CyberLagom

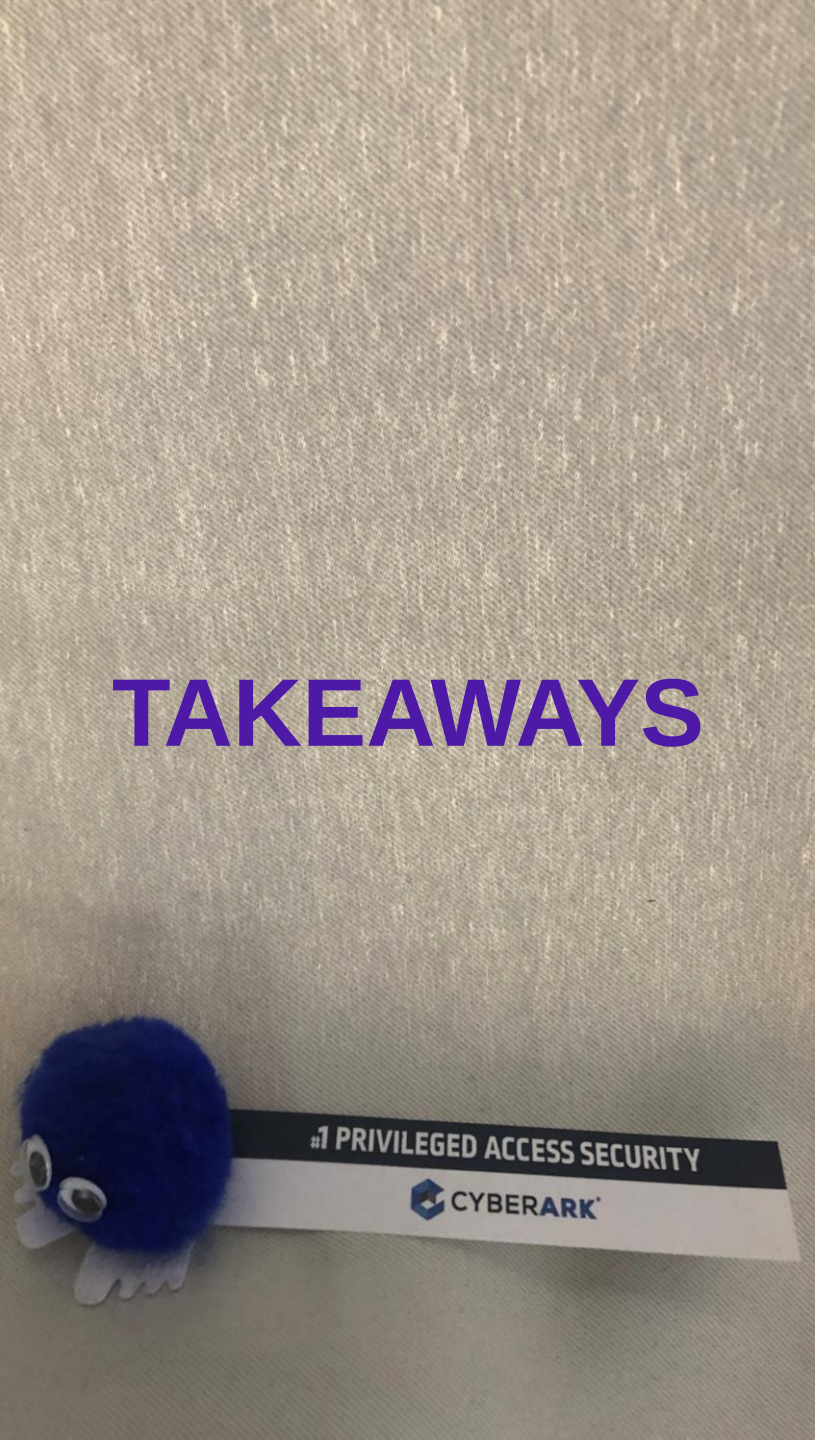
Why Privileged Access is CISO's #1 priority

14 April 2021

Samira Zaker Soltani

ISACA

TAKEAWAYS



Privileged Accounts

- What are they
- Why are they important
- Where do we find them
- CyberArk PAS solution + demo
- Where do you start
- Prioritizing the onboarding roadmap


PRIVILEGED ACCOUNTS
ANY ACCOUNT EXCEEDING NORMAL ACCESS WHICH, IF COMPROMISED, WILL HAVE A HIGH IMPACT ON YOUR BUSINESS
CyberLagom

GARTNER’S KEY PRIORITIES FOR IAM LEADERS IN 2021

“

Nearly every successful security breach involves a failure of privileged access management (PAM).

PAM is the combination of tools used to secure, control and monitor privileged access to an organization’s critical information and resources. And while it may not prevent an initial breach, PAM can reduce or eliminate the impact of the breach.

DID YOU KNOW…

80%

of All Breaches Involve Privileged Credentials

(The Forrester Wave: Privileged Identity Management, Q3 2016)

120 days The median time to discover spilled credentials across 96 incidents.

Often spills are discovered on the dark web before organizations detect or disclose a breach.

(F5 Labs - 2021 Credential Stuffing Report)

Stolen Credentials Have Been Behind Some of the Largest and Most Costly Data Breaches.

(Equifax, U.S. Office of Personnel Management, Yahoo and more)

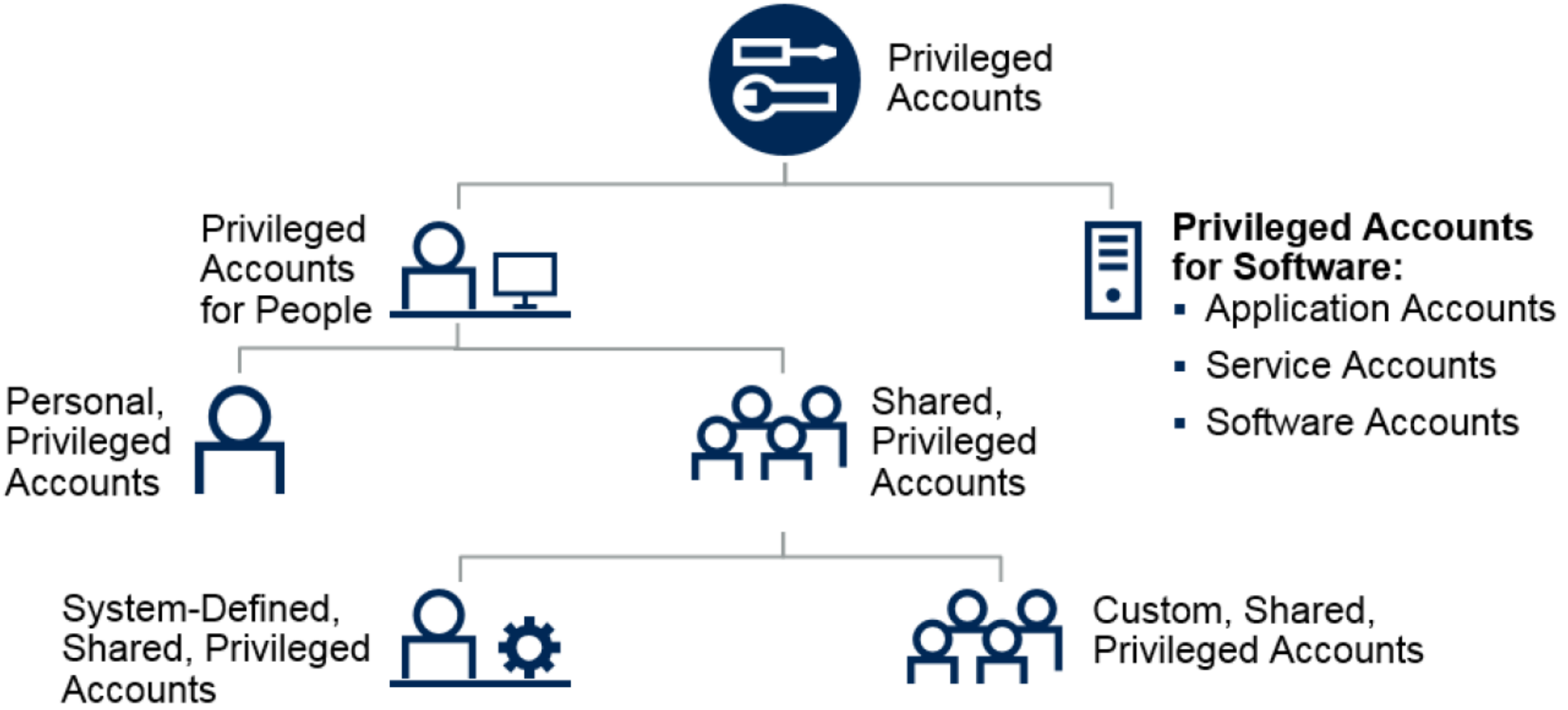
1.8 Billion

Credentials were stolen in 2020

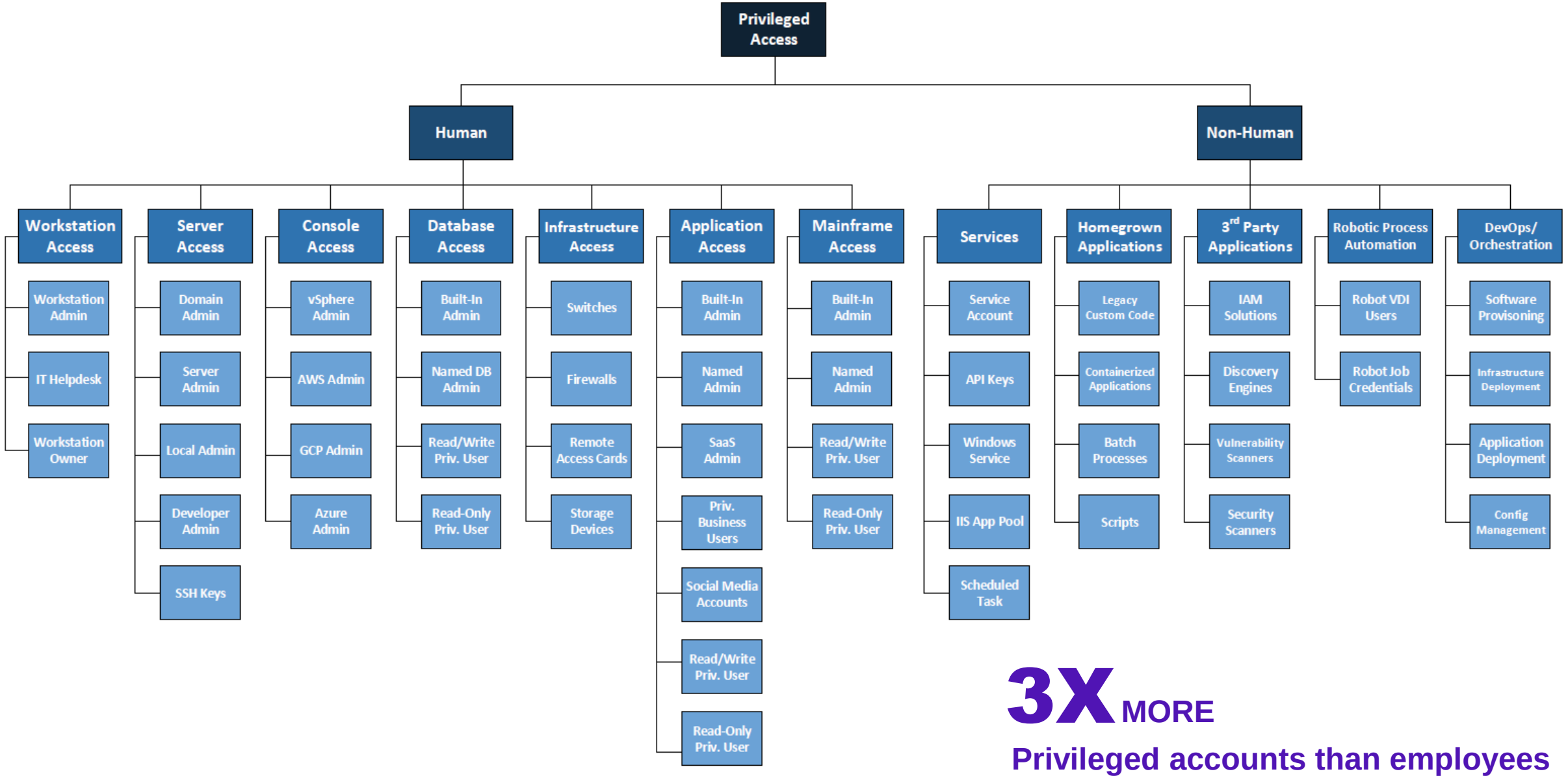
(F5 Labs - 2021 Credential Stuffing Report)

CyberLagom

PRIVILEGED ACCOUNT TAXONOMY



ID: 376315

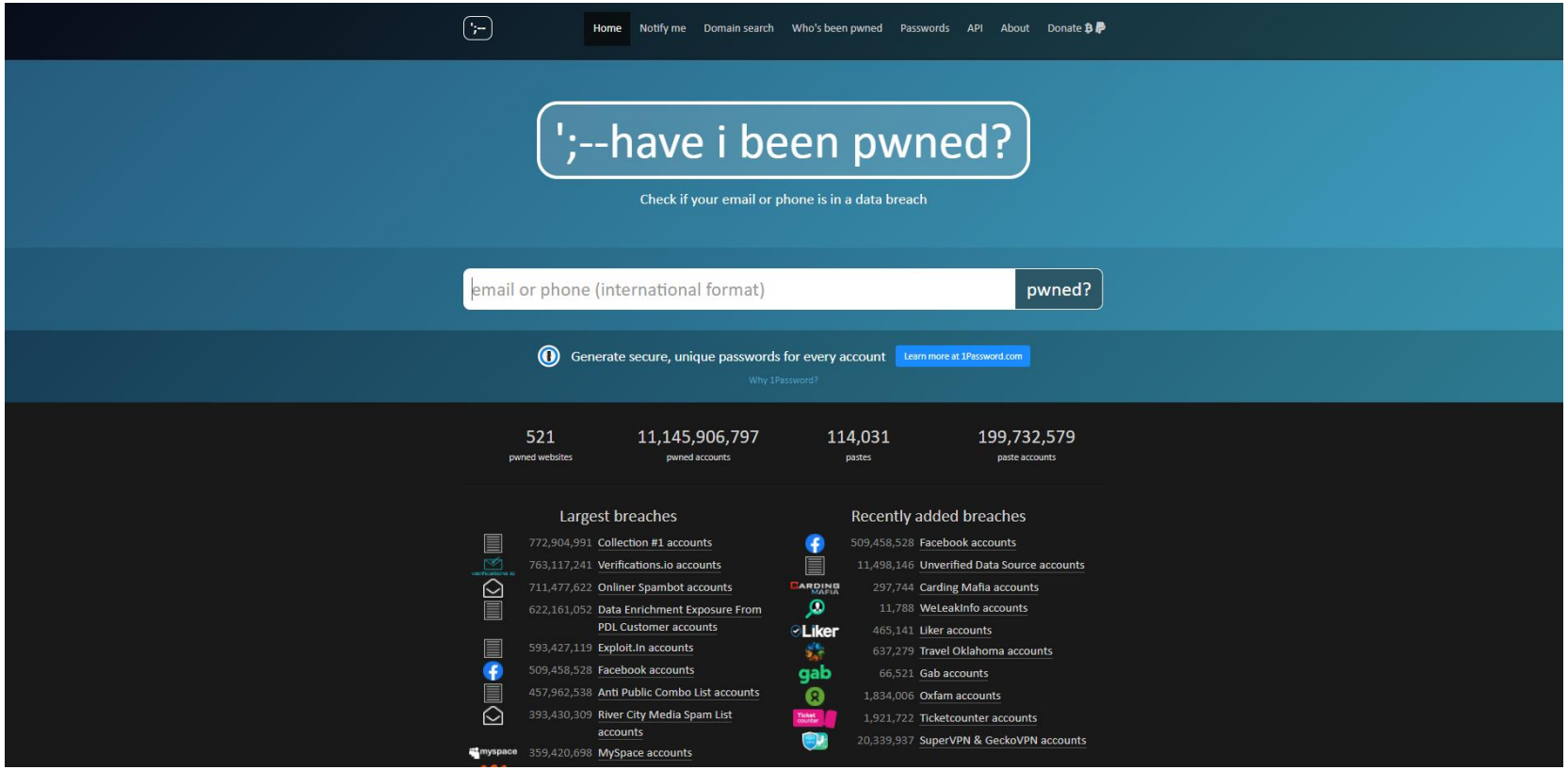


3X MORE

Privileged accounts than employees


LIKE AN ATTACKER
CYBERARK

HAVE I BEEN PWNED?



HAVE I BEEN PWNED?

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

Cit0day (unverified): In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Passwords

Collection #1 (unverified): In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 *billion* records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post The 773 Million Record "Collection #1" Data Breach.

Compromised data: Email addresses, Passwords

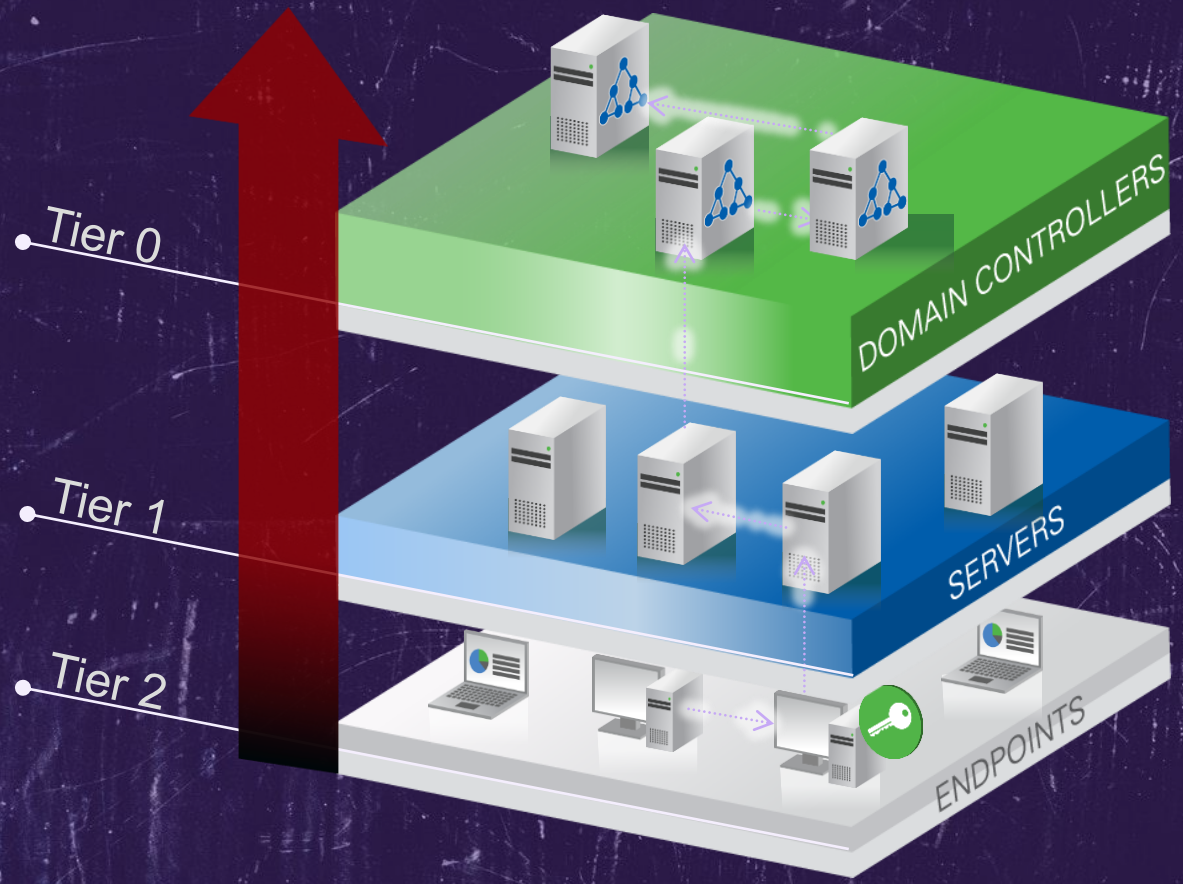
Data Enrichment Exposure From PDL Customer: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles

Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords

CREATING BOUNDARIES

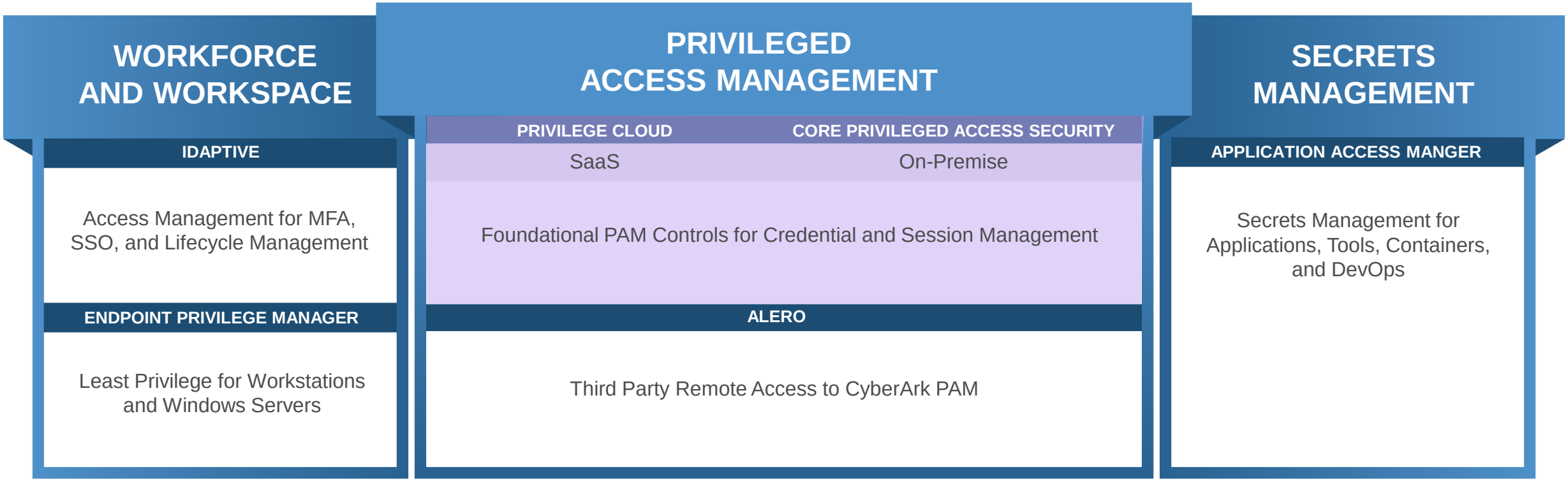


GARTNER 2020 PRIVILEGED ACCESS MANAGEMENT MAGIC QUADRANT

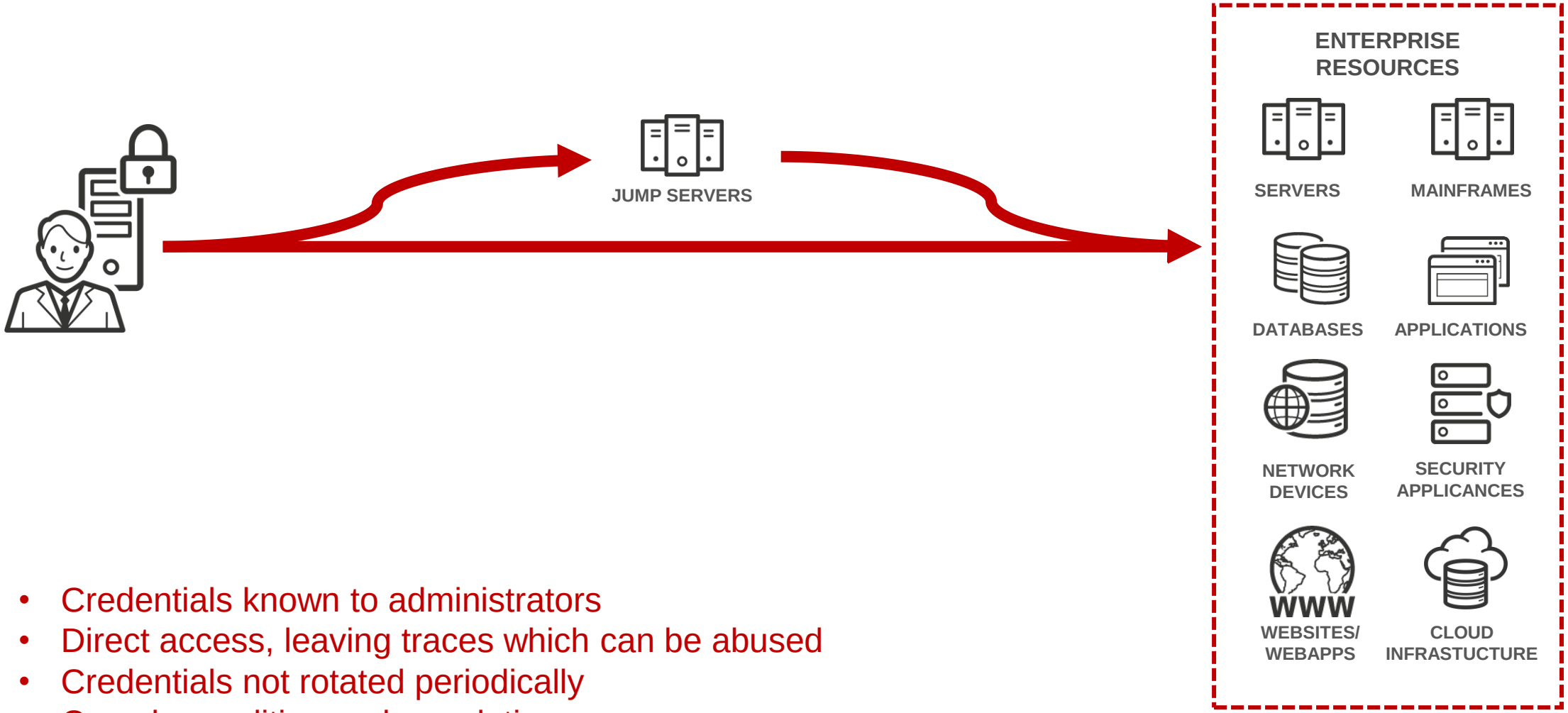
Figure 1. Magic Quadrant for Privileged Access Management

Source: Gartner (August 2020)

CYBERARK IDENTITY SECURITY PORTFOLIO

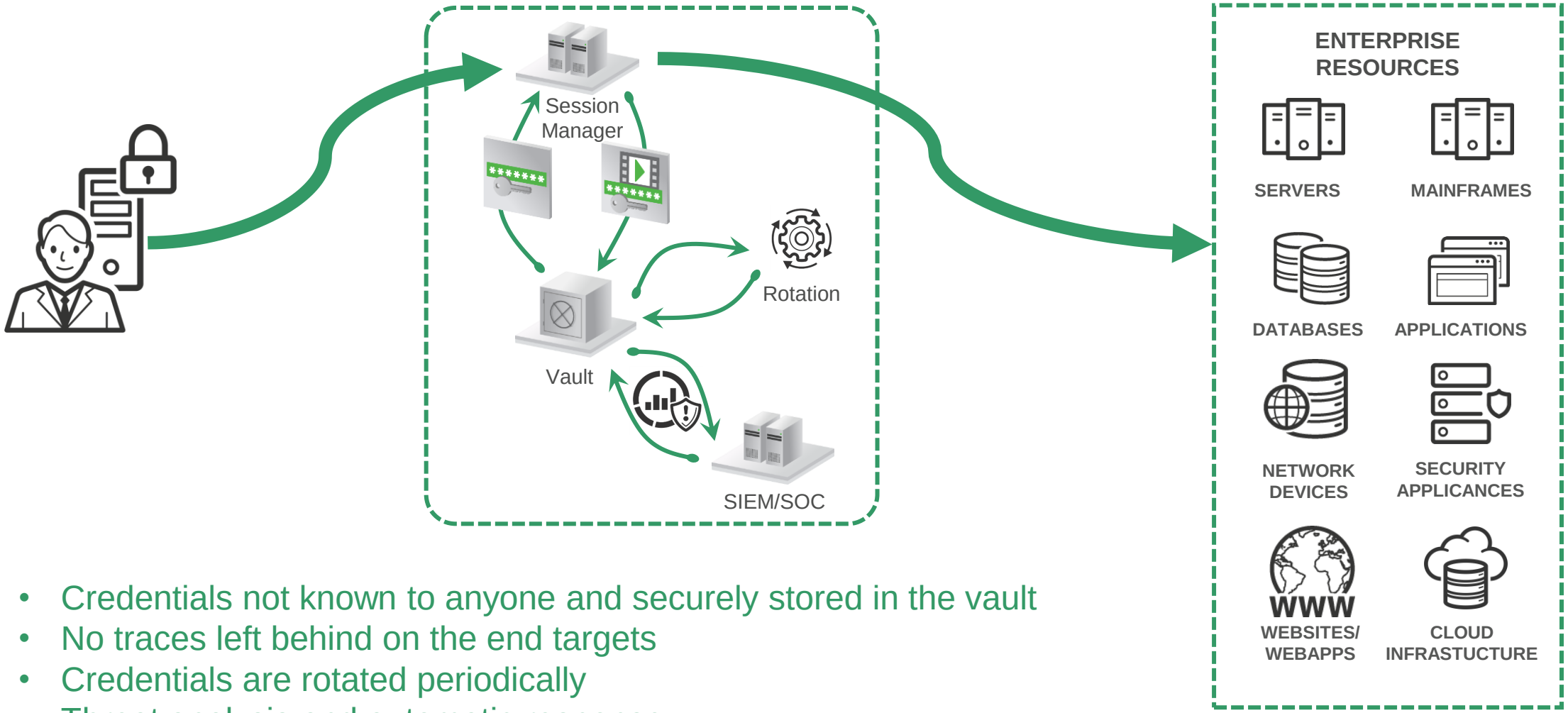


SITUATION WITHOUT PAS



- Credentials known to administrators
- Direct access, leaving traces which can be abused
- Credentials not rotated periodically
- Complex auditing and correlation

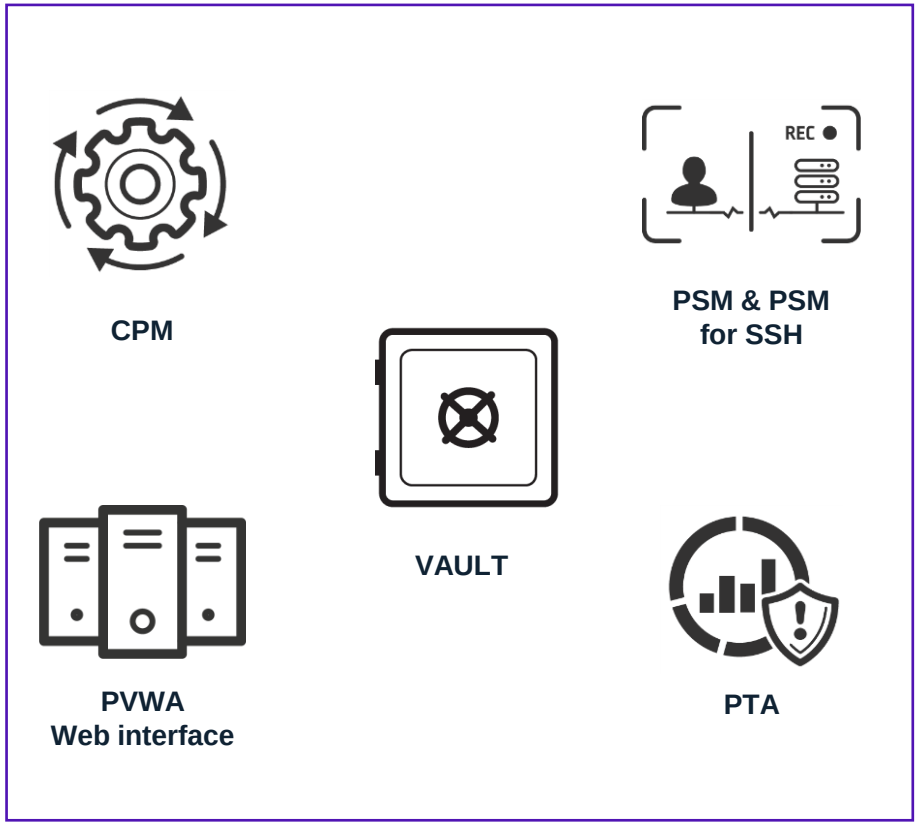
SITUATION WITH PAS



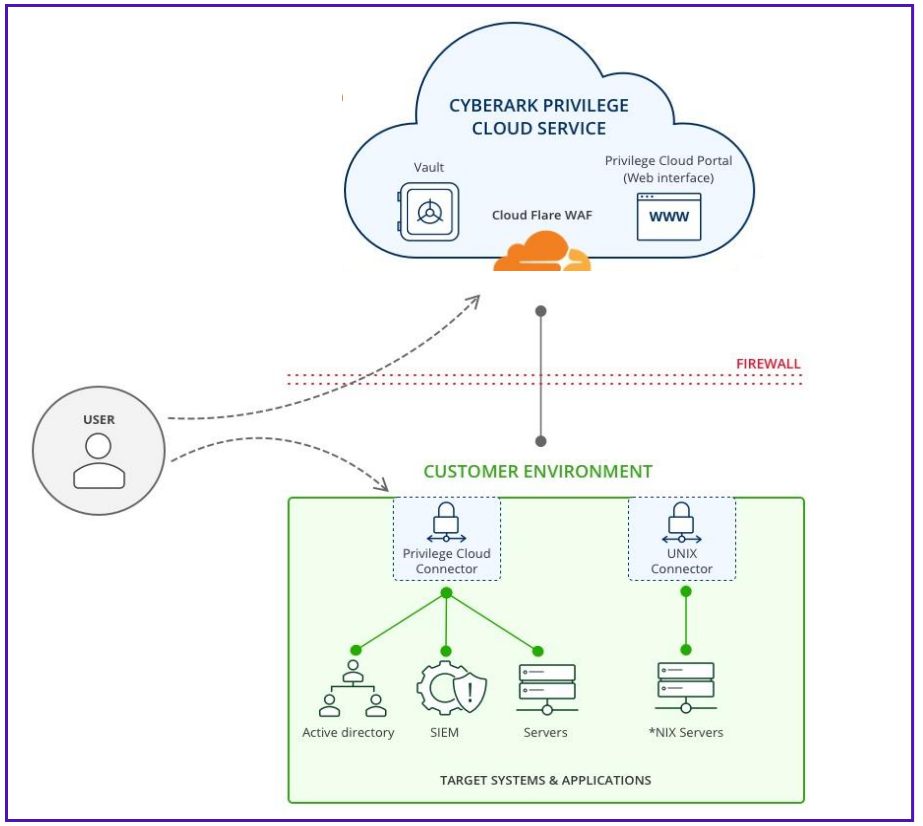
- Credentials not known to anyone and securely stored in the vault
- No traces left behind on the end targets
- Credentials are rotated periodically
- Threat analysis and automatic response

CYBERARK PRIVILEGED ACCESS SECURITY (PAS) PRODUCTS

Core Privileged Access Security

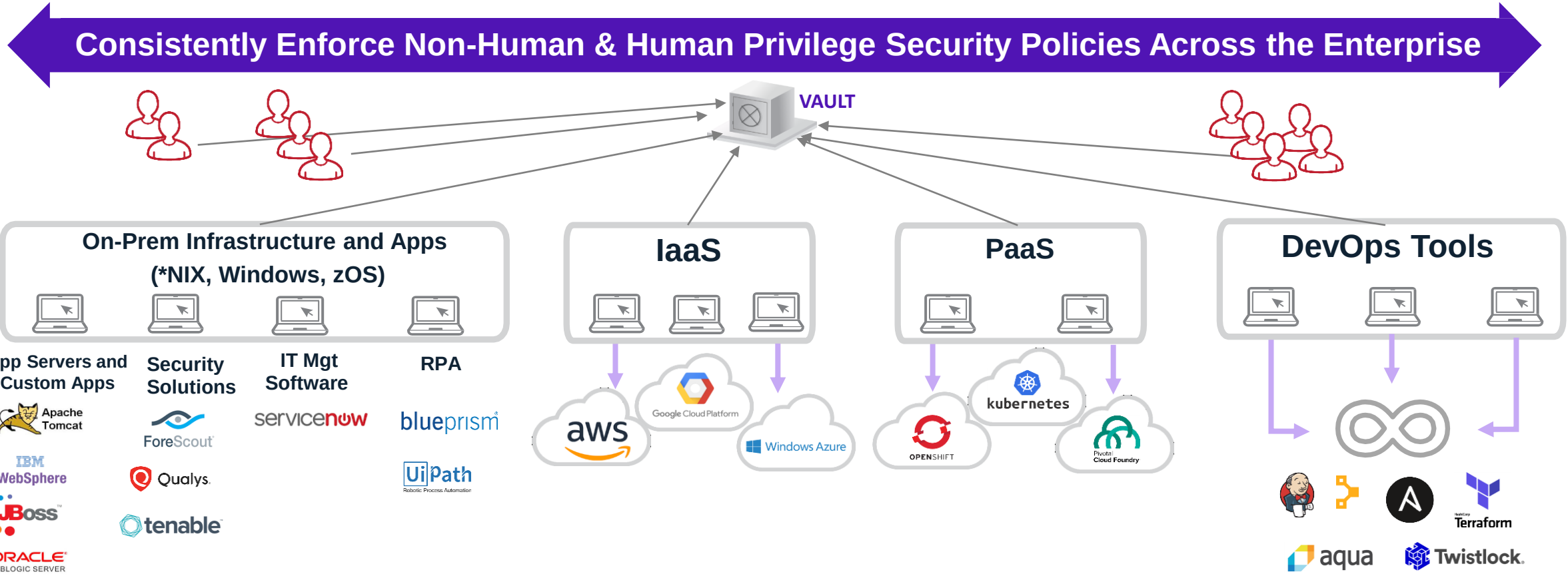


Privileged Cloud



ENTERPRISE-WIDE PRIVILEGE SECURITY POLICIES

CISO AND IT LEADERS WANT TO CONSISTENTLY ENFORCE PRIVILEGE SECURITY POLICIES. BOTH FOR HUMAN & NON-HUMAN IDENTITIES

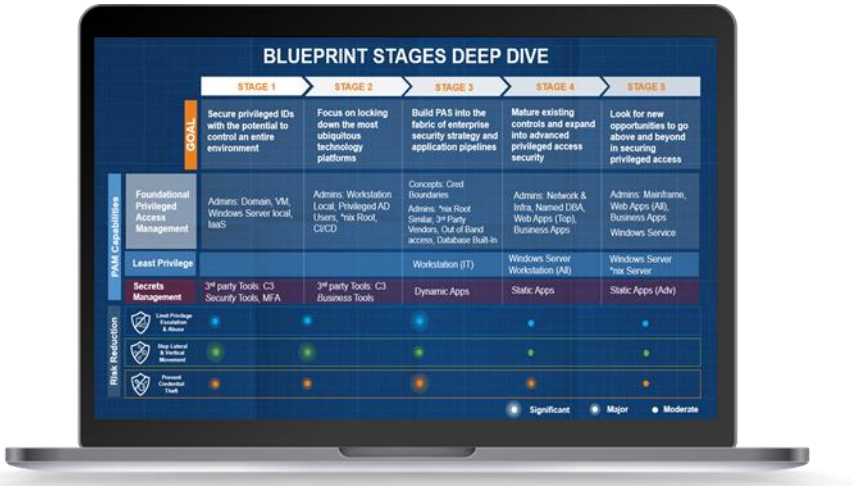


>Demo time...

WONDERING WHERE TO START…?

DNA Tool

Discovery & Audit



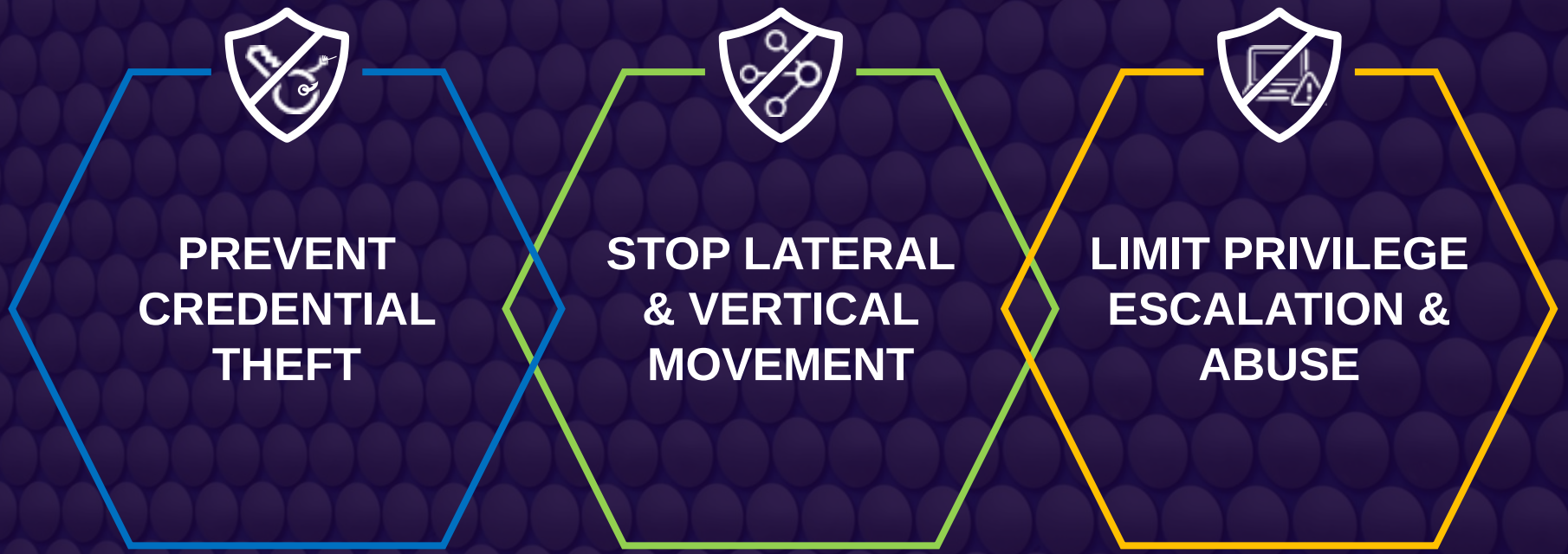
CyberArk Blueprint

CYBERARK DNA SCAN

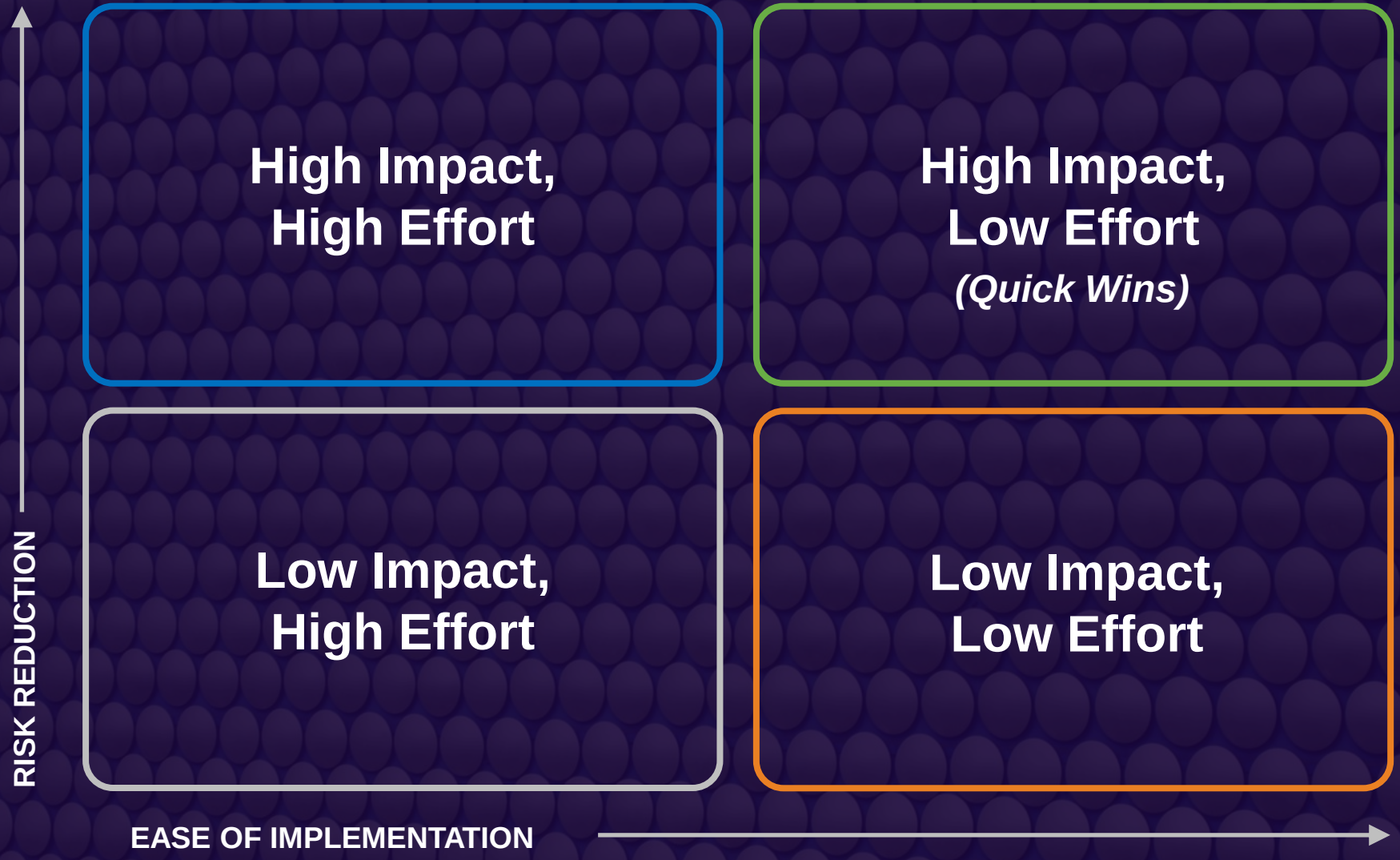
- **Gain visibility of privileged accounts**
  In Windows, *nix, Mac, and then some more.
- **Uncovered vulnerabilities**
  Identify machines vulnerable to credential theft attacks and assess the security risks.
- **Clean up ancient credentials**
  Disable or change the high risk credentials which have not been changed for a long time.
- **Requires:**
  - Executable without installation
  - License file (Free)
  - Connectivity and account to scan machines

THE CYBERARK BLUEPRINT

CYBERARK PAM SUCCESS BLUEPRINT: 3 GUIDING PRINCIPLES



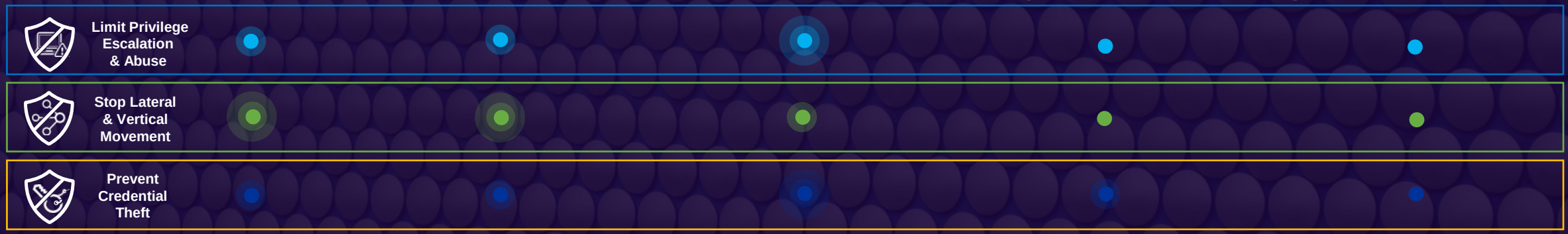
RISK PRIORITIZATION METHODOLOGY



BLUEPRINT STAGES DEEP DIVE

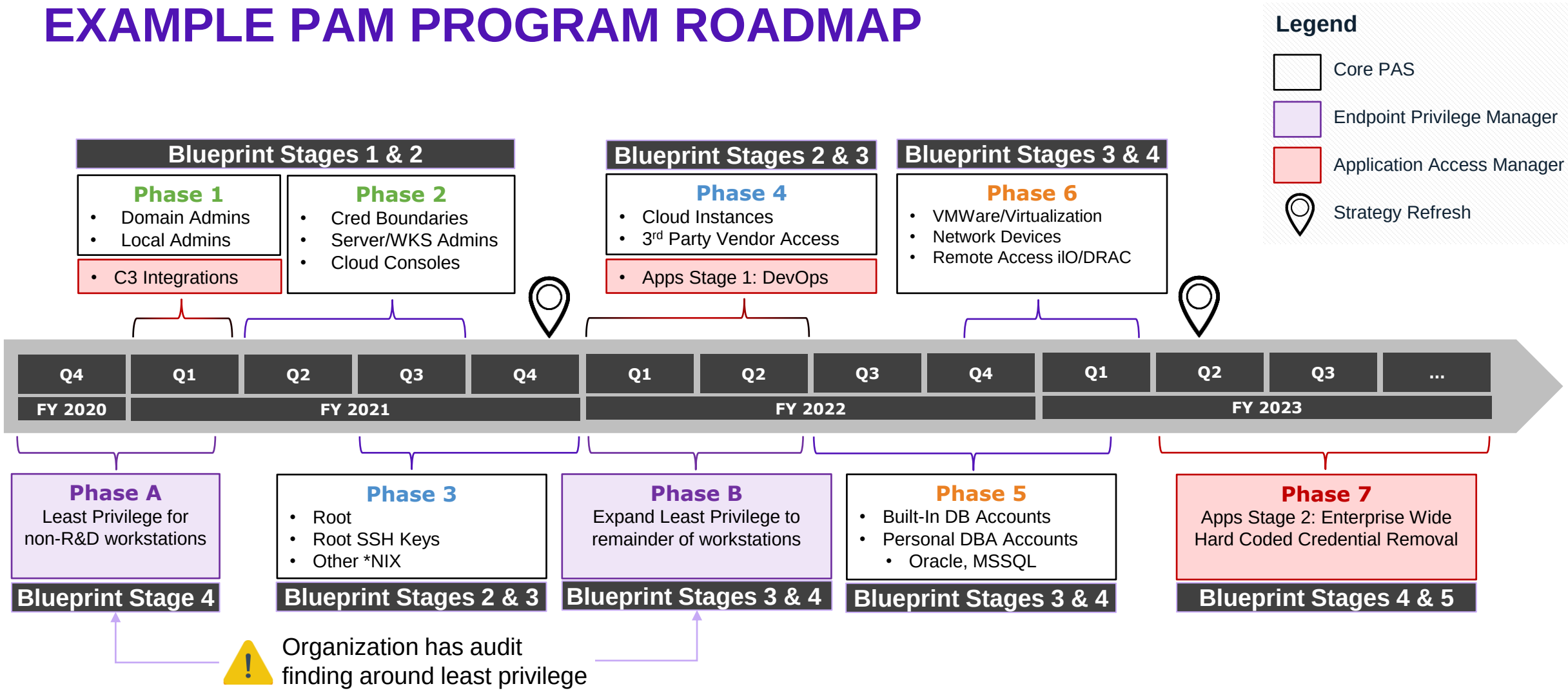
	STAGE 1	STAGE 2	STAGE 3	STAGE 4	STAGE 5
GOAL	**Secure privileged IDs with the potential to control an entire environment**	**Focus on locking down the most ubiquitous technology platforms**	**Build PAS into the fabric of enterprise security strategy and application pipelines**	**Mature existing controls and expand into advanced privileged access security**	**Look for new opportunities to go above and beyond in securing privileged access**
PAM Capabilities					
Foundational Privileged Access Management	Admins: Domain, VM, Windows Server local, IaaS	Admins: Workstation Local, Privileged AD Users, *nix Root, CI/CD	Concepts: Cred Boundaries Admins: *nix Root Similar, 3rd Party Vendors, Out of Band access, Database Built-In	Admins: Network & Infra, Named DBA, Web Apps (Top), Business Apps	Admins: Mainframe, Web Apps (All), Business Apps Windows Service
Least Privilege			Workstation (IT)	Windows Server Workstation (All)	Windows Server *nix Server
Secrets Management	3rd party Tools: C3 *Security* Tools, MFA	3rd party Tools: C3 *Business* Tools	Dynamic Apps	Static Apps	Static Apps (Adv)

Risk Reduction



Significant Major Moderate

EXAMPLE PAM PROGRAM ROADMAP



The CyberArk Blueprint is NOT a definite roadmap. It is a series of recommendations to GUIDE roadmap design.

THANK YOU

Samira Zaker Soltani

szs@cyberlagom.com

+31(0)682019193

CyberLagom.com