ESG a division of TechTarget Enterprise Strategy Group | **Getting to the bigger truth.™**

Technical Validation

CyberArk Conjur Secrets Manager

Secure Secrets Management for Cloud-native, Containerized Applications and DevOps Tools

By Tony Palmer, Principal Validation Analyst

July 2022

This ESG Technical Validation was commissioned by CyberArk and is distributed under license from TechTarget, Inc.

Introduction

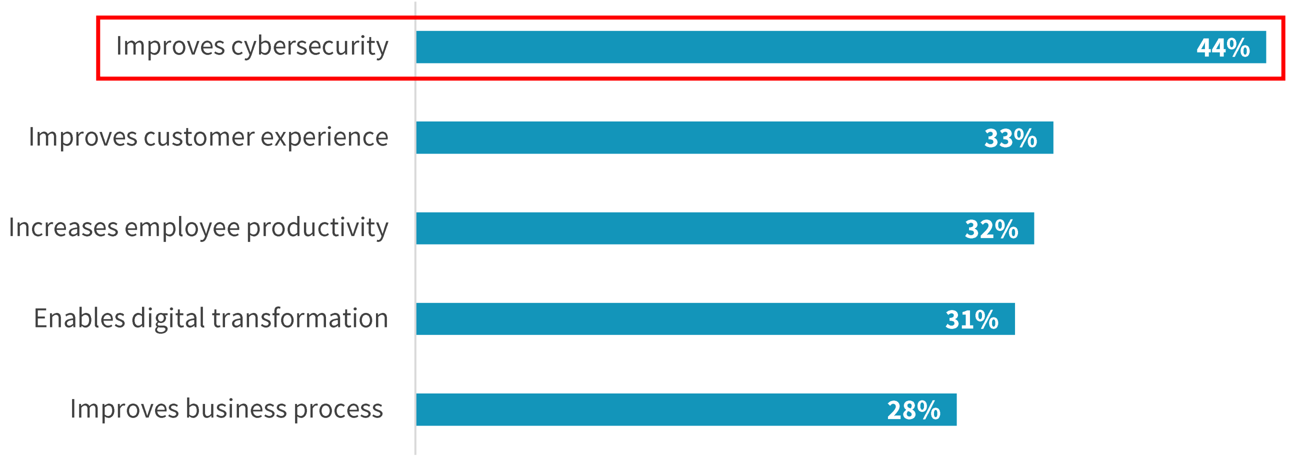
This ESG Technical Validation explores the CyberArk Conjur Secrets Manager platform that provides secure secrets management for cloud-native, containerized applications and DevOps tools. The report includes results of remote validation of CyberArk Conjur Secrets Manager.

Background

Given the unabated increase in security threats, it's no surprise that improving cybersecurity was by far the most popular response of ESG research survey respondents for the most important considerations for justifying IT investments in 2022. Nearly half (44%) cited cybersecurity improvements as a factor they believe will be most important in justifying IT investments to their organizations' business management teams over the next 12 months (see Figure 1). Also, 93% of survey respondents said they expected their organization's spending on identity and access management to increase or stay flat in 2022. In addition, 38% of respondents identified strengthening cybersecurity and 28% identified improving operational resiliency against cyber-attacks as business initiatives that they expected would drive the most technology spending at their organizations over the next 12 months.[1]

Figure 1. Top Five Considerations Justifying 2022 IT Investment

Which of the following considerations do you believe will be most important in justifying IT investments to your organization's business management team over the next 12 months? (Percent of respondents, N=706, five responses accepted)



Source: ESG, a division of TechTarget, Inc.

Developers may cringe at these results, dreading the coming assault of clunky integrations and security checkpoints that slow down development. An essential part of developer productivity in today's security-focused environment is delivering business value securely without slowing delivery down. According to ESG research, 41% of organizations stated that integration with their software development lifecycle and continuous integration and continuous delivery (CI/CD) tools is one of their top priorities for cloud-native security controls.[2]

[1] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021.

[2] Source: ESG Survey Results, *The Maturation of Cloud-native Security: Securing Modern Apps and Infrastructure*, June 2021.

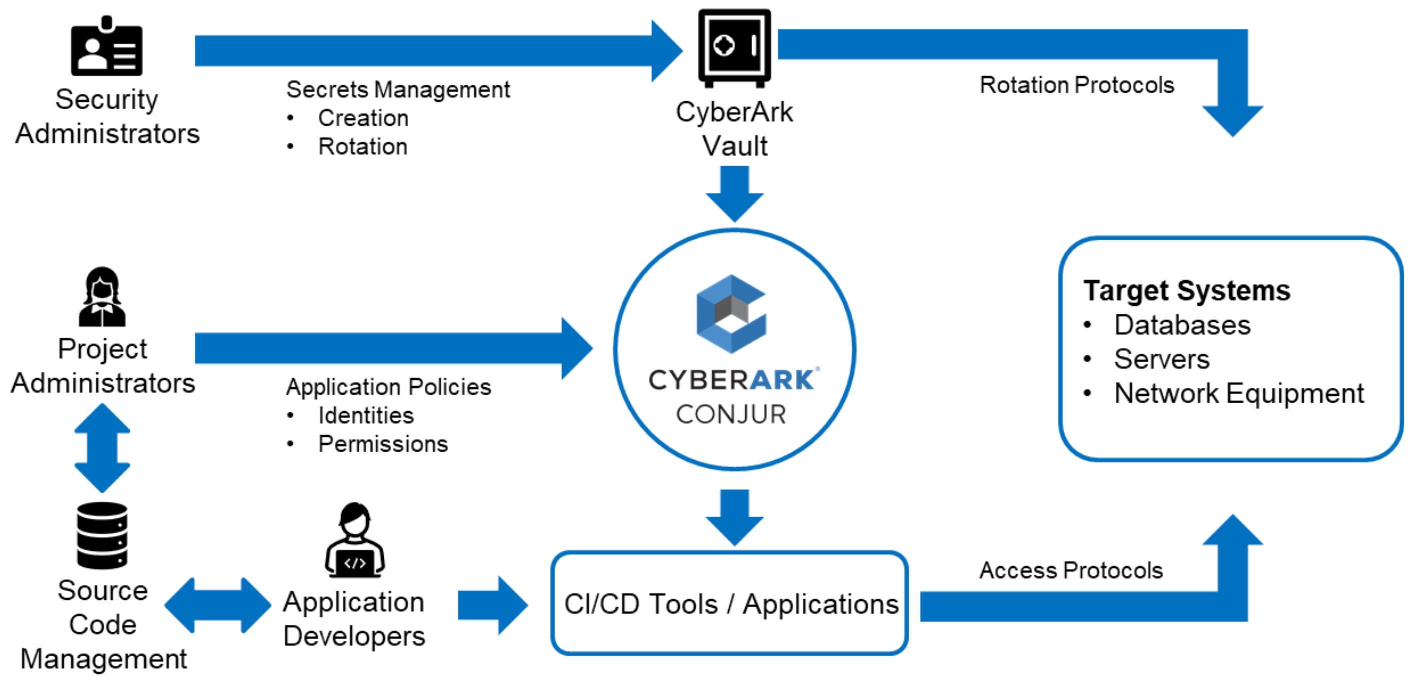
The Solution: CyberArk Conjur Secrets Management

CyberArk Conjur Secrets Manager is designed to secure secrets and credentials used by a broad range of application types in hybrid, cloud-native, and containerized environments. Secrets Manager comprises Conjur Secrets Manager Enterprise (and Open Source) and the Credential Providers and facilitates securing all application secrets across the enterprise. CyberArk understands the importance of securing non-human identities in a way that won't get in the way of developers.

The Conjur Secrets Manager architecture is shown in Figure 2. Security Administrators control the creation and rotation of secrets required to run applications. These secrets are managed in CyberArk Vault, the central secret repository. The Vault rotates credentials used to access target systems such as databases, servers, or network equipment.

On the application side, Project Administrators define application policies within Conjur. These policies define role-based access controls on non-human identities, namely the applications that need access to the target systems. Conjur provides developers with easy-to-use solutions to secure secrets in application and DevOps environments. To the developers, it's just another configuration for the application or platform. When a CI/CD tool or an application requires access to target systems, they authenticate to Conjur, and Conjur provides the secrets at runtime. Every interaction with every secret, whether it's a read, execute, or even a failure, is logged in audit events. Even when a Conjur administrator checks the audit events in the platform, that access is logged.

Figure 2. CyberArk Conjur Secrets Management



Source: ESG, a division of TechTarget, Inc.

CyberArk Conjur eliminates hard-coded secrets in source code while providing a better way to manage those secrets. It inspects all access and changes to provide tamper-resistant audit, rotates secrets automatically according to company policies, and scales with organizations' DevOps environments.

ESG previewed two new functionalities while testing for this report. In early release at the time of this writing, CyberArk has a service called Secrets Hub that allows developers to keep their native secrets management experience in AWS while providing security control. Secrets Hub makes it easy for security teams to manage secrets with the CyberArk tools they are familiar with while allowing developers to continue to use AWS Secrets Manager. With transparent replication of secrets to

AWS Secrets Manager, Secrets Hub provides developers with a simple, secure, and consistent way to access secrets in AWS without changing their workflows. Another new functionality is Conjur Cloud. This is a fully SaaS version of the Conjur Secrets Manager solution designed with the same goals in mind as Conjur Secrets Manager: to accelerate time to value while lowering infrastructure costs with SaaS, centralize secrets management to improve security visibility, remove hard-coded secrets from DevOps tools and compliance violations, eliminate secret zero vulnerabilities with unique machine identities, and leverage native DevOps integrations to secure all application secrets everywhere.

ESG Technical Validation

Conjur Secrets Manager Enterprise provides a secrets management solution designed for the unique requirements of cloud-native and DevOps environments. The solution integrates with numerous DevOps tools and PaaS/container orchestration platforms and supports hybrid and multi-cloud environments. The solution also integrates with the CyberArk Identity Security Platform to provide a single enterprise-wide platform for securing all of an organization’s privileged credentials, including legacy apps.

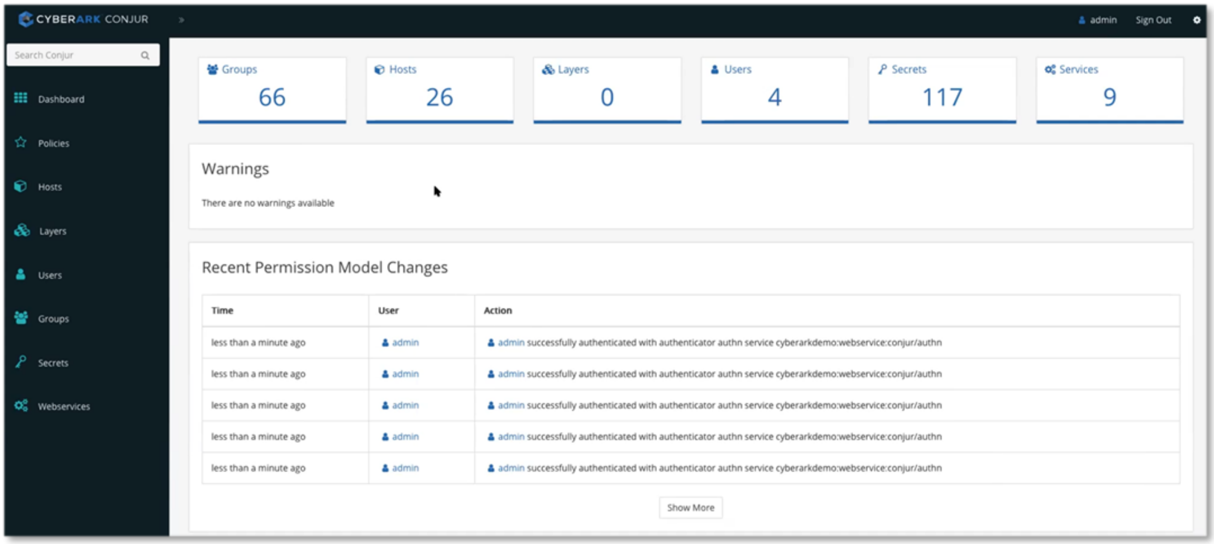
Securing All Apps Everywhere

ESG looked at how CyberArk provides organizations with autonomy, empowering users to obtain credentials using self-service interfaces, and automates the process using a single vault to secure the entire chain of trust for applications, humans, and service accounts, eliminating the security risk of embedded credentials.

ESG Testing

ESG started with the Conjur dashboard (see Figure 3). The dashboard provides a view of everything managed by Conjur. Everything in Conjur—except for the secrets—is defined via “policies as code.” Secrets are created manually and stored in the CyberArk Enterprise Vault. The Conjur policy engine applies authorizations that allows applications and processes to retrieve those secrets. Conjur uses role-based access controls through an authorization engine to control administrative access.

Figure 3. CyberArk Conjur Secrets Manager Dashboard



Groups	Hosts	Layers	Users	Secrets	Services
66	26	0	4	117	9

Warnings

There are no warnings available

Recent Permission Model Changes

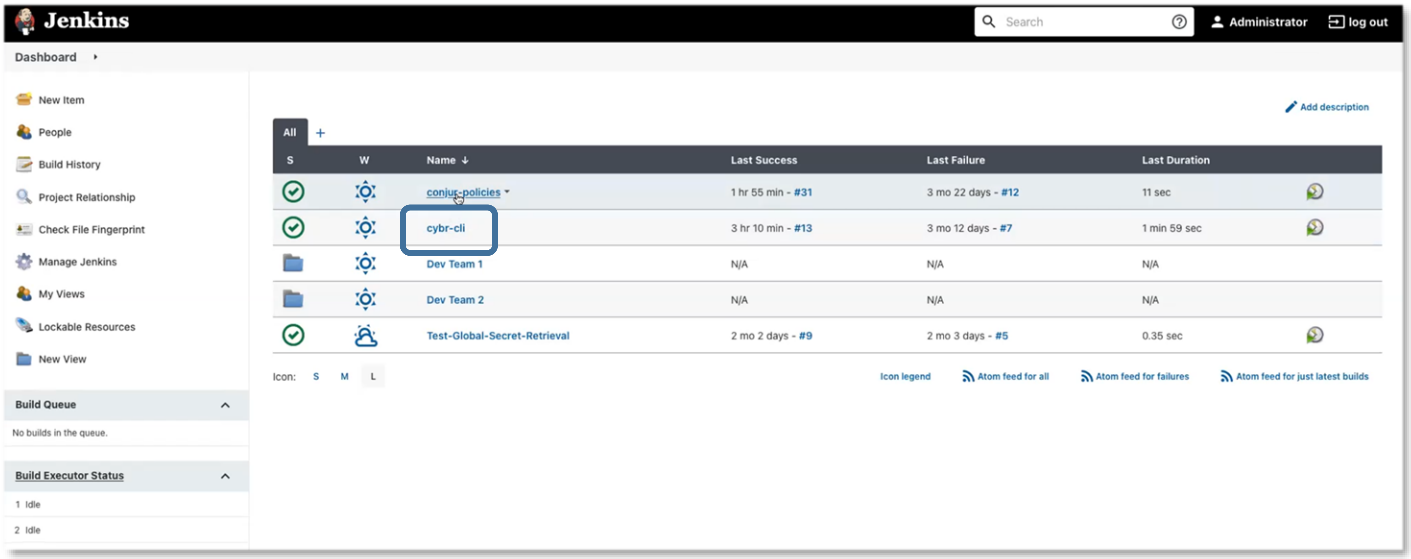
Time	User	Action
less than a minute ago	admin	admin successfully authenticated with authenticator authn service cyberarkdemo:webservice:conjur/authn
less than a minute ago	admin	admin successfully authenticated with authenticator authn service cyberarkdemo:webservice:conjur/authn
less than a minute ago	admin	admin successfully authenticated with authenticator authn service cyberarkdemo:webservice:conjur/authn
less than a minute ago	admin	admin successfully authenticated with authenticator authn service cyberarkdemo:webservice:conjur/authn
less than a minute ago	admin	admin successfully authenticated with authenticator authn service cyberarkdemo:webservice:conjur/authn

Source: ESG, a division of TechTarget, Inc.

Next, we looked at Jenkins, a popular open source automation server used to build, deploy, and automate projects. Jenkins is a critical part of software supply chain security—it's essentially the tool in the middle of building the supply chain. CyberArk also integrates with the CloudBees platform. In Figure 4, you can see several projects, including an open source project *cybr-cli* and a job to load Conjur policies. It's important to note that this job contains no secrets, so it's safe to put this policy on public source control management and show that to customers.

Conjur has a Jenkins plugin available in the Jenkins plugin repository that integrates Jenkins with Conjur using JSON Web Tokens (JWT). CyberArk also offers a generic JWT Authenticator that integrates with many other tools, with Kubernetes and GitLab as two examples.

Figure 4. Projects in Jenkins

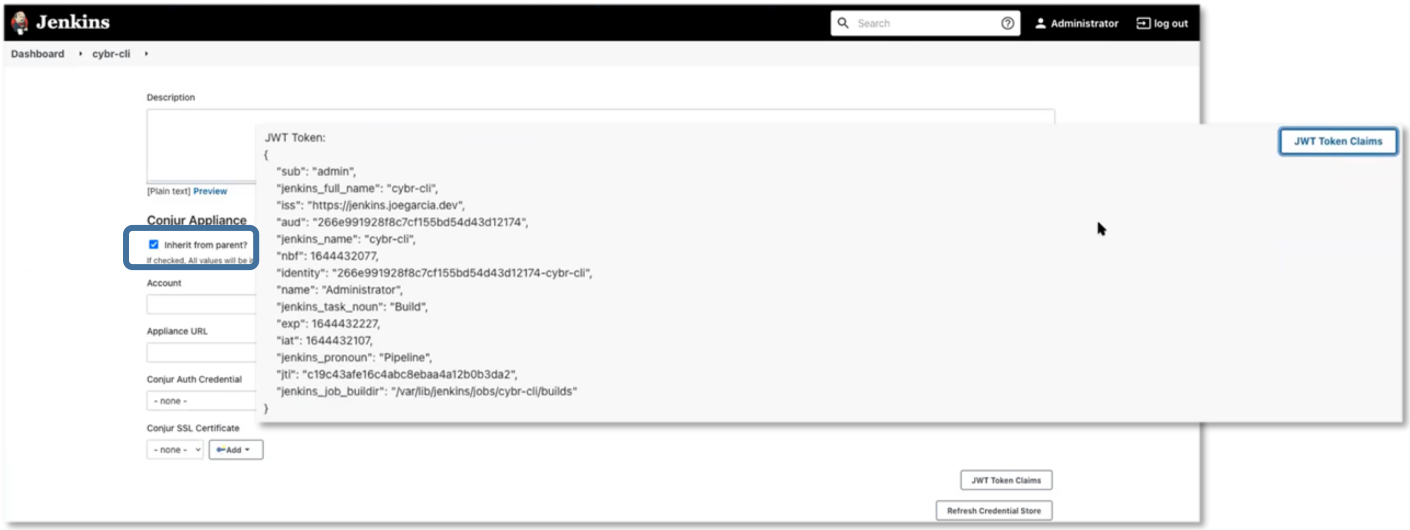


S	W	Name ↓	Last Success	Last Failure	Last Duration
✓	☼	conjur-policies	1 hr 55 min - #31	3 mo 22 days - #12	11 sec
✓	☼	cybr-cli	3 hr 10 min - #13	3 mo 12 days - #7	1 min 59 sec
	☼	Dev Team 1	N/A	N/A	N/A
	☼	Dev Team 2	N/A	N/A	N/A
✓		Test-Global-Secret-Retrieval	2 mo 2 days - #9	2 mo 3 days - #5	0.35 sec

Source: ESG, a division of TechTarget, Inc.

While Conjur supports authenticating with a host identity and API key, JWT authentication eliminates the need to store a secret inside Jenkins. Configuring the *cybr-cli* job pulls the Jenkins file from git. If "Inherit from Parent" is selected, the global configuration is used. When we clicked *JWT Token Claims*, the payload was generated and could be copied for the security team to update policies.

Figure 5. Eliminating Secret Zero



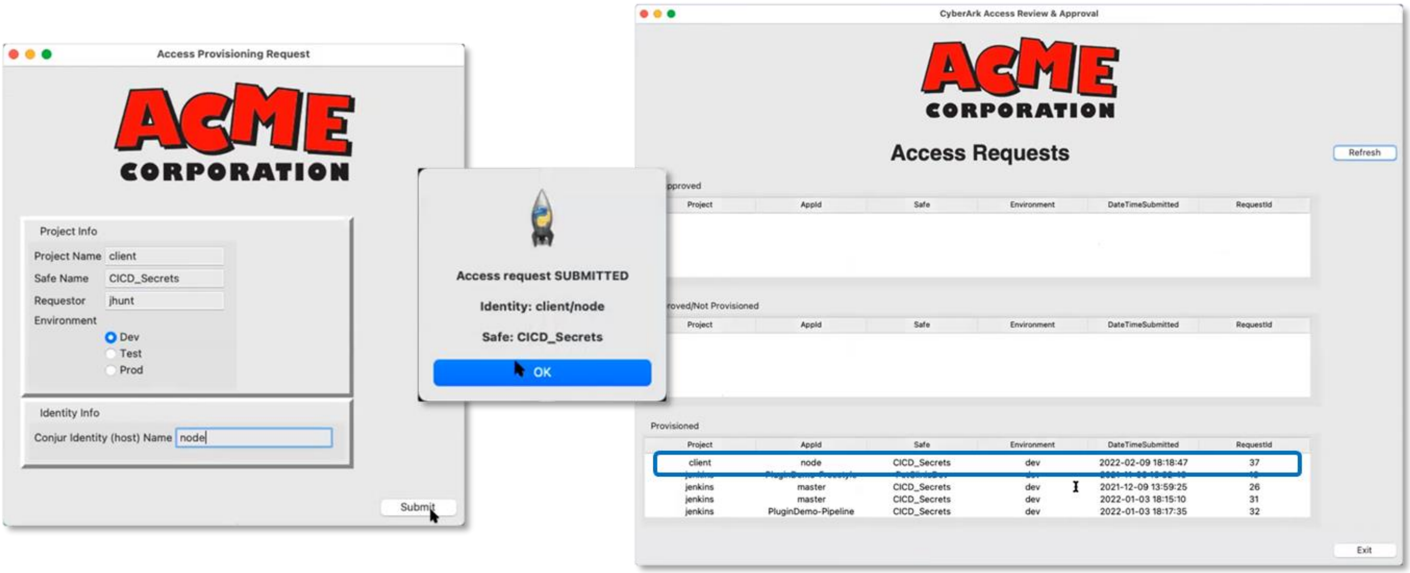
```
JWT Token:
{
  "sub": "admin",
  "jenkins_full_name": "cybr-cli",
  "iss": "https://jenkins.joegarcia.dev",
  "aud": "266e991928f8c7cf155bd54d43d12174",
  "jenkins_name": "cybr-cli",
  "nbf": 1644432077,
  "identity": "266e991928f8c7cf155bd54d43d12174-cybr-cli",
  "name": "Administrator",
  "jenkins_task_noun": "Build",
  "exp": 1644432227,
  "iat": 1644432107,
  "jenkins_pronoun": "Pipeline",
  "jti": "c19c43afe16c4abc8ebaa4a12b0b3da2",
  "jenkins_job_buildir": "/var/lib/jenkins/jobs/cybr-cli/builds"
}
```

Source: ESG, a division of TechTarget, Inc.

Next, we looked at Conjur in action. ESG walked through a scenario where a developer requests access to credentials for an application. In our test environment, we used Terraform as our CI/CD tool and a custom-developed access provisioning interface. In a real-world deployment, this would usually be a workflow automation tool like ServiceNow or Jira.

First, we opened the Access Provisioning request application and entered the project name, the name of the vault, the requestor credentials, and the name of the Conjur Identity host. For this test, we selected *Dev* as the environment type.

Figure 6. Self-service Developer Access


Access Provisioning Request
ACME CORPORATION
Submit
OK
CyberArk Access Review & Approval
ACME CORPORATION
Refresh
Exit

Project Info

Project Name: client

Safe Name: CICD_Secrets

Requestor: jhunt

Environment: ● Dev ○ Test ○ Prod

Identity Info

Conjur Identity (host) Name: node

Access request SUBMITTED

Identity: client/node

Safe: CICD_Secrets

Access Requests

pproved

Project	AppId	Safe	Environment	DateTimeSubmitted	RequestId

roved/Not Provisioned

Project	AppId	Safe	Environment	DateTimeSubmitted	RequestId

Provisioned

Project	AppId	Safe	Environment	DateTimeSubmitted	RequestId
client	node	CICD_Secrets	dev	2022-02-09 18:18:47	37
jenkins	PluginDemo-Freestyle	[illegible]	dev	[illegible]	[illegible]
jenkins	master	CICD_Secrets	dev	2021-12-09 13:59:25	26
jenkins	master	CICD_Secrets	dev	2022-01-03 18:15:10	31
jenkins	PluginDemo-Pipeline	CICD_Secrets	dev	2022-01-03 18:17:35	32

Source: ESG, a division of TechTarget, Inc.

Access was automatically granted to our development environment. For test or production access, approval would be required, and the process would be automatically routed to the appropriate resource for approval.

Why This Matters

ESG research revealed that cybersecurity was cited as one of the most important considerations for justifying IT investments in 2022. Cybersecurity improvements are recognized as an important factor in getting IT projects funded, and a vast majority (93%) of survey respondents expected their organization's spending on identity and access management solutions to increase or stay flat in 2022.[3]

ESG validated that CyberArk can eliminate the risks posed by hard coding secrets and credentials into applications. In our testing, Conjur Secrets Manager proved that it centralizes and secures secrets across platforms. As CyberArk describes it, they secure "all app secrets anywhere." They do this using familiar tools, which enables enforcement of best practices; central control; separation of duty (SoD); and governance, risk management, and compliance (GRC), without compromising business agility.

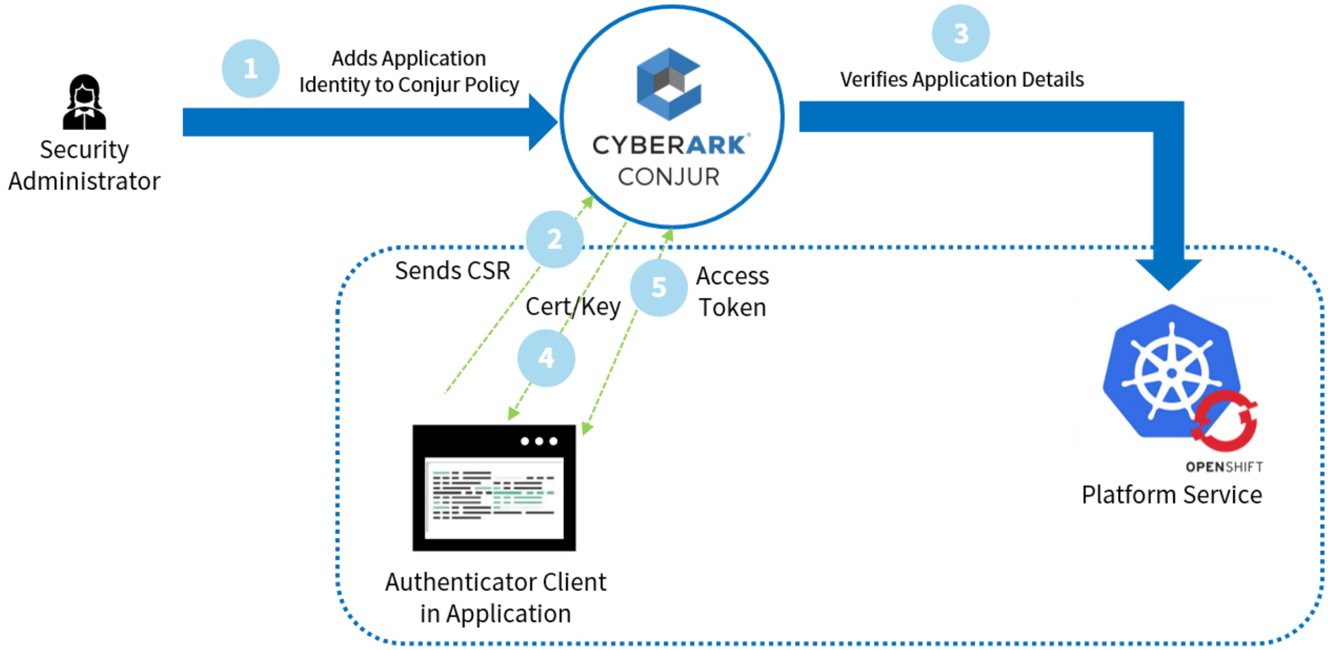
Securing Containerized and Cloud Apps

ESG validated how CyberArk provides centralized security for containerized and DevOps environments and helps organizations efficiently secure, rotate, audit, and manage secrets and other credentials at scale, based on policy.

ESG Testing

As with traditional applications, CyberArk Conjur can utilize multiple methodologies to return secrets to containerized applications. All must start at the same place: authentication. Figure 7 is a high-level representation of the authentication process. First, a policy is created in Conjur that defines the application identity. The granularity of identifying markers is flexible; either Cluster/Namespace or Cluster/Namespace/Service Account can be used.

Figure 7. Authenticating a Kubernetes Application in OpenShift



Security Administrator
1
Adds Application Identity to Conjur Policy
CYBERARK CONJUR
3
Verifies Application Details
2
Sends CSR
Cert/Key
4
5
Access Token
Authenticator Client in Application
OPENSHIFT
Platform Service

Source: ESG, a division of TechTarget, Inc.

[3] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021.

To authenticate, an application submits a certificate signing request (CSR) with its identifying markers to Conjur. Next, Conjur verifies those attributes with the platform service using the Kubernetes API. Once verified, the Conjur instance performs another identity verification, creating a mutual encrypted TLS link between itself and the CyberArk Authenticator Client. This ensures a one-to-one relationship between Conjur and the Authenticator Client. When Conjur sends the signed Certificate and Key that was generated in step two, the Authenticator Client uses the key to generate an access token. At this point, the developer has a range of options as to how they want to retrieve the credential. The access token expires in eight minutes, so the Authenticator Client re-authenticates every six minutes.

It's important to note that, while this looks like a lot of steps and takes a lot of explaining, when ESG tested this process in a resource-constrained test environment, it took approximately two milliseconds to complete.

ESG also walked through app authentication in AWS, Azure, and Google Cloud Platform. In every case, Conjur utilizes tools the platform provides to establish trust with an identity and then authenticate that identity. In AWS, an IAM authenticator is used, so anywhere that a role is applied in AWS, the authenticator can be used. Azure utilizes its Instance Metadata Service (IMDS) and JSON Web Tokens to authenticate and retrieve secrets. Similarly, GCP uses JSON Web Tokens.

Why This Matters

Integration of cloud-native security controls into the software development lifecycle and continuous integration and continuous delivery (CI/CD) tools is one of the top security controls priorities reported to ESG in recent research.[4]

ESG validated that that CyberArk Conjur Secrets Manager makes it easy for application development teams to securely provide cloud-native and containerized applications with the secrets and credentials needed to access sensitive resources, integrating with common tools that are already integrated into organizations' workflows. This enables organizations to use DevOps methodologies, containerize applications, and increase business agility—without compromising security and without slowing the pace of innovation.

The Bigger Truth

Improving cybersecurity is among the most important considerations for justifying IT investments in 2022. In addition, strengthening cybersecurity and/or improving operational resiliency against cyber-attacks are business initiatives that organizations believe will drive the most technology spending at their organizations over the next 12 months. Integration of security with the software development lifecycle and continuous integration and continuous delivery (CI/CD) tools is a top priority, but not at the cost of slowing down development efforts.[5]

CyberArk Conjur Secrets Manager securely vaults the secrets and credentials used by a broad range of application types in hybrid cloud, cloud-native, and containerized environments. Secrets Manager comprises Conjur Secrets Manager Enterprise (and Open Source) and the Credential Providers. CyberArk secures applications and other non-human identities in a way that doesn't get in the way of developers.

ESG validated through hands-on demos and testing that Conjur Secrets Manager enables organizations to secure applications interacting with one another at a privileged level, on-premises, in the cloud, and in containers. Secrets Manager can leverage automation to vault and control access to secrets at scale and reduce friction among developers, administrators, and security teams.

[4] Source: ESG Survey Results, *The Maturation of Cloud-native Security: Securing Modern Apps and Infrastructure*, June 2021.
[5] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021.

The results that are presented in this document are based on testing in controlled environments. Due to the many variables in each organization's ecosystem, it is important to perform planning and testing in your own environment to validate the viability and efficacy of any solution.

If your organization is looking to streamline and optimize security in your DevOps workflows and eliminate the risk of hard coding credentials and secrets into apps and other non-human entities, whether on-premises, in a hybrid or multi-cloud environment, or for containerized apps, ESG believes that you should take a serious look at CyberArk and Conjur Secrets Manager.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

The goal of ESG Validation reports is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Validation reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

a division of TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.