# Who is PAM? Get to Know Her — She Should be a Part of Every Identity Conversation

**Grace Sands**

Manager,
Cyber Security Services

KPMG

**Zach Limacher**

Managing Director,
Cyber Security Services

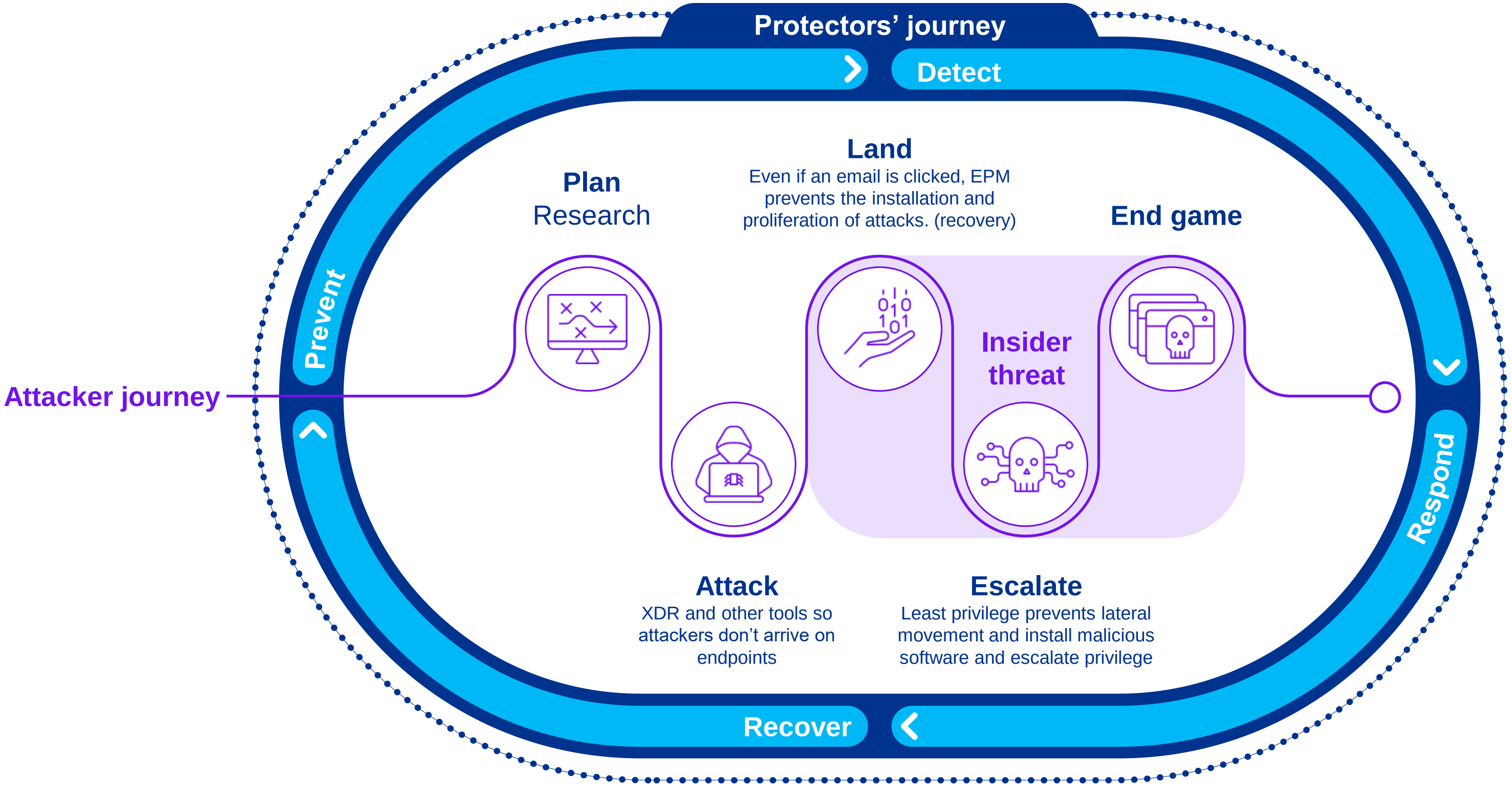
KPMG

# Ice Breaker

Which of the following is not a privileged identity?

1. Privileged accounts
2. Users with privileged access (regardless how privilege is assigned)
3. Administrative authorizations
4. Trust relationships such as SSH keys
5. High risk business users

# Attack surface area and cyber kill chain



**Plan**
Research

**Land**
Even if an email is clicked, EPM prevents the installation and proliferation of attacks. (recovery)

**End game**

**Attack**
XDR and other tools so attackers don't arrive on endpoints

**Escalate**
Least privilege prevents lateral movement and install malicious software and escalate privilege

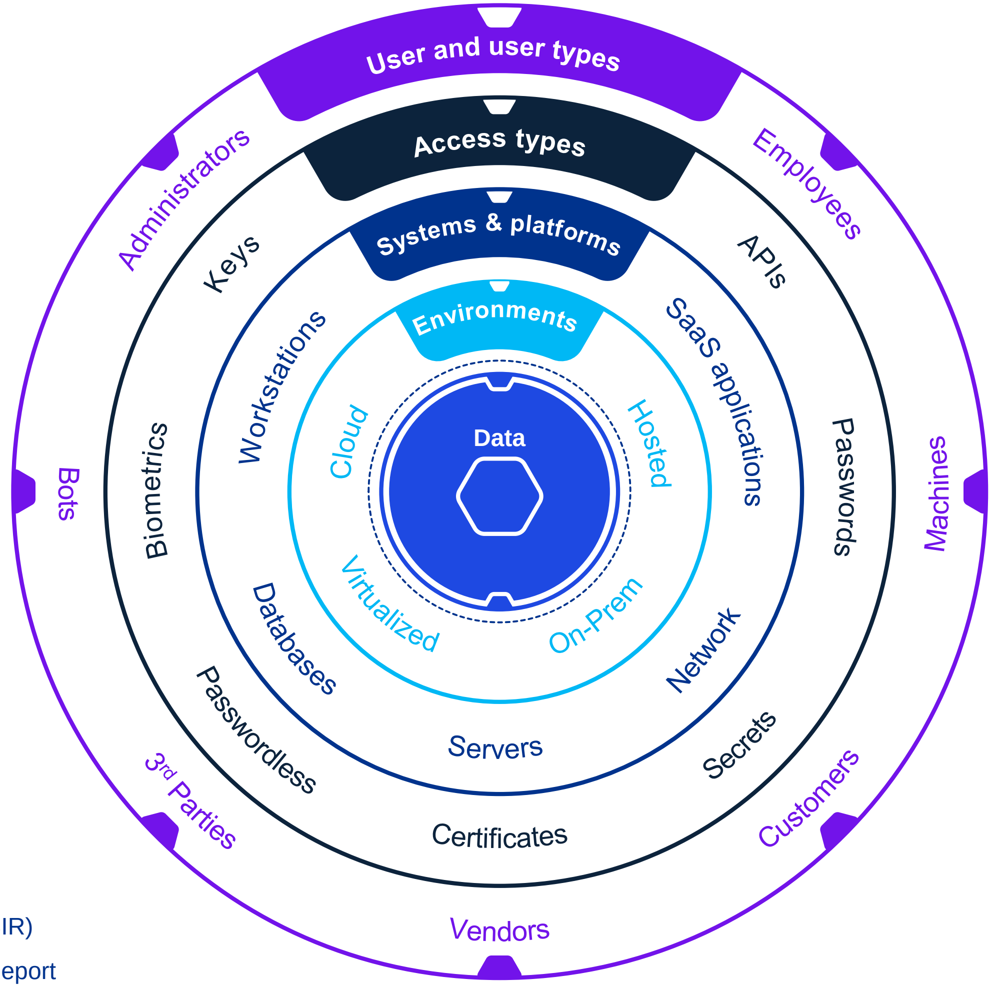
# Widened spectrum of privileged identities

**82% of data breaches** involved a human element[1]

Machine identities outnumber human identities 45:1 and 68% of those nonhuman IDs have access to sensitive data / assets[2]

**Vulnerability exploits from Verizon DBIR**

**Over 25% of workers** have access to business critical data and applications (mostly SaaS) using unprotected identities[2]



**87% of IT decision makers** reported that secrets are stored in multiple places across DevOps environments[2]

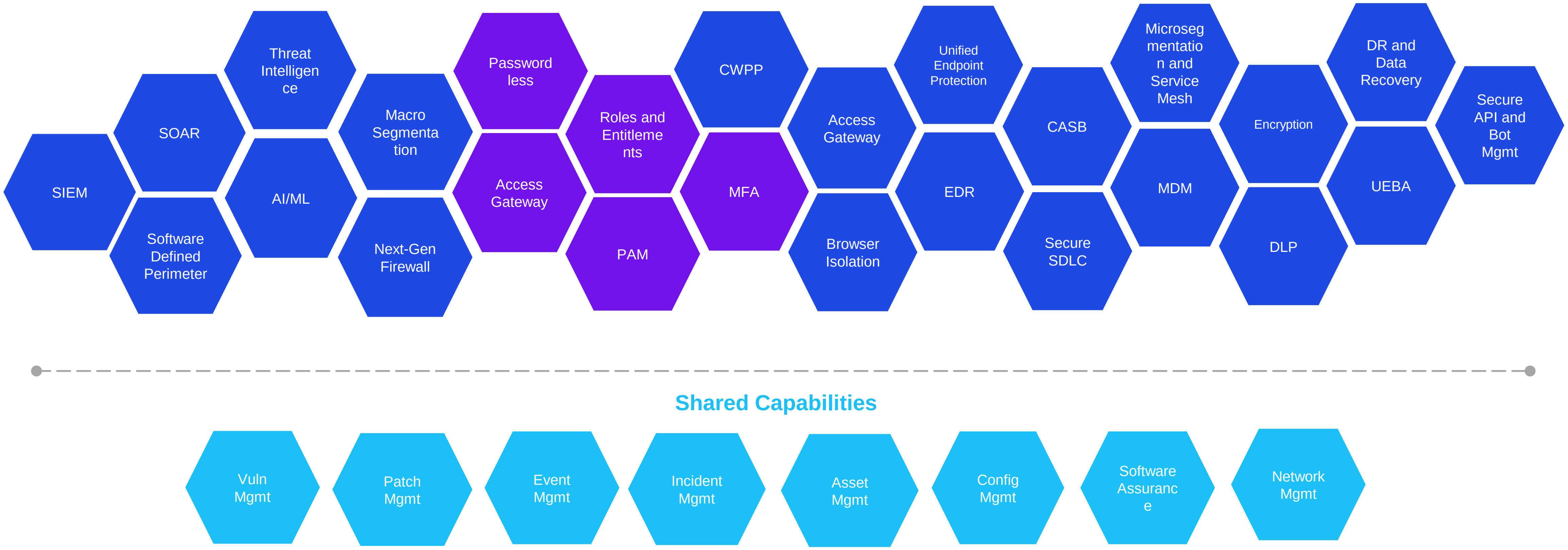
An average staff person accesses more than 30 applications/accounts[2]

**13% of breaches** are due to misconfiguration, most involving cloud storage[1]

[1] 2022 Verizon Data Breach Investigations Report (DBIR)

[2] CyberArk 2022 Identity Security Threat Landscape Report

# Identity security for zero trust



SIEM

SOAR

Software Defined Perimeter

Threat Intelligence

AI/ML

Macro Segmentation

Next-Gen Firewall

Passwordless

Access Gateway

Roles and Entitlements

PAM

CWPP

MFA

Access Gateway

Browser Isolation

Unified Endpoint Protection

EDR

CASB

Secure SDLC

Microsegmentation and Service Mesh

MDM

Encryption

DLP

DR and Data Recovery

UEBA

Secure API and Bot Mgmt

Shared Capabilities

Vuln Mgmt

Patch Mgmt

Event Mgmt

Incident Mgmt

Asset Mgmt

Config Mgmt

Software Assurance

Network Mgmt

# What actions you can take

Actionable steps you can take as an identity professional

### Bringing Identity Capabilities to Others

Bring the historical PAM capabilities such as session management out of the administrative world, and extend into the high-risk business world

### Best of the Best Access Management

Leverage the best of access management and level of assurance to your entire ecosystem e.g., MFA, contextual and step-up authentication, activity risk ranking

### Leverage AI

Proactive and prepared to maximize AI capabilities in your entire program

# Q&A

# THANK YOU!