CYBERARK®

EBOOK

# The New CISO Mandate: Securing All Application Secrets

## Leveraging the CyberArk Blueprint

# Table of Contents

# Introduction

## So Many Applications….

Today's businesses are powered by a wide variety of applications, from traditional software solutions hosted in corporate data centers to modern applications running in the cloud. The diverse application landscape includes:

- **Static applications** – conventional applications hosted on physical or virtual machines, and legacy mainframe applications
- **Cloud-native applications** – contemporary, dynamic and ephemeral applications leveraging containers, serverless compute functions, and microservices architectures
- **Internally developed applications** – homegrown static or cloud-native applications used for internal or customer-facing purposes
- **Commercial off-the-shelf (COTS) software** – third-party software products like business intelligence solutions, RPA tools, vulnerability scanners, etc. that can be hosted internally or consumed as SaaS solutions
- **Application servers** – web application servers like WebLogic, WebSphere, Tomcat, and JBoss hosting Java EE apps
- **Agile software development and delivery tools** – CI/CD automation platforms, configuration management tools and service orchestration solutions, etc.

## The New CISO Mandate: Secure All Applications Secrets, Everywhere

In 2020 and 2021 the SolarWinds digital supply chain attack, CodeCov and other incidents have made enterprise executives increasingly aware of the critical need to secure secrets in applications and application development environments. The consequences of failing to secure apps and CI/CD pipelines are clearer than ever and potentially devastating. In May 2021, the Biden administration issued an **executive order** to improve the nation's cyber security, including enhancing software supply chain security (Section 4). So, it's not surprising that increasingly, executives are asking their security teams to secure all application secrets – everywhere across their entire organization. A potentially daunting task.

Where do security teams begin? This eBook outlines a customer tested systematic approach and blueprint for organizations to take to enhance the security of their application portfolios. It leverages CyberArk's holistic blueprint and methodology for securing the credentials used by both human users as well as applications and other non-human identities.

## …. So Many Security Challenges

Heterogenous IT environments are notoriously complicated to secure. Most applications rely on secrets (passwords, SSH keys, API keys, etc.) to access IT systems and encrypt transactions. But each type of application is typically protected by a distinct security model using distinct security tools. A containerized application running on AWS, for example, is secured differently than a legacy zOS application running on a mainframe computer in a corporate data center.

Disjointed security systems and practices, and manually intensive, error-prone administrative processes can introduce security gaps and blind spots, opening the door for adversaries to launch attacks and steal data. By taking a holistic approach to security—securing all your application secrets, everywhere, using common secrets management tools and uniform security practices—you can reduce security vulnerabilities, improve visibility, and mitigate risk.

# Where to Begin?

Implementing a uniform secrets management program can be a daunting proposition. You have to secure a wide variety of applications that are developed and maintained by different teams using different tools and are hosted in different locations using various deployment models (on-prem, private cloud, public cloud, hybrid cloud, multi-cloud). Some applications are more critical to the business than others. Some applications are more mature and more difficult to adapt than others. And each application poses a unique set of risks.

Few security teams have the time, resources, and budget to take on all these challenges at once, by themselves. So where do you begin? How do you identify and mitigate the greatest potential threats as quickly as possible? This is where CyberArk has answers and can help.

We've developed a comprehensive blueprint to help organizations assess and prioritize vulnerabilities, strengthen identity security, and reduce risks. The CyberArk **Blueprint for Identity Security Success** lays out a prescriptive, risk-aligned approach for establishing and maintaining an effective identity security strategy—including a robust, unified secrets management program for your entire application portfolio.

# CyberArk Blueprint for Identity Security Success

| | GOAL | IDENTITY SECURITY CONTROL FAMILIES & TECHNOLOGIES | | | |
|---|---|---|---|---|---|
| | | Access | Least Privilege | Privileged Access | **Secrets Management** |
| **STAGE 1** | Secure highest privilege identities that have the potential to control an entire environment | Adaptive MFA &Cloud Admins | Cloud Admins& Shadow Admins | Cloud Admins,Domain Admins, Hypervisor Admin &Windows Local Admins | **3rd Party Security Tools(via C³ Alliance) &Domain Admin Services** |
| **STAGE 2** | Focus on locking down the most universal technology platforms | PaaS Admins,Cloud Privileged Entities& CI/CD Console Admins | Cloud Privileged Entities | Workstation Local Admins,Privileged AD Users &*NIX Root + SSH Keys | **3rd Party Business Tools & Application Servers(via C³ Alliance)** |
| **STAGE 3** | Build identity security into the fabric of enterprise strategy and application pipelines | Web Applications(Mission Critical) | IT Admin Workstations | *NIX Root (Similar),Out of Band Access &Database Built-In Admins | **CI/CD Toolchain Pipeline & Dynamic Applications (Containers & Microservices)** |
| **STAGE 4** | Mature existing controls and expand into advanced identity security controls | Web Applications(Core) | Workforce Workstations& Windows Servers | Network & Infra. Admins,Database Named Admins,Client-Based Apps(Mission Critical) | **Static Applications (Homegrown Legacy& OS-based)** |
| **STAGE 5** | Look for new opportunities to shore up identity security across the enterprise | Web Applications(All) | *NIX Servers | Mainframe Administrators& Client-Based Apps (All) | **Windows Services(Embedded Usages)** |

CyberArk Identity Security Blueprint Overview

The CyberArk Blueprint is designed to help organizations defend against the techniques adversaries most often use to penetrate systems, traverse networks, steal data, and wreak havoc. It is based on three guiding principles:

1. Prevent credential theft.
2. Stop lateral and vertical movement.
3. Limit privilege escalation and abuse.

The Blueprint lays out a pragmatic, risk-based strategy that introduces security controls in stages, helping businesses address their most pressing needs in the short-term, while providing a long-term plan to take on more advanced use cases. The Blueprint helps address all aspects of identity security including secrets management. By following the Blueprint and other recommendations, you can secure all your application secrets. The approach helps you mitigate security vulnerabilities, increase visibility and reduce risk.

# Stage 1 – Third-Party Security Tools and Domain Admin Services

## Secure highest privileged identities that have the potential to control an entire environment

Stage 1 of the Blueprint helps you address your most glaring security vulnerabilities as quickly as possible—the low-hanging fruit. The goal is to secure any non-human identity that has the privileges to control your entire environment(s). In terms of secrets managements, third-party security tools such as vulnerability scanners are low-effort, high-reward opportunities and perfect Stage 1 candidates.

You can also remove domain admin privileges from Windows Service accounts for a quick, easy win. Windows Service accounts are common targets for attackers. As a first step, you can reduce risk by simply moving those Windows Service accounts to a non-domain admin group within Active Directory (we'll look to expand the scope of Windows Service accounts in Stage 5).

Note, for the services left with domain admin permissions, it should be an immediate priority to manage those service usages.

THIRD PARTY SECURITY TOOLS

## The Challenge

Third-party security applications typically require the highest level of privileged access to a variety of IT systems to run scans and interrogate software for vulnerabilities. Privileged account credentials are often hard-coded into these security tools and left unmanaged.

Additionally, out of expediency, Windows Services are often given domain admin privileges, rather than the appropriate level of permission required – and those services use local hashes for authentication and are also left unmanaged. External attackers or malicious insiders can exploit unmanaged credentials to gain unauthorized access to IT systems, traverse networks, and potentially execute an entire network takeover.

## The Solution/CyberArk Product Capabilities

CyberArk offers integrations with a variety of commercial off-the-shelf security solutions from providers like Qualys, Tenable, and Rapid7 through the **CyberArk C³ Alliance Program**. C³ Alliance **integrations** make it easy to extend the benefits of CyberArk secrets management solutions to third-party applications. You can remove hard-coded credentials from these security tools, securely store them with CyberArk, deliver them to authorized applications on-demand, and rotate them automatically based on security policies.

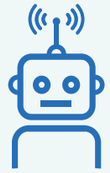
# Stage 2 – Third-Party Business Tools and Application Servers

## Focus on locking down the most prevalent technology platforms

Stage 2 of the Blueprint helps you achieve some additional quick wins through C3 Alliance integrations with third-party business tools and web application servers.

## The Challenge

Third-party business applications like Robotic Process Automation (RPA) solutions and business intelligence platforms require privileged access to various IT systems and datastores. And the same goes for popular J2EE application servers. Just like with third-party security tools, privileged account credentials are often hard-coded into these business tools and web application servers, and left unmanaged. Savvy threat actors—internal and external—can exploit compromised privileged account credentials to breach networks, steal data, and carry out attacks.



RPA

UiPath

blueprism
Robotic Process Automation Software

AUTOMATION ANYWHERE

AUTOMATION AND BUSINESS TOOLS

SailPoint

servicenow

APPLICATION SERVERS

ORACLE

JBoss by Red Hat

IBM WebSphere

## The Solution/CyberArk Product Capabilities

CyberArk offers C3 Alliance integrations for RPA solutions like UiPath, Blue Prism, and Automation Anywhere; for business intelligence platforms like Informatica; and for automation tools such as Red Hat Ansible as well as for **many other business tools**. Those same integrations are also available for java-based web application servers like WebLogic,

WebSphere, Tomcat, and JBoss. The integrations make it easy to rotate and replace hard-coded privileged access credentials from third-party business tools and web application servers. You can safely store secrets in the tamper resistant CyberArk Privileged Access Manager, rotate them automatically based on policy, and deliver them to authorized applications on-demand.

# Stage 3 – CI/CD Toolchain Pipeline & Dynamic Applications

## Build identity security into the fabric of the enterprise strategy and application pipelines

Stage 3 of the Blueprint improves the security of CI/CD pipelines, other DevOps tools, as well as software development and delivery environments for dynamic applications. Organizations are increasingly adopting DevOps methodologies and microservices architectures, and implementing containerized and serverless compute applications. It makes sense to take on these tools and apps first, before turning your attention to legacy applications that will likely take more time and effort to modify and test.

## The Challenge

DevOps teams rely on a diverse collection of CI/CD automation platforms, configuration management tools, internal and external code repositories as well as service orchestration solutions to build and deploy applications. Automation tools require privileged access to IT systems to configure resources and provision services. Developers and operations teams often hard-code privileged access credentials into automation scripts and playbooks, opening the door for malicious attackers.

CI/CD TOOLS

Jenkins

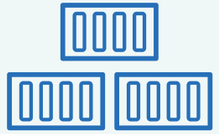
Azure DevOps

puppet

Terraform

aqua

RED HAT ANSIBLE



CONTAINER PLATFORMS

kubernetes

RED HAT OPENSHIFT

VMware Tanzu

Most businesses take a phased approach to improving the security of homegrown applications, tackling different apps over time. See Prioritizing Internally Developed Applications for tips on building out a secrets management roadmap that aligns with your company's priorities.

Modern dynamic applications—short-lived apps running in containers, as serverless compute functions or on auto-scale VMs—also need privileged access to various IT systems and datastores. And just like with CI/CD tools, developers often hard-code secrets into dynamic applications opening the door for adversaries. To make matters worse, developers often store their code on internal repositories or public repositories like GitHub, making the attacker's job even easier.

## The Solution/CyberArk Product Capabilities

Conjur Secrets Manager from CyberArk helps you improve security by removing secrets from dynamic applications and automation scripts. With Conjur you can secure and rotate secrets used by automation scripts and dynamic applications. When an application requests access to a resource, Conjur authenticates and authorizes the application, and securely distributesthe secret.

CyberArk offers C3 Alliance integrations for popular CI/CD tools, configuration management platforms, and service orchestrators including Ansible, Jenkins, Puppet, Terraform, Kubernetes, Red Hat OpenShift, VMware Tanzu, and Cloud Foundry.

# Stage 4 – Static Applications

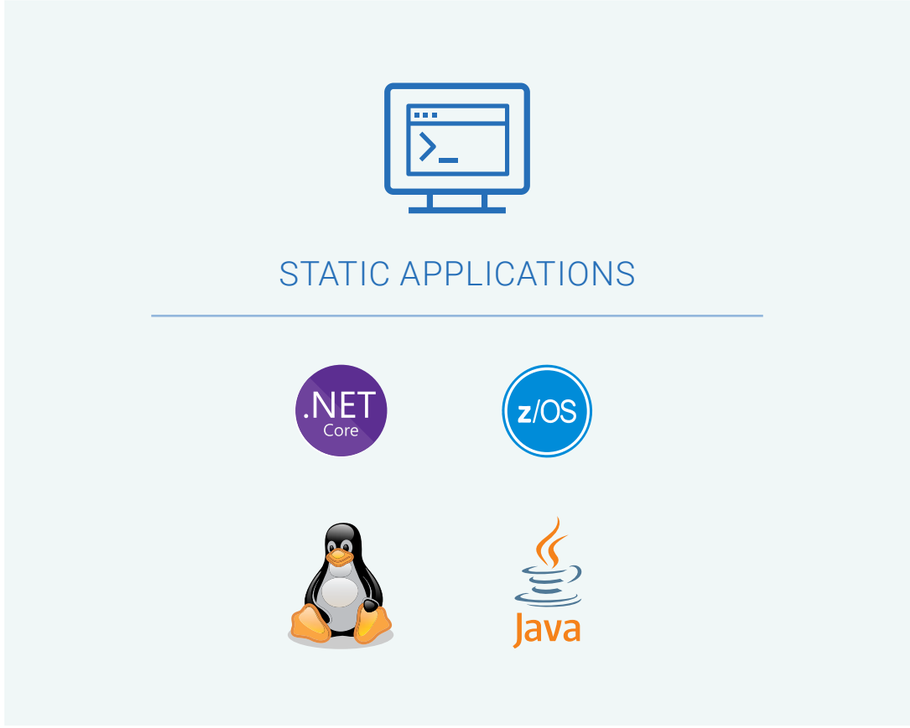
## Mature existing controls and expand into advanced identity security controls

Stage 4 of the Blueprint shores up the security of legacy applications and scripts running on physical or virtualized servers. Most businesses still leverage a variety of internally

developed applications hosted in corporate datacenters or in the cloud. Modifying these aging homegrown applications can be a labor-intensive, time-consuming proposition. They are often poorly documented, not well understood, and fragile. In many cases the developers or contractors originally responsible for the application are long gone. For all these reasons it is best to tackle these apps after you've taken care of third-party software solutions and newer cloud-native apps.

## The Challenge

Legacy, static applications require privileged access to various IT systems and datastores. And just like with dynamic, cloud-native apps, developers often hard-coded secrets into these applications, providing an opening for malicious attackers and cyberthieves. These legacy applications commonly have overprivileged permissions, a remnant of a time where some developers requested any and all permissions rather than figuring out the appropriate access rights.



Most businesses take a phased approach to improving the security of homegrown applications, tackling different apps over time. See **Prioritizing Internally Developed Applications** for tips on building out a secrets management roadmap that aligns with your company's priorities.

## The Solution/CyberArk Product Capabilities

CyberArk Secrets Manager helps you strengthen security by eliminating hard-coded credentials from static, internally developed applications and scripts. With Secrets Manager you can safely store secrets in CyberArk Privileged Access Manager, rotate them automatically based on policy, and deliver them to authorized applications on-demand. The solution supports a variety of traditional application environments and operating systems including Unix/Linux, Windows, and zOS.

# Stage 5 – Windows Services (Embedded Usages)

## Look for new opportunities to shore up identity security across the enterprise

Stage 5 of the Blueprint takes on the more challenging use cases like fully securing Windows Service accounts.

## The Challenge

Windows Service accounts are non-human privileged accounts used to launch embedded Operating System usages and automated services. Unlike regular software that is launched by the end-user and only runs when the user is logged on, Windows Services can start without user intervention and can be used to launch a variety of tasks, creating unique security challenges. These Windows Services typically leverage credential hashes to authenticate and those hashes are stored locally on the filesystem. Windows Service accounts can be used for many usages, including standard OS Services, scheduled tasks, COM objects, Internet Information Services (IIS) app pools, etc., and reside on on-premises servers as well as cloud-based infrastructure (AWS EC2, Azure VMs, etc.). Windows Service accounts are difficult to manage, are often overlooked by IT, and are a common target for malicious attackers.

## The Solution/CyberArk Product Capabilities

In Stage 1 we focused on securing domain admin privileged Windows Services as a simple first step. In Stage 5 we shore up Windows Service account security by using CyberArk Privileged Access Manager to vault Windows Service accounts credentials, create complex and unique credentials for each account, and automatically rotate at regular intervals (at least every 90 days).

# Priortizing Internally Developed Applications

## Choosing the right approach for your business

The Blueprint is intended to serve as a prescriptive guide to help you map out your identity security strategy. It is not a roadmap or an implementation plan in and of itself. There are other factors you must take into consideration to develop an application security plan that meets the specific needs of your organization.

Most businesses are fueled by dozens or even hundreds of internally developed applications. When building out your secrets management roadmap, you'll need to figure out which applications to tackle, in which order. There are many different ways to prioritize applications.

You can rank applications based on perceived business risk, based on vulnerabilities discovered during red team exercises, or in response to known breaches and security incidents. You can also take into account compliance risks and audit findings, prioritize pet projects for executives, or factor in other internal priorities.

There is no right way or wrong way to go about this. Pick the approach that works best for your business.


## Making your Roadmap a Reality

Once you've identified and prioritized the applications you want to secure, you'll need to figure out the best way to achieve your plan. If you work in a security-oriented organization and have the CISO's support, you may be able to take a "top-down" approach and mandate the changes.

On the other hand, if you work in an organization that is less security-conscious, you may need to become more of an evangelist, and take a "bottom-up" approach. You can build grassroots support by educating development teams about privileged access security risks and making it easy for developers to secure secrets.

## Blueprint Toolkit

Use CyberArk's Blueprint Toolkit to lay out your own secrets management roadmap based on the guiding principles of The CyberArk Blueprint for Identity Security Success. The toolkit includes instructional videos and self-guided templates to help you define a staged identity security program, including a phased secrets management plan, tailored to your specific operating environment, application landscape, and business requirements.

# Getting Started

Developing a comprehensive secrets management plan and roadmap takes time and expertise. As every customer's journey is unique, CyberArk offers customers a range of Blueprint planning tools and services from do-it-yourself toolkits and guides, to support from our professional services teams and partners. The goal to help you simplify the process, save time and effort, and leverage CyberArk's expertise and IP, so that you can most effectively secure your organizations applications.

## Accelerate Your Success with CyberArk Getting Started Packages

CyberArk can help you accelerate your secrets management journey with Getting Started packages for securing commercial-off-the shelf software solutions, legacy home-grown applications, and cloud-native applications and CI/CD pipelines. Depending on the package selected, our professional Security Services team will review your solution

architecture, help you build out your secrets management infrastructure, and address various use cases—all in accordance with the CyberArk Blueprint. We offer a variety of Getting Started packages to address a range of operating environments and customer requirements.

## CyberArk Secrets Management Solutions

CyberArk's secrets management solutions are designed to let you secure all your application secrets using common tools and practices, and the same CyberArk Privileged Access Manager you use to manage human privileged access credentials.

Conjur Secrets Manager Enterprise is a feature-rich secrets management solution tailored to the unique infrastructure requirements of cloud- native, container, and DevOps environments. The solution lets you secure, rotate, audit, and manage secrets and other credentials used by dynamic applications, automation scripts, and other non-human identities. Conjur Enterprise is an enterprise-class solution, backed by CyberArk's world-class support and services organization. An open-source version is available as Conjur Secrets Manager Open Source at www.conjur.org.

The Credential Providers, as part of CyberArk Secrets Manager provide a comprehensive secrets management solution for traditional static applications. The solution lets you secure, rotate, audit, and manage secrets and other credentials used by legacy applications running on a variety of operating systems including Unix/Linux, Windows, and zOS.

Conjur Enterprise and CyberArk Secrets Manager are part of CyberArk's Identity Security Platform and both integrate with CyberArk Privileged Access Manager, including Privilege Cloud, which is offered as SaaS. The end-to-end solution lets you manage credentials used by applications and people in a consistent manner, using a single set of tools across datacenters and clouds.

**Explore CyberArk solutions for securing applications of all types:**

***Securing All App Types*** ***Securing COTS and Static Apps*** ***Securing RPA and Bots*** ***Securing CI/CD Pipelines and Cloud Native Apps***

# Next Steps

A unified secrets management strategy is designed to help reduce security vulnerabilities and mitigate risk across applications and development environments. CyberArk can help you secure all your application secrets using the CyberArk Identity Security Platform. By using CyberArk Secrets Manager and the CyberArk Identity Security Platform organizations can centrally manage the credentials used by virtually all application types across the entire enterprise as well as manage human privileged access credentials – consistently and according to policy.

Leverage the available resources to develop and implement plans to improve the security of the secrets used by applications to access your organization's resources.

- Visit the **CyberArk Blueprint for Identity Security Success** to learn more.
- Read the **CyberArk Blueprint for Identity Security Success Whitepaper** to dive into the details.
- Download the **Blueprint Toolkit** to develop your own secrets management roadmap.
- Visit the **CyberArk Marketplace** to explore CyberArk integrations.
- Contact your account team or **sales@cyberark.com** to learn about Getting Started packages.

CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blogs or follow us on Twitter via @CyberArk, LinkedIn or Facebook.


U.S., 03.22 Doc: TSK-902 (WRQ-266)

CYBERARK®