



SECURITY IN THE CLOUD: PROTECTING PRIVILEGED ACCOUNTS

CLOUD SECURITY SUMMIT - MILANO 31TH OCTOBER 2018

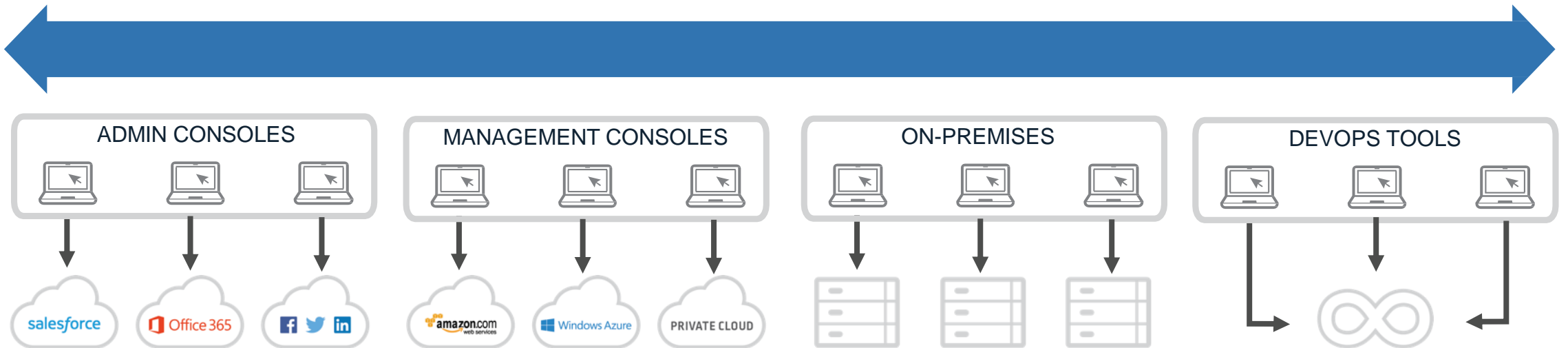
Massimo Carlotti – Sales Engineer -CyberArk

massimo.carlotti@cyberark.com

WHAT WE'LL COVER TODAY

Focus on Cloud (IaaS/PaaS):

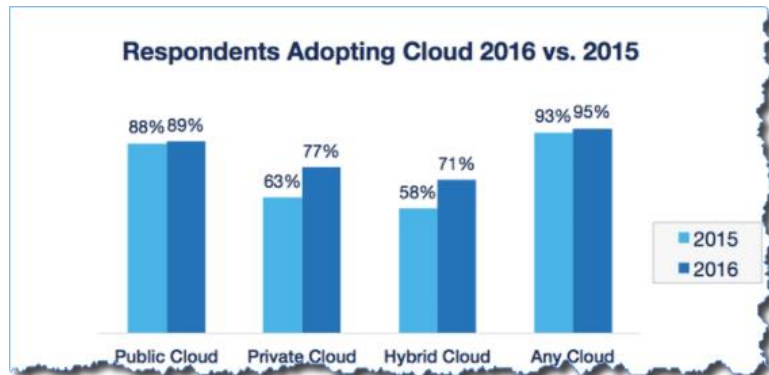
- Customer apps and workloads running on the cloud
- Best Practices to secure them



STATE OF CLOUD & DEVOPS ADOPTION IN ENTERPRISE CRITICAL INITIATIVES TIED TO COMPETITIVENESS... STAKES ARE HIGH!

Many are adopting...

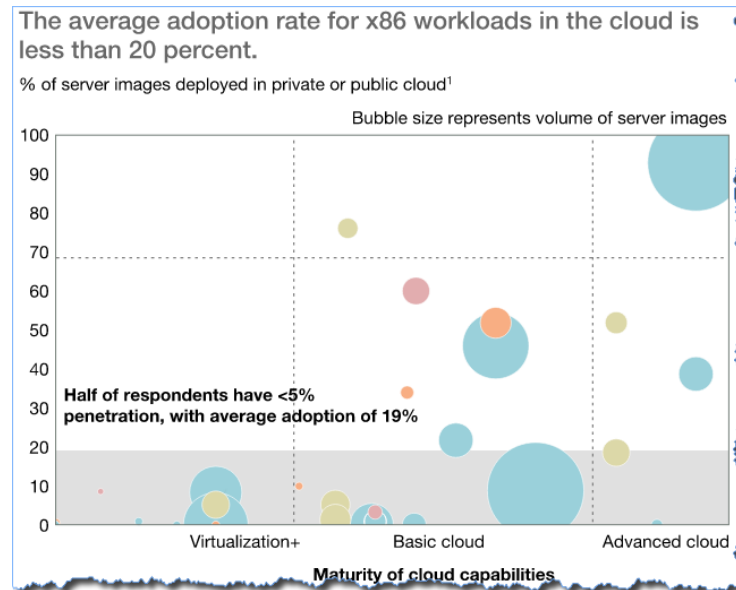
+90% adoption rates



RightScale..[Cloud Computing Trends : 2016 State of the Cloud Survey](#)

Few are excelling...

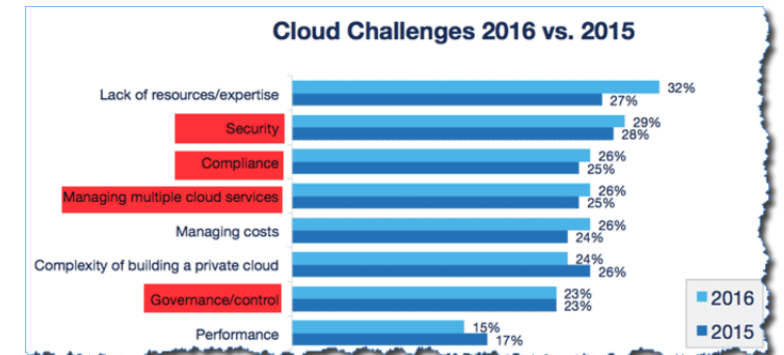
<20% of workloads migrated



McKinsey...[Leaders and laggards in enterprise cloud infrastructure adoption](#)

Security is impeding...


Security & Compliance remain top cited impediments



RightScale..[Cloud Computing Trends : 2016 State of the Cloud Survey](#)

HIGH PROFILE BREACHES AND ATTACKS

Does cloud create a bigger attack surface?




MarketsTechPursuitsPoliticsOpinionBusinessweek

Sign In
Subscribe to Businessweek





Uber Paid Hackers to Delete Stolen Data on 57 Million People

By Eric Newcomer
November 21, 2017, 4:58

→ Company paid hackers to delete stolen data
→ Chief Security Officer says company was not aware of breach



Zeljka Zorz - Managing Editor
April 26, 2017







Hackers explain how they "owned" FlexiSpy

Read the latest issue of the (IN)SECURE Magazine

How did the hackers that go by the name Decepticons breach stalkerware manufacturer FlexiSpy?

According to information purportedly provided by the attackers themselves, it took them a while to thoroughly "own" the company's networks and wreak as much havoc as possible, but it was ultimately not that difficult.

News




521

Yet Another Misconfigured Amazon S3 Bucket Exposes Dow Jones Customer Data

By David Ramel ■ 07/19/2017

Security firm UpGuard Inc. has found yet another unprotected S3 storage bucket on the Amazon Web Services Inc. (AWS) cloud, this one exposing personal data of millions of Dow Jones & Company customers.

The firm has been steadily identifying and





AWS urges developers to scrub GitHub of secret keys

By Munir Kotadia (@author/munir-kotadia) on Mar 24, 2014 10:18AM

Devs hit with unexpected bills after leaving secret keys exposed.

Amazon Web Services (AWS) is urging developers using the code sharing site



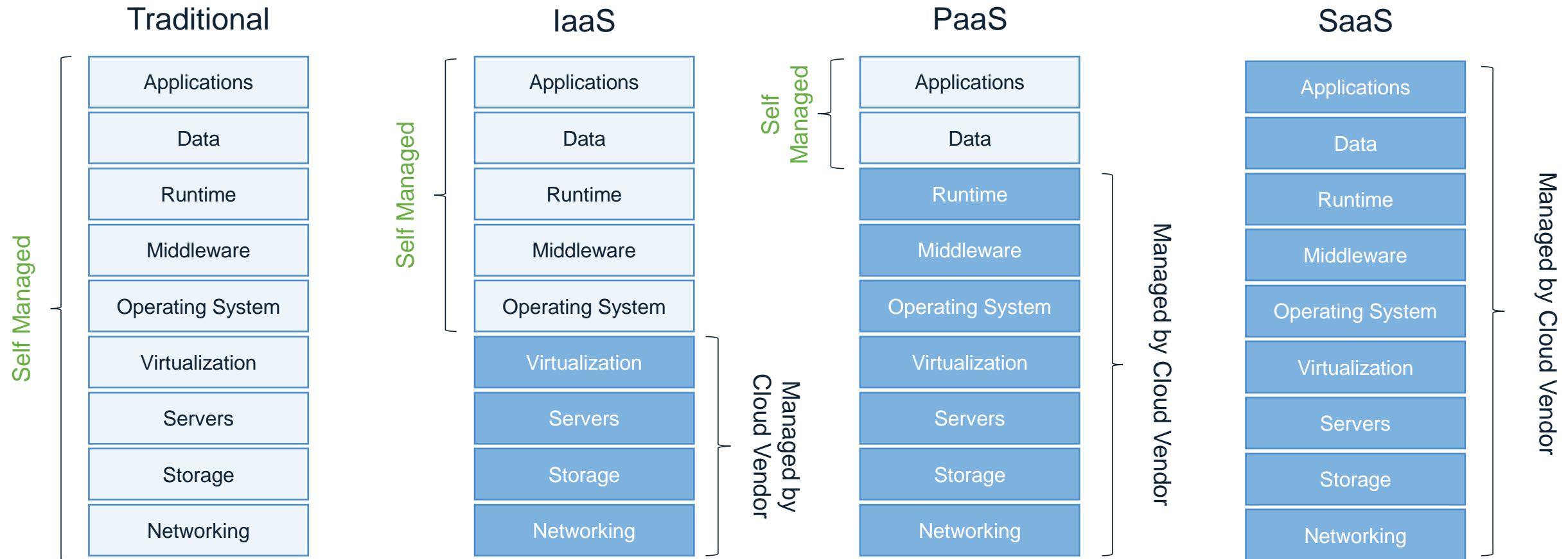
 CYBERARK

ORIGINAL SIN: THERE IS NO CLOUD ...



There is no cloud
it's just someone else's computer

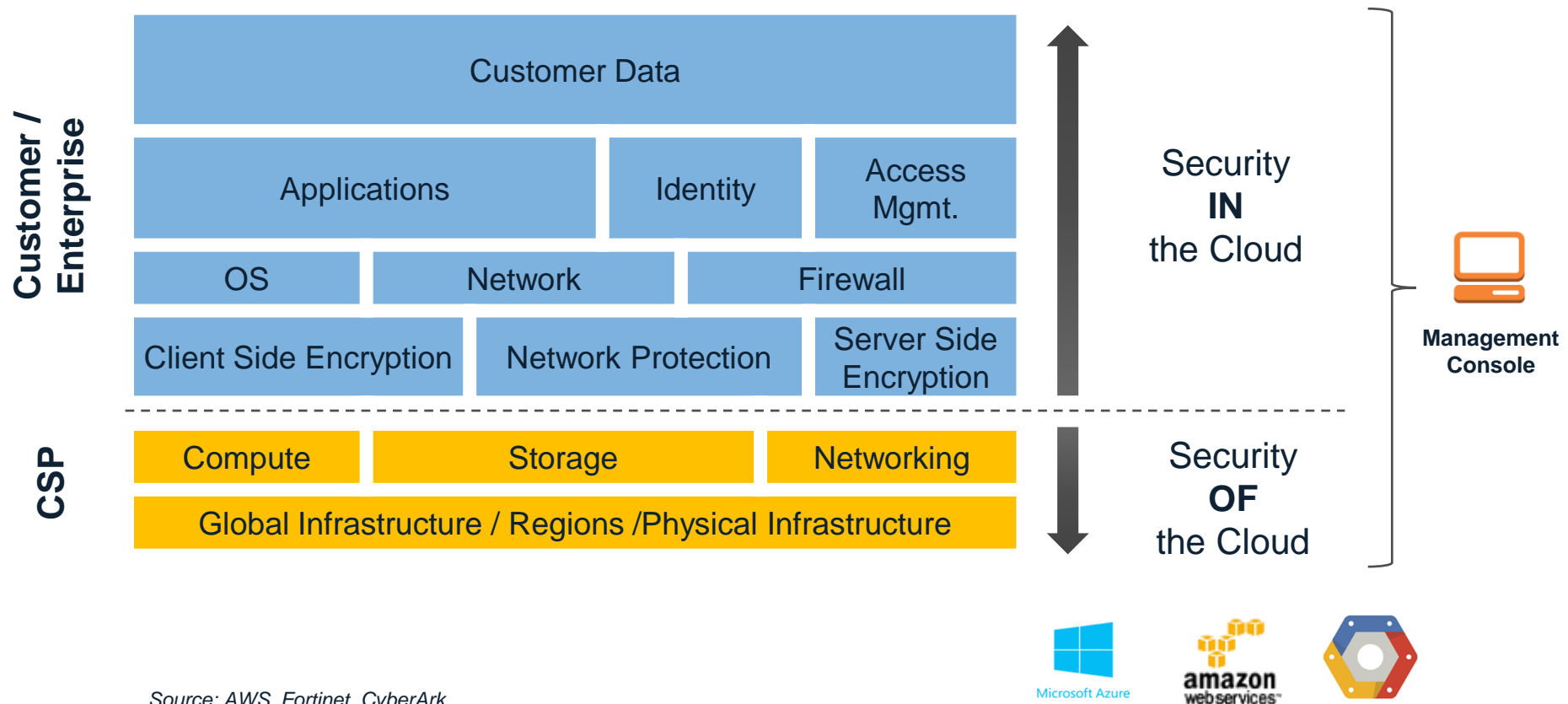
MOVING TO THE CLOUD = SHARED RESPONSIBILITY



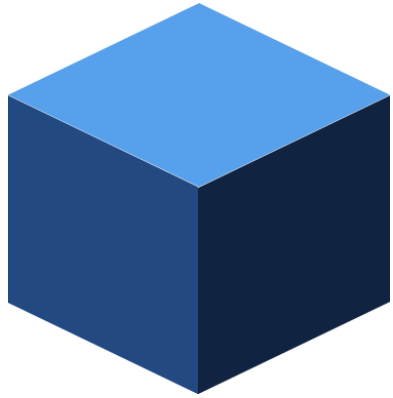
Zero Risk does not exist !!!

CLOUD SECURITY IS A SHARED RESPONSIBILITY (IAAS EXAMPLE)

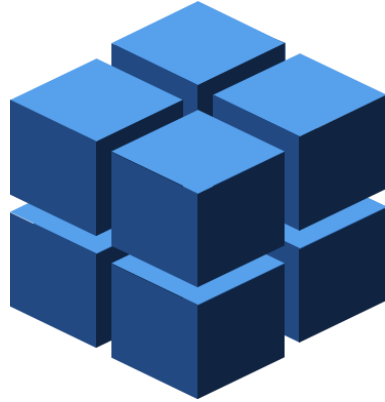
- Security **OF** the Cloud – AWS, Azure, etc./**Cloud Service Provider**
- Security **IN** the Cloud – **You** - Customer/Enterprise



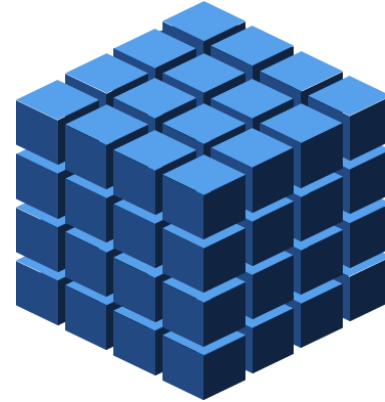
BUT... WITH MOVE TO MICRO SERVICES APP ARCHITECTURES GET PULVERIZED



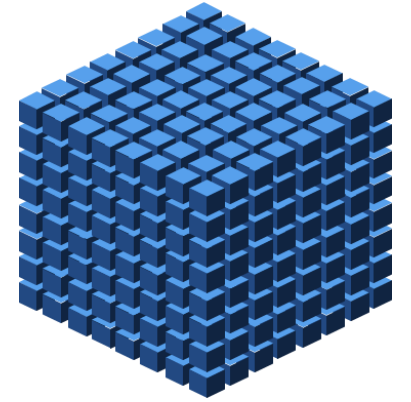
Monolith



Virtualized



Containerized



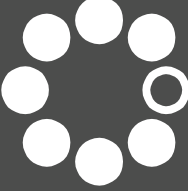
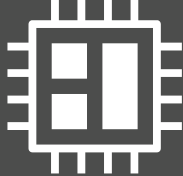



Micro Services

Increased: agility, pace, automation, automation tools

All need access to secrets and other credentials. Some are very short-lived.

THE CHALLENGE OF “NEW” PLATFORMS

 Scale	 Dynamism	 Heterogeneity	 Non-Human Actors	 Human Actors
Services are provisioned on scale of thousands to tens of thousands of instances in the cloud vs. hundreds of physical servers in a data center	No more static inventory of servers and hosts to secure. Instances are spun up and torn down elastically and in bulk	No more homogeneous infrastructure. Services span multiple cloud providers each with different security interfaces & capabilities	Explosive proliferation of privileged, non-human automation and agents that must be controlled	Excessive access privileges , role confusion

IAAS /PAAS SECURITY FAILURES ARE CAUSED BY PRIVILEGE FAILURES



According to
Gartner

Through 2020, more than half of security failures
associated with IaaS and PaaS will be attributable to significant
security gaps caused by *failure to adopt Privileged Access*
Management technology and processes.²

2. Gartner "Market Guide for Privileged Access Management" by Felix Gaehtgens, Amnol Singh, Dale Gardner, August 22, 2017

THINK LIKE AN ATTACKER

**It's all automatic -
nobody really looks on it**

**Look for API keys, AWS
servers/images that are
publicly available & use
default secrets**

**Unchanged, shared,
over-provisioned
secrets**

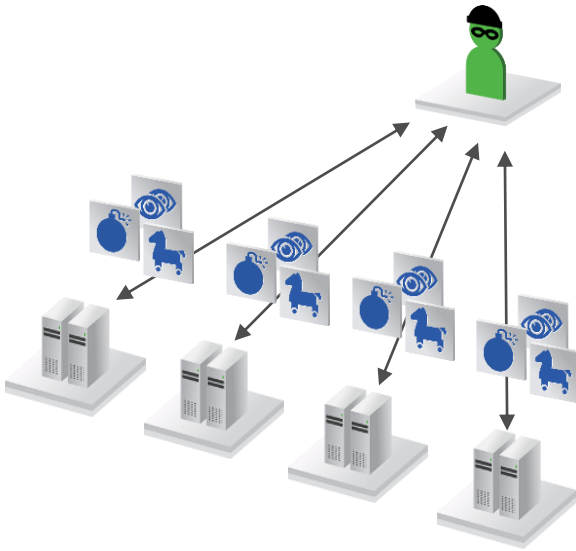
**High speed,
highly scalable**

**Another way to
access servers**

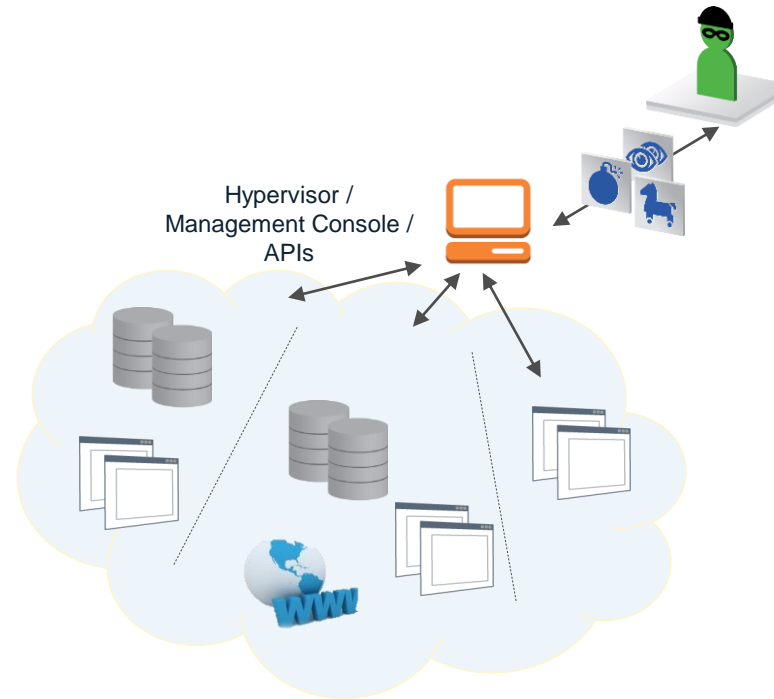
So many new tools...

SWEET SPOT: THE POWER OF PRIVILEGE IN THE CLOUD

Old Way
“Hack a System”

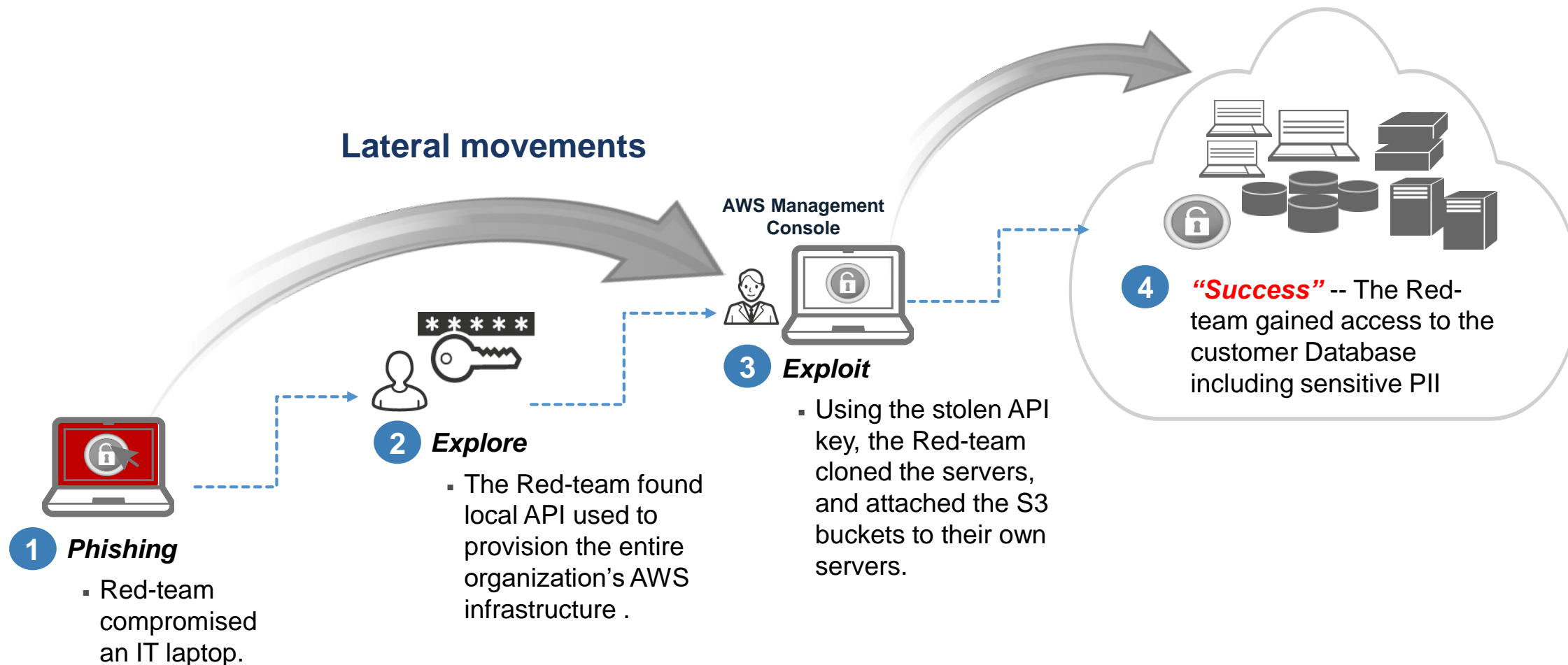


New Way
“Hack Cloud Infrastructure”



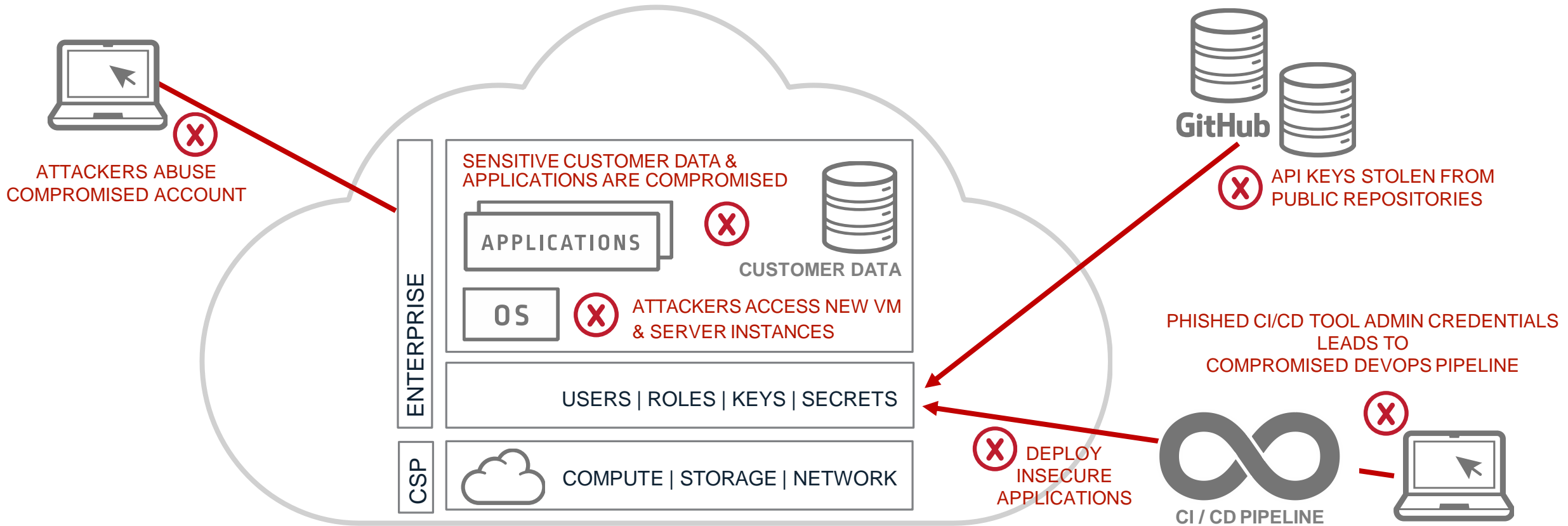
BASIC RED TEAM EXAMPLE: EXPOSES ENTERPRISES' CLOUD VULNERABILITIES

Red Team asked by a client to test potential vulnerabilities



WHAT IS THE THREAT MODEL FOR CLOUD WORKLOADS? ARE THEY VULNERABLE?

Examples of potential vulnerabilities and threat model that the enterprise must consider



WHAT CAN YOU DO TO SECURE YOUR CLOUD WORKLOADS?

Key Challenges to Secure Cloud Workloads	Privileged Accounts	
	Implications	Ability to Solve
Enterprise Wide Security Policies	●	✓
Multiple Cloud Environments, Hybrid, DevOps	●	✓
1. Management /Admin consoles – Cloud & CI/CD	●	✓
2. Access Keys, Secrets	●	✓
3. Apps & Assets Accessing Resources	●	✓
4. Newly Provisioned Resources /Elastic Compute	●	✓
5. DevOps CI/CD Pipeline	●	✓

Customer
Deployments

Industry
Experience

Best
Practice
Examples

“Security First” Focus

1

Discover and measure risks in cloud environments

2

Lock down cloud management consoles

3

Adopt enterprise wide security policies across compute & dev environments

4

Secure credentials and secrets for apps, scripts and other cloud assets

5

Automatically discover and secure privileged credentials in elastic compute environments

6

Plan for multiple cloud environments

DISCOVER AND MEASURE RISKS IN CLOUD ENVIRONMENTS

- Use tools like CyberArk DNA to discover cloud assets and identify risks in cloud workloads and environments
 - Discover user access keys and compute instances
 - Highlight and prioritize areas at the highest risk



CyberArk DNA™ | Discovery and Audit Report | Cloud Users

SCAN SUMMARY

Total IAM users identified: 26
Total IAM users access keys identified: 19
Unique non-compliant users identified: 1 (4%)

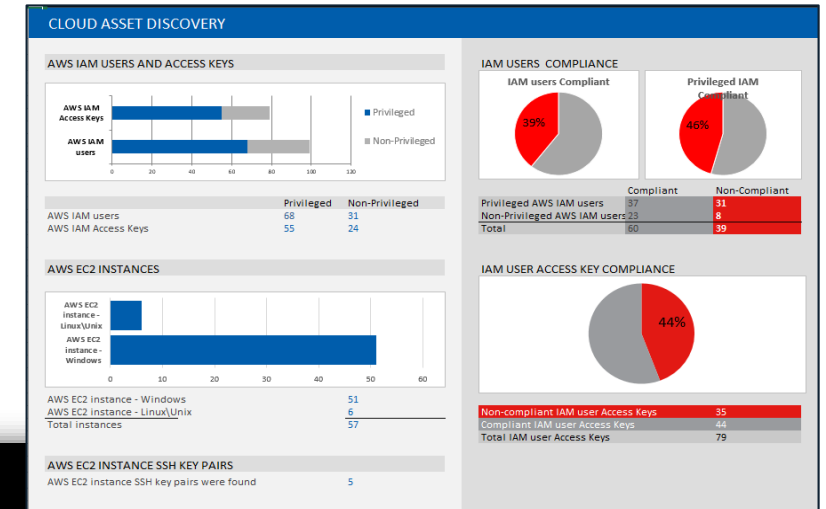
SCAN DETAILS

Date: 12:30:24 2016 יום שיני 12 דצמבר
Licensed to: CyberArk
Account ID: 085857639847
Object types: IAM users, IAM Access Keys
Password policy (to identify non-compliant users): Password change every 500 days (from AWS Password Policy)

LEGEND

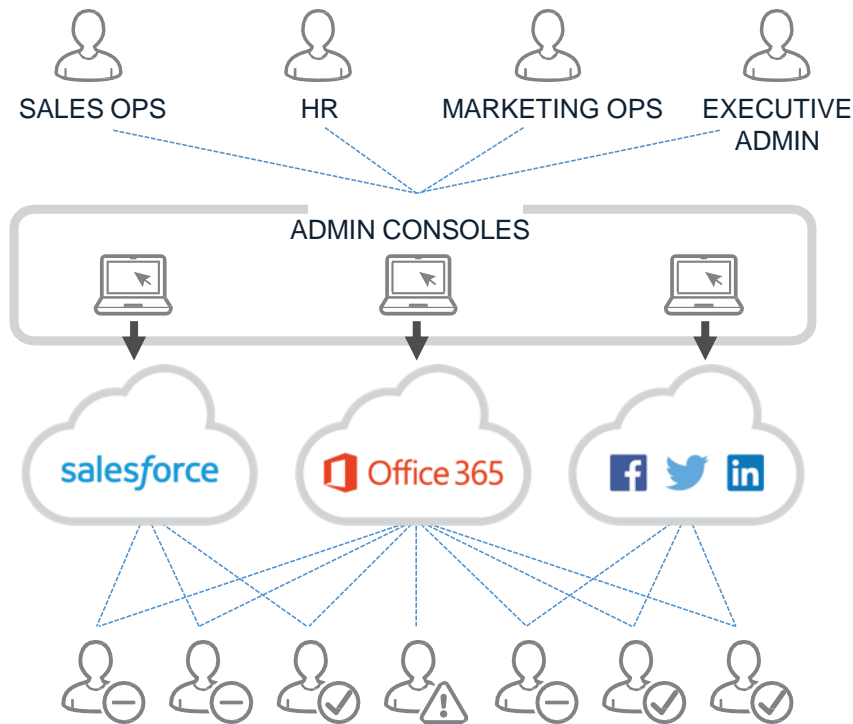
Non-compliant

User Name	Type	ARN	Access Key ID	Account Category	Status	Compliance Status	Passw
DNASystemTestsExpiredUser	Access Key	arn:aws:iam::085857639847:AKIAIEB22CSGBJGK5QHQ		Non-Privileged	Active	Compliant	63
DNASystemTestsInOneGroup	IAM User	arn:aws:iam::085857639847:N/A		Non-Privileged	N/A	Compliant	0
DNASystemTestsInOneGroup	Access Key	arn:aws:iam::085857639847:AKIAILWY2SEWKDSRDDLA		Non-Privileged	Active	Compliant	63
DNASystemTestsInTwoGroups	IAM User	arn:aws:iam::085857639847:N/A		Non-Privileged	N/A	Compliant	0
DNASystemTestsInTwoGroups	Access Key	arn:aws:iam::085857639847:AKIAIGTP3I2SRAKKFRHA		Non-Privileged	Active	Compliant	63
DNASystemTestsNoGroups	IAM User	arn:aws:iam::085857639847:N/A		Non-Privileged	N/A	Compliant	0
DNASystemTestsNoGroups	Access Key	arn:aws:iam::085857639847:AKIAJAZ662DFV6LAFSZQ		Non-Privileged	Active	Compliant	63
DNASystemTestsNonComplaintUse	IAM User	arn:aws:iam::085857639847:N/A		Non-Privileged	Expired	Non-Compliant	3716
DNASystemTestsNonComplaintUse	Access Key	arn:aws:iam::085857639847:AKIAJS5NDE3MMIK4IPSA		Non-Privileged	Active	Compliant	63
DNASystemTestsNonPrivilegedUse	IAM User	arn:aws:iam::085857639847:N/A		Non-Privileged	N/A	Compliant	0



SECURING COMMERCIAL SAAS APP CREDENTIALS

SaaS Administrators



Individual Users:
Employees, Contactors,
Partners, Former Employees!

Challenges with Credentials

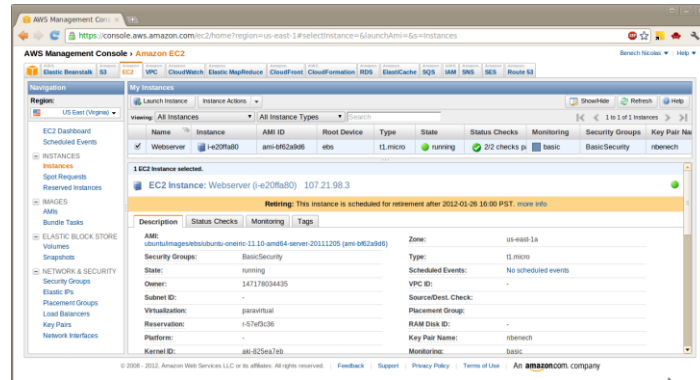
- Enable access to corporate data
- Used by Salesforce, HR admins, etc. not traditional IT
- Often shared and unchanged

Implications

- Proliferation of credentials, large attack surface
- Undetected access to data can continue for long periods
- Difficult to track and account for legitimate usage

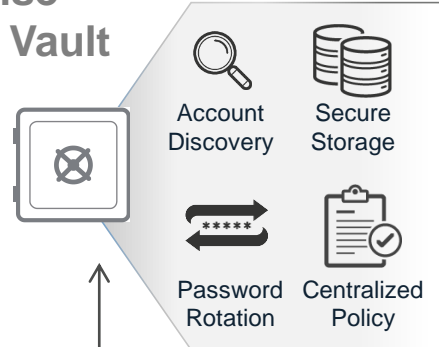
SECURE THE CLOUD MANAGEMENT CONSOLE/PORTAL

- Protect the “*keys to your cloud kingdom*”
 - Operations and configuration
 - Security / Authentication
 - Billing



Administrator /
End Users

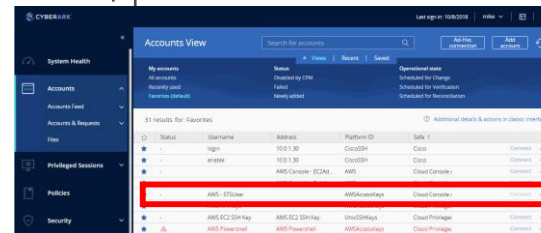
Enterprise
Password Vault



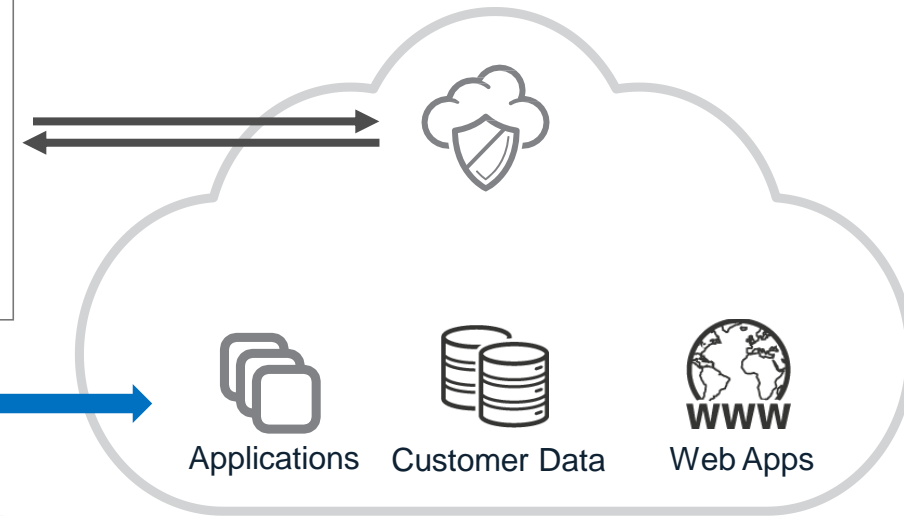
Web Portal



Accounts Available to Access



Integration with Cloud Provider
Enables Secure Single Sign On

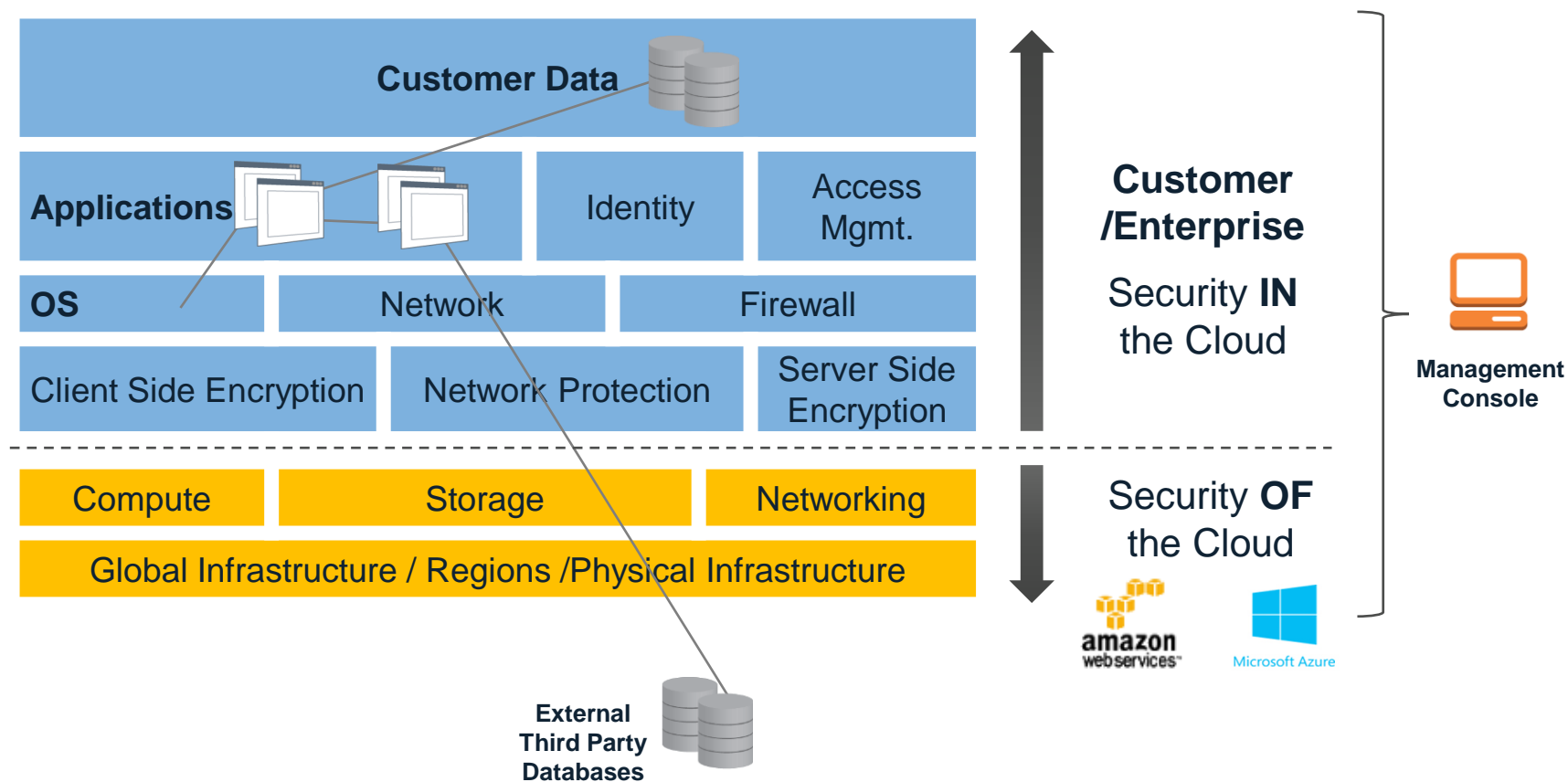


Cloud Infrastructure

APPS NEED TO INTERACT AND ACCESS SECRETS

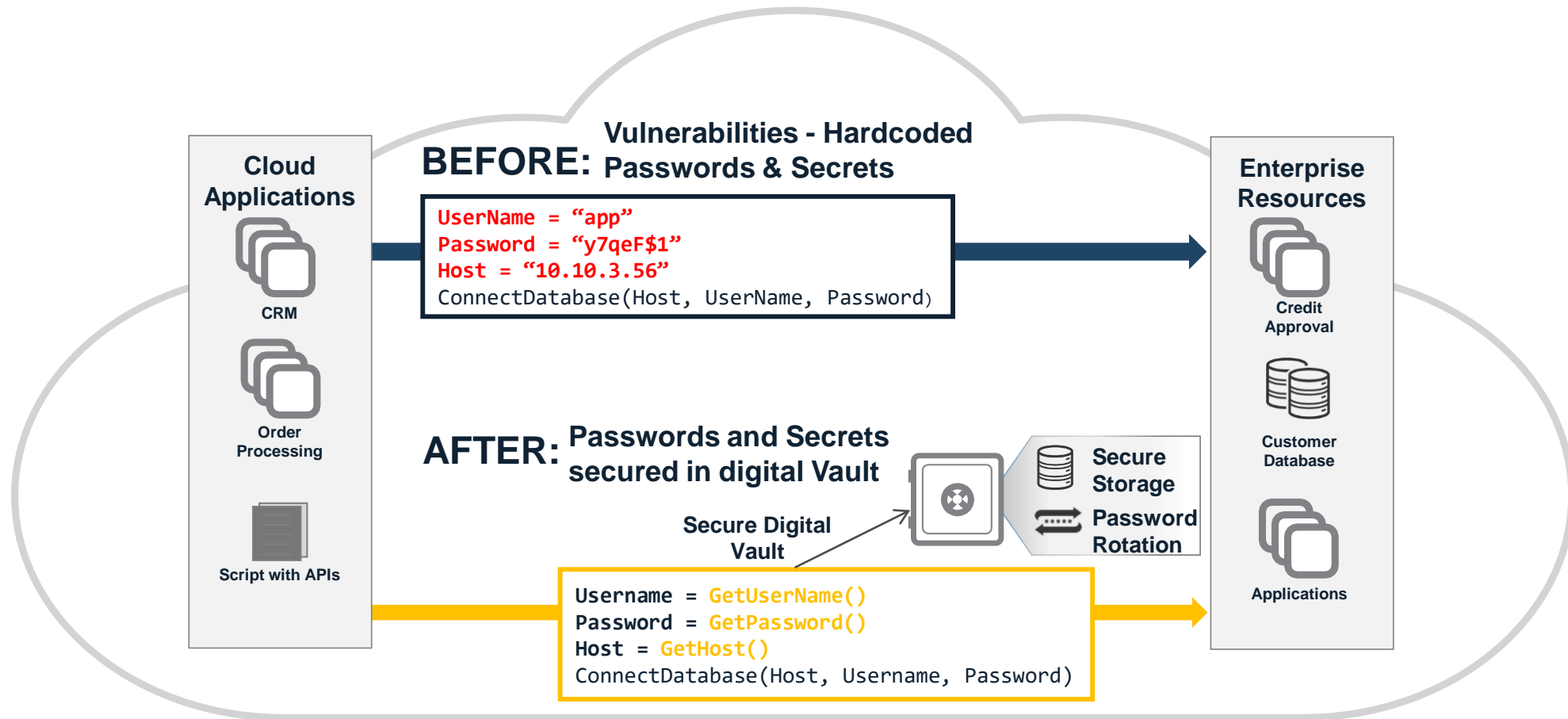
Applications and cloud assets need permissions

- Accessing customer data, third party data, etc.
- Interacting with other applications



SECURE CREDENTIALS & SECRETS FOR CLOUD WORKLOADS

Eliminate hardcoded passwords and secrets, and automate for elastic compute.



AUTOMATION IS REQUIRED IN ELASTIC ENVIRONMENTS

- Key business benefit of cloud is elasticity

ability to easily, instantaneously scale up and scale down

- Only pay for what you use
- Assign resources on the fly

- Approach: Automate

- Dynamically assign privilege and other credentials when app instances are created
- Immediately store secrets
- Leverage REST APIs, “**privilege as code**”, integrate with DevOps and cloud vendor tools

CyberArk REST API

Privilege_as_Code



AWS Auto
Scaling



SECURE YOUR ORGANIZATION'S CLOUD INFRASTRUCTURE

BENEFIT

On Demand Computing

Automation tools launch new virtual servers and resources dynamically

PROBLEM

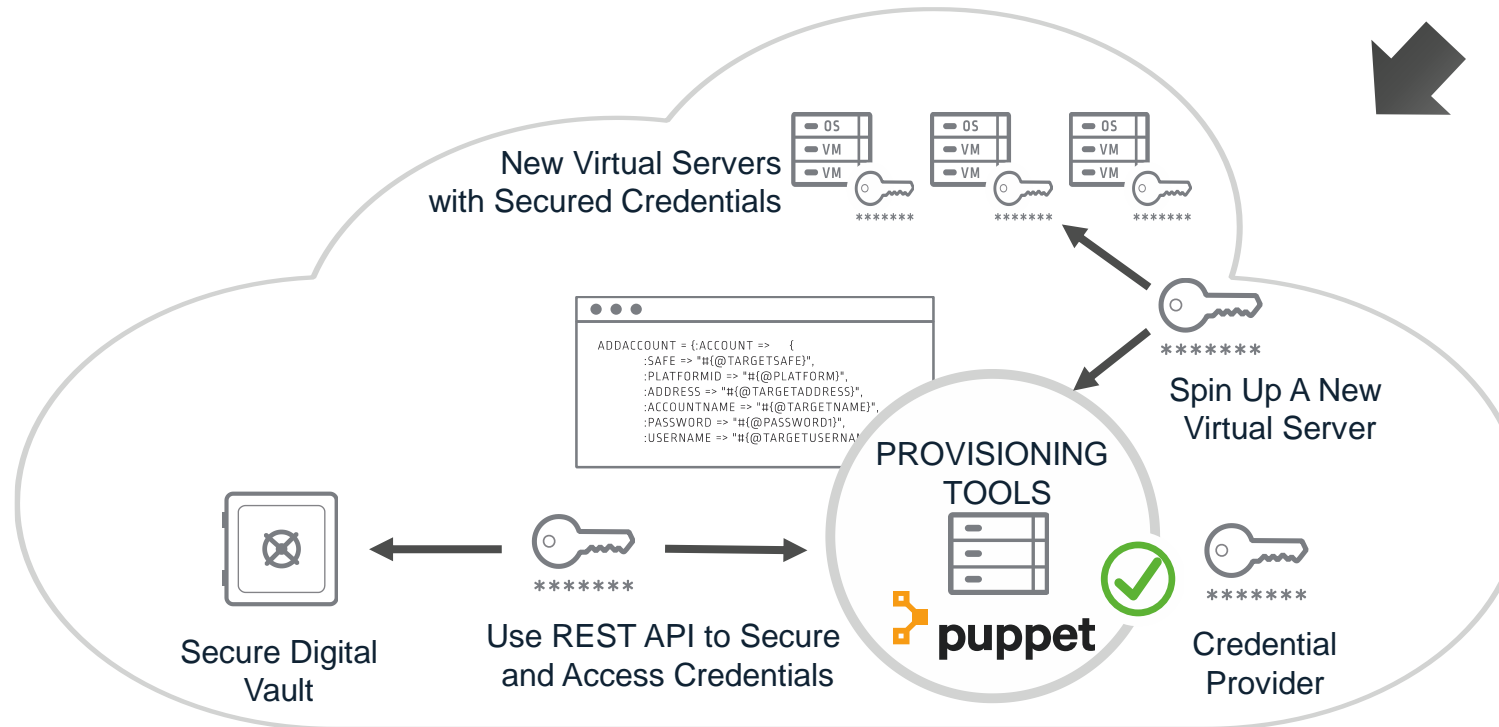
Credentials not Secured

New credentials assigned, but not secured

SOLUTION

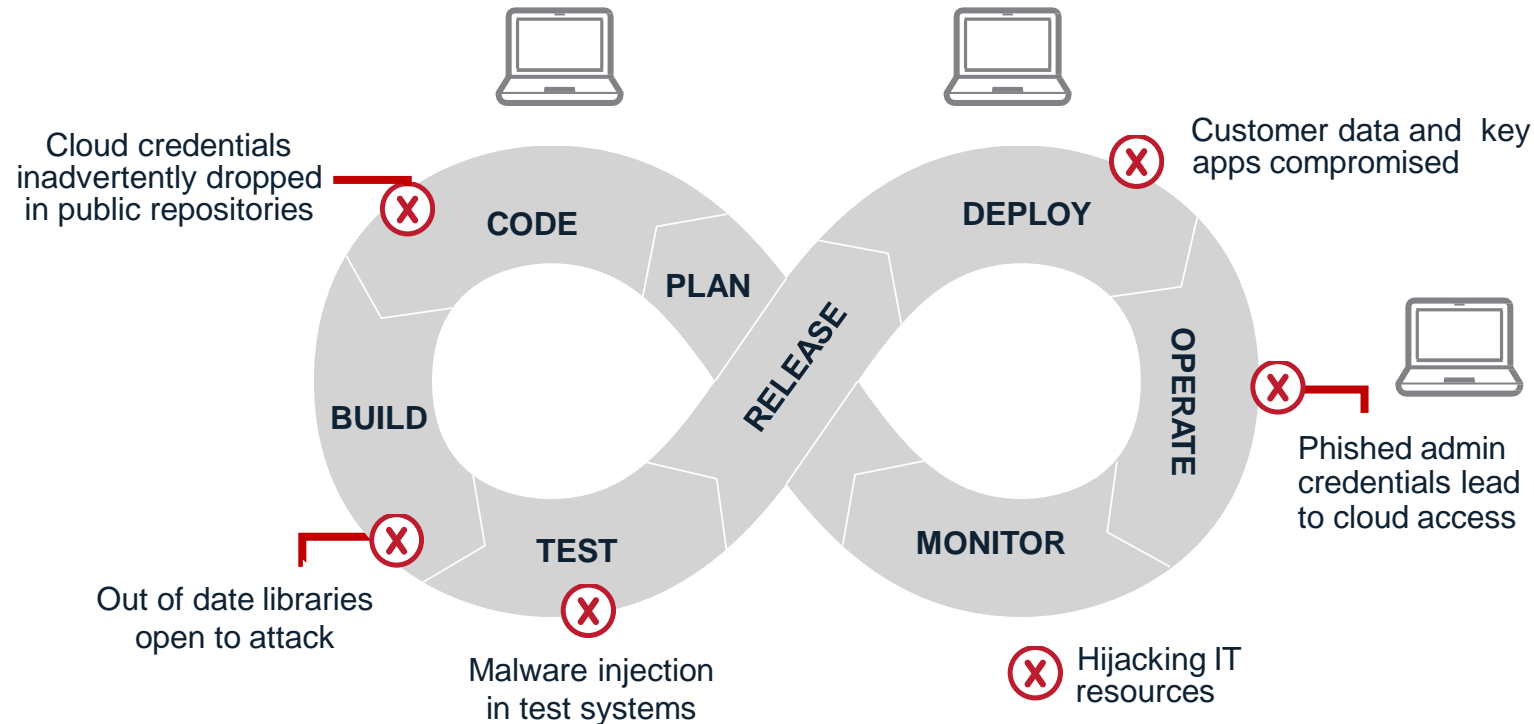
Use REST APIs to Automate

Automate securing credentials when new resources are provisioned



DEVOPS PIPELINE INCREASES AGILITY OF CLOUD ENVIRONMENTS

- Continuous Integration/Continuous Delivery (CI/CD) reduces time to deploy
- Need to secure secrets, credentials and privileged accounts throughout the DevOps pipeline
 - Secure secrets, credentials and privileges in scripts, application instances, etc.
 - Protect orchestration, build and deployment tool management consoles

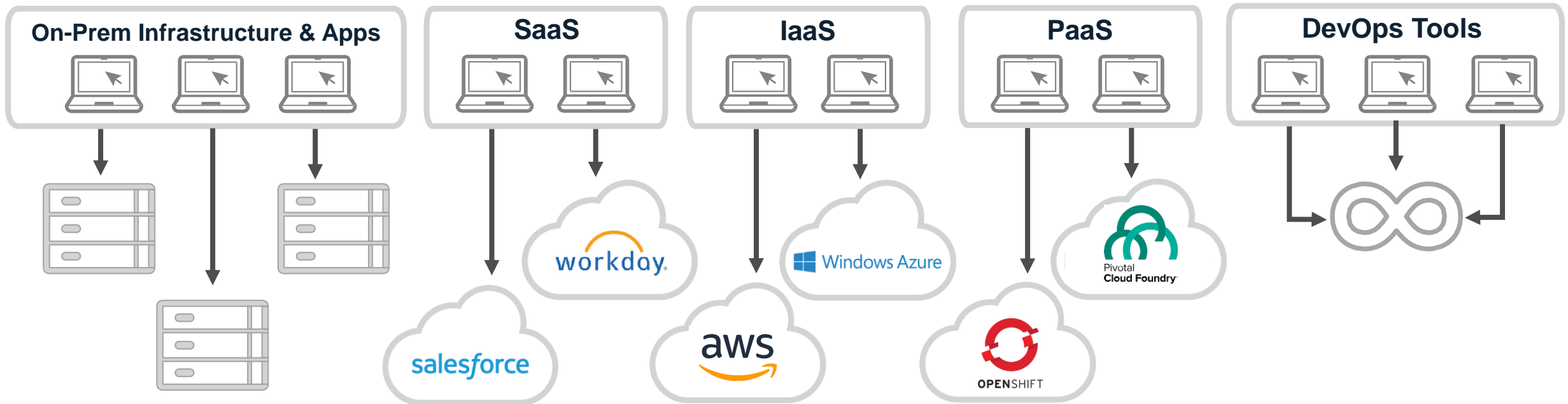


Try the Conjur open source secrets management solution for developers (Conjur Community Edition) => conjur.org

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

Consistently Enforce Privilege Security Policies End to End Across The Enterprise



THANK YOU!