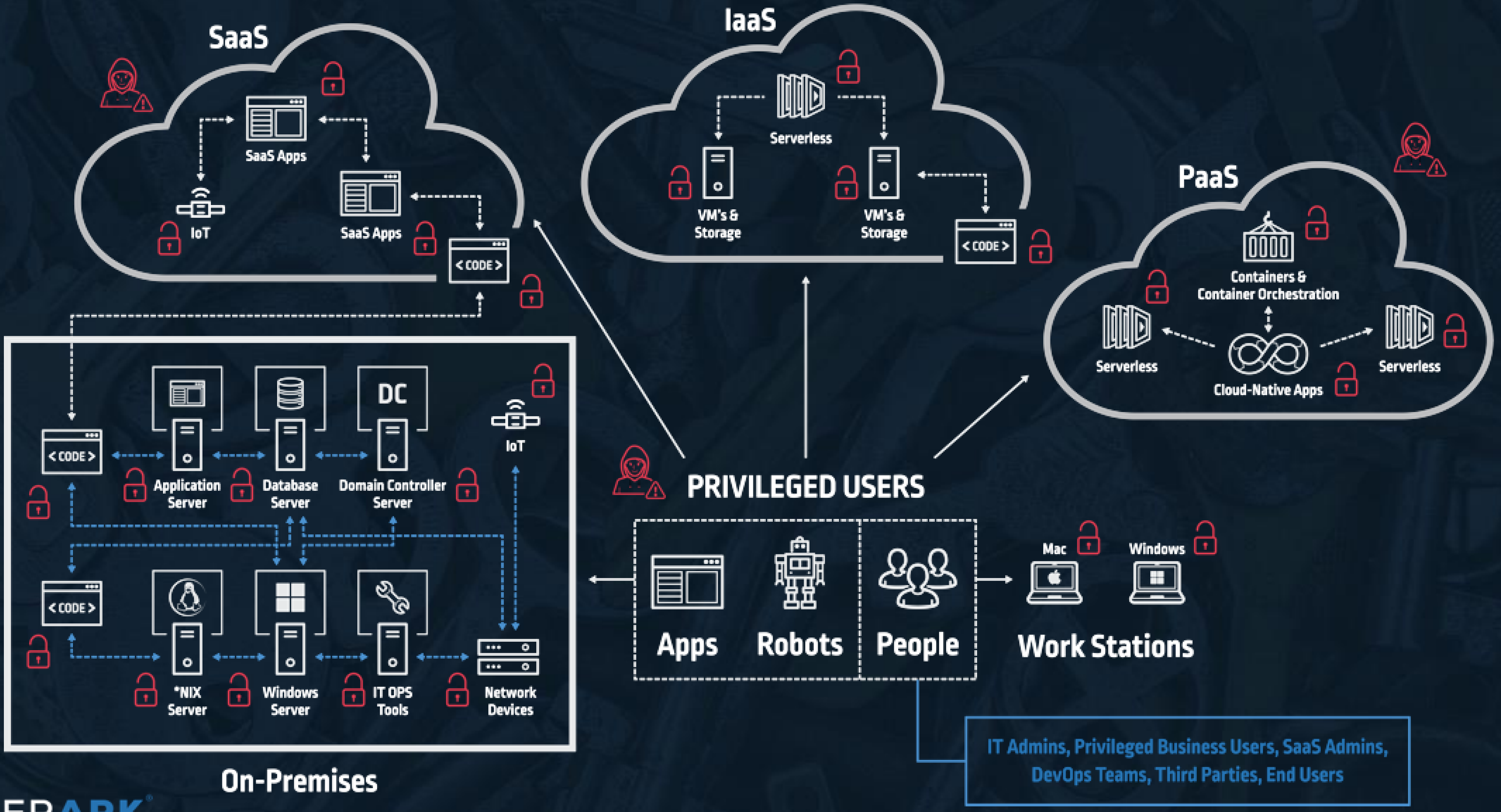
EXTERNAL ATTACKERS

PRIVILEGED ACCOUNTS

“KEYS TO THE KINGDOM”

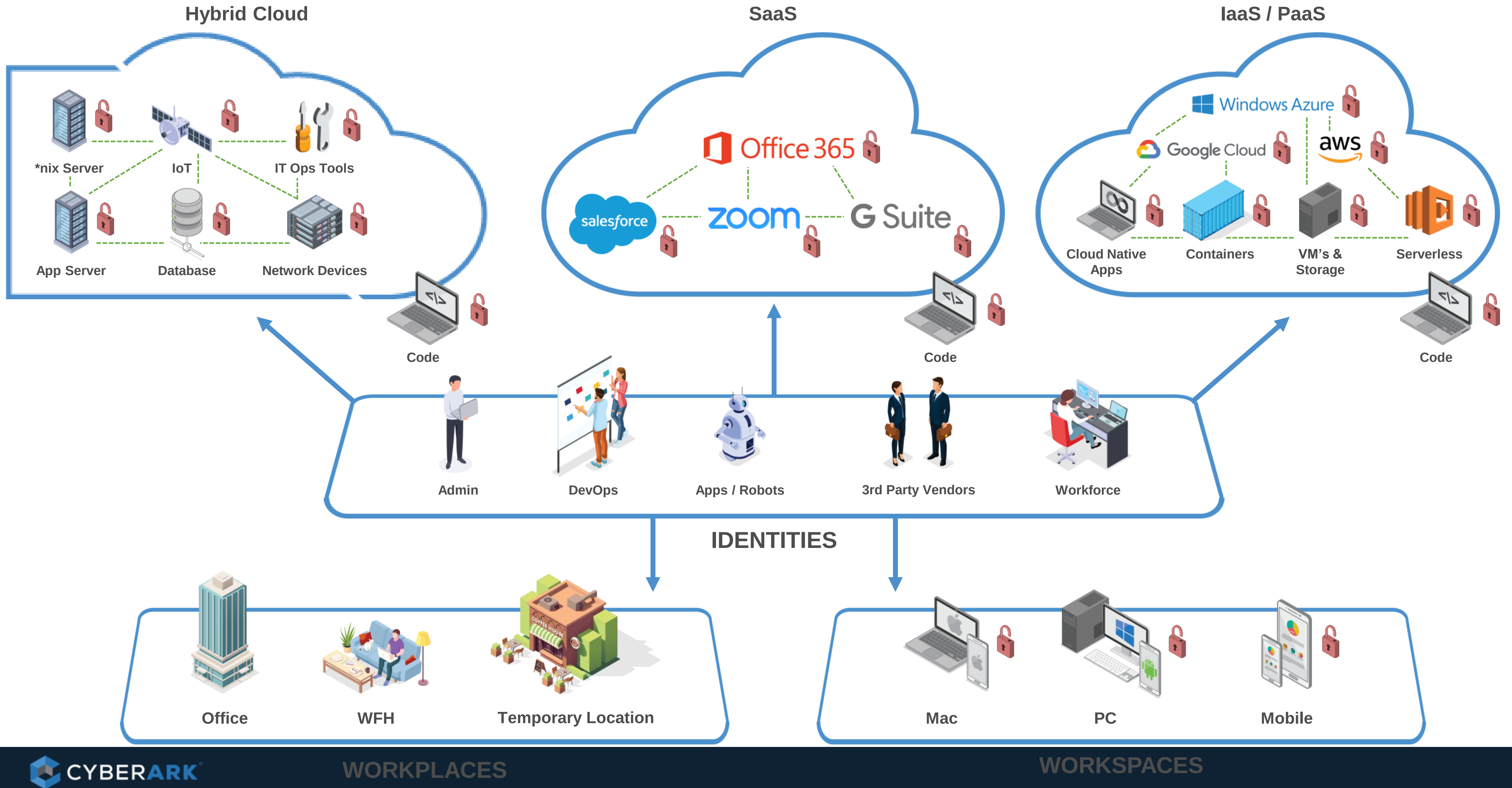
MALICIOUS INSIDERS

PRIVILEGE IS EVERYWHERE

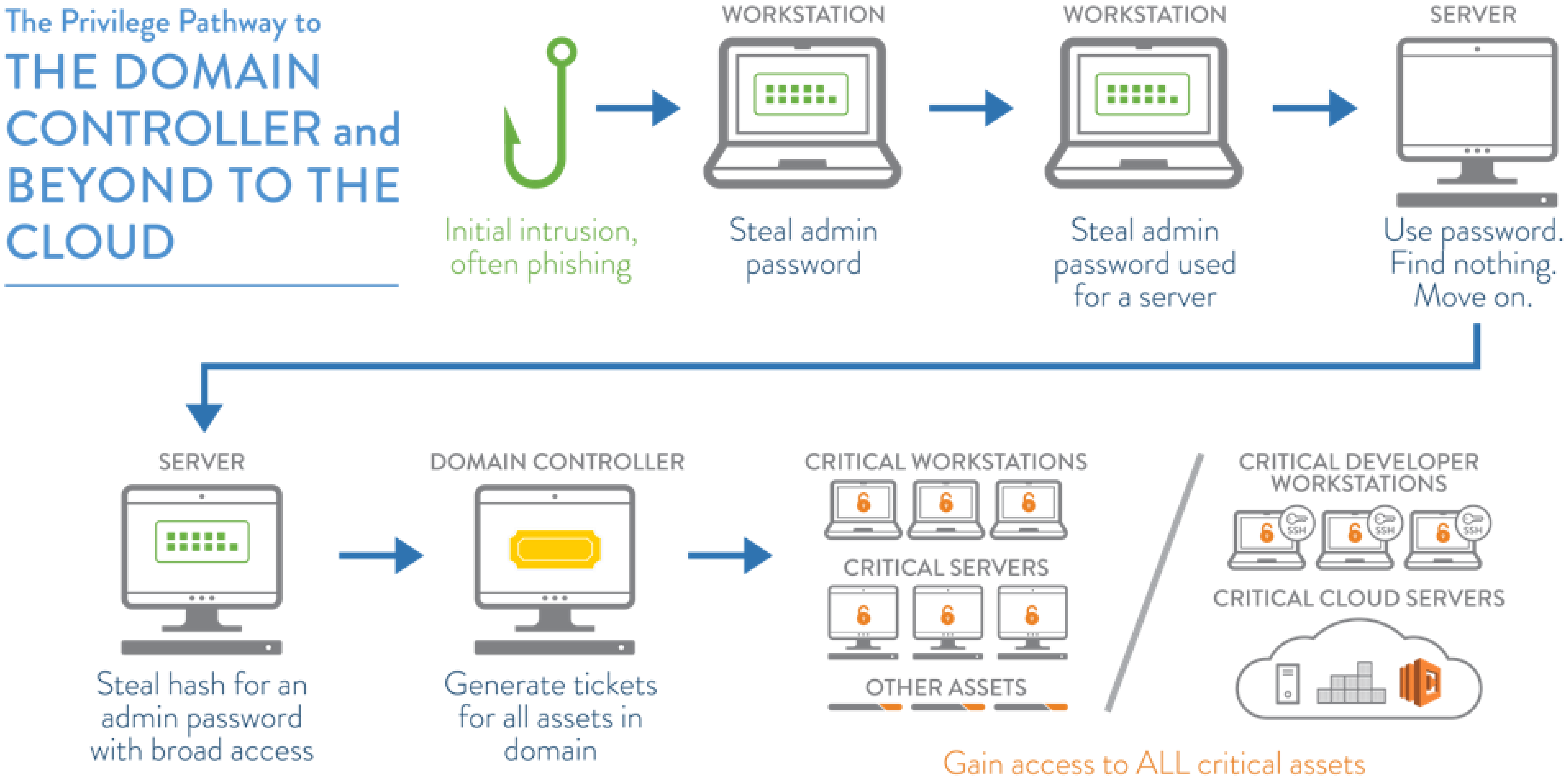


IT Admins, Privileged Business Users, SaaS Admins, DevOps Teams, Third Parties, End Users

ALL IDENTITIES CAN BE PRIVILEGED UNDER CERTAIN CONDITIONS



SAMPLE SCENARIO 1: THE PRIVILEGE PATHWAY



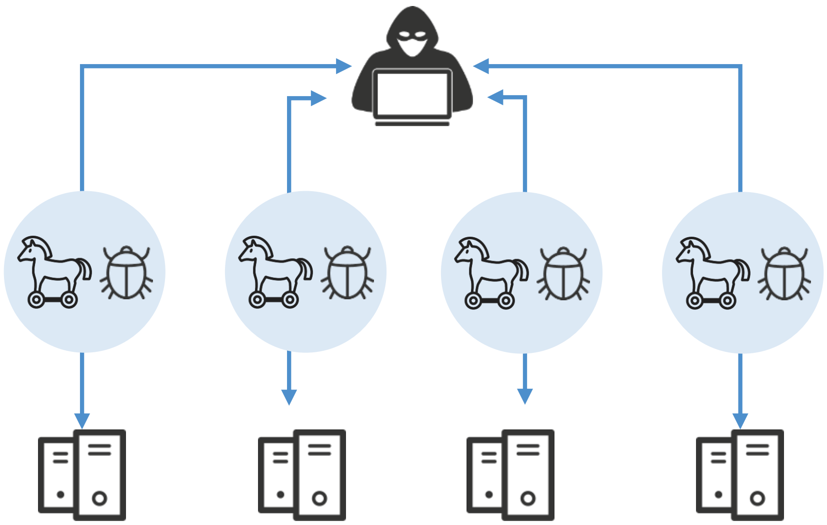
The Privilege Pathway to THE DOMAIN CONTROLLER and BEYOND TO THE CLOUD

Initial intrusion, often phishing
WORKSTATION
Steal admin password
WORKSTATION
Steal admin password used for a server
SERVER
Use password. Find nothing. Move on.
SERVER
Steal hash for an admin password with broad access
DOMAIN CONTROLLER
Generate tickets for all assets in domain
CRITICAL WORKSTATIONS
CRITICAL SERVERS
OTHER ASSETS
CRITICAL DEVELOPER WORKSTATIONS
SSH
CRITICAL CLOUD SERVERS
Gain access to ALL critical assets

SAMPLE SCENARIO 2: THE POWER OF PRIVILEGE IN THE CLOUD

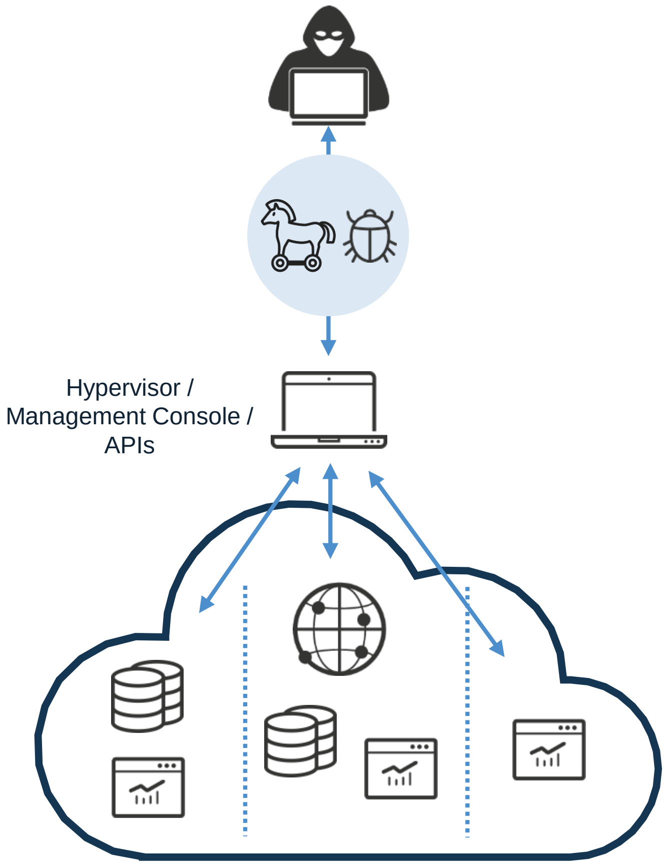
OLD WAY

Compromise a system, then another, then another, then own a domain

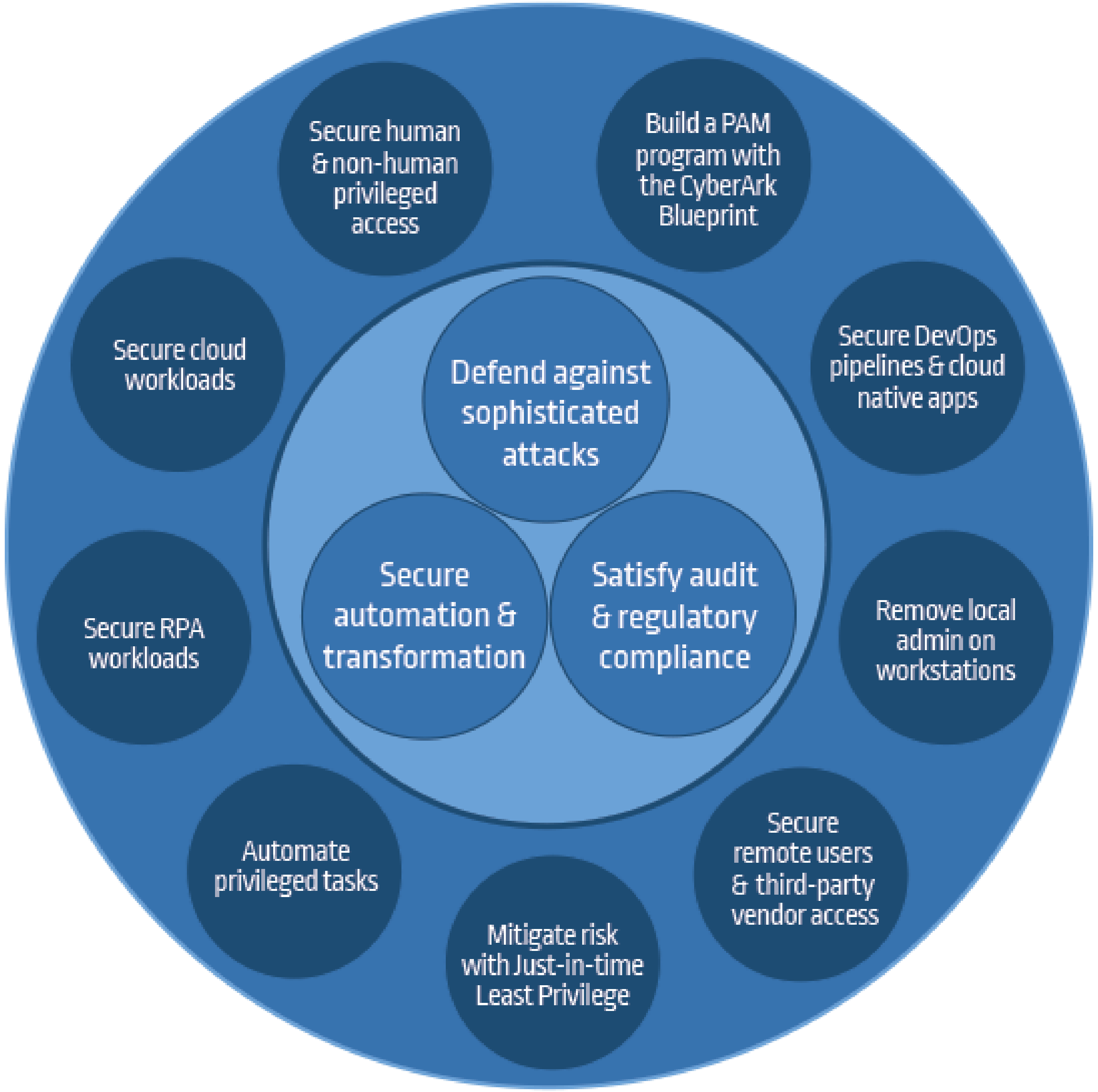


NEW WAY

Compromise one user, then own Cloud infrastructure



TOP USE CASES



Defend against sophisticated attacks

Secure automation & transformation

Satisfy audit & regulatory compliance

Secure human & non-human privileged access

Build a PAM program with the CyberArk Blueprint

Secure DevOps pipelines & cloud native apps

Remove local admin on workstations

Secure remote users & third-party vendor access

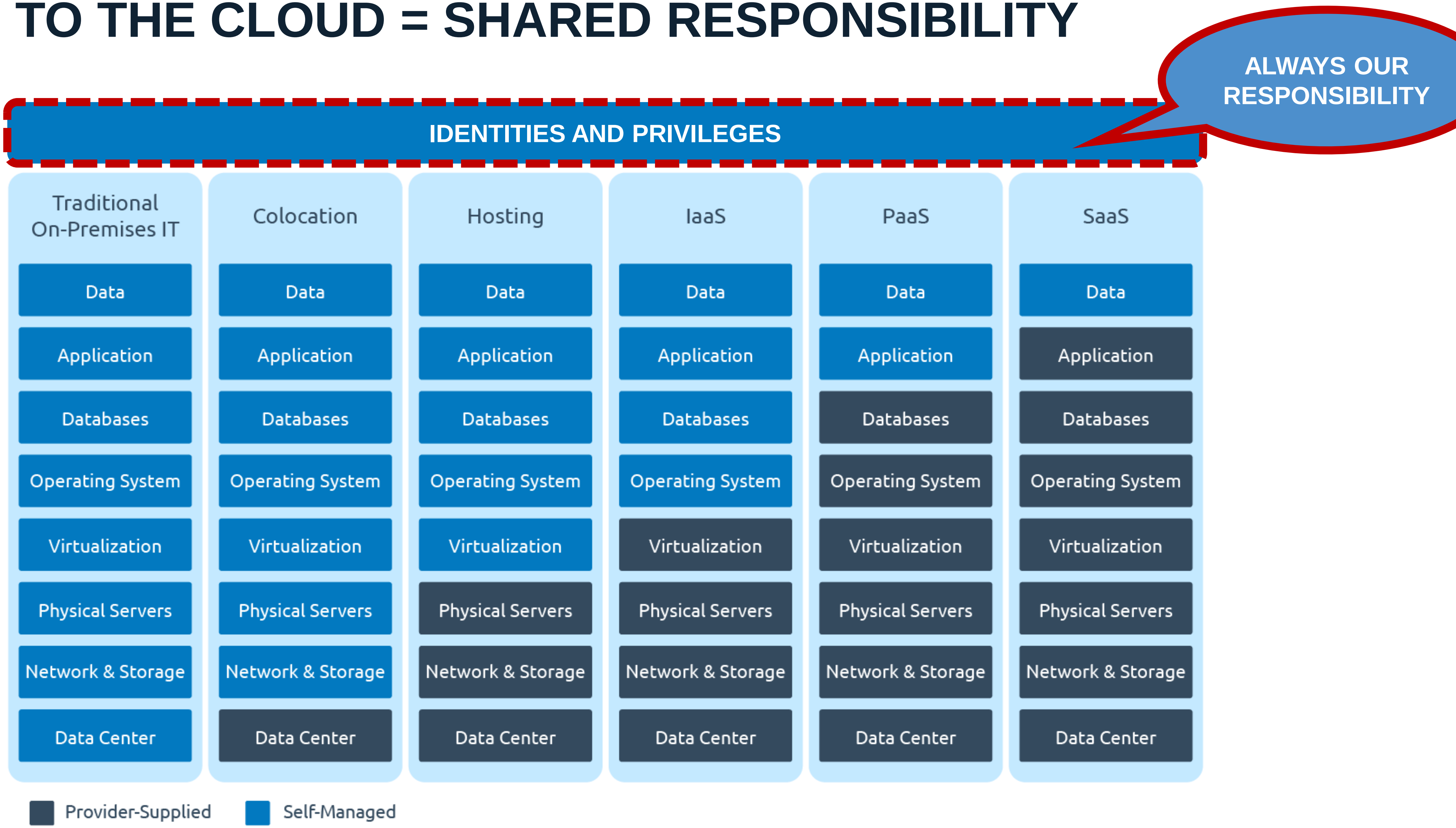
Mitigate risk with Just-in-time Least Privilege

Automate privileged tasks

Secure RPA workloads

Secure cloud workloads

MOVING TO THE CLOUD = SHARED RESPONSIBILITY



ALWAYS OUR RESPONSIBILITY

IDENTITIES AND PRIVILEGES

Traditional On-Premises IT	Colocation	Hosting	IaaS	PaaS	SaaS
🟦 Data	🟦 Data	🟦 Data	🟦 Data	🟦 Data	🟦 Data
🟦 Application	🟦 Application	🟦 Application	🟦 Application	🟦 Application	⬛ Application
🟦 Databases	🟦 Databases	🟦 Databases	🟦 Databases	⬛ Databases	⬛ Databases
🟦 Operating System	🟦 Operating System	🟦 Operating System	🟦 Operating System	⬛ Operating System	⬛ Operating System
🟦 Virtualization	🟦 Virtualization	🟦 Virtualization	⬛ Virtualization	⬛ Virtualization	⬛ Virtualization
🟦 Physical Servers	🟦 Physical Servers	⬛ Physical Servers	⬛ Physical Servers	⬛ Physical Servers	⬛ Physical Servers
🟦 Network & Storage	🟦 Network & Storage	⬛ Network & Storage	⬛ Network & Storage	⬛ Network & Storage	⬛ Network & Storage
🟦 Data Center	⬛ Data Center	⬛ Data Center	⬛ Data Center	⬛ Data Center	⬛ Data Center

⬛ Provider-Supplied 🟦 Self-Managed

PRIORITIZING PRIVILEGED ACCESS SECURITY

AGENDA – Privilege Management

- Why
- **HOW**
- What
- Q&A

A GOAL WITHOUT A PLAN
IS JUST A WISH

THINK LIKE THE ATTACKER

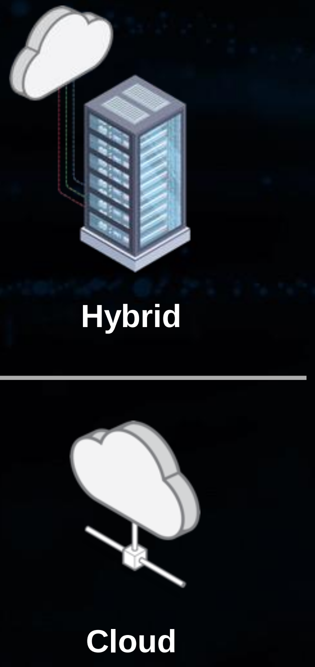
LOOK FOR EXPOSED PRIVILEGED ACCOUNTS

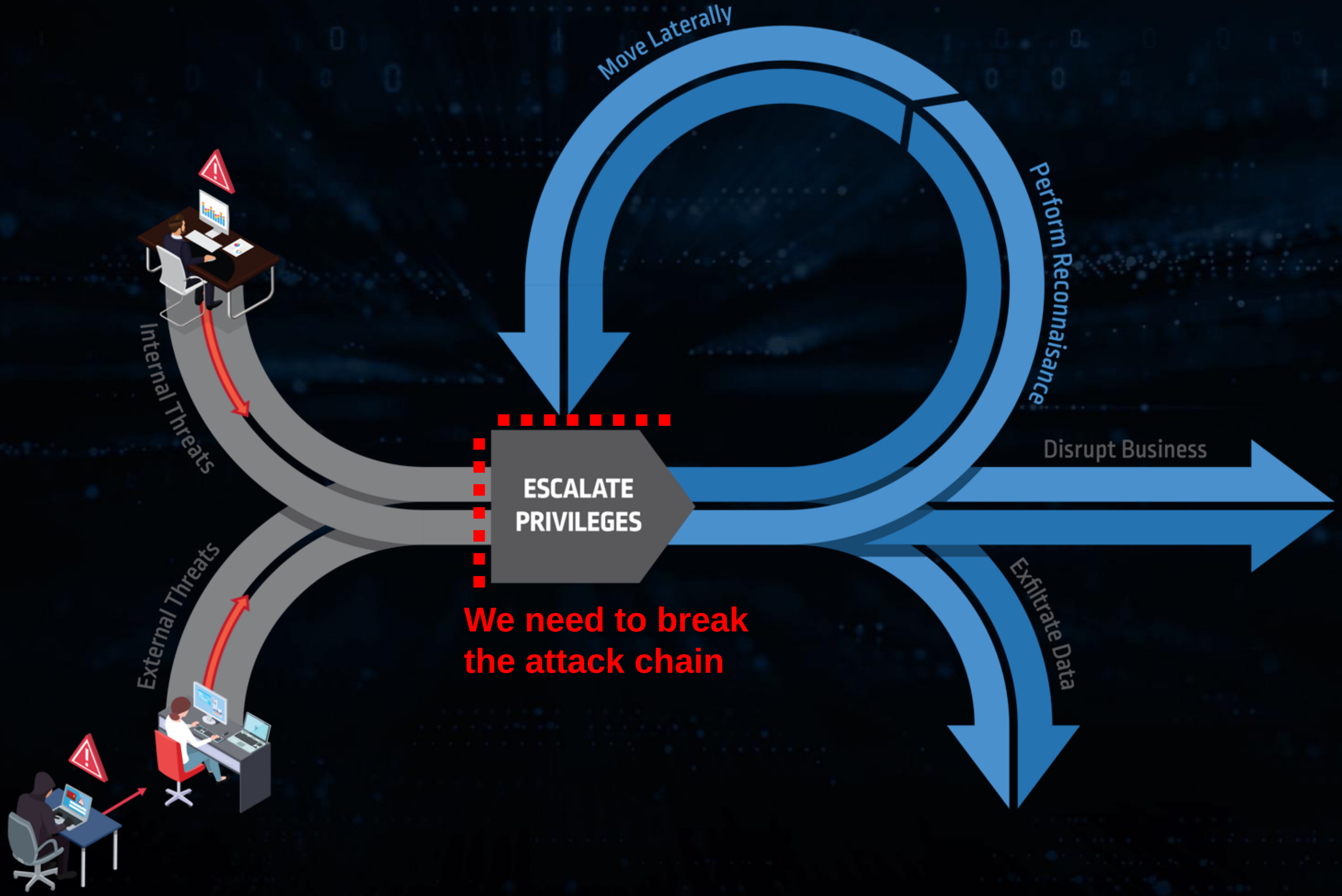
BYPASS PRIVILEGED ACCOUNT SECURITY CONTROLS

LEVERAGE KNOWN ATTACKS FOR BYPASSING AUTHENTICATION

GO UNDETECTED WHILE ABUSING PRIVILEGED ACCESS

THE ATTACK CHAIN IS STILL THE SAME





We need to break the attack chain

CYBERARK BLUEPRINT: 3 GUIDING PRINCIPLES

PREVENT CREDENTIAL THEFT

STOP LATERAL & VERTICAL MOVEMENT

LIMIT PRIVILEGE ESCALATION & ABUSE

← **ON PREMISES** — **HYBRID** — **CLOUD** →

Risk based program designed to secure privileged access across all environments

CYBERARK BLUEPRINT STAGES OVERVIEW

		STAGE 1	STAGE 2	STAGE 3	STAGE 4	STAGE 5
GOAL		**Rapid Risk Mitigation** Secure privileged IDs that have the potential to control an entire environment	**Core Security** Focus on locking down the most universal technology platforms	**Enterprise Program** Build PAS into the fabric of enterprise security strategy and application pipelines	**Mature the Program** Mature existing controls and expand into advanced privileged access security	**Advanced Security** Look for new opportunities to shore up privileged access across the enterprise
Risk Reduction	Prevent Credential Theft	◉	◉	◎	●	●
	Stop Lateral & Vertical Movement	◎	◎	◉	●	●
	Limit Privilege Escalation & Abuse	●	●	◎	◉	●

◉ Major ◎ Moderate ● Minor

THE VALUE OF A RED TEAM ASSESSMENT

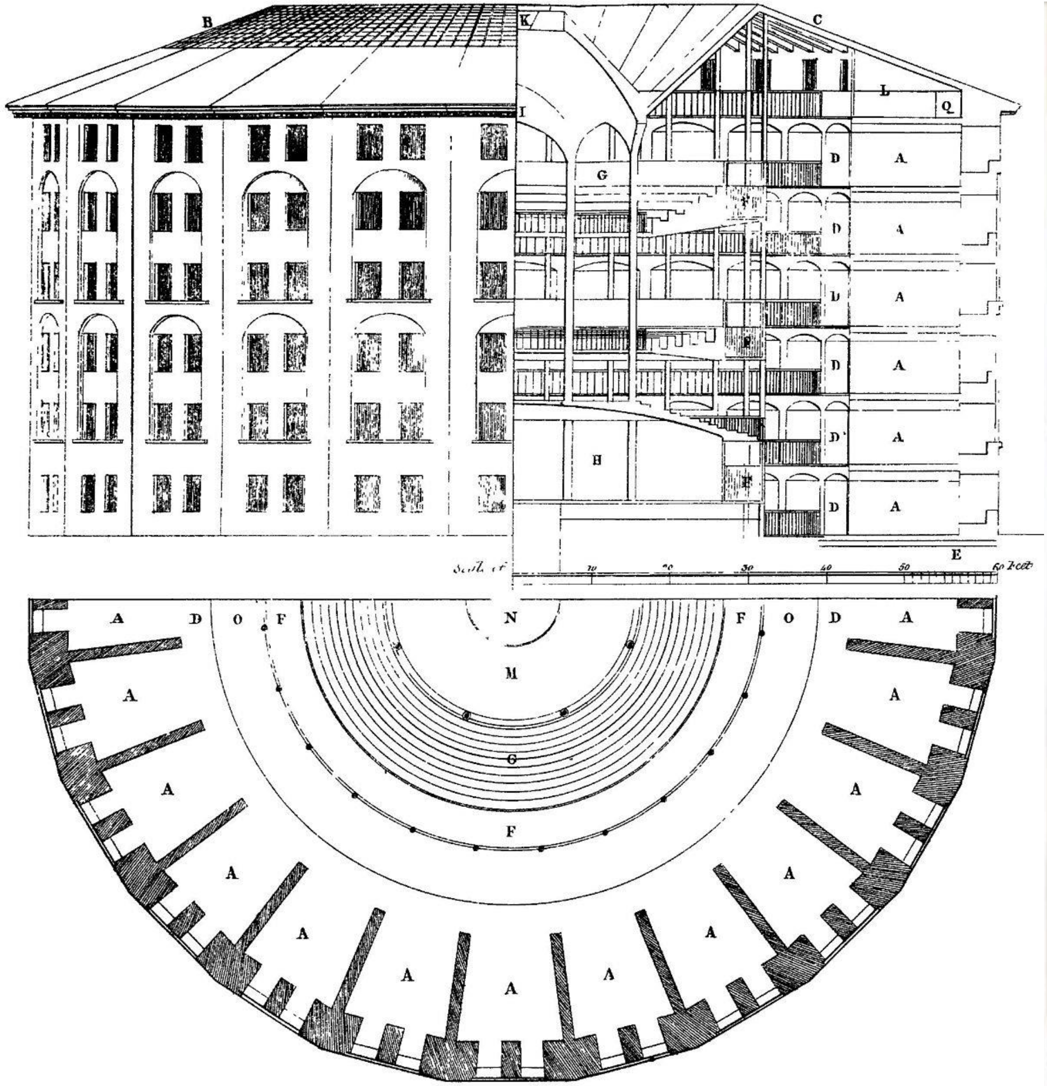
RED TEAM HELP TEST ABILITIES TO DETECT AND RESPOND TO ATTACKS

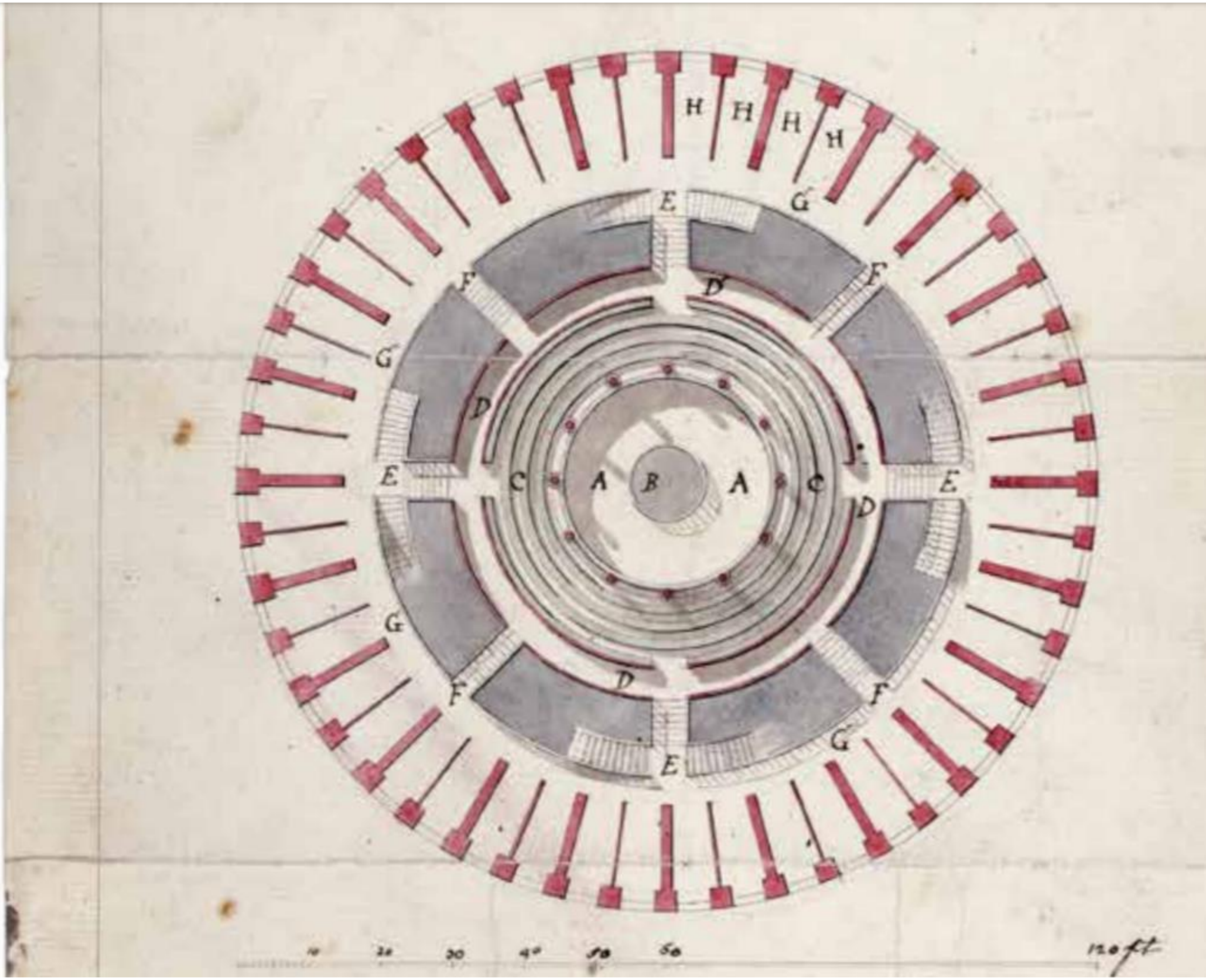
- **Understand strengths and weakness** under fire during real attack against their infrastructure.
- **Gain a view of how attacker’s TTP** (tactics, techniques and procedures) circumvent existing defensive solutions.
- **Mitigate risks found** during engagements with actionable deliverables.
- **Optimize CyberArk solutions** to mitigate real weakness found during the Red-Team engagement.

AGENDA – Privilege Management

- Why
- How
- **WHAT**
- Q&A

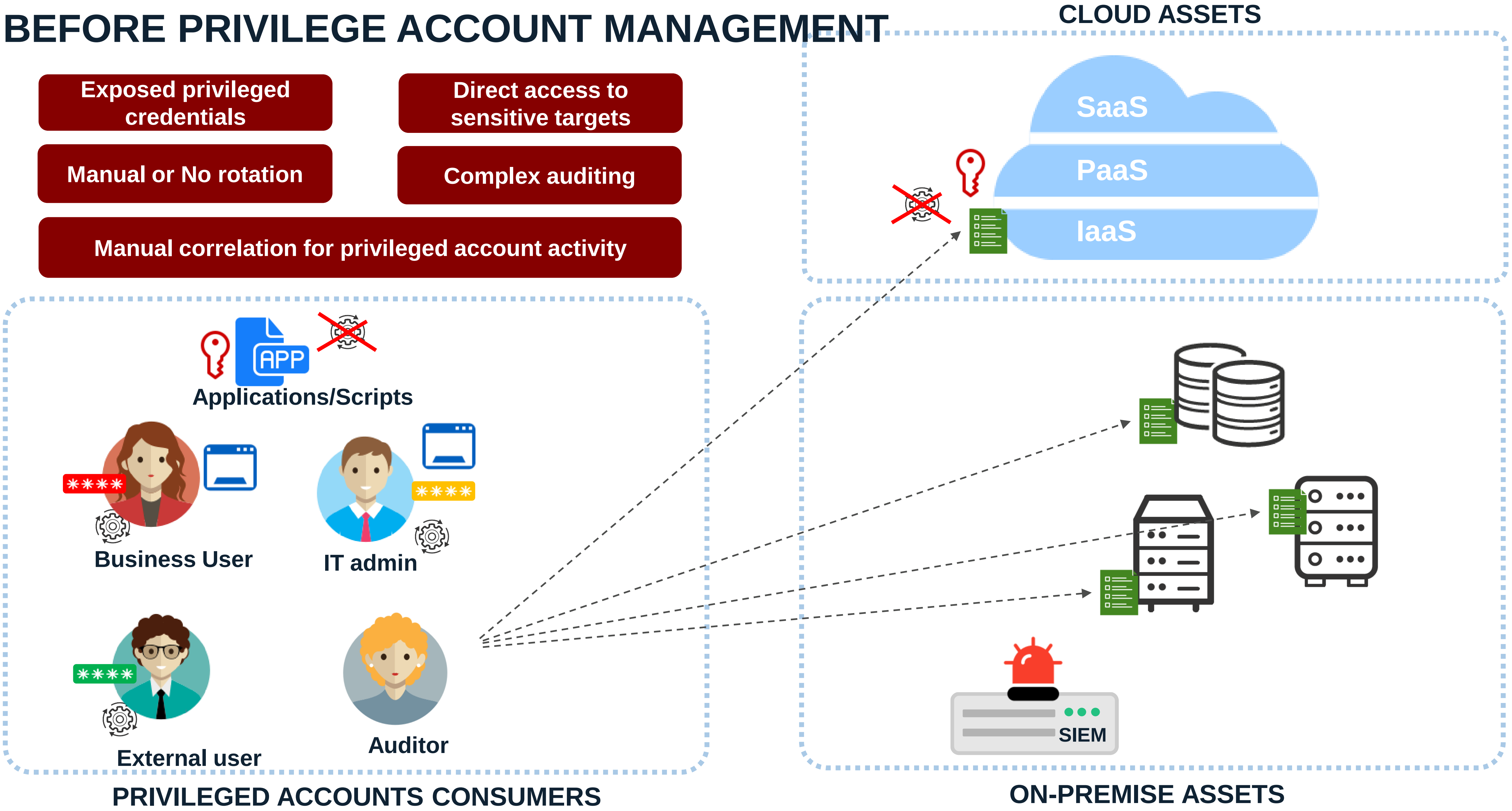
DO I REALLY HAVE TO…?!





BEFORE PRIVILEGE ACCOUNT MANAGEMENT

- Exposed privileged credentials
- Direct access to sensitive targets
- Manual or No rotation
- Complex auditing
- Manual correlation for privileged account activity



CLOUD ASSETS

SaaS

PaaS

IaaS

Applications/Scripts

APP

Business User

IT admin

External user

Auditor

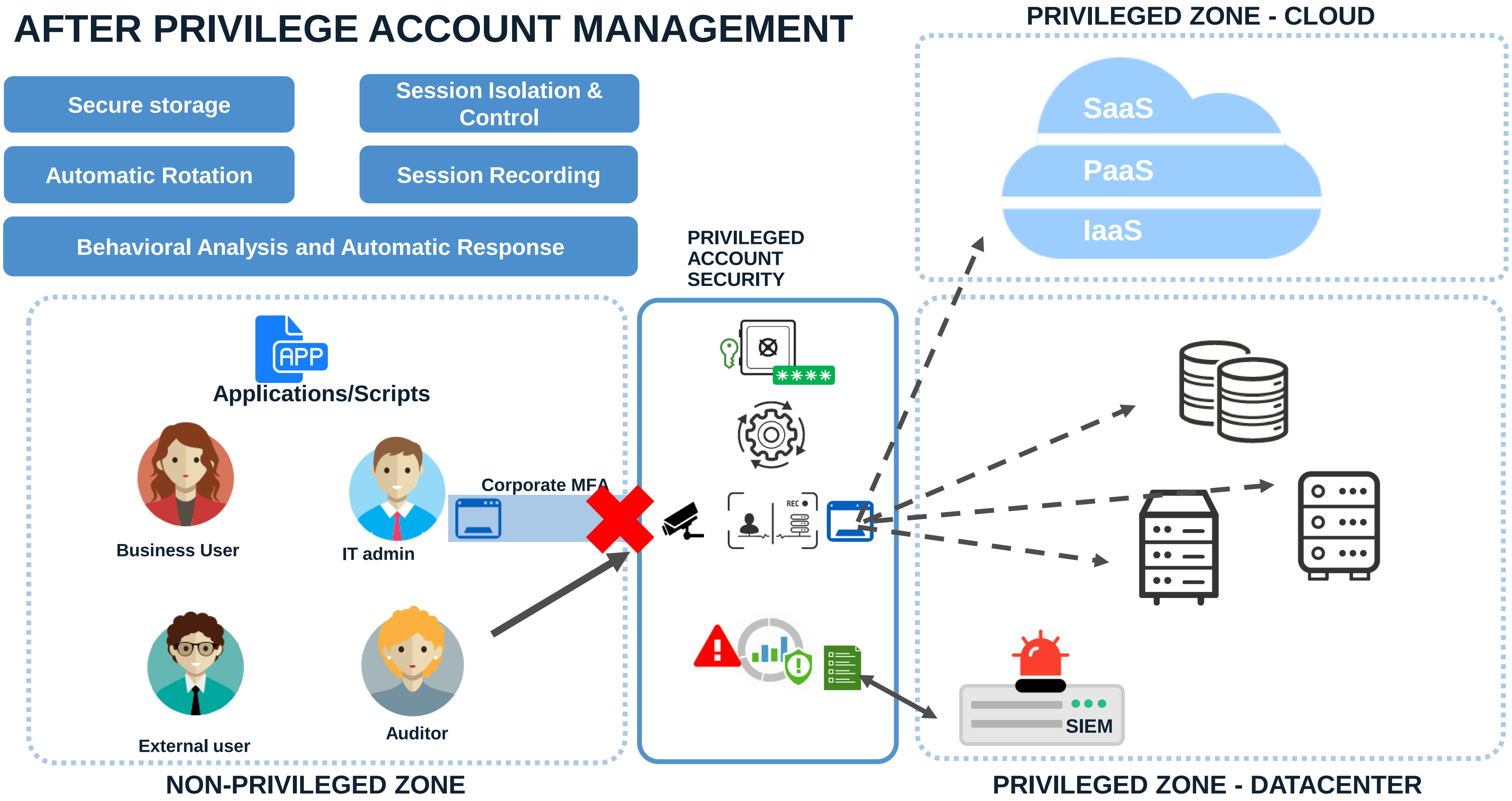
PRIVILEGED ACCOUNTS CONSUMERS

SIEM

ON-PREMISE ASSETS

AFTER PRIVILEGE ACCOUNT MANAGEMENT

- Secure storage
- Session Isolation & Control
- Automatic Rotation
- Session Recording
- Behavioral Analysis and Automatic Response



CYBERARK

RISK-BASED CREDENTIAL PROTECTION

DISCOVER

CONTINUALLY SCAN THE ENVIRONMENT TO DETECT PRIVILEGED CREDENTIALS AND ACCOUNTS

ONBOARD

ADD ALL DISCOVERED PRIVILEGED ACCOUNTS TO THE PENDING QUEUE TO VALIDATE PRIVILEGE

MANAGE

AUTOMATICALLY ADD PRIVILEGED ACCOUNTS TO BE MANAGED AND ROTATED IN THE DIGITAL VAULT

PRIVILEGED SESSION MANAGEMENT

ISOLATE

SEPARATE ENDPOINTS FROM CRITICAL TARGET SYSTEMS TO PREVENT LATERAL MOVEMENT

MONITOR

MONITOR, TRACK AND DETECT SUSPICIOUS PRIVILEGED ACTIVITIES AND EVENTS IN REAL TIME

RECORD

SUPPORT FORENSIC ANALYSIS AND AUDIT WITH DETAILED AUDIT OF PRIVILEGED ACTIVITY

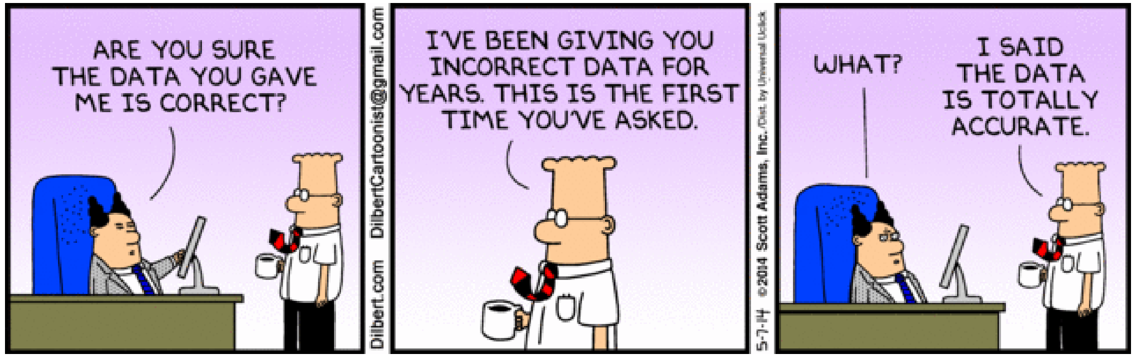
FOCUS ON: ANALYTICS

THE NEED FOR ANALYTICS

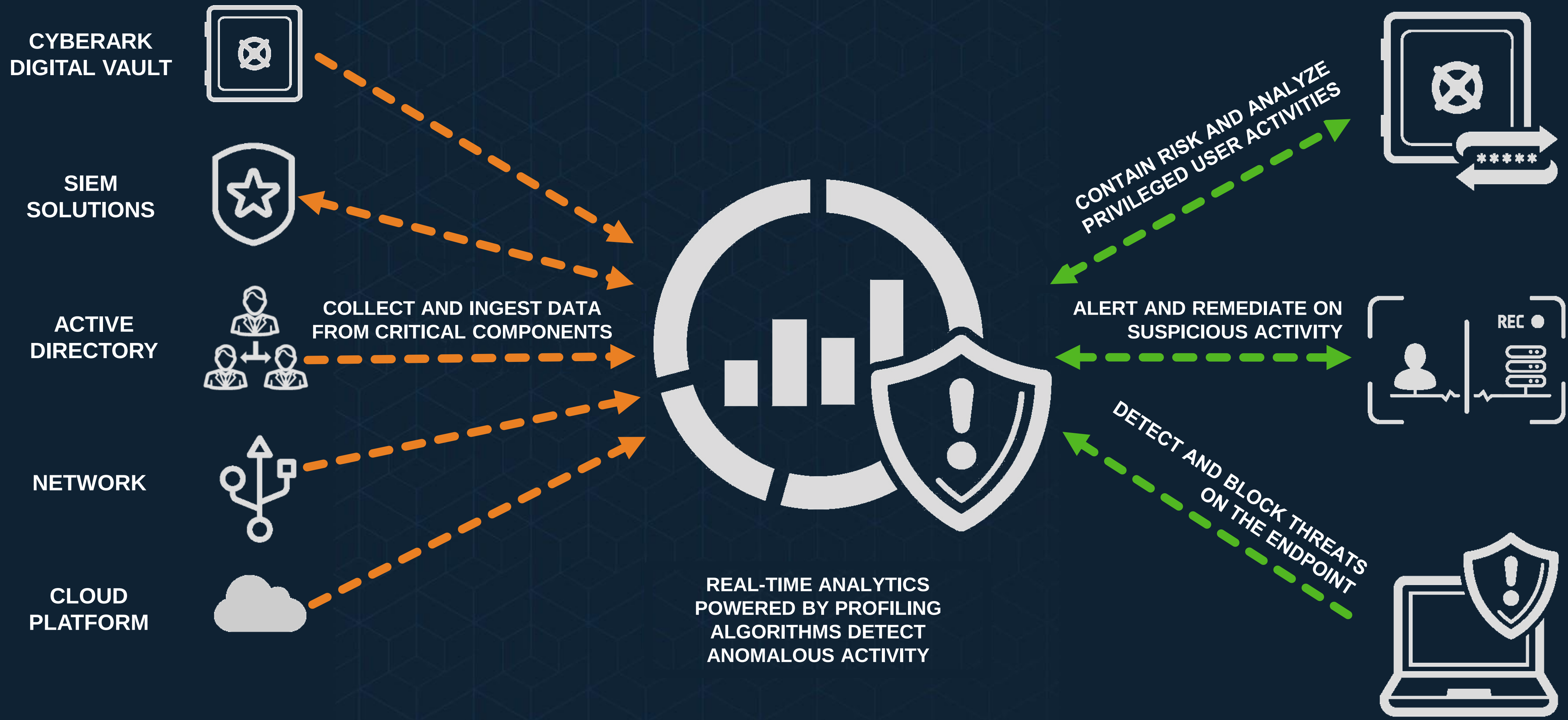
Assuming that…
Privileged accounts are most often compromised as part of an attack

We need some tool that

- Detects privileged accounts related anomalies
- Detects privileged accounts related security incidents
- Detects privileged accounts related risks
- Contains security incidents


ARE YOU SURE THE DATA YOU GAVE ME IS CORRECT?
I'VE BEEN GIVING YOU INCORRECT DATA FOR YEARS. THIS IS THE FIRST TIME YOU'VE ASKED.
WHAT?
I SAID THE DATA IS TOTALLY ACCURATE.
Dilbert.com DilbertCartoonist@gmail.com
5-7-14 ©2014 Scott Adams, Inc./Dist. by Universal Uclick

HOW COULD AN ANALYTICS ENGINE WORK IN A PAM SCENARIO


CYBERARK DIGITAL VAULT
SIEM SOLUTIONS
ACTIVE DIRECTORY
NETWORK
CLOUD PLATFORM
COLLECT AND INGEST DATA FROM CRITICAL COMPONENTS
CONTAIN RISK AND ANALYZE PRIVILEGED USER ACTIVITIES
*****
ALERT AND REMEDIATE ON SUSPICIOUS ACTIVITY
REC
DETECT AND BLOCK THREATS ON THE ENDPOINT

REAL-TIME ANALYTICS POWERED BY PROFILING ALGORITHMS DETECT ANOMALOUS ACTIVITY

FOCUS ON: LEAST PRIVILEGE FOR THE ENDPOINT

THE PROBLEM: USERS WITH ADMIN RIGHTS CAN…

Change system configurations

Install malware

Access and change accounts

> “87% of organizations have not removed local admin rights which represents a significant increase YoY.”
>
> Source: CyberArk Threat Landscape Survey, February 2018

THE DILEMMA – SECURITY VS. OPERATIONAL IMPACT

	USERS HAVE LOCAL ADMIN RIGHTS	LOCAL ADMIN RIGHTS ARE REMOVED
OPERATIONS IMPACT	Happy, productive users	Increased burden on the support team. Increased calls and costs.
SECURITY IMPACT	Increased security incidents	Contain attacks on the endpoint

LEAST PRIVILEGE

Privilege Management– prevent attacks that start at the endpoint by removing local admin rights on Windows workstations, servers, and Macs.

Application Control allows IT operations and security teams allow approved applications to run while restrict the unapproved ones. Unknown applications runs in ‘Restricted Mode’ which prevents them from accessing corporate resources, sensitive data or the Internet.

Just-in-time user elevation and access on a by-request basis for a time limited period of time with full audit of privileged activities.

LEAST PRIVILEGE

Privilege Management
Application Control
Just-In-Time Access and Elevation

PRIVILEGE DEFENSE

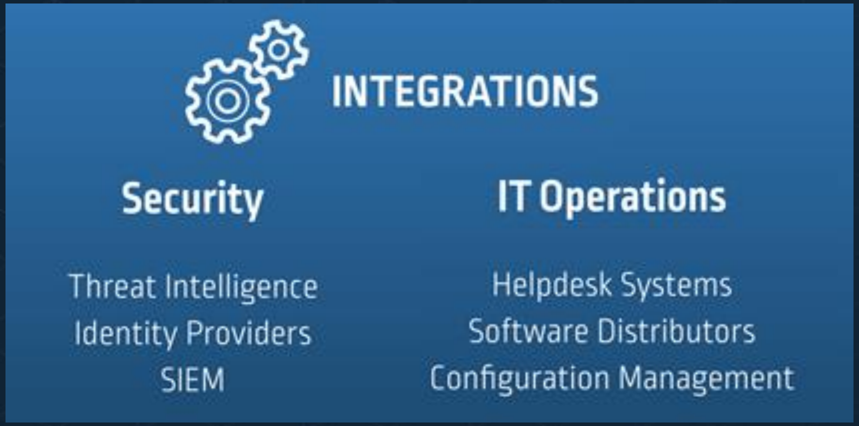
Credential theft blocking capabilities helps organizations detect and block attempted theft of Windows credentials and those stored by popular web browsers and file cache credential stores.

Ransomware protection provides another layer of security to the endpoint – the ability to detect ransomware with certainty and respond before the attack can cause damage.

Privilege Deception detects an insider threat or an attacker impersonating to an insider, who tries to operate undetected. Privilege Deception detect and block lateral movement by placing deception components in the attack path.

INTEGRATIONS

Technology Partnerships allow the customer to leverage on maximizing the positive outcome from adopting layered security solutions to create unified, integrated experiences across diverse disciplines. Ideally, these integrations should be — **secure, easy, robust.**



INTEGRATIONS

Security

Threat Intelligence
Identity Providers
SIEM

IT Operations

Helpdesk Systems
Software Distributors
Configuration Management

FOCUS ON: SHADOW ADMINS

SHADOW ADMIN, WHO ART THOU?

- Shadow Admin accounts are accounts in your network that have **sensitive privileges** and are typically **overlooked** because they are **not members of a privileged group** (tipically Active Directory). Instead, Shadow Admin accounts were granted their privileges through the **direct assignment of permissions** (using ACLs on AD objects).
- From the attacker’s perspective, **these accounts are highly desired** because they provide the administrative privileges necessary to advance an attack, and they have a lower profile compared to accounts under the well-known admin groups (ex: Domain Admins).

THE CHALLENGE OF LEAST PRIVILEGE: IN THE CLOUD

Huge Proliferation of Privileges

Microsoft Azure	5000+ Azure IAM permissions
aws	7,200+ AWS IAM permissions
Google Cloud	3200+ GCP IAM permissions

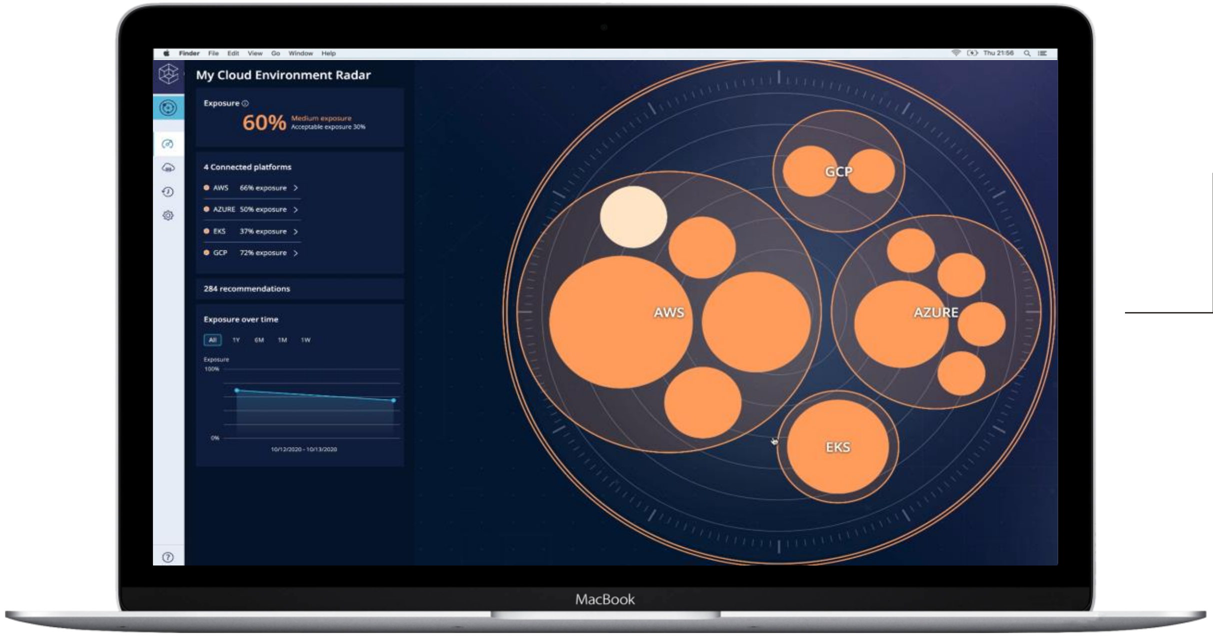
(as of October 2020)

SHADOW ADMINS – SUBSCRIPTION LEVEL

Permissions	Actions permitted
Microsoft.Authorization/classicAdministrators/write	Add new classic administrators
Microsoft.Authorization/roleAssignments/write	Grant permissions
Microsoft.Authorization/roleDefinition/write	Change permissions’ definitions
Microsoft.Authorization/elevateAccess/Action	Elevate to user access admin
Microsoft.Authorization/roleDefinition/*	Sensitive wildcard character “*”
Microsoft.Authorization/roleAssignments/*	
Microsoft.Authorization/*/Write	
Microsoft.Authorization/*	

Shadow Admin accounts are accounts in your network that have **sensitive privileges** and are typically overlooked because they are not members of a privileged Active Directory (AD) group and/or they are not assigned to known privileged roles.
Instead, Shadow Admin accounts were granted their privileges through the **direct assignment of permissions** (like using ACLs on AD objects or similar).

CLOUD ENTITLEMENTS MANAGEMENT


My Cloud Environment Radar

Exposure 60% Medium exposure
Acceptable exposure 30%

4 Connected platforms
- AWS 66% exposure
- AZURE 50% exposure
- EKS 37% exposure
- GCP 72% exposure

284 recommendations

Exposure over time

- Analyzing granted permissions
- Identifying unused and excessive permissions
- Modeling Exposure Level
- Providing actionable Recommendations
- Providing deployable Remediation

Identify…

unused and risky permissions that could be exploited by attackers

Remediate…

risky and excessive access with AI-generated policy corrections

Defend…

proactively against internal and external threats

FOCUS ON:
INTEGRATION

SECURE THE ECOSYSTEM: SECURITY IS A TEAM GAME!

CERTIFIED PARTNERS

- Ab Initio
- ActiveNavigation
- ANTWORKS (Reimagine · Rethink · Recreate)
- Advanced Systems Concepts, Inc.
- algosec (Business-driven security management)
- Apica
- APPDYNAMICS
- AppViewX
- aqua
- asg technologies
- atarlabs
- Atos
- Automation Anywhere
- AutomationEdge
- aws
- Axios Systems
- ayehu
- BigID
- beyond security
- blueprism
- bmc
- BRANDLE
- Bromium
- ca technologies (A Broadcom Company)
- cavirin
- Check Point Software Technologies LTD.
- CHEF
- cloudbees
- cortex
- CYBERBIT
- cyber OBSERVER
- CyberX
- DATA 443
- datablink
- DataSunrise
- DB NETWORKS
- DBmaestro
- DBSH
- DEMISTO
- DETACK
- Devolutions
- DEVICE42
- digitate
- docker
- DUO
- edgeverve
- EMERGYNT
- Eracent
- Evidian
- EZMCOM
- FIREEYE
- exabeam
- FOCAL POINT
- ForeScout
- FLEXERA
- FORTINET
- GE Power
- Google
- harness
- HIDEEZ
- IBM
- illusive
- Informatica
- intel
- IPsoft
- iQuate
- SONAR NoSQL Analytics
- KEYFACTOR
- leidos
- logpoint
- LogRhythm
- McAfee
- Microsoft
- CIPHER
- NICE
- netwrix
- okta
- Omada
- onelogin
- OpsRamp
- Outpost24
- paloalto networks
- PCYSYS
- PEGA
- Phantom
- Phosphorus
- Ping Identity
- Pivotal
- proofpoint
- puppet
- Qualys
- RADIANT LOGIC
- redhat
- RAPID7
- RSA
- SAASPASS
- SailPoint
- SAP
- SCADAfence
- ScriptRunner
- SECRET DOUBLE OCTOPUS
- SECUREAUTH
- SECURELINK (Vendor privileged access)
- SECURONIX
- servicenow
- SIEMPLIFY
- simeio
- SILVERFORT
- SKYBOX security
- SO RO CO
- softomotive
- SOFT WARFARE
- splunk>
- SPHERE
- STEALTHbits technologies
- StreamSets
- SyferLock
- Symantec
- talend
- tenable
- THALES
- tripwire
- Twistlock
- UiPath
- UNBOUND
- utimaco
- VENAFI
- VARONIS
- VISTARA
- WorkFusion
- WATERFALL
- XYPRO (Mission Critical Security)
- yubico

CERTIFIED JOINT SOLUTIONS

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

PLUG-INS

- CPM Plug-ins
- PSM Plug-ins

CYBERARK

CYBERARK®

AGENDA – Privilege Management

- Why
- How
- What
- **Q&A**

CYBERARK

QUESTIONS?

THANK YOU

WHAT'S NEXT: GUIDED TOUR

CYBERARK GUIDED TOUR

Take the First Step to a Stronger Security Posture.

www.cyberark.com/cyberark-guided-tour/