

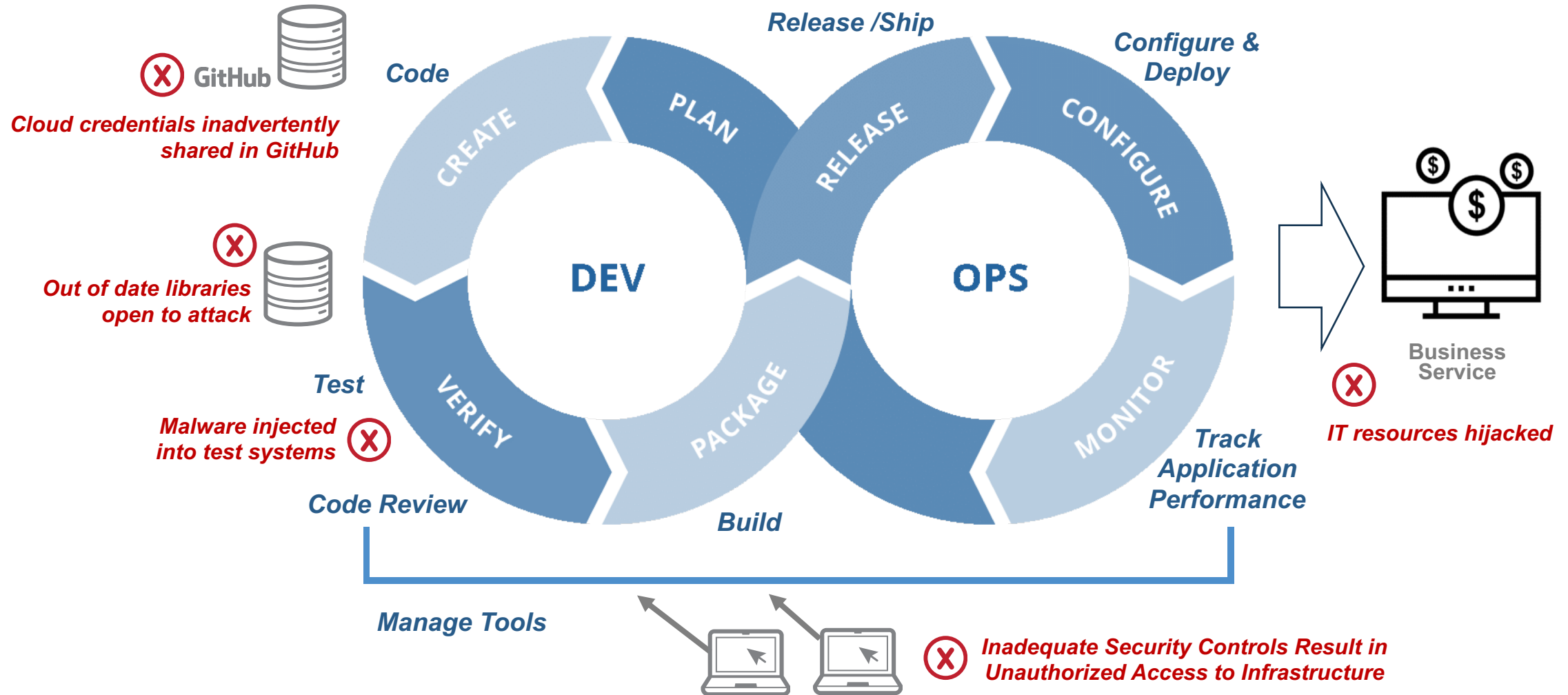
CENTRALLY MANAGE APPLICATIONS SECRETS RUNNING IN OPENSIFT

REDHAT FORUM
Paris, October 2018

Djamel Bourokba, Principal Solution Engineer EMEA at CyberArk

THE CHALLENGE

DevOps Introduces New Threat Models & Expands the Attack Surface



Attackers Find New Opportunities: Keys In The Build Systems

Build

Execute shell

Command `#!/bin/bash -e`

```
# note that us-east-1 is not required in this list because the source AMI is built in us-east-1
REGIONS="us-west-1,us-west-2,\
eu-west-1,eu-central-1,\
ap-southeast-1,ap-southeast-2,ap-northeast-1,ap-northeast-2,\
sa-east-1"

AWS_ACCOUNT='732831827364'
AWS_ACCESS_KEY_ID='AKIAIOSFODNN7EXAMPLE'
AWS_SECRET_ACCESS_KEY='wJalrXUtnFEMI/K7MDENG/bPxRfiCYzEXAMPLEKEY'

make build

echo "-----"

echo -n "AMI to promote: "
read AMI
```










See [the list of available environment variables](#)

Advanced...

Add build step ▾

But, Native Tools Create Challenges With “Islands Of Security”

Islands of Security

| | | |
|--|--|---|
|  docker Secrets |  RED HAT OPENSIFT.io Secrets |  kubernetes Secrets |
|  puppet Hiera |  ANSIBLE Vault |  CHEF Databags |
|  aws IAM / KMS |  Azure IAM / KMS |  Google Cloud Platform IAM / KMS |

- Native tool vendors not focused on security, most not enterprise ready

Vs.

- Central view and control of Privileged Access Security
- Enterprise wide solution for on-premises, hybrid, cloud only
- Leverage the portfolio of CyberArk capabilities (Vault, monitoring, etc.)

THE SOLUTION

CONJUR IS A DEVOPS & CLOUD SECURITY SOLUTION

Addresses the secrets management and privileged access challenges of containers and the CI/CD pipeline

- **Native integrations avoid impacting developer velocity**

- Leading container platforms
- DevOps tools
- Cloud management solutions



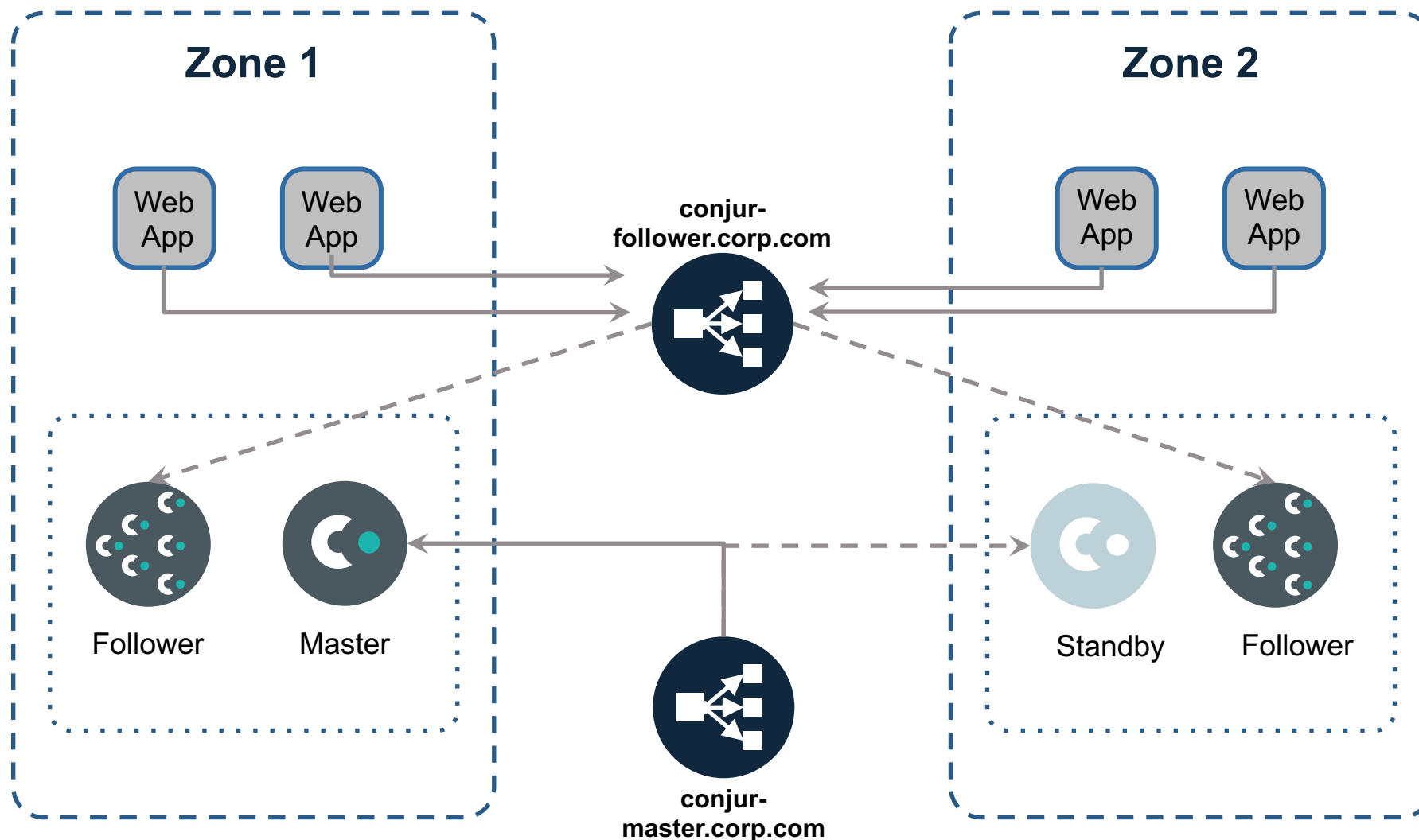
- **Powerful security features improve overall security**

- Separation of Duties, Role Based Access, Policy based workflows
- Vault integration enables policies to be consistency applied

- **Open Source and “as code” appeals to developers**

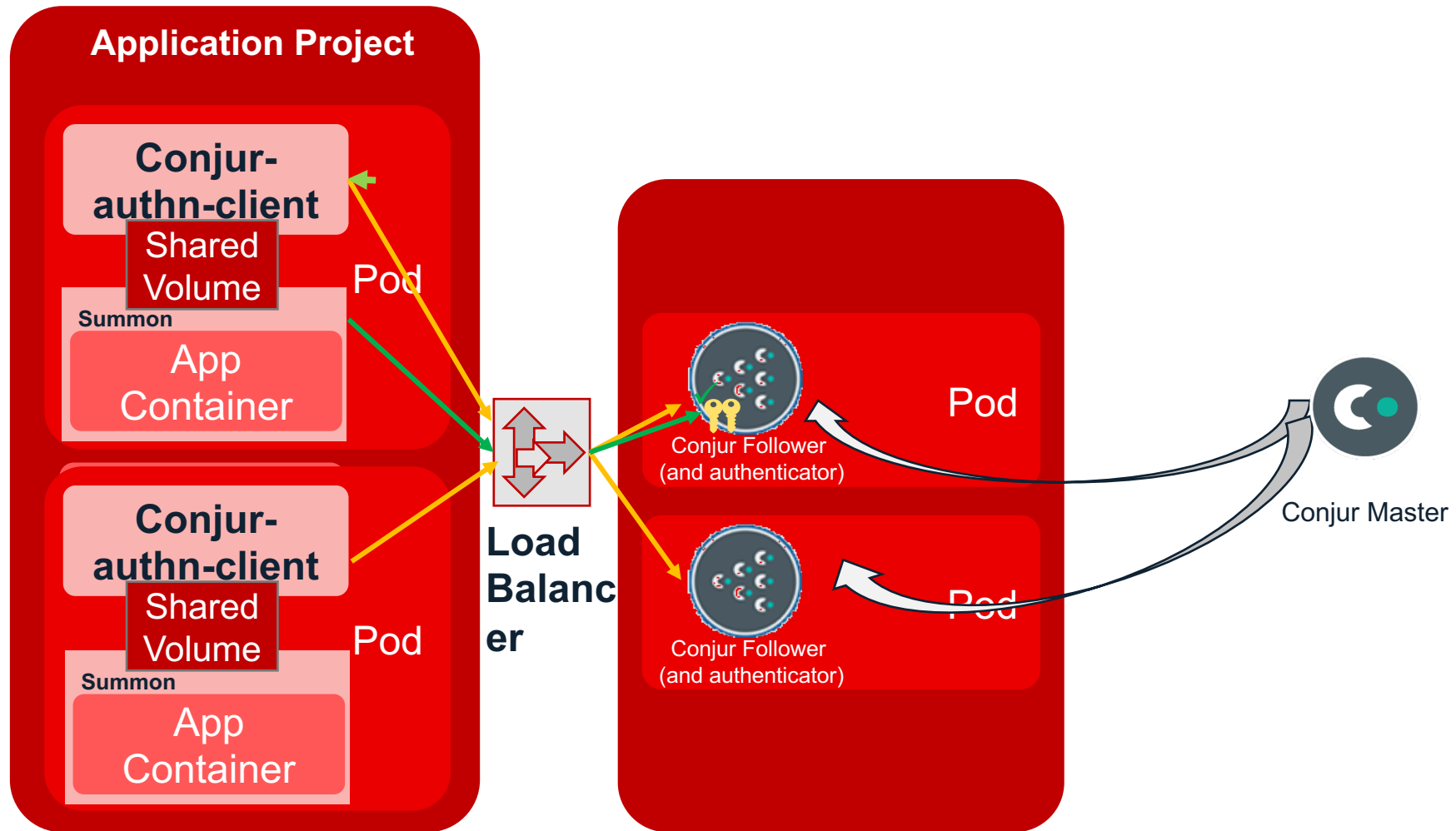
- Easily upgraded to fully supported enterprise version
- “as code” enables version control, automated replication, etc.

CyberArk Conjur Is Highly Scalable And Available



Confidential and Proprietary. © CyberArk Software Ltd. All rights reserved.

OPENSIFT – CONJUR DETAILED FLOW

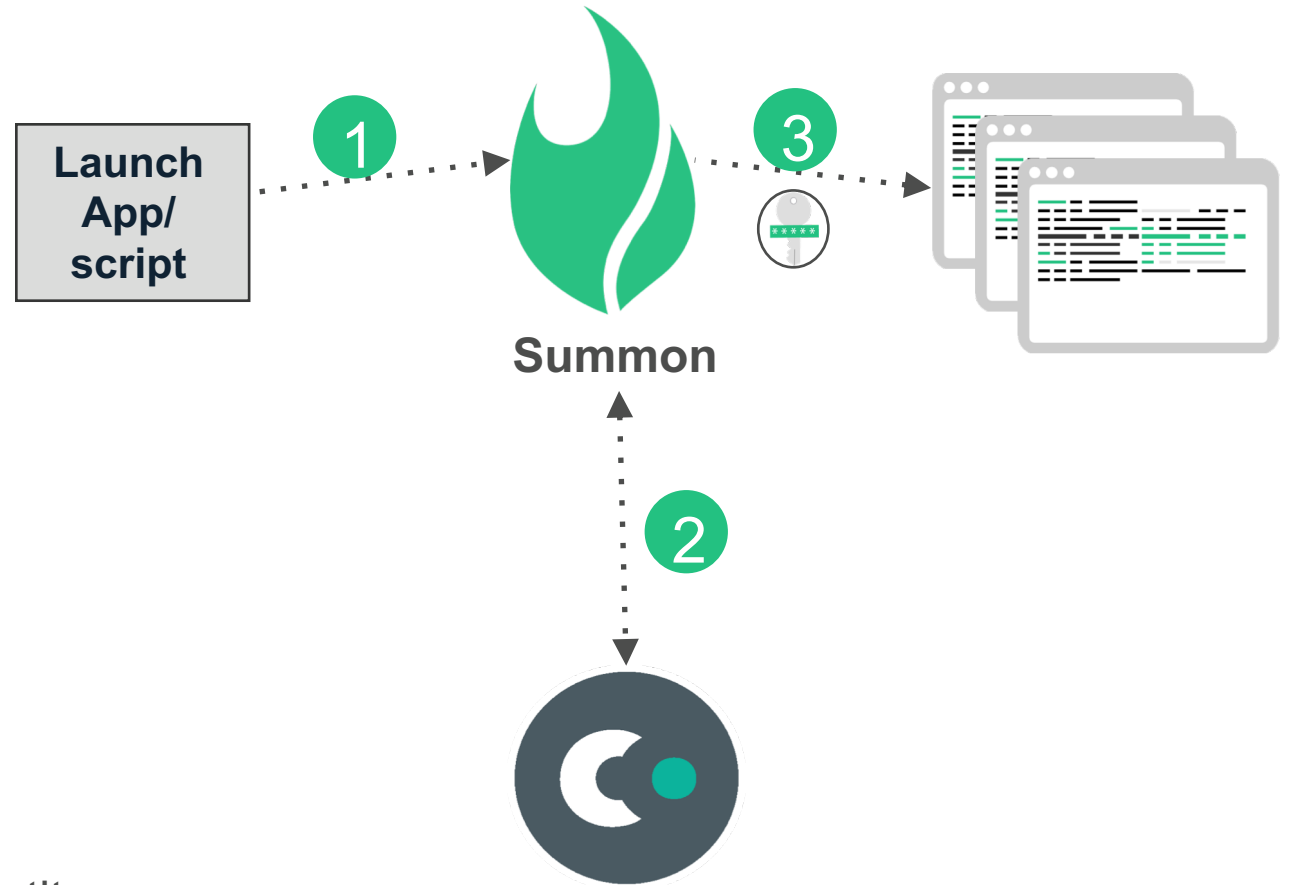


SECRETS MANAGEMENT BECOMES EASIER USING SUMMON

An open-source tool to help developers and sysadmins improve workflows that involve access to secrets.

Summon fetches the secrets and makes them available in the environment of the specified process.

Once the process exits the environment variables do not remain on the system.



- 1 Processes started using Summon
- 2 Summon fetches secrets using machine identity
- 3 Processes launched with secrets in environment

©CyberArk Software Ltd. All rights reserved.

THE DEMO

WHAT'S NEXT ?

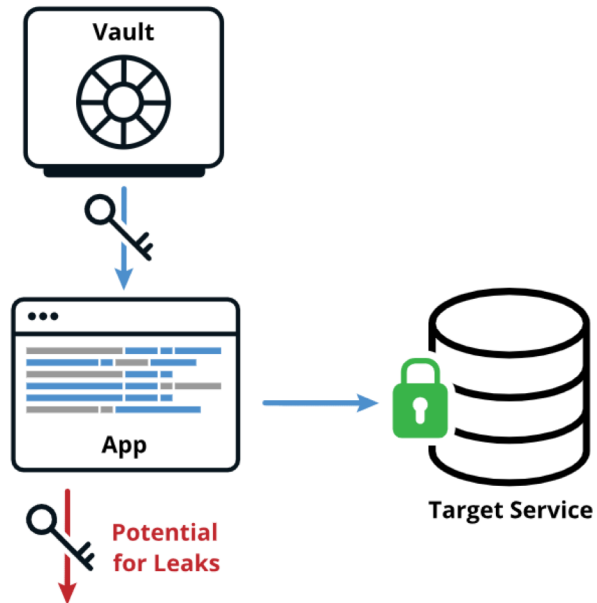
SECURE ANSIBLE WITH CYBERARK -CONJUR

- Secrets managed by CyberArk and Conjur are delivered securely to Ansible hosts
- Least privilege enforced on Ansible hosts
- Security Teams enabled to bring best practices to Ansible and meet compliance requirements
- Removes the need to duplicate Secrets Management functionality across multiple platforms.
- Audit privileged activity on Ansible hosts



REMOVE COMPLETELY SECRETS PROBLEM FROM DEVELOPERS WITH SECRETLESS

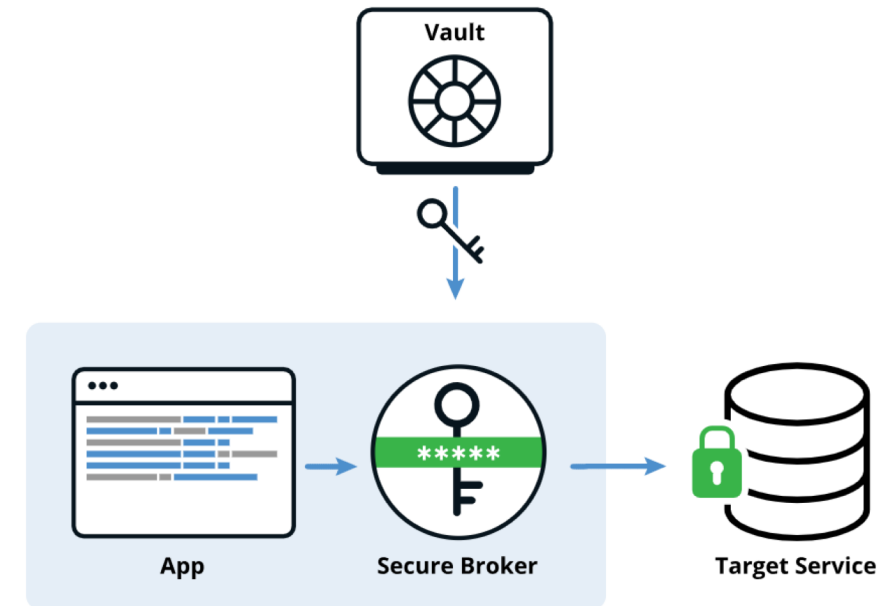
The Old Way



Developer Responsibilities

- Fetch secrets from vault
- Securely handle fetched secrets within app
- Resiliently handle secret rotations
- Manage connection disruptions
- Connect to target services using fetched secrets

With Secretless Broker



Developer Responsibilities

- Manage connection disruptions
- Connect to target services using local sockets and URLs

Secretless Broker Automates the Rest

IT'S EASY TO GET STARTED



- Visit us at www.cyberark.com/conjur
- Try CyberArk Conjurer Open Source at www.conjur.org
- Summon Open Source at <https://github.com/cyberark/summon>
- Secretless Open Source at <https://secretless.io/>
- Read our DevOps Security Blog www.conjur.org/blog