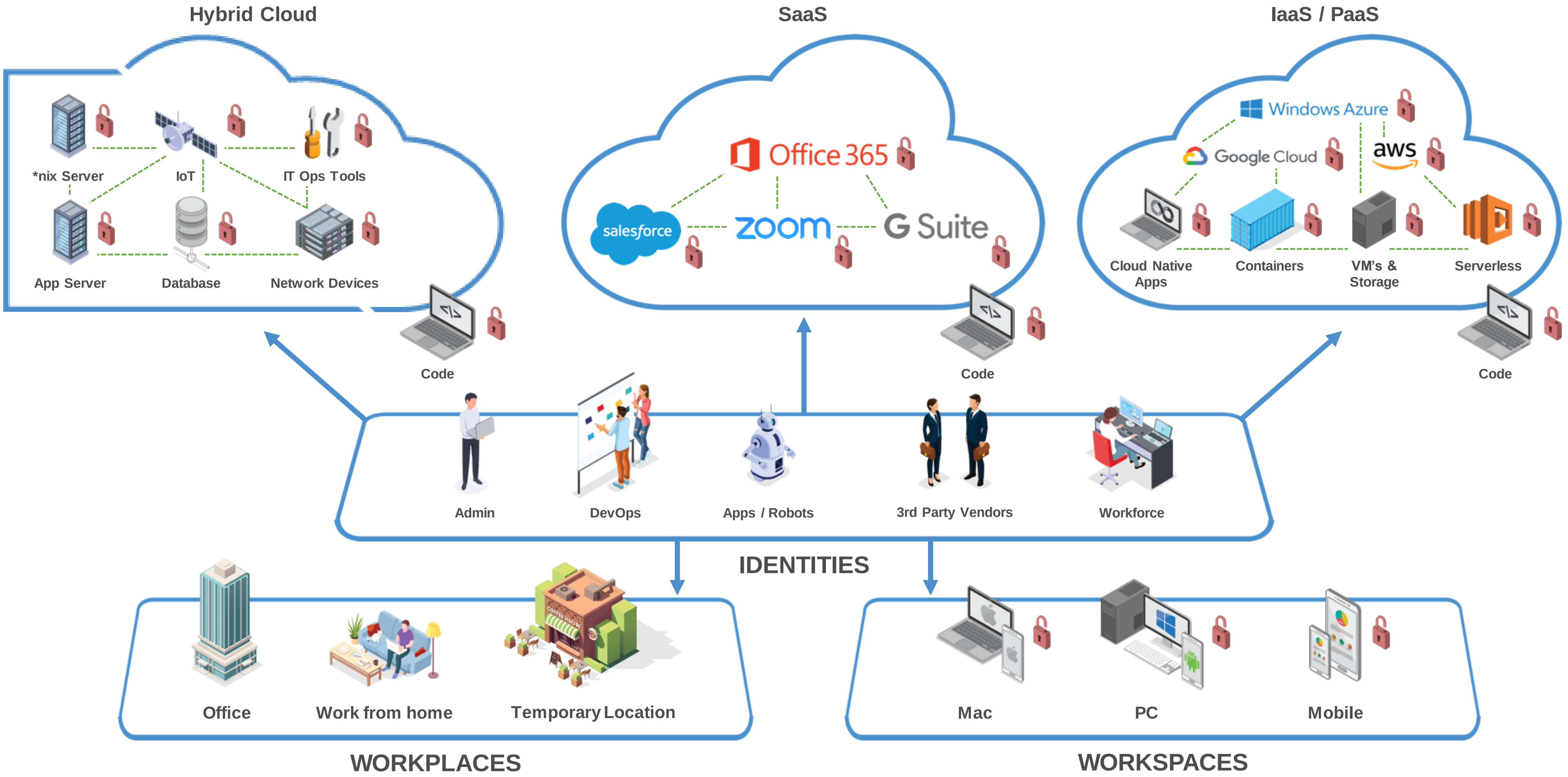
CYBERARK®

IDENTITY PROTECTION

AS THE KEY OF SECURITY

Marcin Paciorkowski
Senior Solutions Engineer, CISSP
marcin.paciorkowski@cyberark.com

ENTERPRISES TODAY



2020 – ANOTHER YEAR OF IDENTITY COMPROMISE

80% of Data Breaches involved Stolen Credentials*

77% of [those] Cloud Breaches also involved breached credentials*

Source https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

IDENTITY SECURITY IS THE KEY

CHALLENGES

SECURING PERIMETERLESS ENTERPRISE

MANAGING ACCOUNTS AND PASSWORDS

ENABLING REMOTE WORKFORCE

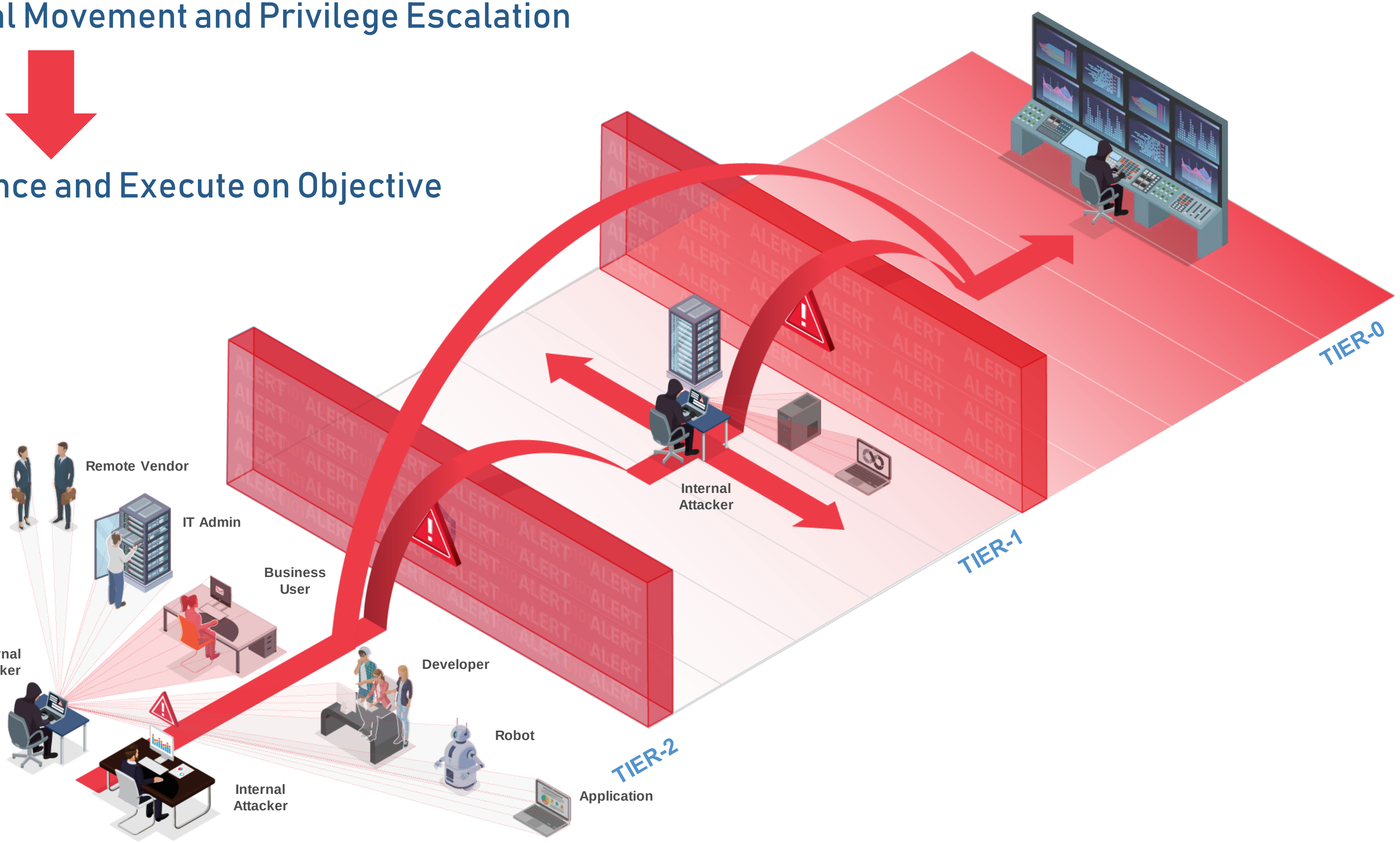
IDENTITY WITHIN THE ATTACK CHAIN

Credential Theft, Lateral Movement and Privilege Escalation

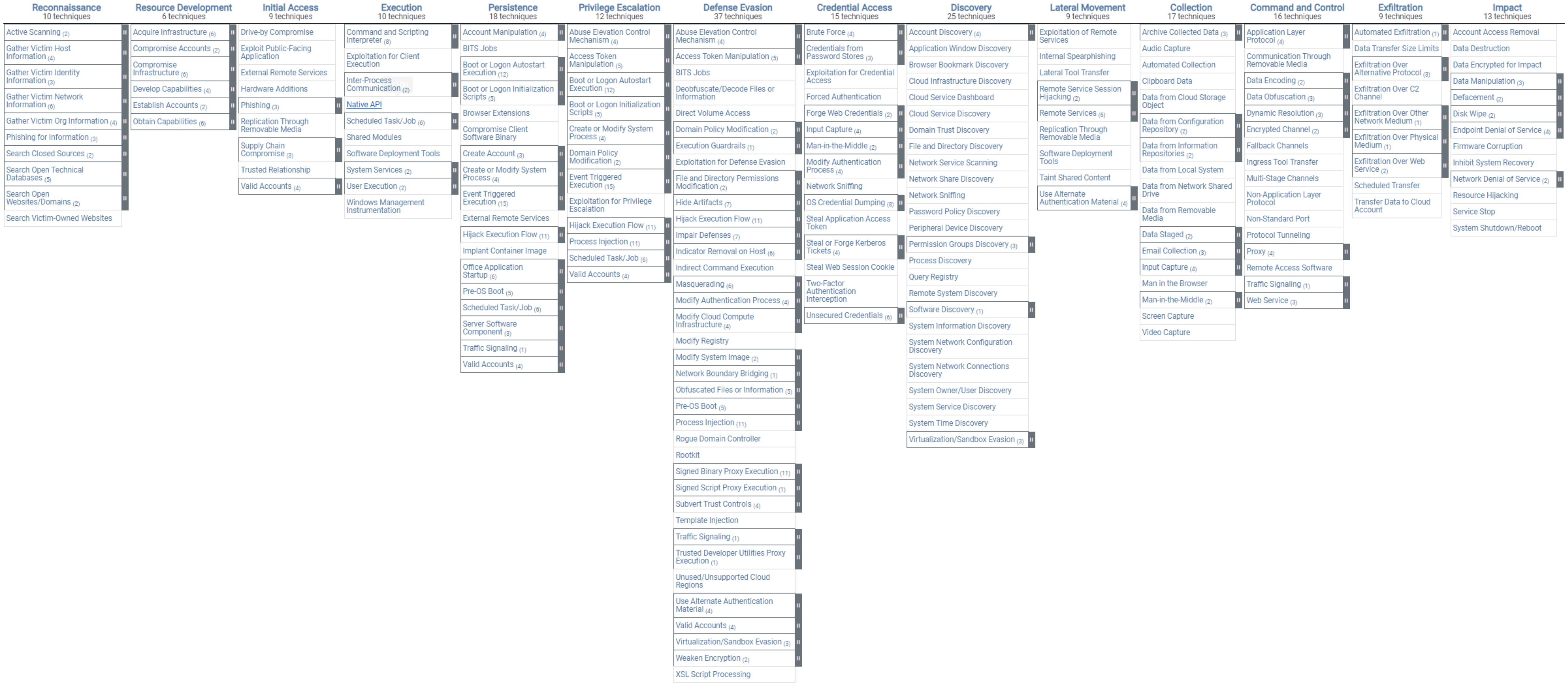
↓

Establish Persistence and Execute on Objective

Ransomware



ATTACK TRENDS – MITRE ATT&CK FRAMEWORK



Reconnaissance
10 techniques

- Active Scanning (2)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (2)
- Search Victim-Owned Websites

Resource Development
6 techniques

- Acquire Infrastructure (6)
- Compromise Accounts (2)
- Compromise Infrastructure (6)
- Develop Capabilities (4)
- Establish Accounts (2)
- Obtain Capabilities (6)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution
10 techniques

- Command and Scripting Interpreter (8)
- Exploitation for Client Execution
- Inter-Process Communication (2)
- Native API
- Scheduled Task/Job (6)
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (2)
- Windows Management Instrumentation

Persistence
18 techniques

- Account Manipulation (4)
- BITS Jobs
- Boot or Logon Autostart Execution (12)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (15)
- External Remote Services
- Hijack Execution Flow (11)
- Implant Container Image
- Office Application Startup (6)
- Pre-OS Boot (5)
- Scheduled Task/Job (6)
- Server Software Component (3)
- Traffic Signaling (1)
- Valid Accounts (4)

Privilege Escalation
12 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (12)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Event Triggered Execution (15)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (11)
- Process Injection (11)
- Scheduled Task/Job (6)
- Valid Accounts (4)

Defense Evasion
37 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (7)
- Hijack Execution Flow (11)
- Impair Defenses (7)
- Indicator Removal on Host (6)
- Indirect Command Execution
- Masquerading (6)
- Modify Authentication Process (4)
- Modify Cloud Compute Infrastructure (4)
- Modify Registry
- Modify System Image (2)
- Network Boundary Bridging (1)
- Obfuscated Files or Information (5)
- Pre-OS Boot (5)
- Process Injection (11)
- Rogue Domain Controller
- Rootkit
- Signed Binary Proxy Execution (11)
- Signed Script Proxy Execution (1)
- Subvert Trust Controls (4)
- Template Injection
- Traffic Signaling (1)
- Trusted Developer Utilities Proxy Execution (1)
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material (4)
- Valid Accounts (4)
- Virtualization/Sandbox Evasion (3)
- Weaken Encryption (2)
- XSL Script Processing

Credential Access
15 techniques

- Brute Force (4)
- Credentials from Password Stores (3)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Man-in-the-Middle (2)
- Modify Authentication Process (4)
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (4)
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials (6)

Discovery
25 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (3)

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

Collection
17 techniques

- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (2)
- Data from Information Repositories (2)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)
- Email Collection (3)
- Input Capture (4)
- Man in the Browser
- Man-in-the-Middle (2)
- Screen Capture
- Video Capture

Command and Control
16 techniques

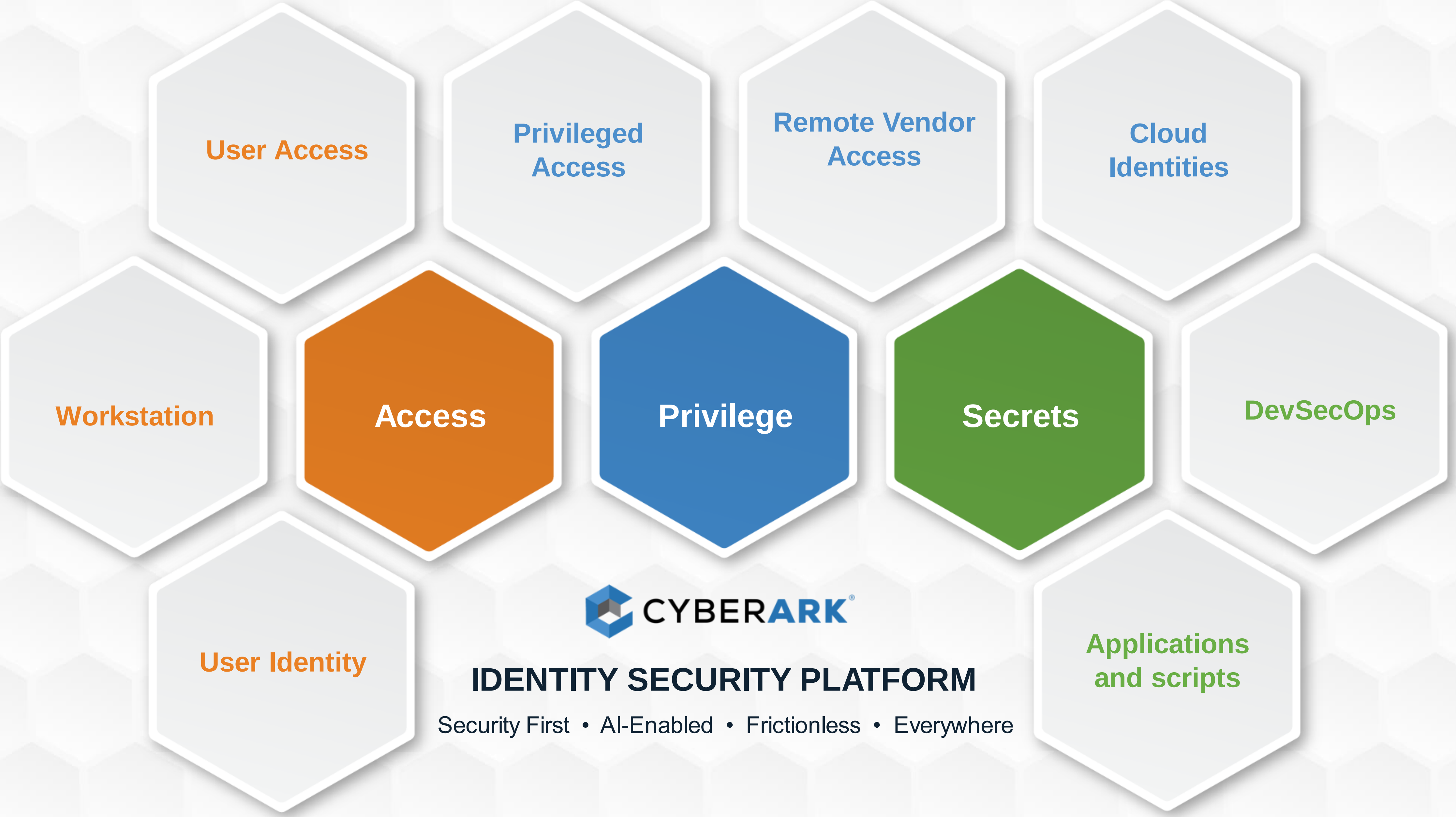
- Application Layer Protocol (4)
- Communication Through Removable Media
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)
- Remote Access Software
- Traffic Signaling (1)
- Web Service (3)

Exfiltration
9 techniques

- Automated Exfiltration (1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (2)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3)
- Defacement (2)
- Disk Wipe (2)
- Endpoint Denial of Service (4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot



User Access

Privileged Access

Remote Vendor Access

Cloud Identities

Workstation

Access

Privilege

Secrets

DevSecOps

User Identity

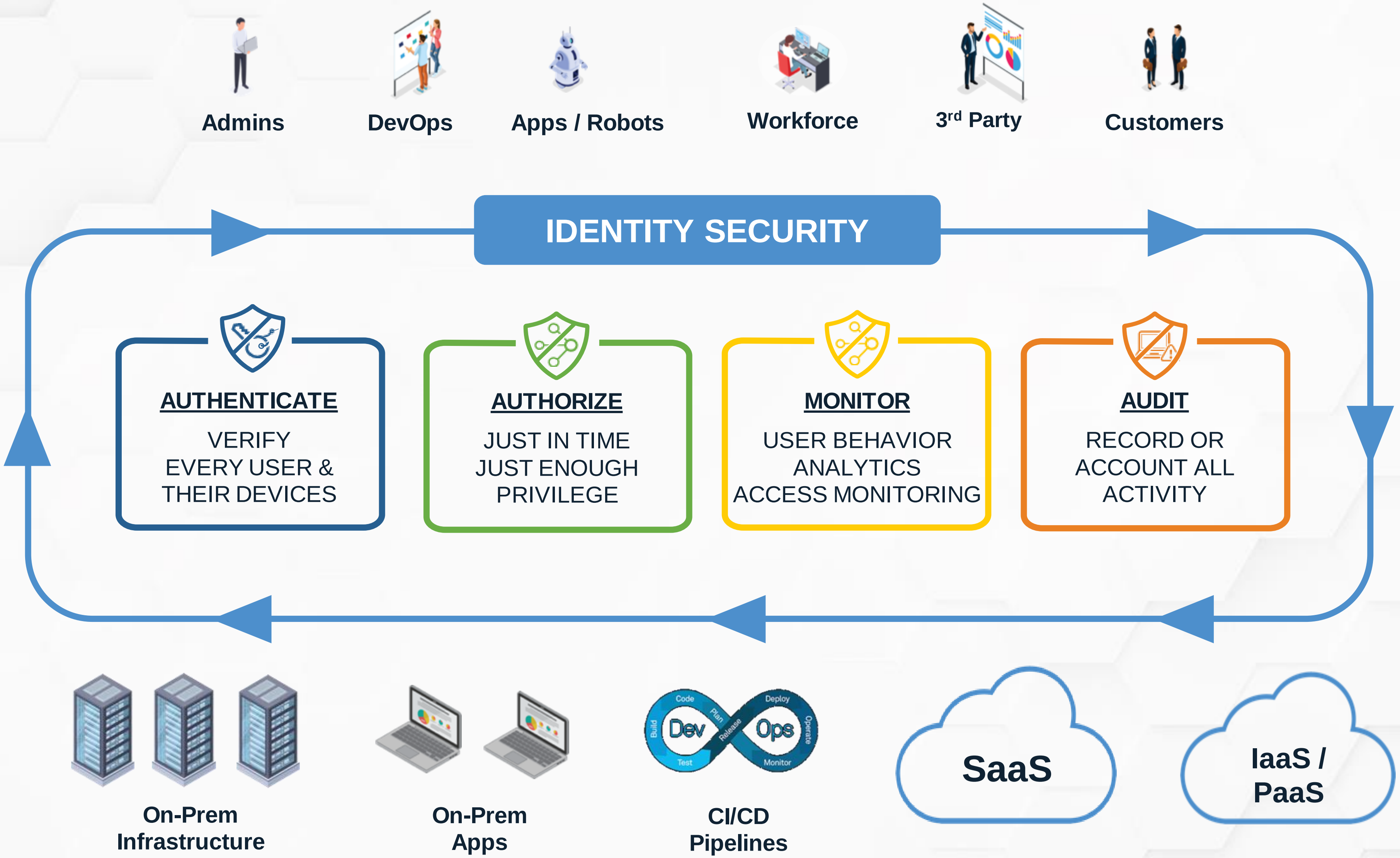
Applications and scripts

CYBERARK

IDENTITY SECURITY PLATFORM

Security First • AI-Enabled • Frictionless • Everywhere

WHAT IS IDENTITY SECURITY



Admins

DevOps

Apps / Robots

Workforce

3rd Party

Customers

IDENTITY SECURITY

AUTHENTICATE

VERIFY
EVERY USER &
THEIR DEVICES

AUTHORIZE

JUST IN TIME
JUST ENOUGH
PRIVILEGE

MONITOR

USER BEHAVIOR
ANALYTICS
ACCESS MONITORING

AUDIT

RECORD OR
ACCOUNT ALL
ACTIVITY

On-Prem
Infrastructure

On-Prem
Apps

CI/CD
Pipelines

SaaS

IaaS /
PaaS

CYBERARK BLEUPRINT WORKSHOP FRIDAY, 16.00 – 16.45

Marcin Paciorkowski

Senior Solutions Engineer, CISSP

marcin.paciorkowski@cyberark.com

CYBERARK®

THANK YOU!!!

Marcin Paciorkowski
Senior Solutions Engineer, CISSP
marcin.paciorkowski@cyberark.com