Fortifying the Digital Citadel: Navigating the Privileged Access Management Maturity Journey for Enhanced Security Posture

Securing Identities at Every Interaction

Patrick van der Veen, CISSP, CCSP, OSCP

Director Sales Engineering – Northern Europe

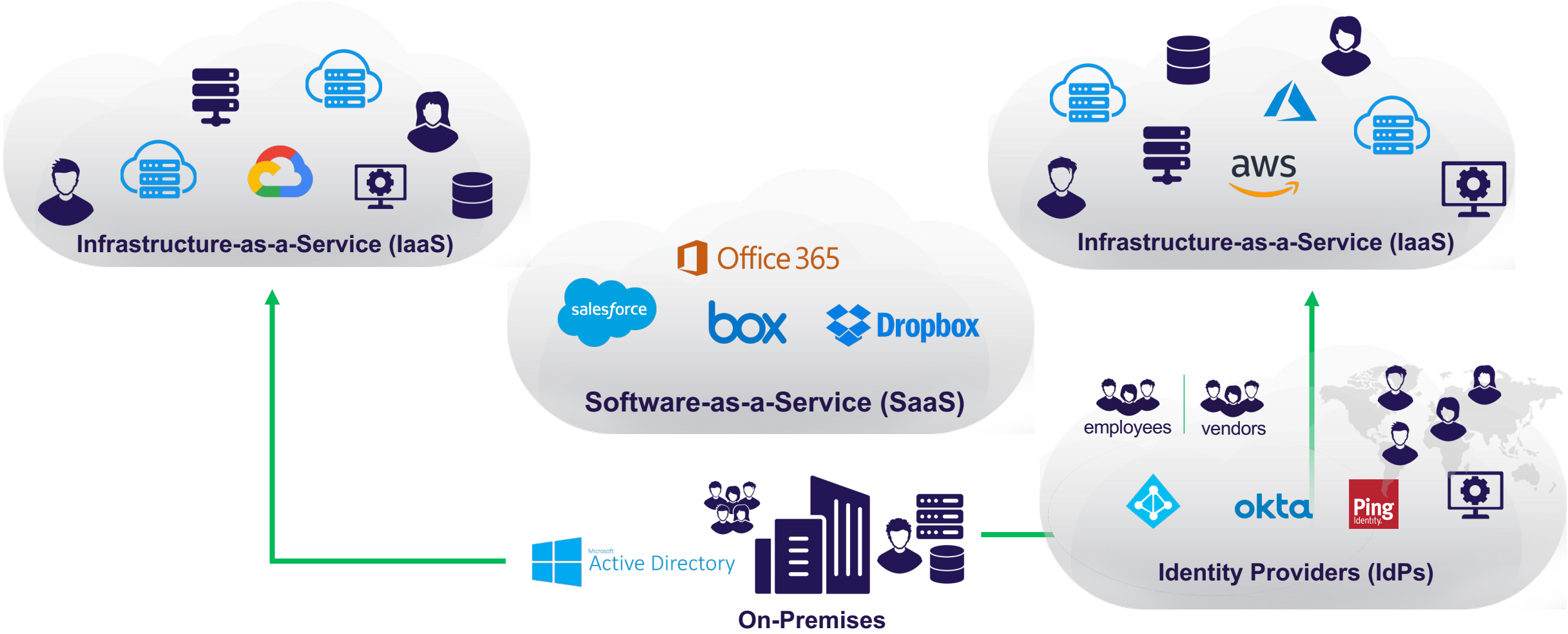
The Reality Check

What keeps security leaders up at night?

- **Data Breach**
- **Ransomware**
- **Financial Fraud**
- **Insider Risk**
- **Malware**
- **Revenue/Brand Loss**
- **Data Poisoning**
- **Compliance Failure**
- **Service/Application Downtime**

The rising complexity: What do you actually control?

Improperly configured identities throughout cloud infrastructure introduce risk



80% of modern attacks are identity-driven

CROWDSTRIKE

99% of cloud identifies are too permissive

UNIT 42 BY PALO ALTO NETWORKS

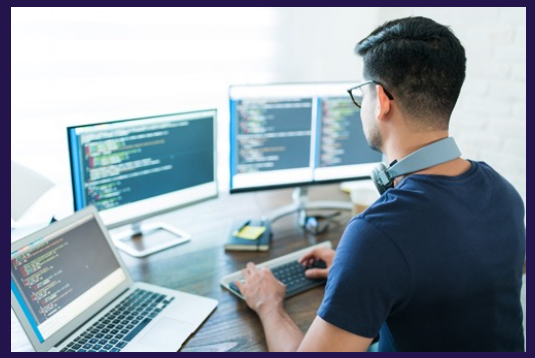
More than **5 machine identities** for every user identity

paloalto NETWORKS

75% of security failure will come down to the inadequate management of identity and privileges

Gartner

Most Cyberattacks target Privileged Access?



Admin/Security/
Helpdesk/3rd Party

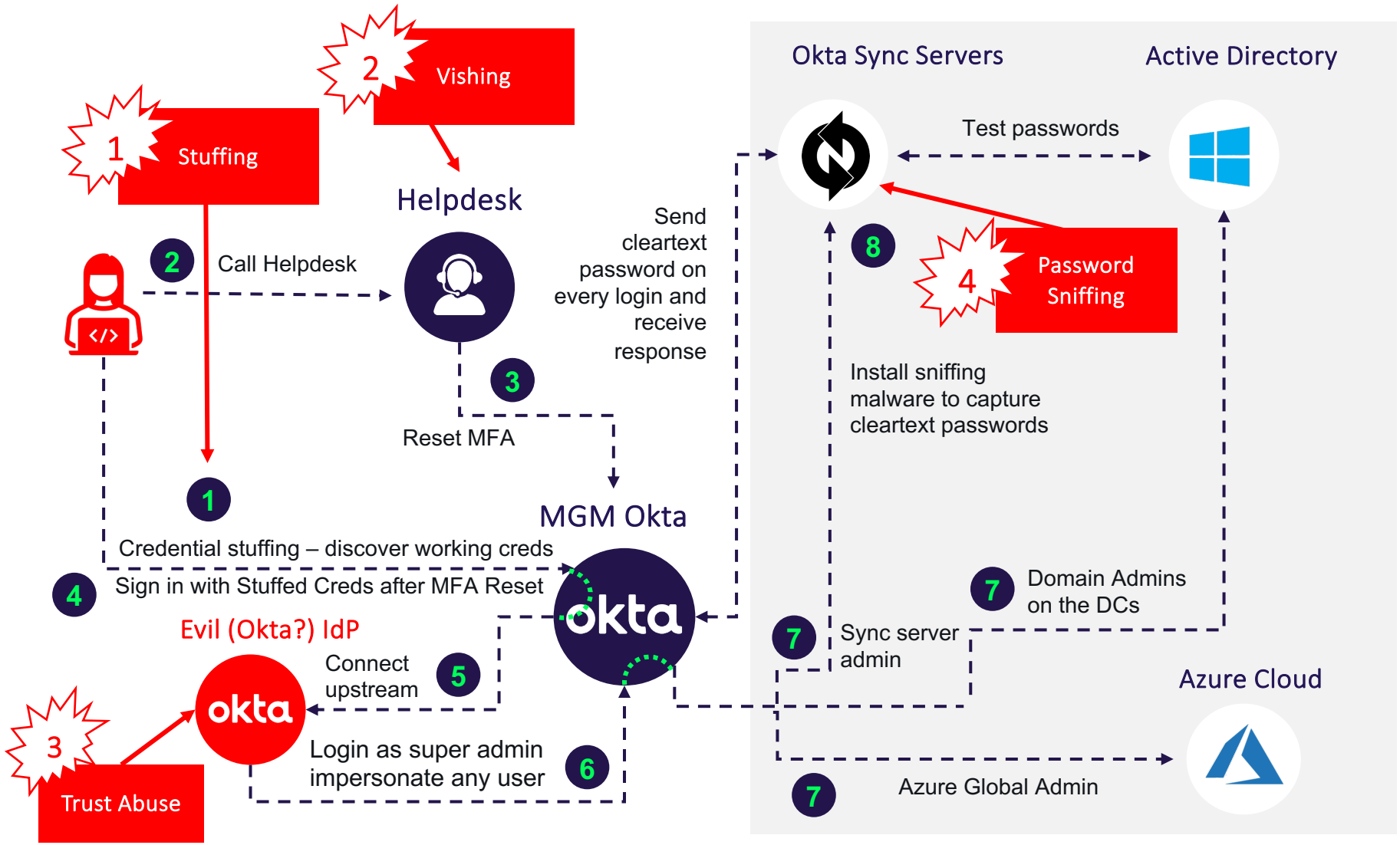
Apps/API/RPA/
Service Accounts

Int./Ext. Business User
or 3rd Party

Almost ALL Identities are PRIVILEGED

MGM Case Study: Attack Kill Chain

* Because some details are left unpublished, we added logical conjectures based on what's known about the attack and Scattered Spider TTPs



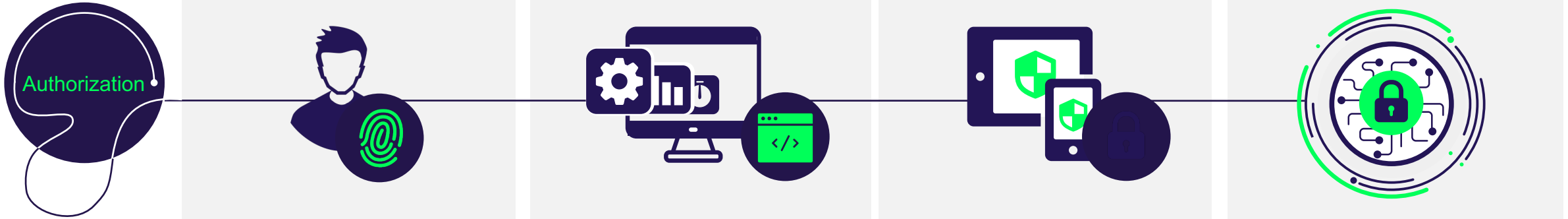
1

Source of Cyber Fatigue

Remembering and changing passwords

Users tend to reuse passwords

Current approaches and tools don’t address the common thread: Authorization



IAM SOLUTIONS	APPLICATION SECURITY	ENDPOINT SECURITY	NETWORK SECURITY
Identities provide access but are easily compromised	Complex to implement for multiple app layers & related services	Identities can still bypass endpoint controls	Monitoring network traffic isn’t meaningful: 90% is encrypted anyway

Impacting the ability to deliver business initiatives

Ransomware Resilience

Digital Transformation

Cyber Insurance

Regulatory Compliance

Securing Distributed Workforce

Zero Trust

DEFINE:
What is Privileged Access and Authorization?

- ✓ Human, Machines, Services, Application?
- ✓ Hardware, Software, On Premise or in the Cloud
- ✓ Who needs to use them? Internal or External
- ✓ How often do they need to be used?
- ✓ Are they location or department specific?
- ✓ Sensitivity of the application or data the account is protecting
- ✓ Service/System Owner?

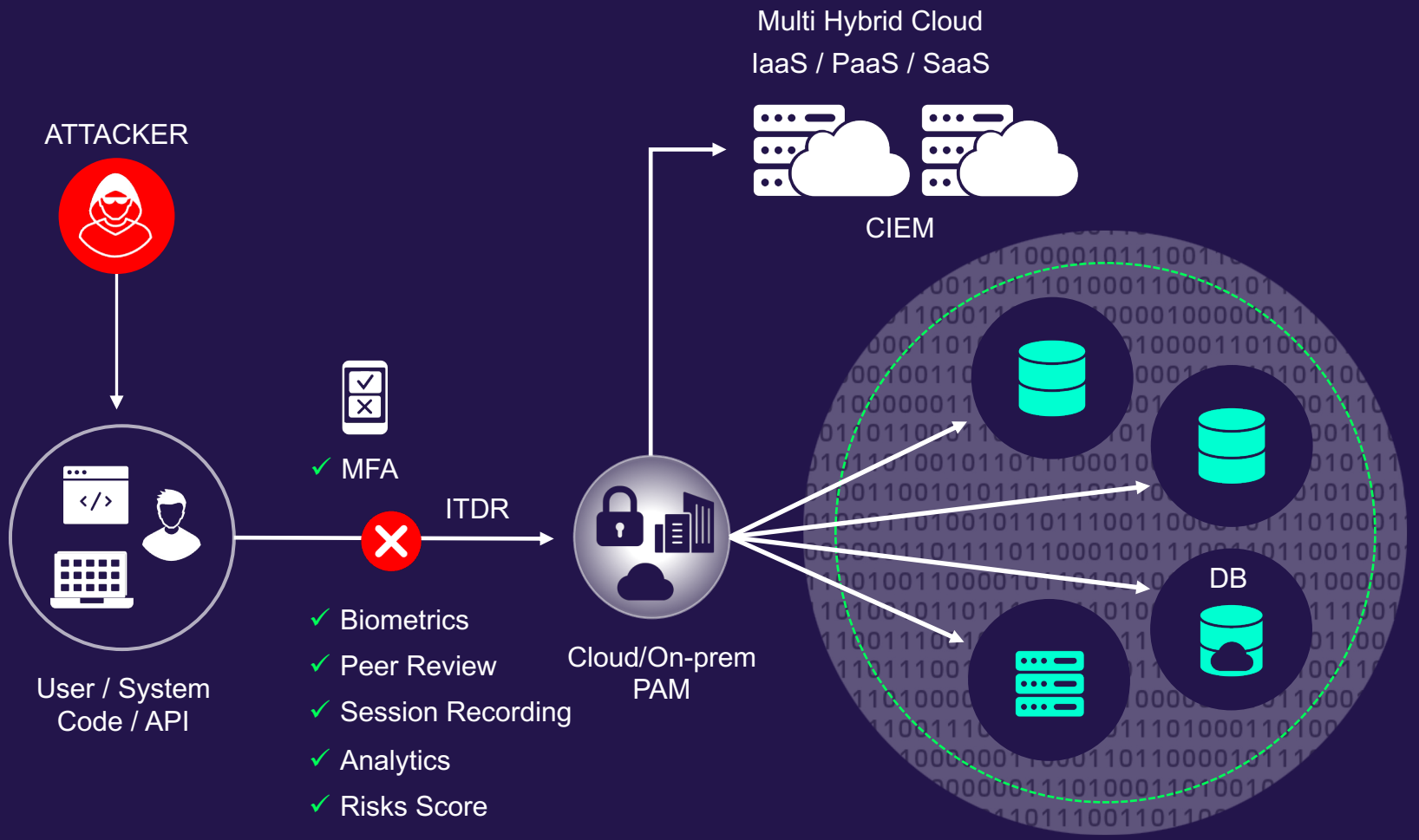
Privileged Access Management Lifecycle

1. Define Privileged Access / Authorization
2. Automate Discovery of Privileges
3. Manage and Secure Privileged Access
4. Monitor Usage and Access
5. Alert on privilege abuse
6. Enable PAM for Incident Response
7. Continuous Review, Audit & Update

Classifying Trust Dynamically

Adaptive and Context-based Security

- ✓ Secure Digital Identity
- ✓ Multi fA (Trust Level)
- ✓ Secure Privileged Access
- ✓ Secure Data Vaults
- ✓ Check Reputation
- ✓ Check Behavior
- ✓ Check Risks
- ✓ Secure Cloud

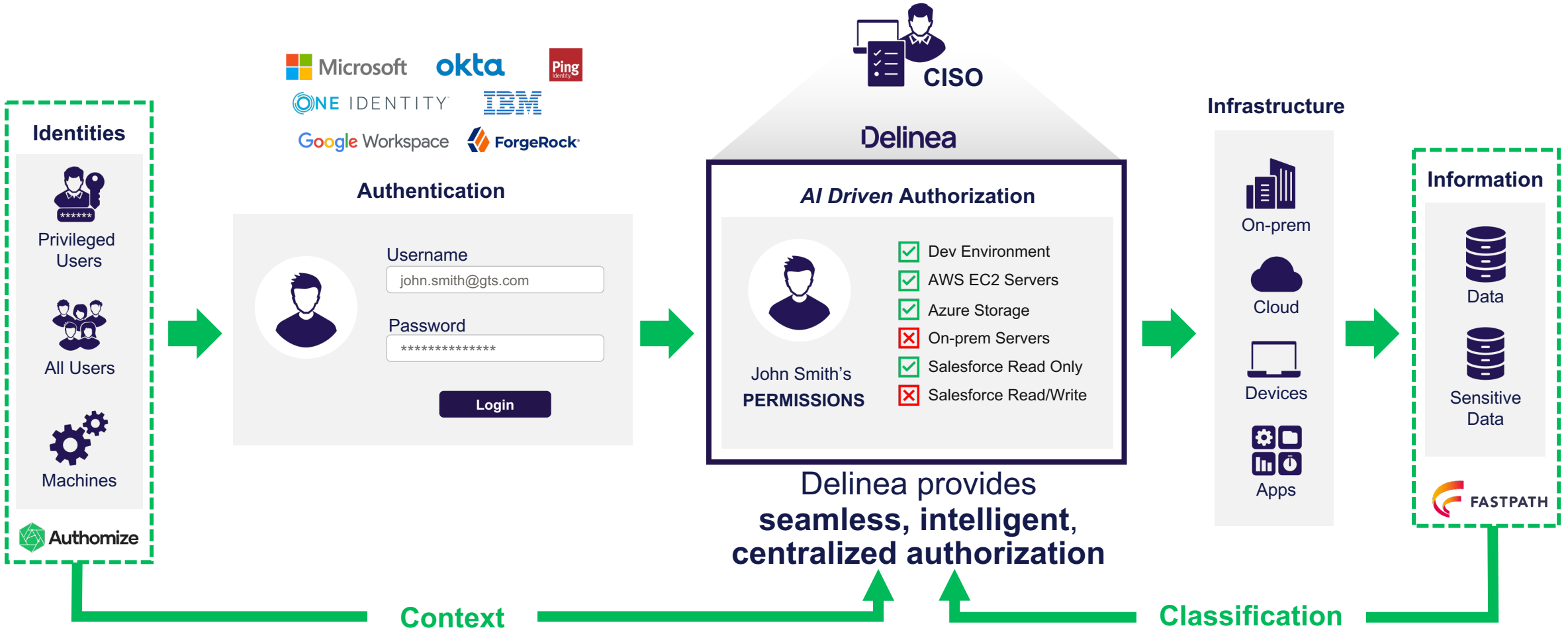


Delinea

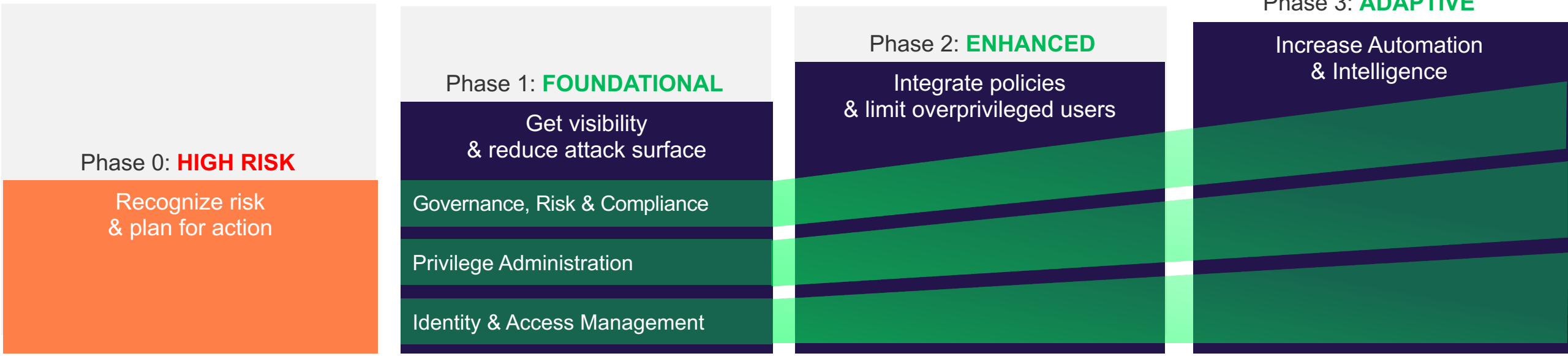
WHY?
Privileged Access Management is a Top Priority & Good for Everyone

- ✓ PAM is **MORE THAN SECURITY**: It saves money
- ✓ PAM is a **POSITIVE SECURITY** experience and empowers employees
- ✓ PAM is a **WIN** for the CISO
- ✓ PAM is a **FAST TRACK** to compliance/cyber insurance
- ✓ PAM helps you **RECOVER QUICKLY** from cyber-attacks
- ✓ PAM is a powerful security solution and makes a **CYBER CRIMINAL'S JOB MORE DIFFICULT**

The vision is to build context around identities and data to drive authorization



The authorization maturity model



- → **No/limited visibility**
- → **Manual employee join, move, leave**
- → **Credentials manually managed**
- → **Full admin rights**

- → **Discover & vault IDP, CSP, ERP credentials**
- → **Enforce MFA for credential access**
- → **Detect account takeover threats**
- → **Establish privileged remote access**
- → **Monitor critical business apps**
- → **Automate user identity lifecycle**

- → **Discover and vault all credentials**
- → **Clean up admin accounts**
- → **Enforce temporary least privilege**
- → **Enforce MFA for system & app login**
- → **Enforce MFA for privilege elevation**
- → **Risk analytics for access request workflows**
- → **Certify entitlements for critical apps**

- → **Automate app identity lifecycle**
- → **Enrich SOC with identity threat intel**
- → **Manage service account lifecycle**
- → **Risk scoring for enhanced conditional access**
- → **Leverage audit data & ML analytics to detect and respond to threats**
- → **Automate identity threat remediation**

Delinea's expanding portfolio

Delinea Platform

Secure Credentials
Identify & Vault Secrets


Vaulting

Machine Secrets


Service Accounts

Privileged Remote Access
VPN-less Remote Access

Secure Remote Access

Vendor PAM

Privilege & Entitlement Elevation
Granular Real-time Controls


Servers


Workstations


Cloud


Identity Lifecycle


Access Review

Identity Governance & Access Controls


Auditing & Analytics


Segregation of Duties

Identity Protection

- Discover Identity Vulnerabilities, Misconfigurations, and Over-privileged Users
- Detect Identity-based Breaches
- Remediate

Shared Capabilities

- Continuous Discovery
- Audit and Analytics
- AI
- MFA
- Ecosystem

Why Delinea

Seamless, intelligent, centralized authorization to better secure the modern enterprise

We make you more secure

Accelerated adoption through seamless authorization controls

Detect & address identity threats in real-time

We make you more productive

Deploy in weeks, not months

Requiring 90% fewer resources to manage than the nearest competitor

We futureproof identity security

Guaranteed 99.99% uptime & zero downtime upgrades

Code to production in 30 minutes

Leader

IN ALL 5 MAJOR PAM ANALYST REPORTS IN 2023

9,000+

CUSTOMERS

4.8 / 5

CSAT RATING

800+

5-STAR GARTNER PEER REVIEWS

400+

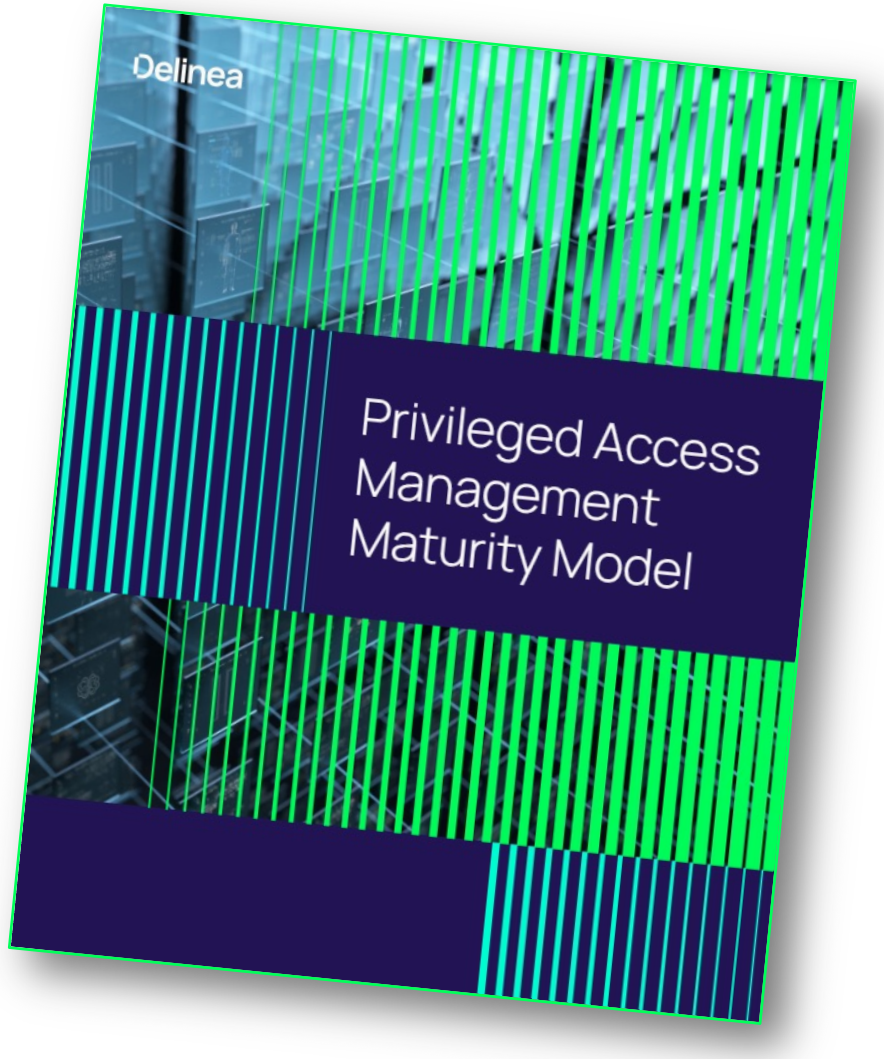
INTEGRATIONS, TEMPLATES, & TOOLS

Delinea

Privileged Access Management Maturity Model

A framework to help organizations systematically lower privileged account risk, increase business agility, and improve operational efficiency.

GET THE WHITEPAPER



Thank You.

Delinea

Securing identities at every interaction