CYBERARK®

THREAT LANDSCAPE 2019
A PERSPECTIVE OF PRIVILEGE

Andy Thompson, CISSP GPEN

WHOAMI – ANDY THOMPSON

- Programs Office - Customer Success ¯_(ツ)_/¯
- B.S. MIS – Univ of Texas at Arlington
- Credentials:
  - COMPTIA A+ & Sec+
  - (ISC)2 SSCP & CISSP
  - GIAC – Certified Penetration Tester (GPEN)
- DC214 / DHA / ISSA / NTXCSG +++
- Travel-Hacker

CYBERARK

CIO Journal.

Malware Targets Vulnerable Admin Accounts

Many a CIO has warned employees about malicious links in e-mail that potentially give hackers an entry into corporate networks. Increasingly, sophisticated cyber attacks are using so-called privileged accounts.

SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Privileged Accounts Play Key Role in Advanced Cyber Attacks

Malware and attackers are increasingly targeting privileged accounts as part of multi-stage operations where they breach networks, gather information, and exfiltrate

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

Privileged Account Details Are Often Shared and Can Be a Weak Entry Point for Attackers

Privileged user accounts can be a way for attackers to infiltrate an entire network

infosecurity
STRATEGY | INSIGHT | TECHNOLOGY

Privileged Accounts at Root of Most Data Breaches

If enterprises ever were given wake-up call, it should be this: stealing and exploiting privileged accounts is a critical success factor for attackers in 100% of all

Forbes

Grasping the Problem with Privileged Accounts

Many in the security industry tend to focus on authentication strength a

The New York Times

Attack Gave Chinese Hackers Privileged Access to U.S. Systems

By DAVID E. SANGER, NICOLE PERLROTH and MICHAEL D. SHEAR JUNE 20, 2015

InformationWeek
DARKReading

Watch the Watchers: 'Trusted' Employees Can Do Damage

CSO

Privilege Comes with Peril in World of Cybersecurity

Security experts have been warning enterprises for some time that the greatest security threats come from within: their own employees. And that message has apparently

USA TODAY

Privileged Accounts: The Master Keys Hackers Know Best

One big reason cyberintruders can easily roam far and wide, once they crack inside a company network, is that many organizations pay scant heed to privileged accounts

FINANCIAL TIMES myFT

England + Add to myFT

England's NHS hit by large scale cyber attack

6 HOURS AGO by: Financial Times

England's National Health Service has been hit by a large scale cyber attack, with hospitals across the country reporting IT systems are down.

THINK LIKE THE ATTACKER -> WHY THEY ARE SUCCESSFUL

LOOK FOR EXPOSED PRIVILEGED ACCOUNTS

BYPASS PRIVILEGED ACCESS SECURITY CONTROLS

LEVERAGE KNOWN ATTACKS FOR BYPASSING AUTHENTICATION

GO UNDETECTED WHILE ABUSING PRIVILEGED ACCESS


IIOT / OT Security
DevOps
Identity Security
Cloud Security
PRIVILEGED SECURITY · PRIVILEGED SECURITY · PRIVILEGED SECURITY · PRIVILEGED SECURITY
CROWN JEWELS
Sensitive Infrastructure, Assets, and Data
Data Security
SIEM and Threat Intelligence
Endpoint Security
Network Security

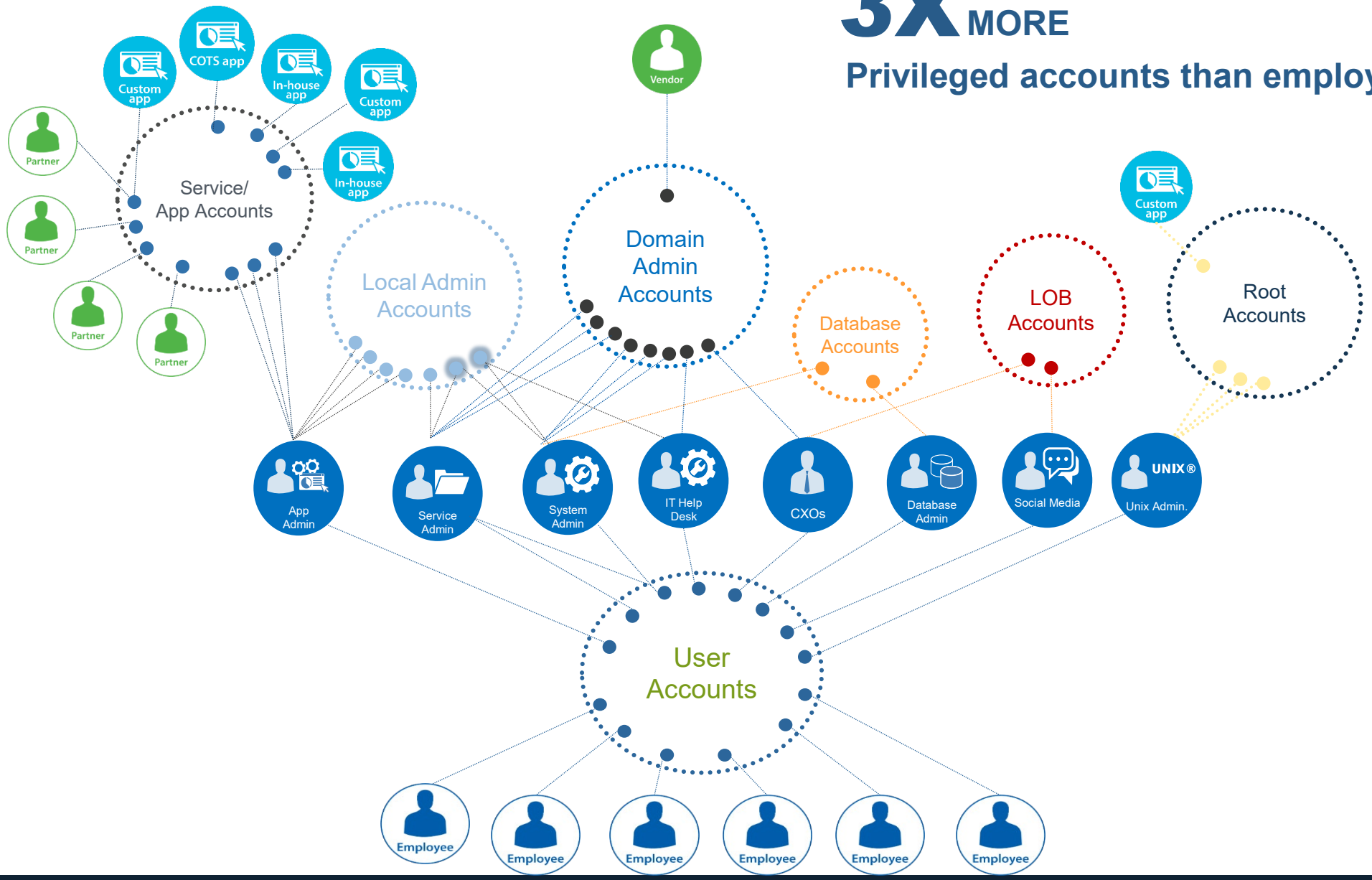
WHAT IS A PRIVILEGED ACCOUNT?

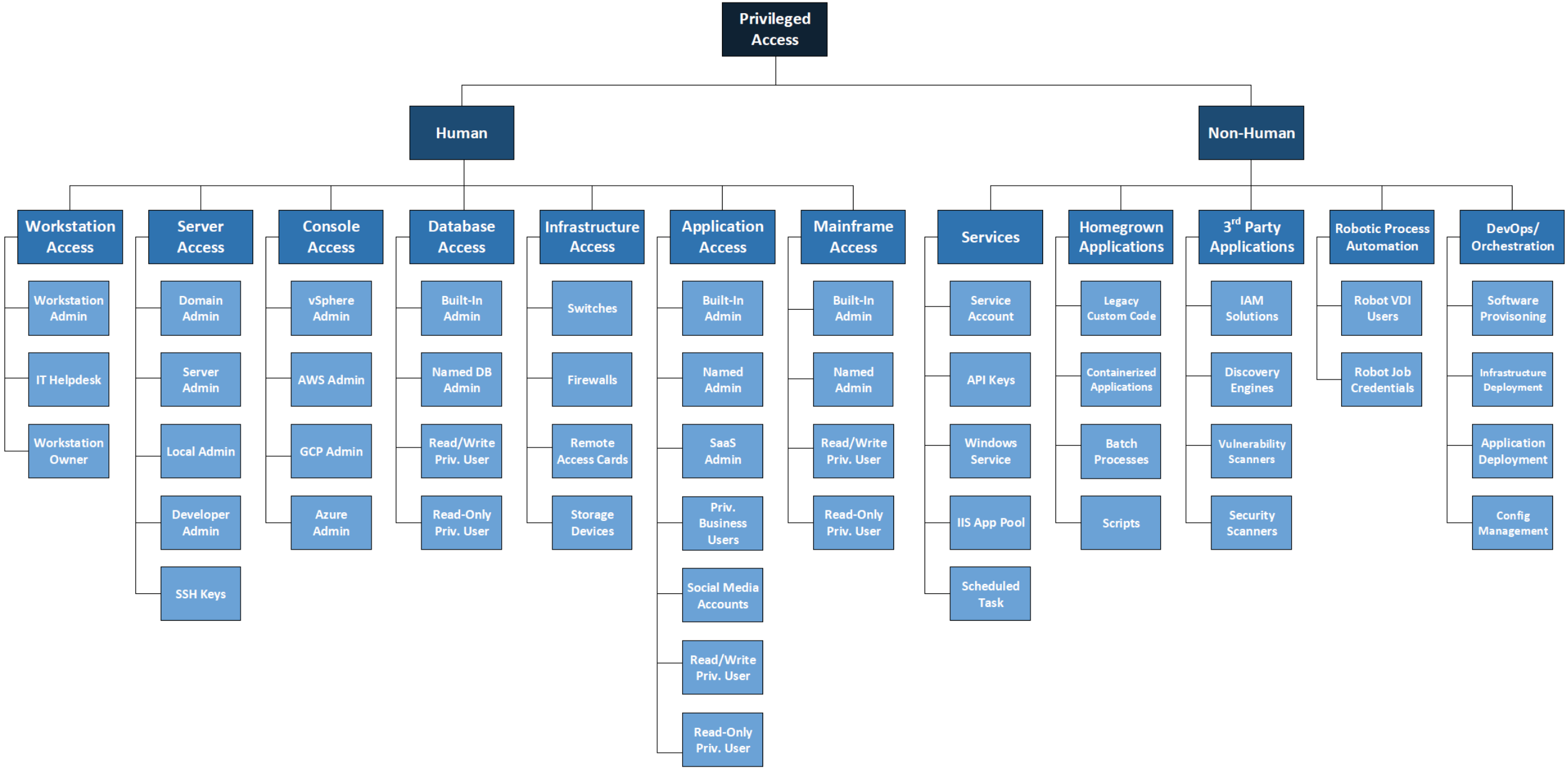
	Type	Used by	Used for
Elevated Personal Accounts	• IT personnel accounts • Executive accounts • SaaS administrators • Local admin account	• IT staff • Executives • Any employee	• Privileged operations • Access to sensitive data • Managing web-based apps
Shared Privileged Accounts	• Administrator • Root • Cisco Enable • Oracle SYS • Local Administrators	• IT staff • Sys admins • DBAs • Help desk • Developers • Social media managers	• Privileged operations • Disaster recovery • Emergency • Administration • Access to sensitive data
Application Accounts	• Service Accounts • Hard coded/ embedded App IDs	• Applications/scripts • Windows Services • Scheduled Tasks • Batch jobs, etc • Developers	• Online database access • Batch processing • App-2-App communication

THE EXPANDING ATTACK SURFACE

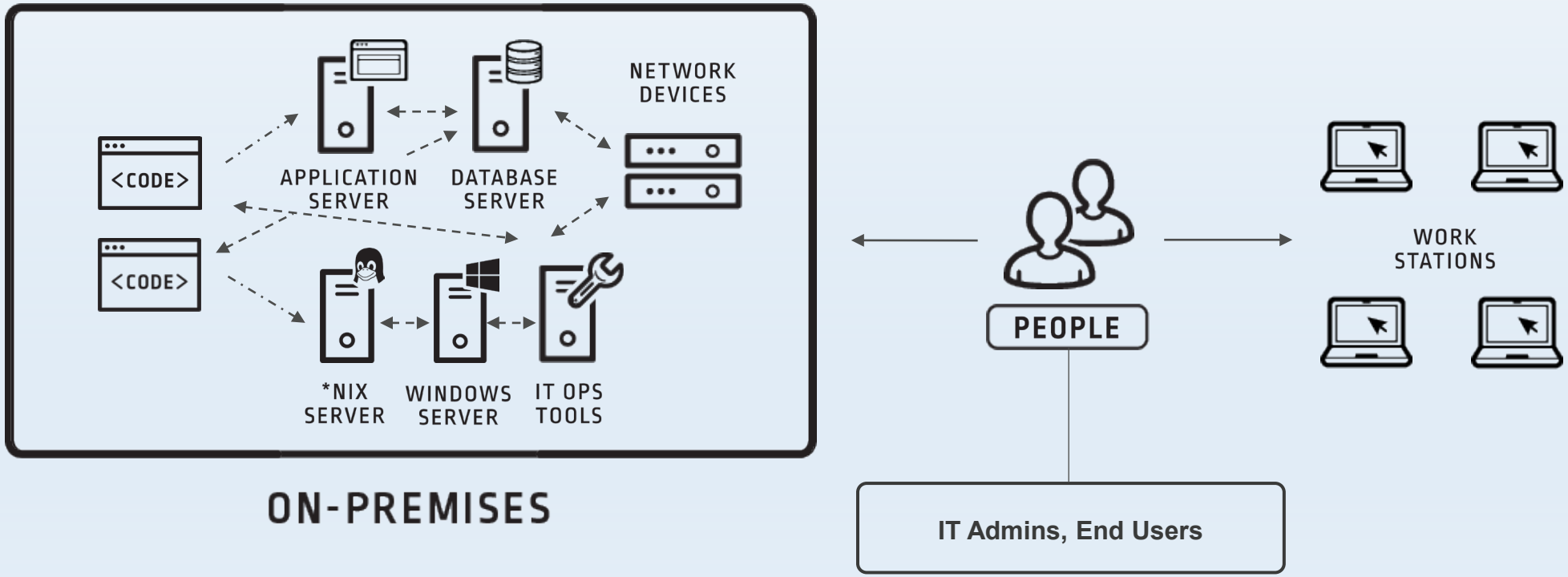
3X MORE

Privileged accounts than employees

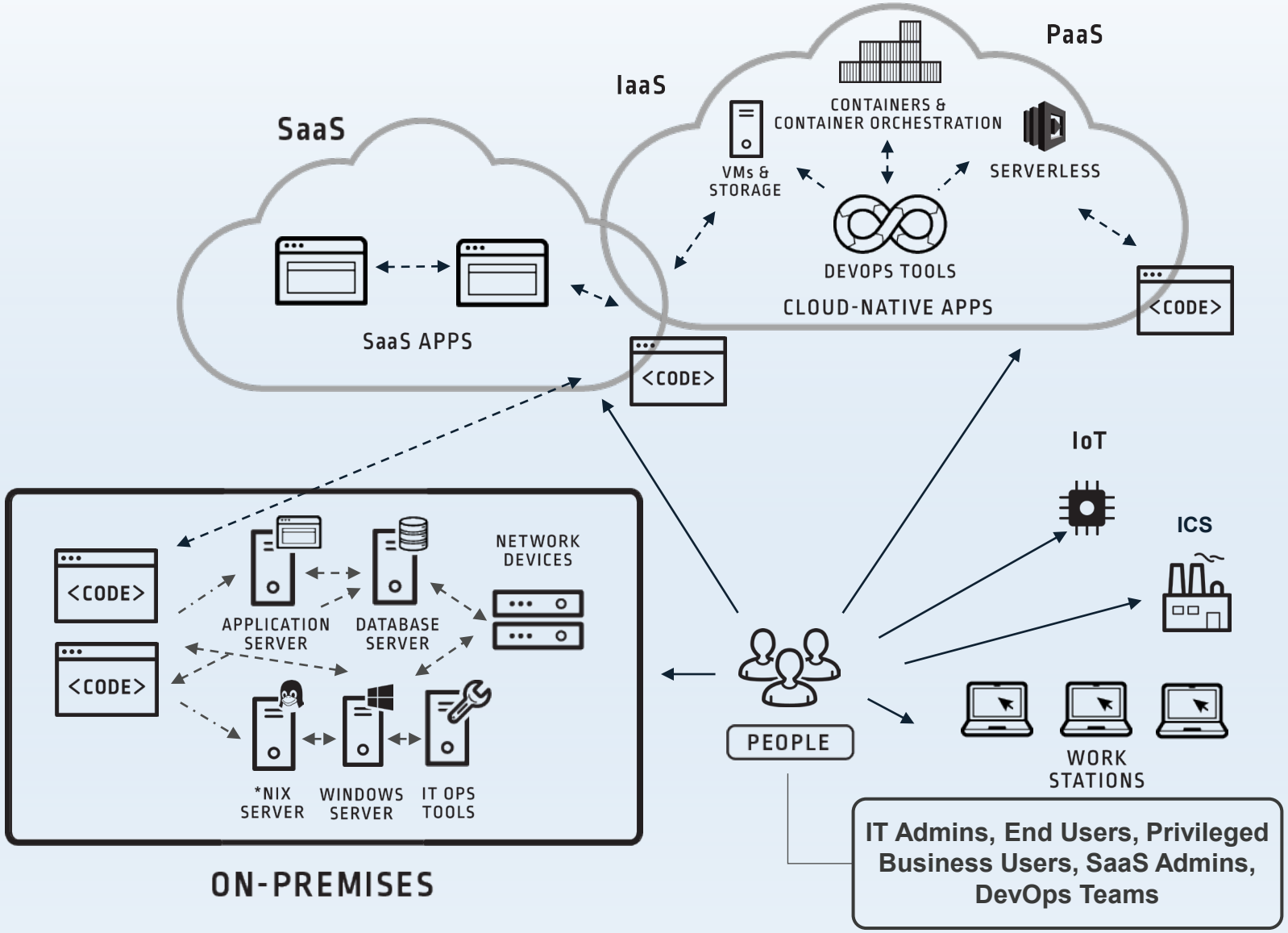



Privileged Access
Human
Non-Human
Workstation Access
Workstation Admin
IT Helpdesk
Workstation Owner
Server Access
Domain Admin
Server Admin
Local Admin
Developer Admin
SSH Keys
Console Access
vSphere Admin
AWS Admin
GCP Admin
Azure Admin
Database Access
Built-In Admin
Named DB Admin
Read/Write Priv. User
Read-Only Priv. User
Infrastructure Access
Switches
Firewalls
Remote Access Cards
Storage Devices
Application Access
Built-In Admin
Named Admin
SaaS Admin
Priv. Business Users
Social Media Accounts
Read/Write Priv. User
Read-Only Priv. User
Mainframe Access
Built-In Admin
Named Admin
Read/Write Priv. User
Read-Only Priv. User
Services
Service Account
API Keys
Windows Service
IIS App Pool
Scheduled Task
Homegrown Applications
Legacy Custom Code
Containerized Applications
Batch Processes
Scripts
3rd Party Applications
IAM Solutions
Discovery Engines
Vulnerability Scanners
Security Scanners
Robotic Process Automation
Robot VDI Users
Robot Job Credentials
DevOps/ Orchestration
Software Provisoning
Infrastructure Deployment
Application Deployment
Config Management

CUSTOMER AND INDUSTRY REALITIES

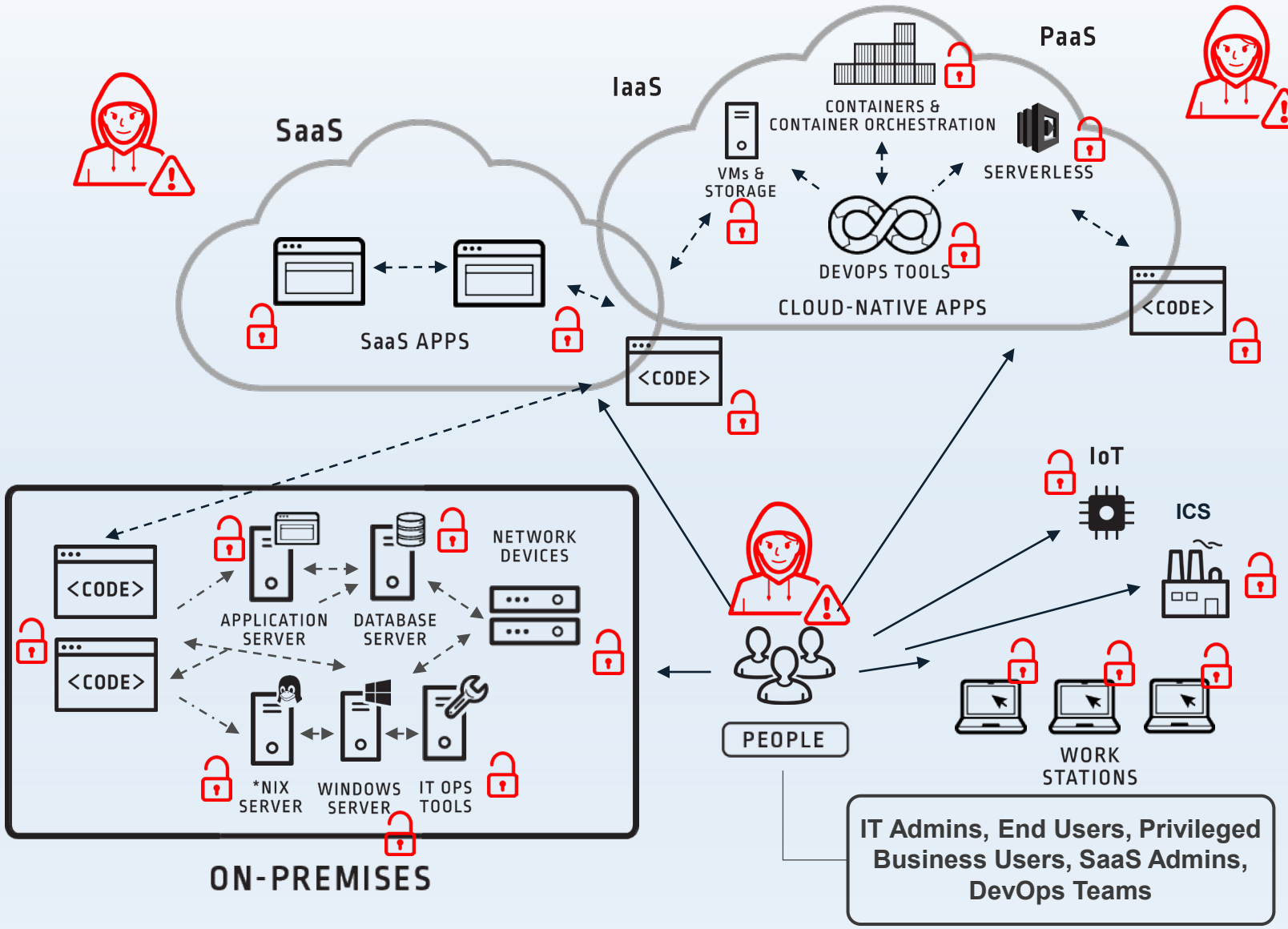


CUSTOMER AND INDUSTRY REALITIES



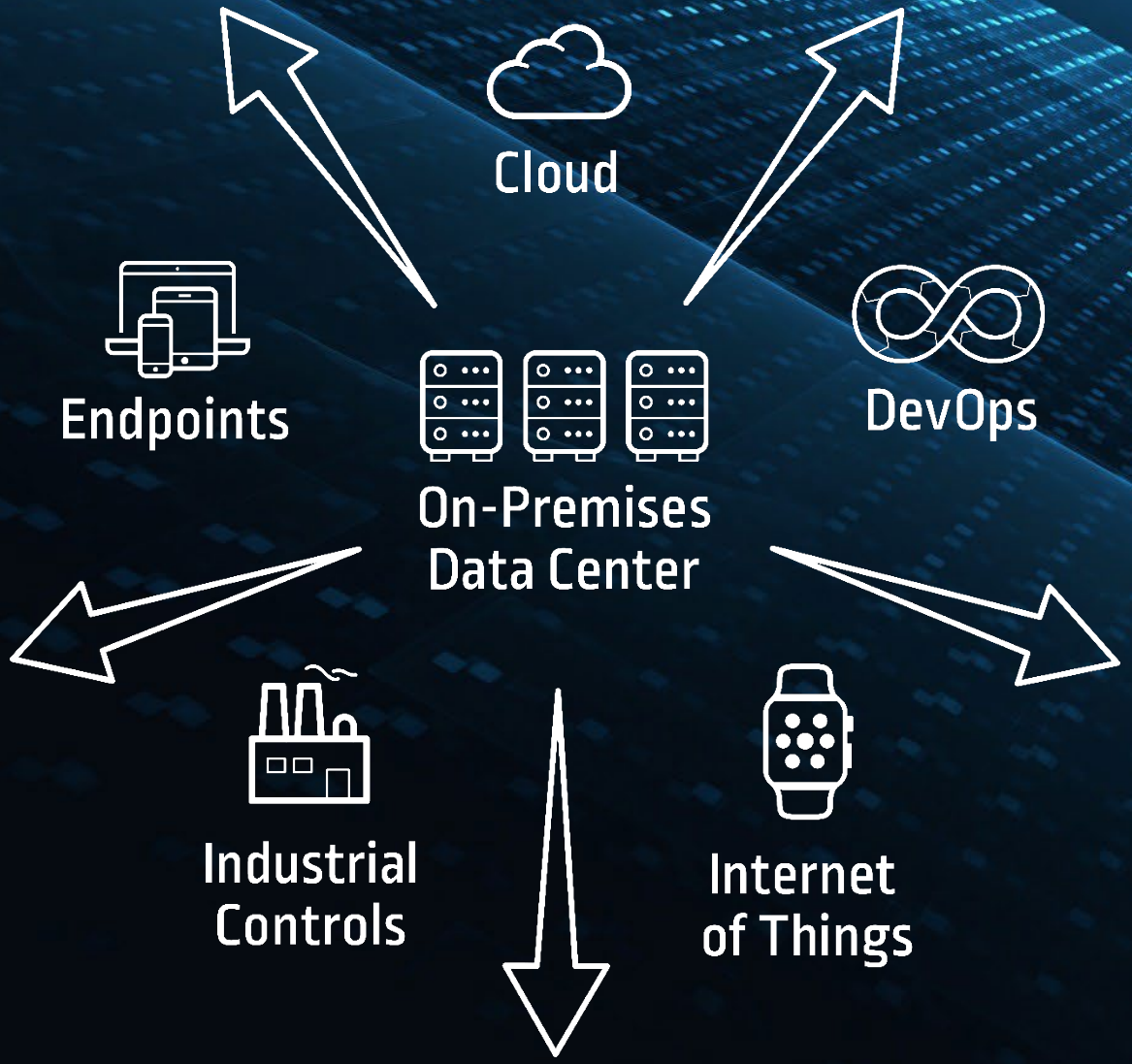
- More Infrastructure
- More Applications
- More Privileged Actors
- More Automation

THESE REALITIES CONTRIBUTE TO EXPANDED ATTACK SURFACE



- More Infrastructure
- More Applications
- More Privileged Actors
- More Automation
- **More Privileged Security Risk**

THE ATTACK SURFACE CONTINUES TO GROW



Default Credentials

- Windows
- Linux
- Network Devices
- Applications
- Databases
- HP iLO / Dell iDRAC
- Time-clocks
- And many many more

CYBERARK

Internet of Things

15

CYBERARK

Dice Tech Careers Career Explorer Insights

Home Career Toolkit Subjects Employer Resources About

Internet of Things Tip: Don't Get Hacked Through Your Fish Tank

Nick Kolakowski
April 20, 2018
3 min read

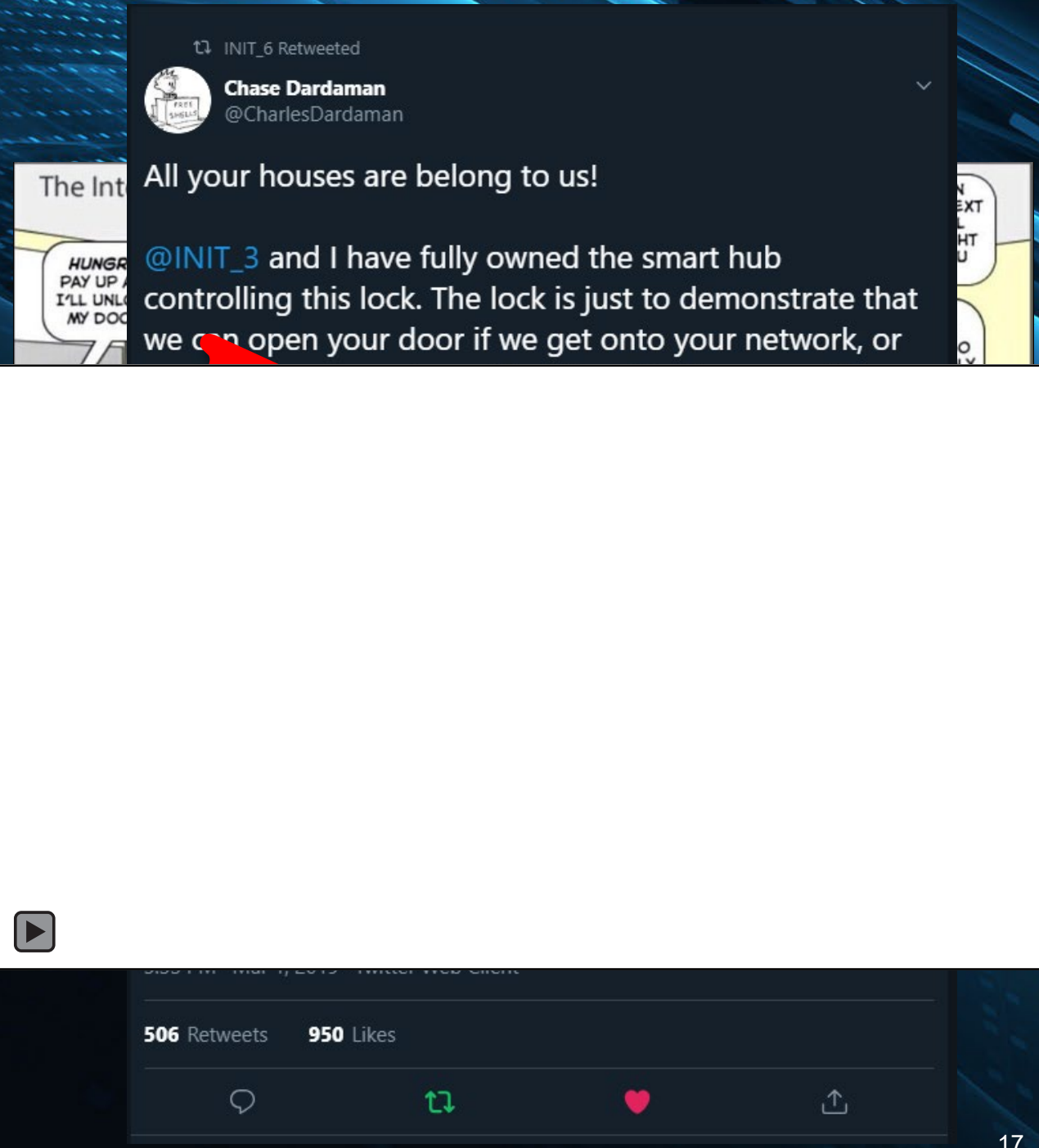
CLOUD HACKING INTERNET OF THINGS IOT SECURITY

If you're a network administrator, sysadmin, or security head, your job hinges on keeping your tech stack secure. And the Internet of Things (IoT) can make that goal a nightmare.

Case in point: an unknown hacker (or hackers) who managed to steal a database of rich

The Internet of Sh*t

- Brute-Forcing and Default Passwords
- Insufficient testing and updating.
- IoT Ransomware
- IoT Distributed CryptoCurrency Mining



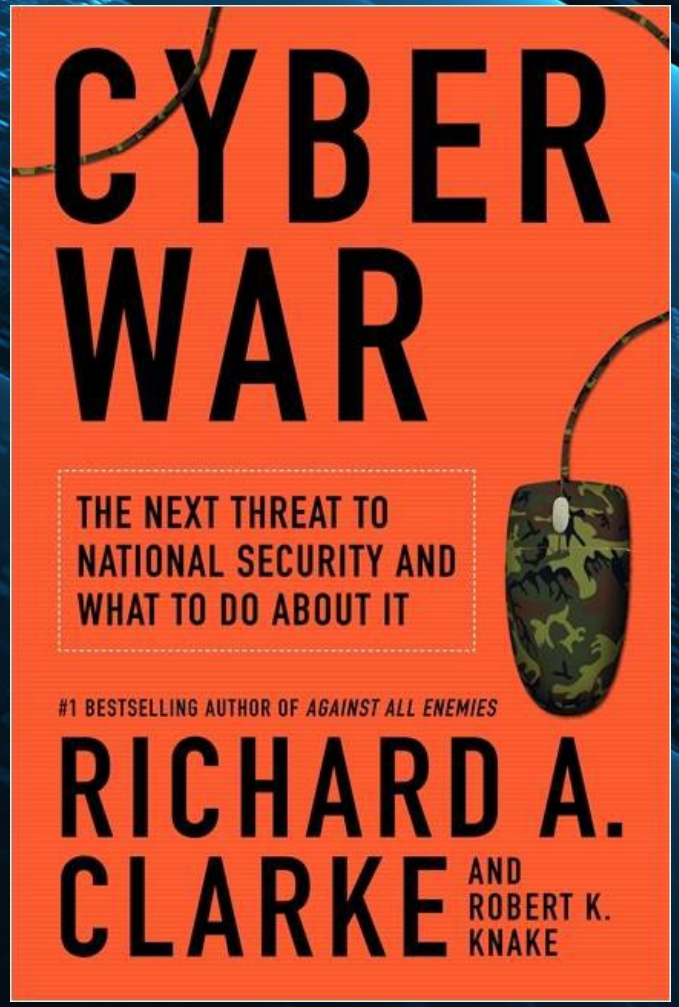
CYBERARK

Industrial Controls

18

In anticipation of hostilities, nations are already “**preparing the battlefield**.” They are hacking into each other’s networks and infrastructures, laying in trapdoors and logic bombs- now, in peacetime. This ongoing nature of cyber war, the blurring of peace and war, adds a dangerous new dimension of instability.

- Richard A Clarke.



CYBERARK

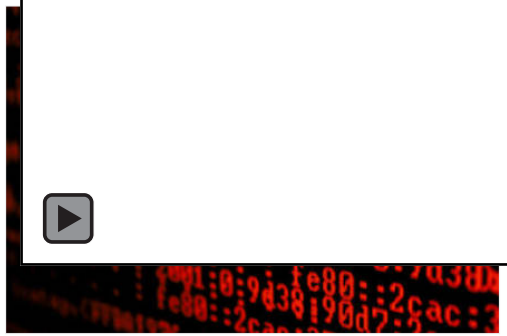
DATA CENTRE

Securi

Spo
hac
aero

High-
dump

By Shau



Miscreants are using a trio of NSA hacking tools, leaked last year by the Shadow Brokers, to infect and spy on computer systems used in aerospace, nuclear energy, and other industries.

This is according to Kaspersky Lab, whose researchers today said the

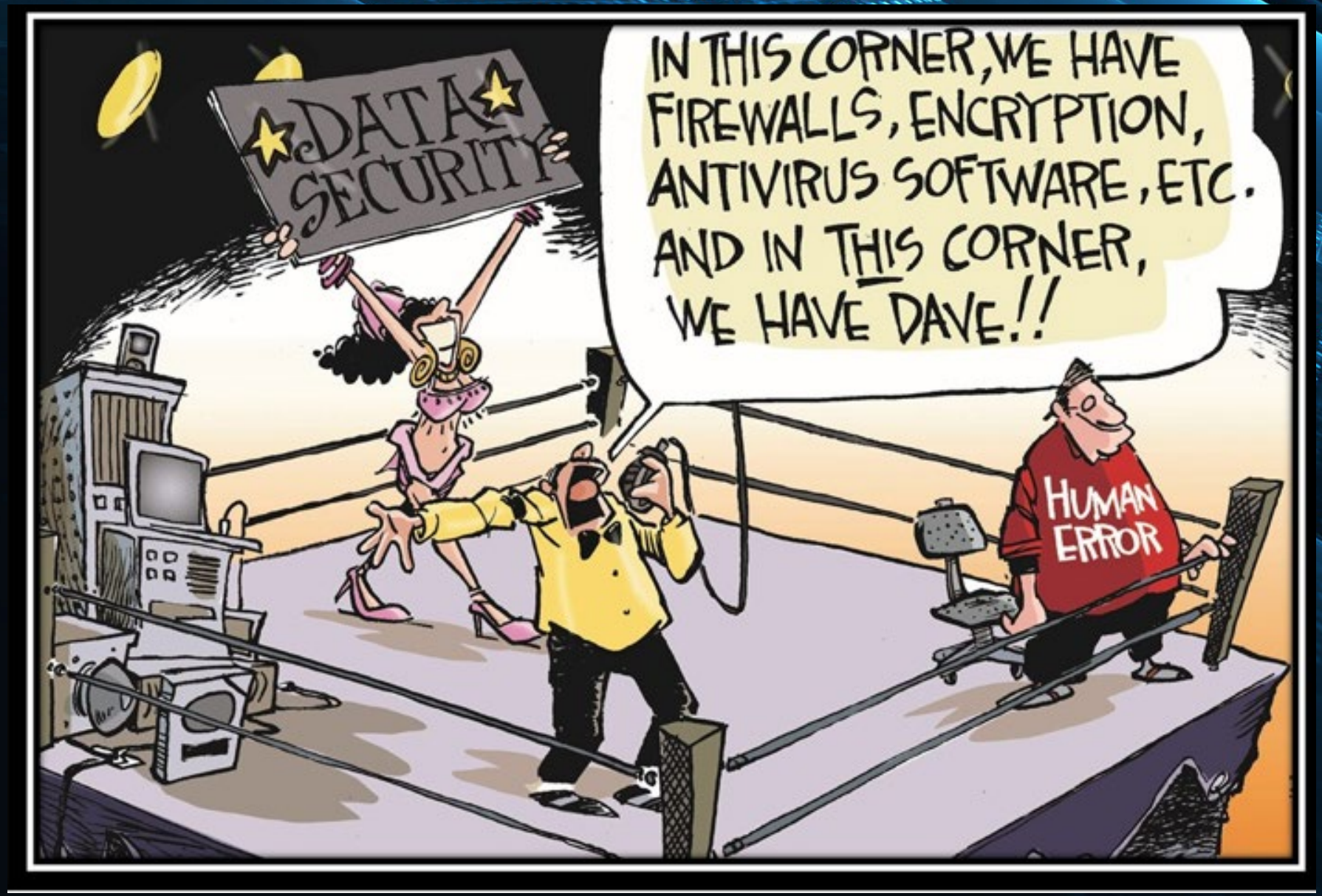
e Was
l in an
tage a
nt

the finger at the Russian government and a government-linked facility for creating a destructive malware.

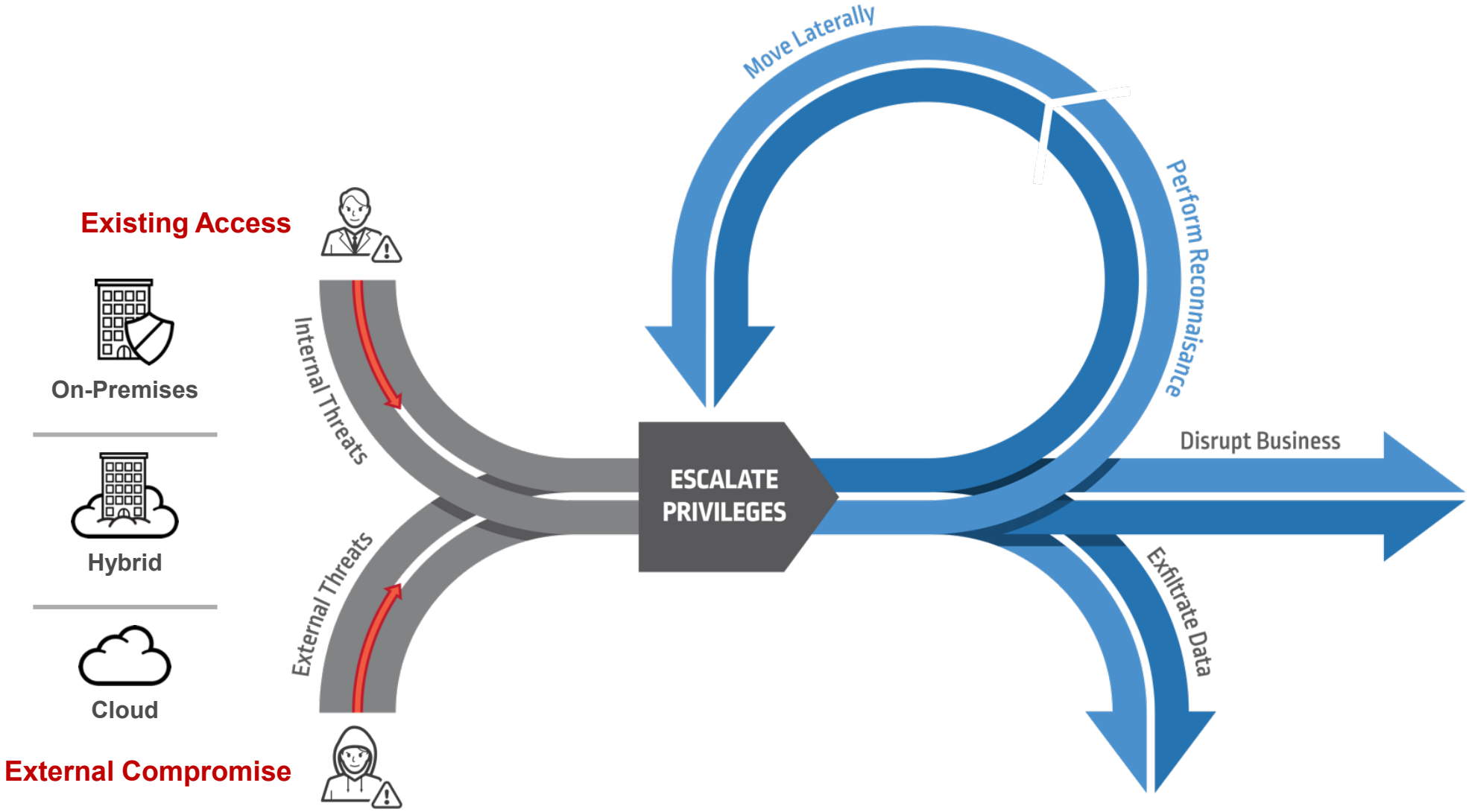
CYBERARK

Endpoints

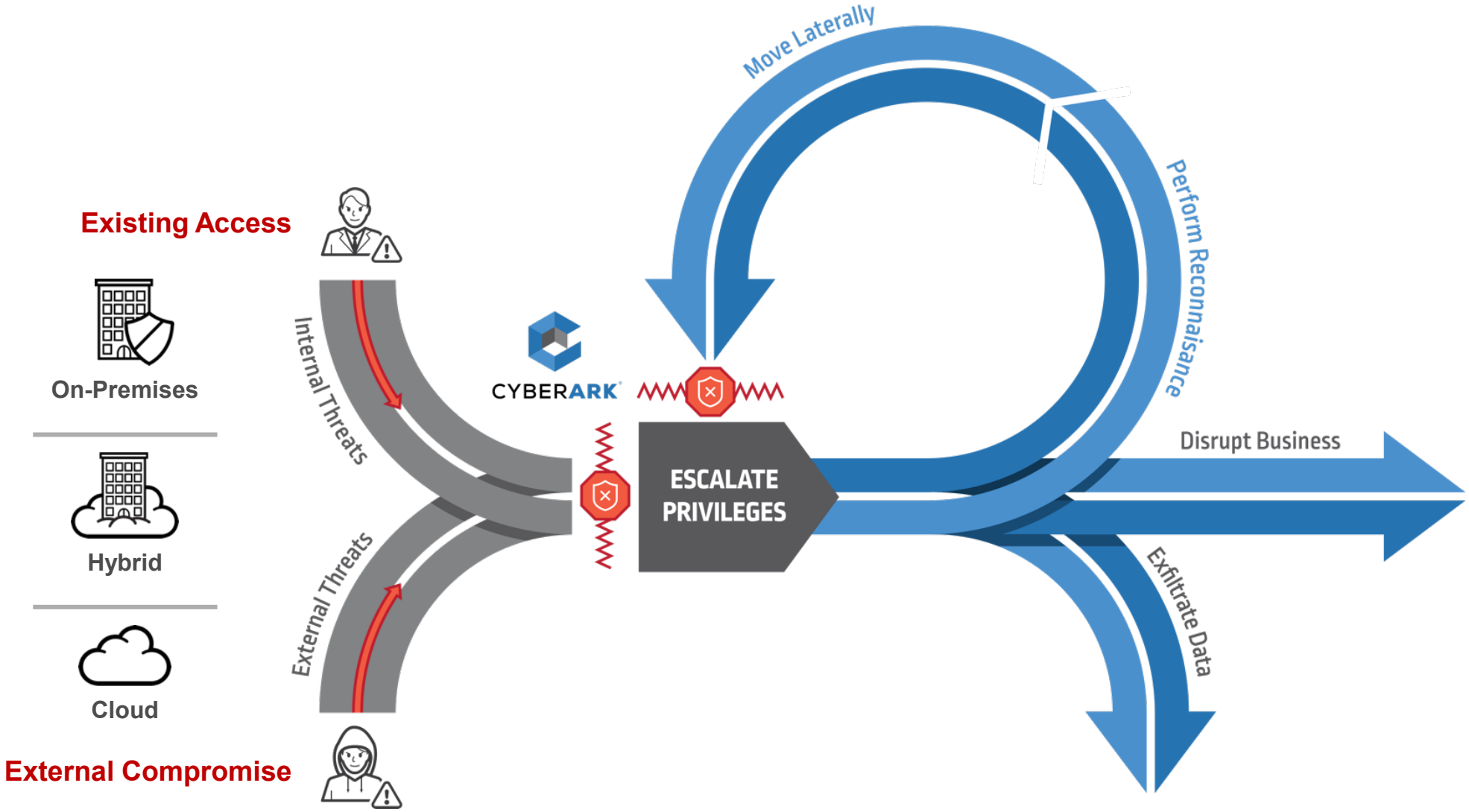
21


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR

CYBERARK BREAKS THE ATTACK CHAIN



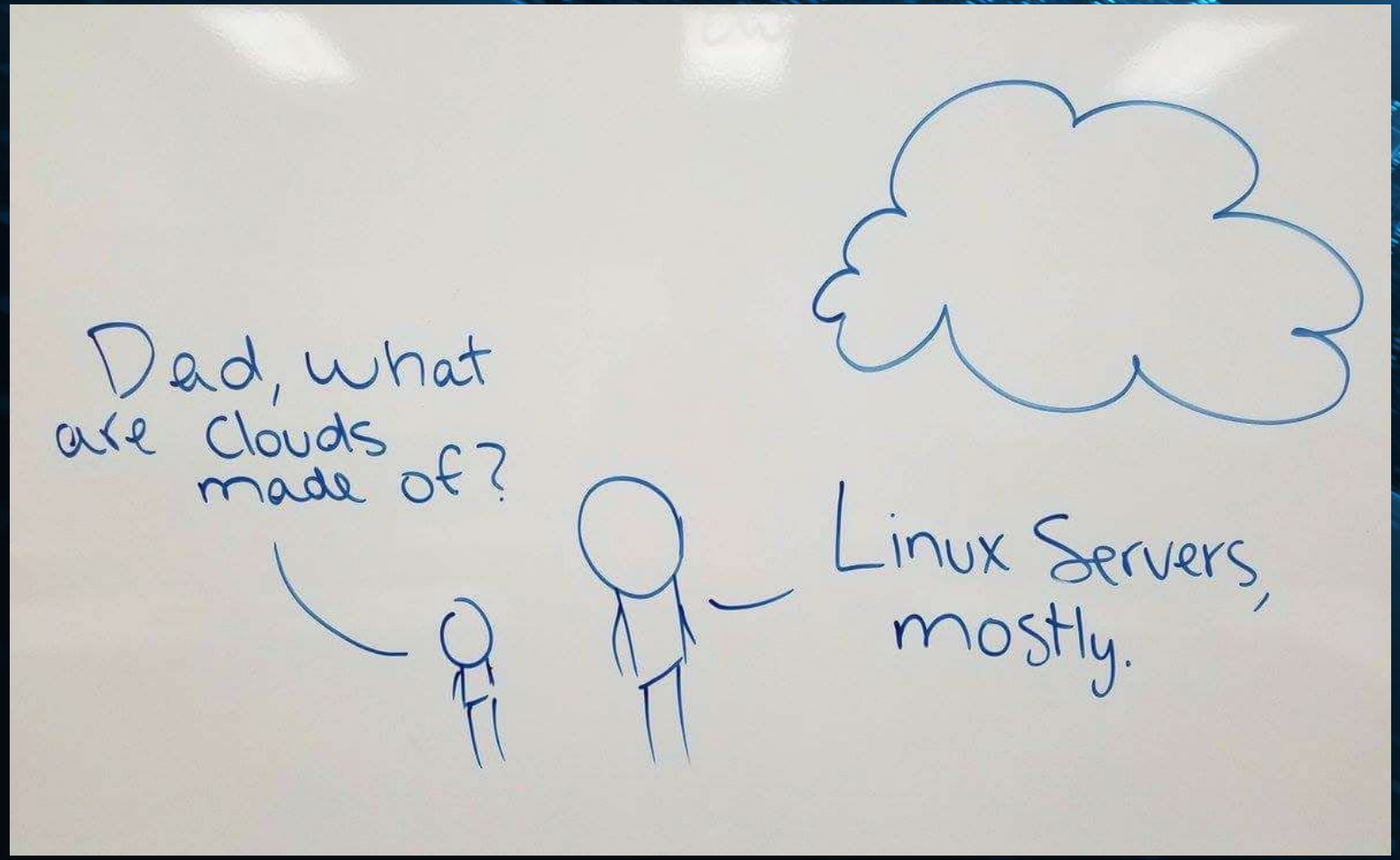
CYBERARK BREAKS THE ATTACK CHAIN



CYBERARK

Cloud

27


Dad, what are Clouds made of?
Linux Servers, mostly.

CYBERARK

DevOps

29

DevOps Introduces New Risks

- Sharing secrets over chat/email
- Saving plaintext secrets on local machines and code repositories

Result: Phished admin creds leads to cloud access

- Hard-coding secrets in executables without rotation or audit
- Uncontrolled user access to build, test tool consoles & infrastructure

Result: Malware injection in test systems/ build process

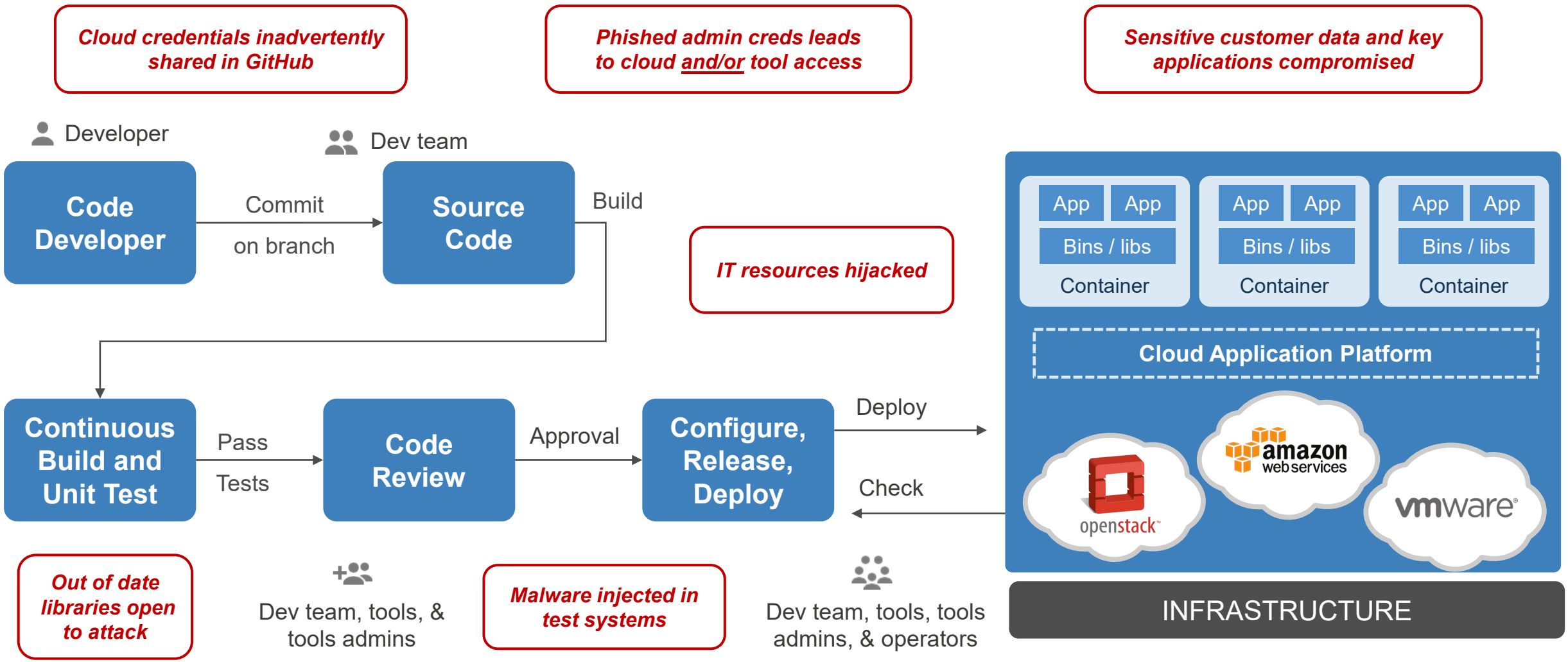
- Uncontrolled user access to artifact repositories

Result: Uncontrolled /malicious access to artifact repositories

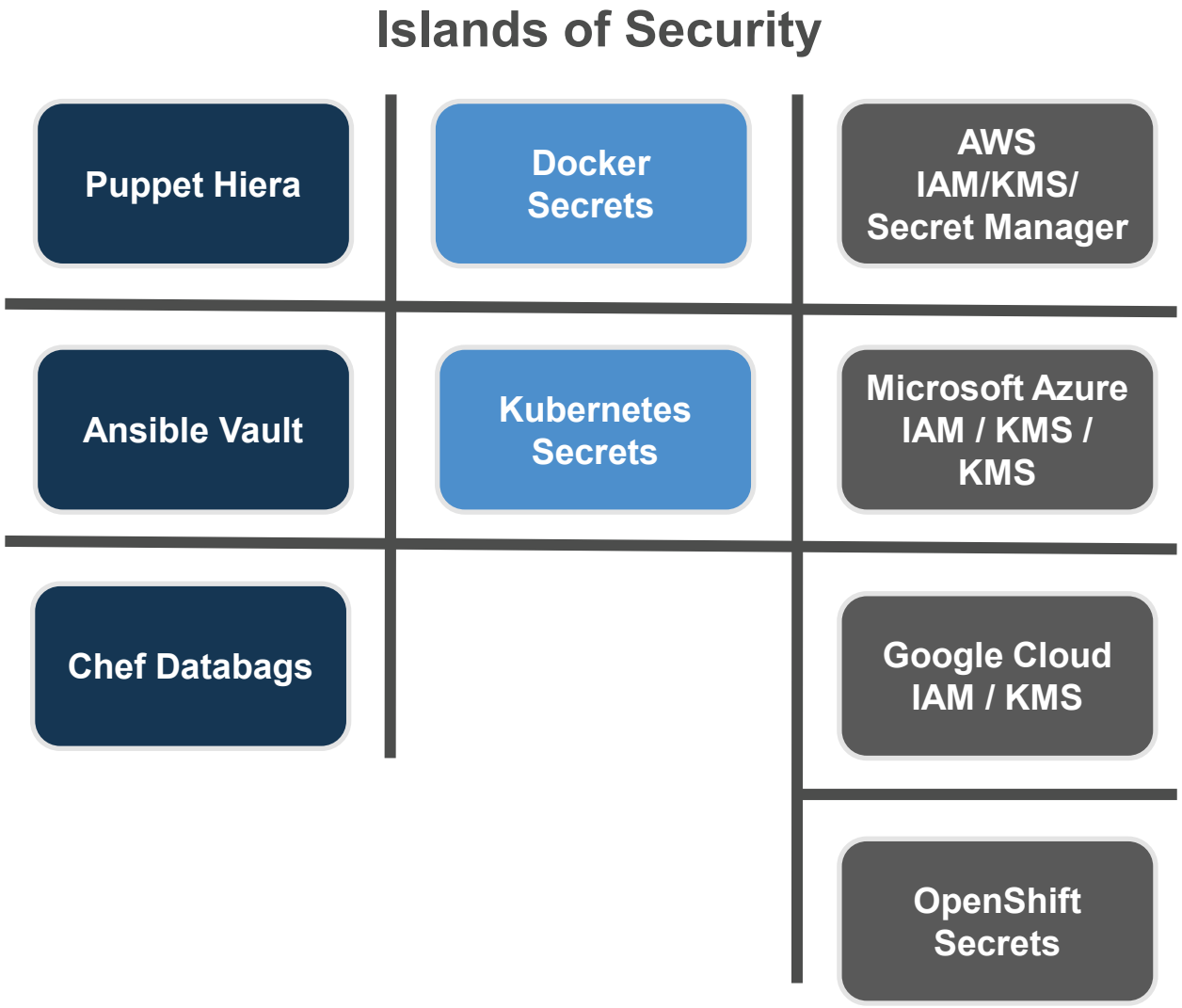
- Hardcoded secrets within production code
- DevOps users with unlimited permissions on production machines

Result: Sensitive customer data and key applications compromised

New Threat Models And Expands The Attack Surface



Islands Of Security In Access Management Create Challenges

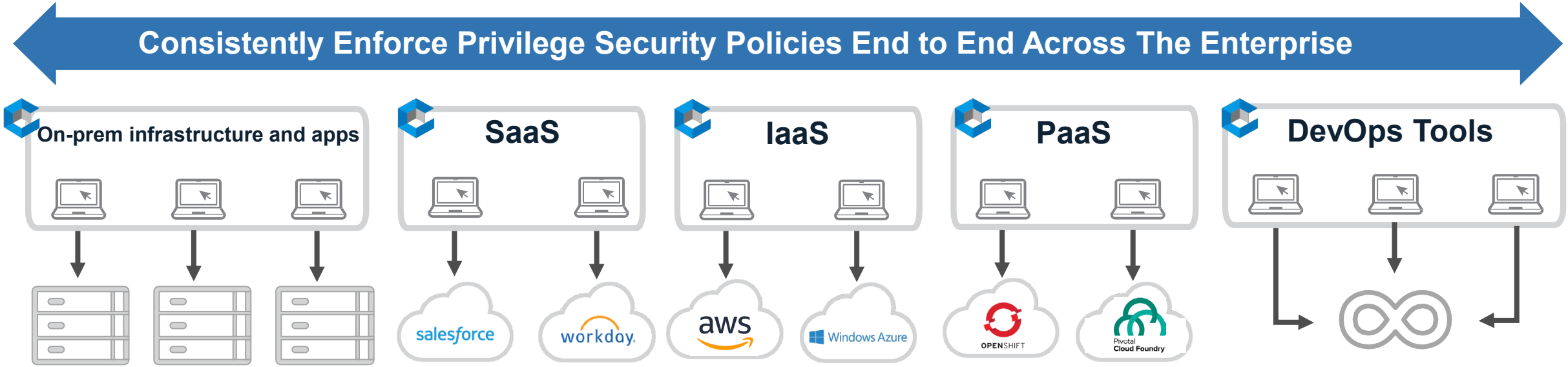


Native tool solutions for secrets: Create "Security Islands"

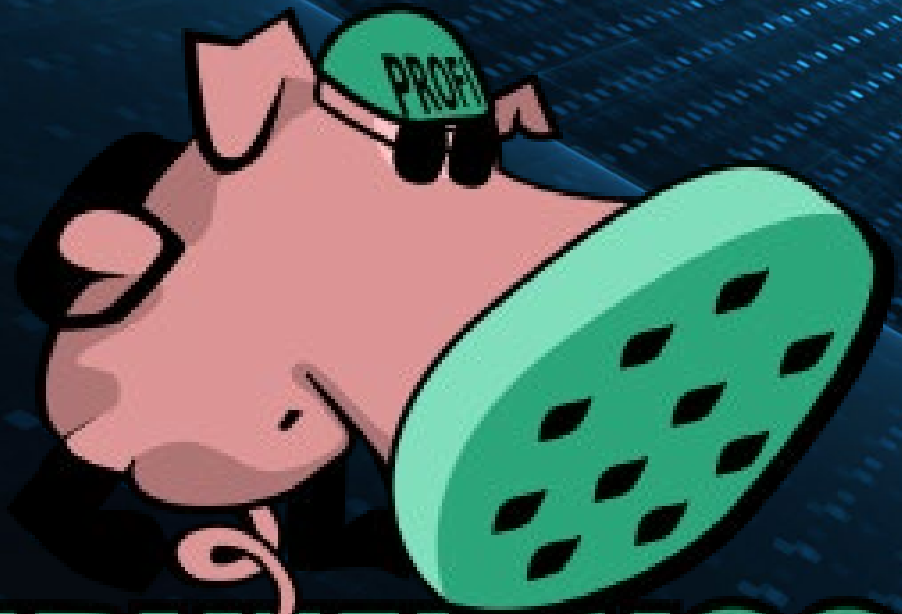
- Provide a specific and different solution for each tool
- Not built with security in mind -- Secret repository only
  - No rotation of secrets
  - No audit
- Have limited integration capabilities
- No central view of Privileged Account Security

CISOs WANT ENTERPRISE-WIDE PRIVILEGE SECURITY POLICIES

As a best practice, CISO and IT Leaders want to consistently enforce privilege security policies across their evolving infrastructure and application environments



CYBERARK

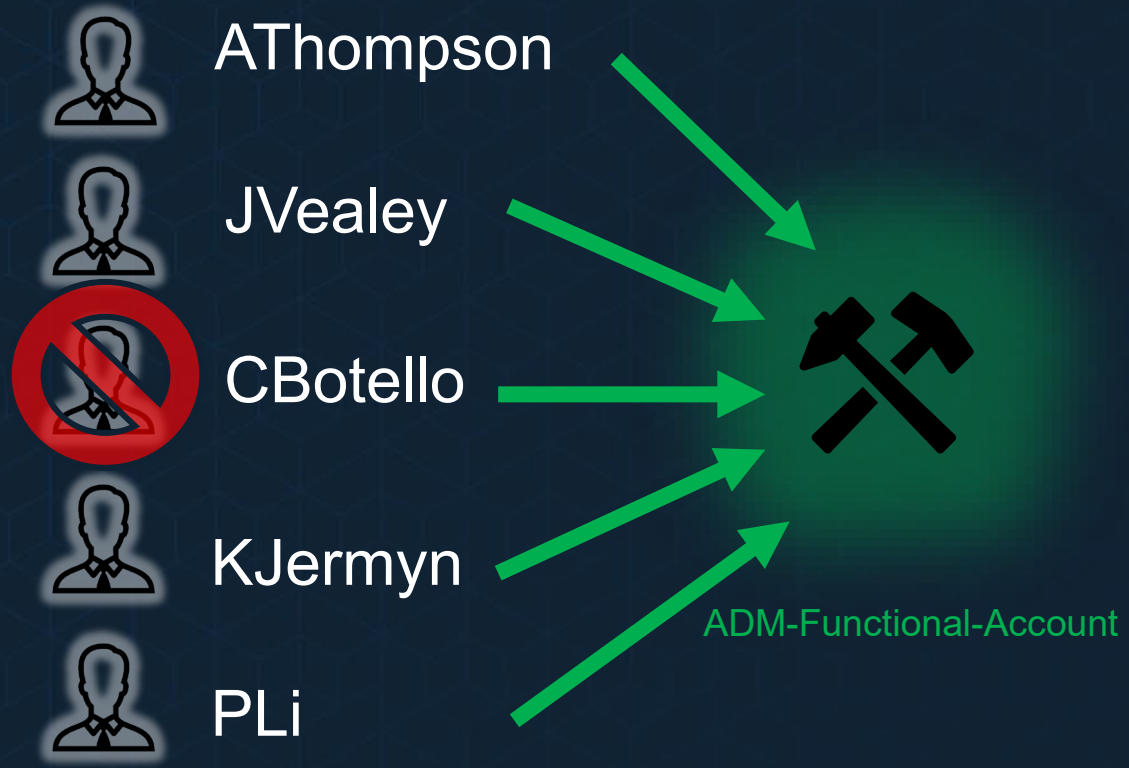


TRUFFLEHOG

CYBERARK

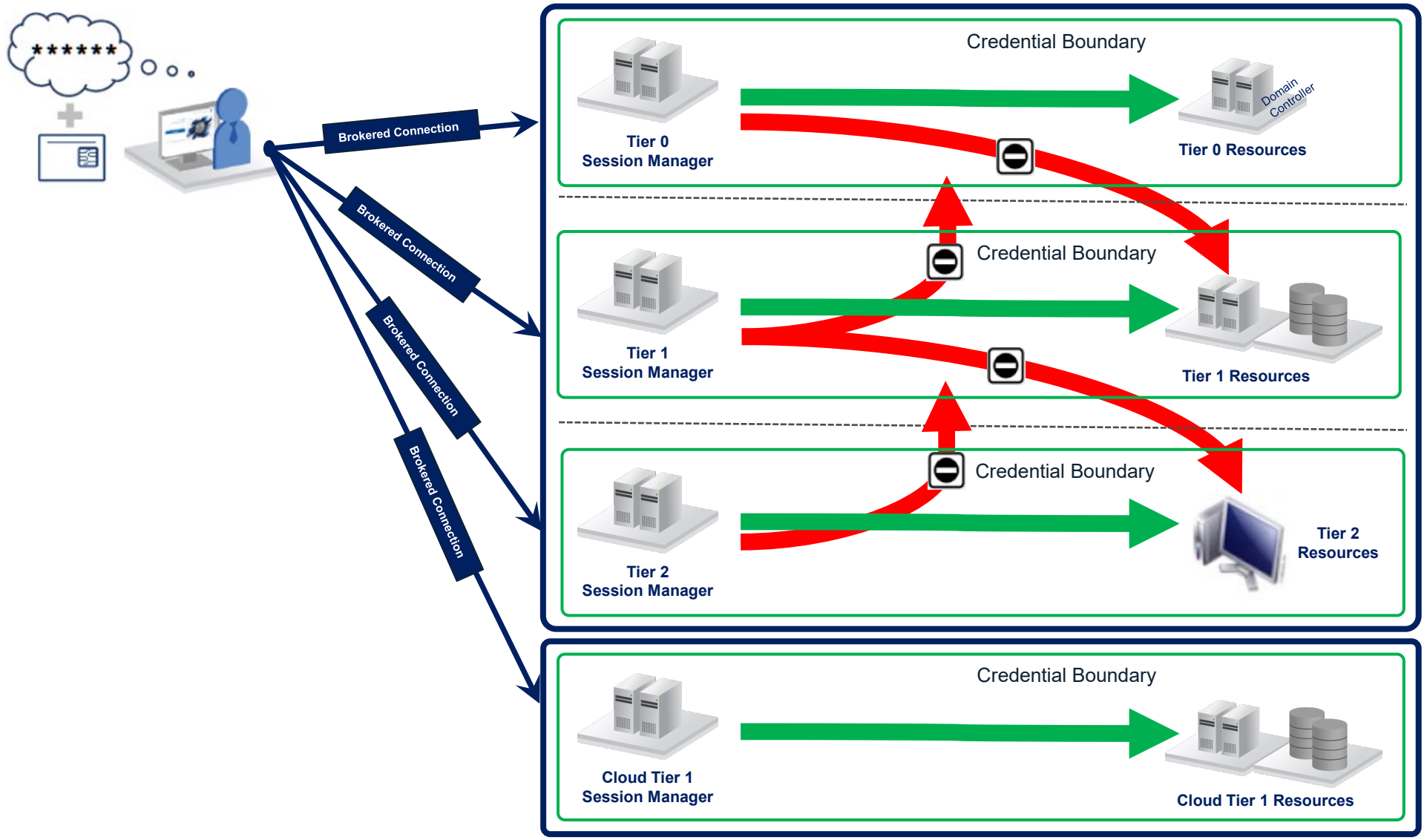
FUNCTIONAL ACCOUNT MODEL

5 Privileged Accounts



1 Privileged Account

RBAC + PSM = TRUE CREDENTIAL BOUNDARIES



Eliminate Irreversible Network Takeover Attacks

Control and Secure Infrastructure Accounts

Limit Lateral Movement

Protect Credentials for Third-Party Applications

Systematically Address Organization's Top Control Goals

Manage *NIX SSH Keys

Defend DevOps Secrets in the Cloud and On-Premises

Secure SaaS Admins and Privileged Business Users

Discovery and Audit

Executive Summary Dashboard with detailed privileged credentials data including:

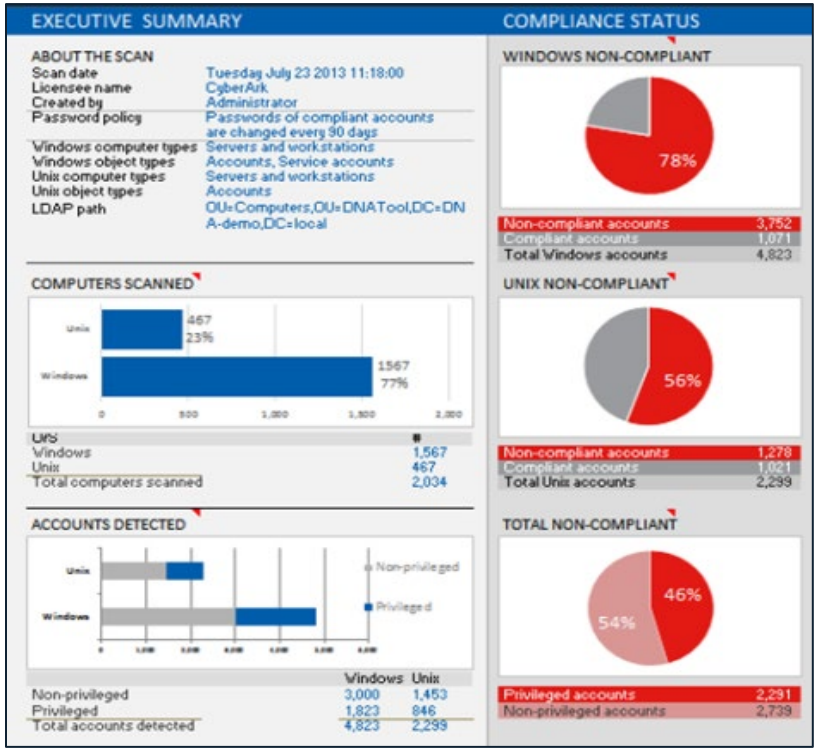
- Embedded creds in WebSphere, WebLogic, IIS hosts
- SSH keys
- Credential activity and metadata
- AWS IAM Users, Access Keys and EC2 Key pairs
- Ansible Secrets

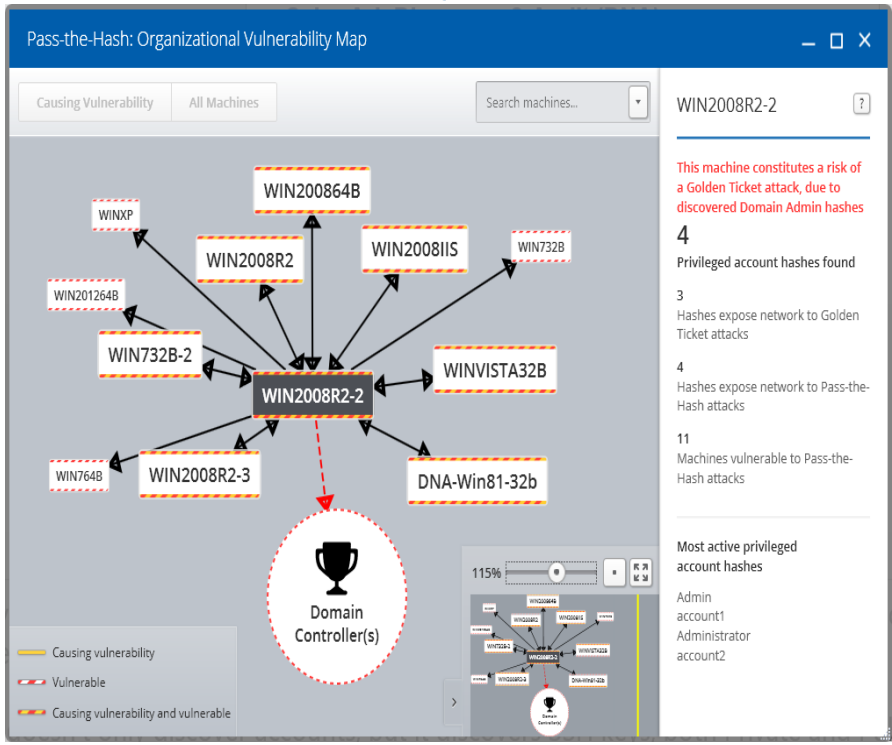
Interactive Vulnerability Mapping:

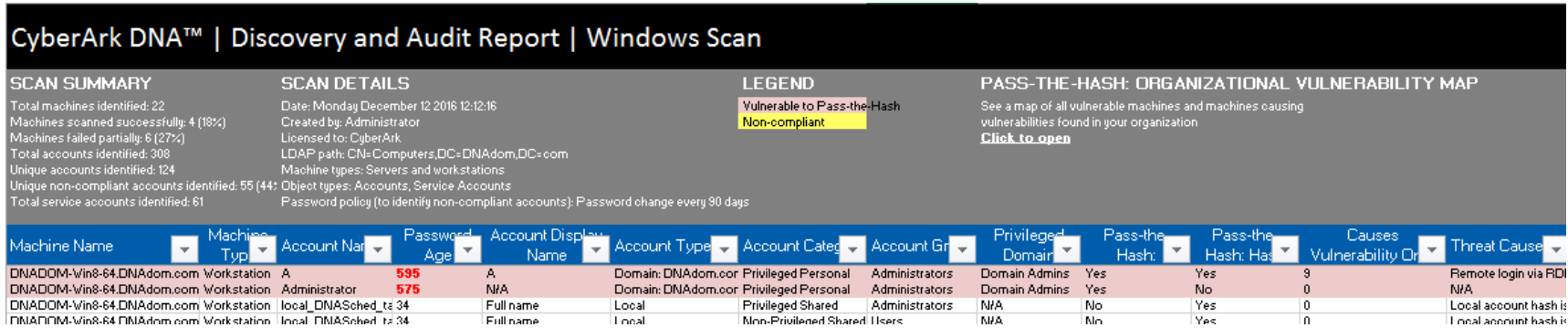
- Golden Ticket
- Pass The Hash
- SSH key trust relationships

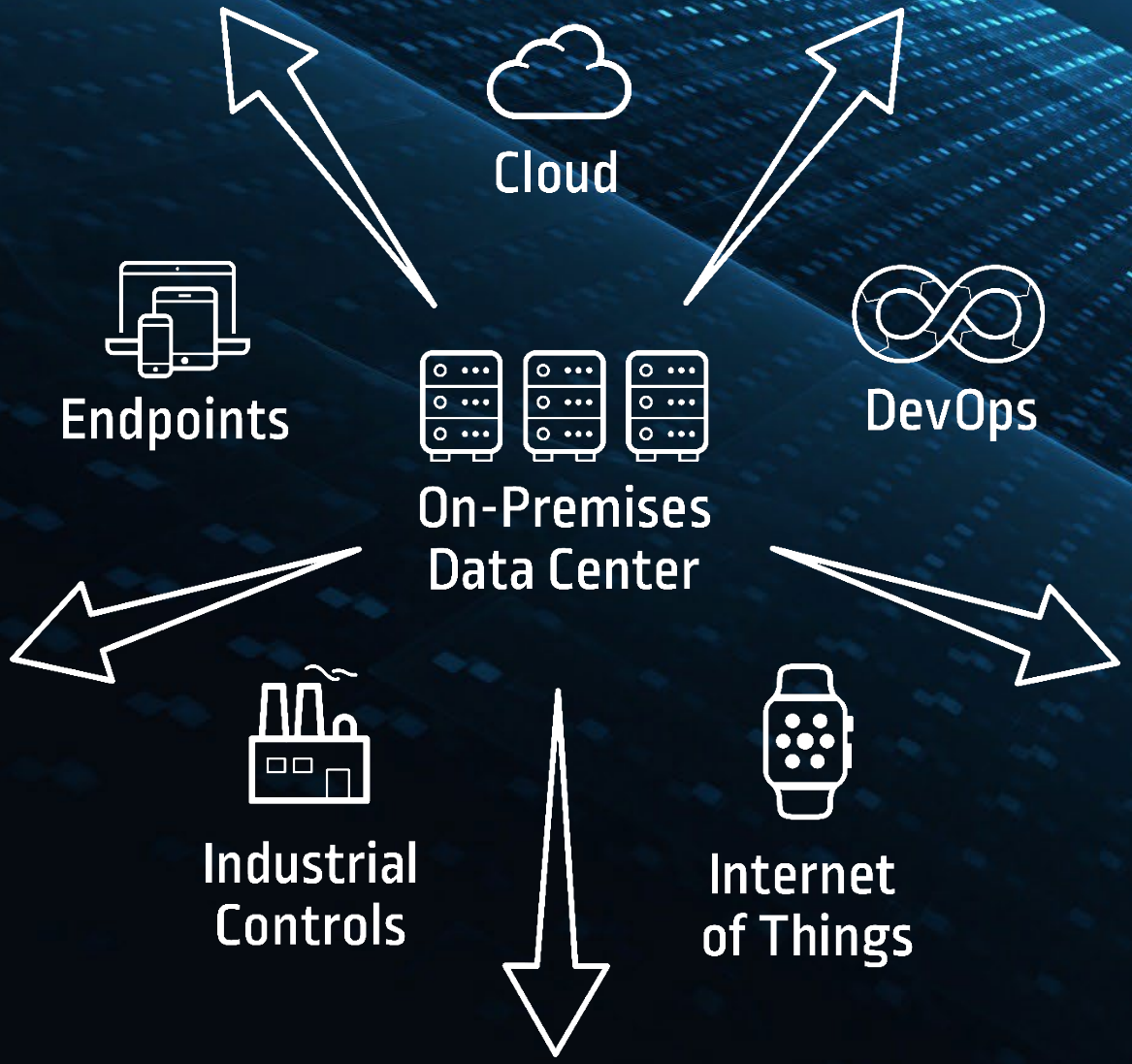
Step Zero – Discovery and Audit (DNA)

CYBERARK








Cloud
Endpoints
DevOps
On-Premises
Data Center
Industrial
Controls
Internet
of Things

CYBERARK

Lock Down Credentials

- Protect privileged passwords and SSH keys

Isolate & Control Sessions

- Prevent malware attacks and control privileged access

Continuously Monitor

- Implement continuous monitoring across all privileged accounts

CYBERARK

QUESTIONS?

CYBERARK

THANK YOU!