DevSecOps

Securing Cloud-Native Apps and CI/CD Pipelines at Scale

Increase Business Agility, Improve Developer Productivity, Reduce Risk

Introduction

Enterprises are adopting DevOps practices and leveraging continuous integration and deployment (CI/CD) processes to increase the pace of innovation and accelerate their digital transformation. But disjointed security systems and practices can slow down CI/CD pipelines, delay applications from going into production, frustrate developers, and lead to risky workarounds. Developers too often hard-code credentials into applications or take other shortcuts, exposing the business to costly data breaches and crippling cyberattacks. Forward-looking organizations are shifting security left in the software development lifecycle to engage development teams earlier, and improve coordination and collaboration. And they are using secrets management solutions to increase automation, reduce vulnerabilities, and accelerate application delivery.

This whitepaper examines DevOps security challenges and outlines how new DevSecOps practices and tools help organizations strengthen security without impairing business agility.

pwc | CYBERARK®

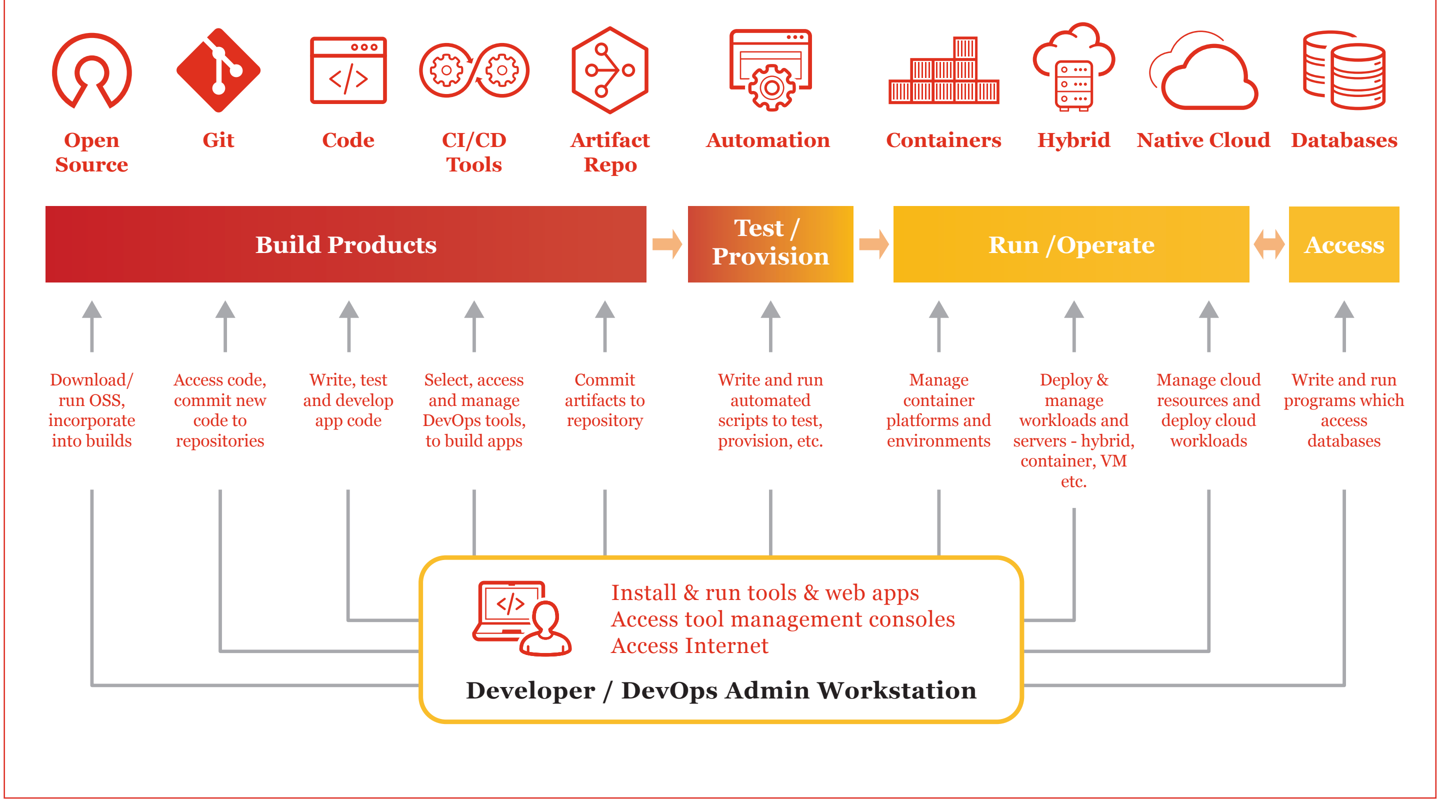
DevOps Security Challenges

DevOps can help accelerate business performance, but the dynamic nature and the sheer scale and diversity of the DevOps ecosystem can make it inherently difficult to secure. The DevOps ecosystem includes:

- A diverse collection of configuration management tools, CI/CD automation platforms, build tools, code repositories, and service orchestration solutions used to streamline development and deployment.
- A variety of hybrid compute and storage resources used to version-control, build, test, maintain, and run code across development and production environments.
- A range of technical professionals—developers, cloud architects, QA engineers, DevOps and system administrators, operations managers—each with distinct roles and privileges.

Table of Contents

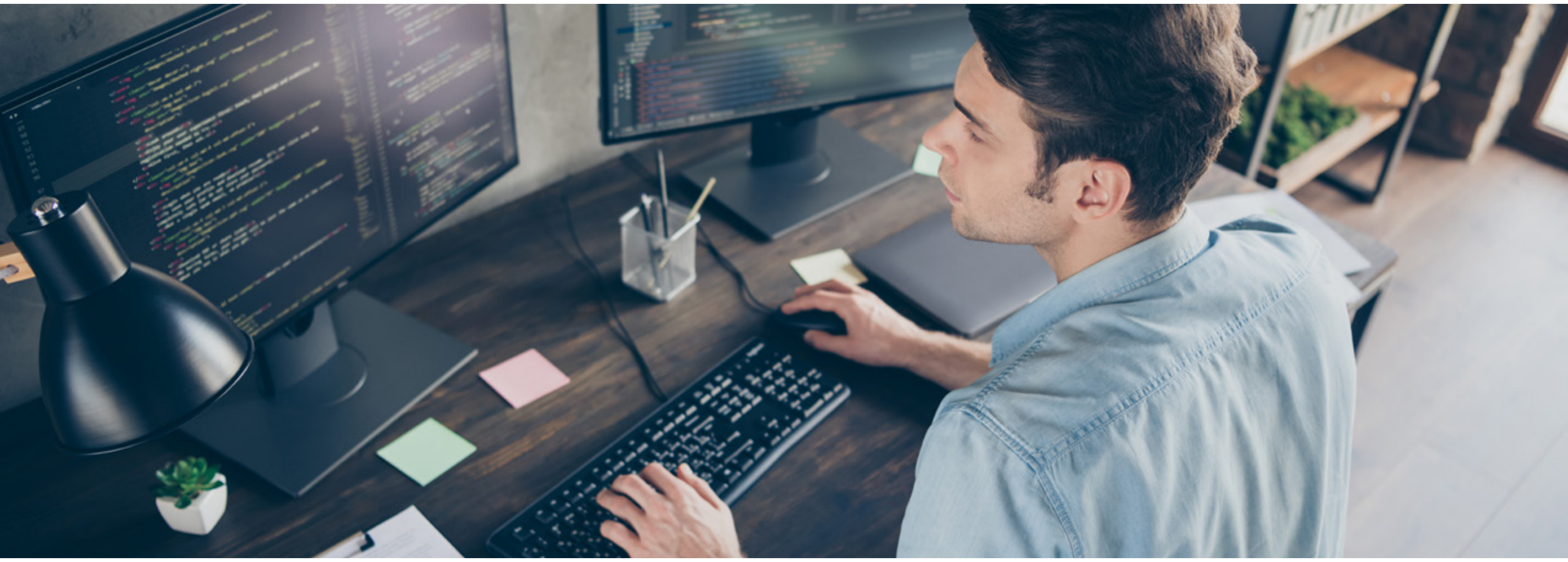
The DevOps Ecosystem Includes Diverse Tools and Resources


Open Source
Git
Code
CI/CD Tools
Artifact Repo
Automation
Containers
Hybrid
Native Cloud
Databases
Build Products
Test / Provision
Run /Operate
Access
Download/ run OSS, incorporate into builds
Access code, commit new code to repositories
Write, test and develop app code
Select, access and manage DevOps tools, to build apps
Commit artifacts to repository
Write and run automated scripts to test, provision, etc.
Manage container platforms and environments
Deploy & manage workloads and servers - hybrid, container, VM etc.
Manage cloud resources and deploy cloud workloads
Write and run programs which access databases
Install & run tools & web apps
Access tool management consoles
Access Internet
Developer / DevOps Admin Workstation

Securing CI/CD pipelines across the enterprise is a complex proposition. Consider the following challenges:

- The development process is dynamic and highly automated. Each development and test tool, configuration management platform, and service orchestration solution has its own security credentials. Fragmented islands of security can lead to security gaps, secrets sprawl and administrative complexity.
- Applications are decomposed into distinct code elements and microservices, which are independently managed and updated, creating additional administrative complexity.
- The secrets, (passwords, SSH keys, API keys) applications and microservices use to access systems and encrypt transactions are often scattered across machines and clouds, making them nearly impossible to consistently track and manage.
- And to make matters worse, developers often hard-code secrets into executables, stored in code repositories. Repositories are sometimes inadvertently configured as public, making secrets easy prey for hackers and cybercriminals, exposing the business to malicious attacks, code injection, loss of confidential data and hijacked resources.

Organizations must take a systematic and deliberative approach to DevOps security to overcome these complex challenges.



Negative Consequences

Businesses that don't take a proactive approach to securing credentials used by applications and the DevOps pipeline can suffer catastrophic consequences. Adversaries can use exposed DevOps credentials to penetrate infrastructure and wreak havoc. Security breaches can disrupt business, damage a company's reputation, and lead to data leakage, revenue loss, and costly regulatory penalties.

In addition, fragmented security systems and practices can impair developer productivity, impede the pace of development, and introduce unnecessary risk and uncertainty. Manually intensive secrets management processes are more likely to be error prone and can slow down application delivery, hamper compliance monitoring and reporting, and expose application credentials to attackers.

DevOps Requires More Scalable and Agile Security Methodologies

Conventional security systems and practices, conceived to secure traditional enterprise applications and development methodologies, aren't well suited for the dynamic world of DevOps, containers, and microservices. Forward-thinking organizations are turning to a new generation of secrets management solutions to improve the security of today's highly diverse and dynamic IT environments.

Automated secrets management solutions let development, operations, and security teams efficiently control and manage the credentials used by a variety of applications and processes (commercial and internally developed apps, development tools, CI/CD automation scripts) across a variety of systems (development, build, test, production) and deployment models (cloud, hybrid, multi-cloud).

Secrets management solutions help organizations produce higher quality, lower-risk code, more quickly and cost-effectively, by making it easier for developers to secure the credentials applications use to access sensitive resources. And they reduce vulnerabilities and inefficiencies by eliminating security islands and by automating security operations.

Organizations can use secrets management solutions to remove hard-coded credentials from applications and scripts, and to centralize credential storage and administration. Secrets can be stored in a central vault for effective control and manageability. And they can be rotated automatically based on policy—without modifying code, restarting applications or disrupting business-critical services.

Ideally, secrets are centrally managed to consistently secure the DevOps environments used by development teams across the entire organizations, not just for an individual project team.

Secrets Management Solutions Strengthen Security and Simplify Operations

- *Eliminate Security Islands*
- *Automatically Rotate Secrets*
- *Reduce Attack Surfaces*
- *Avoid Service Disruptions*
- *Control and Monitor Access*
- *Improve Compliance*

Avoid the Secret Zero Problem

Beware of secrets management solutions that rely on a master key to secure credentials stored in the vault. Master keys open the door to your entire digital infrastructure, and are an irresistible target for bad actors.

Look for a secrets management solution that avoids the "secret zero" problem by using multi-factor authentication to confirm machine, container, and application identities. Best-of-breed secrets management solutions use native characteristics and multiple attributes (IP address ranges, randomly generated UUIDS, roles, names etc.) to validate identities and establish trust.

DevOps Requires a New Security Mindset

Many organizations are introducing secrets management solutions in conjunction with new DevSecOps practices. DevOps requires an entirely new security mindset. Many software development organizations are hampered by siloed organizational structures and disjointed project planning processes. Security is typically the responsibility of a distinct organization with distinct business objectives.

Unfortunately, too often, the Security team becomes engaged late in the development cycle after a project team has already made critical security decisions without understanding the broader implications. For example, with automated CI/CD processes, configuration (and security) decisions are made early in the development process, yet security may not be fully engaged with the development team until development is well underway, sometimes even as late as when code is scheduled for production. Programs are then delayed while security capabilities are bolted on, midstream. This is costly and frustrating for the business, developers, and the security team, and sometimes projects are put on hold altogether until security issues are resolved.

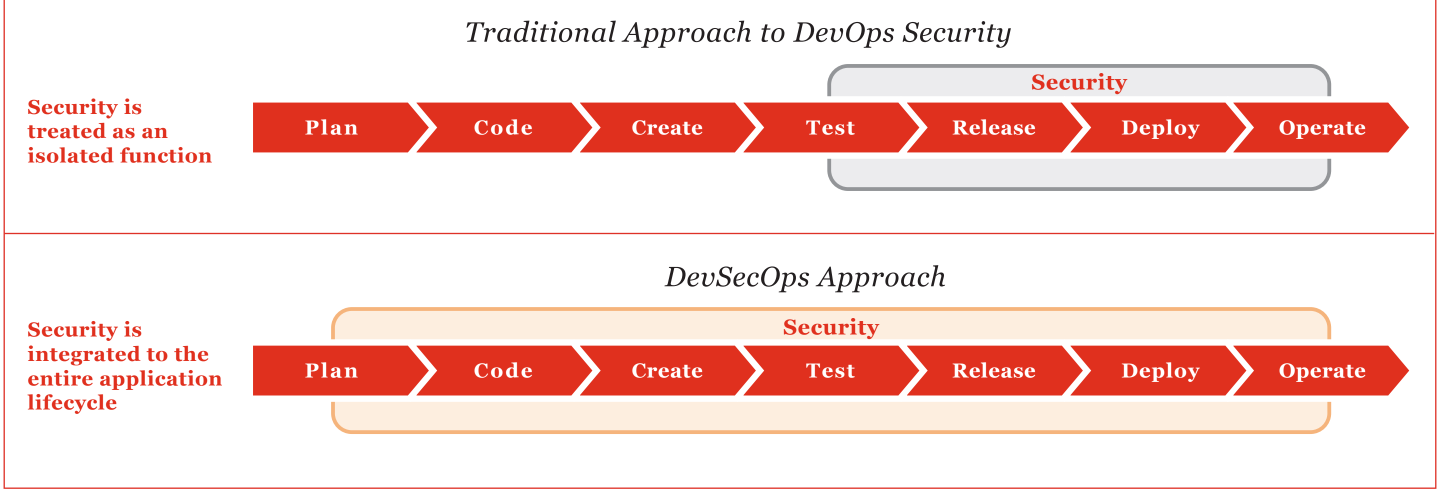
There's a natural tension between development teams, who are under pressure to get new applications to market as quickly as possible, and security teams whose mission is to protect the business, safeguard critical systems, and secure confidential data. DevSecOps practices can break down cultural barriers by factoring security into every phase of the software development and delivery lifecycle.

With DevSecOps, development, test, security, and operations professionals work together, collaborating throughout the entire application lifecycle, from inception through deployment. By shifting security left and working with developers earlier in the development process, security capabilities and threat analysis functionality can be embedded into DevOps workflows to reduce vulnerabilities. When security "shifts left" developers can avoid rework and delays later in the lifecycle. By making it easy for developers to secure their apps Security teams can reduce objections, increase adoption and accelerate development cycles.

DevSecOps Benefits

- Identify code vulnerabilities early
- Avoid rework and schedule delays
- Free up developers to focus on innovation
- Improve productivity and agility

DevSecOps Integrates Security into the DevOps Chain


Traditional Approach to DevOps Security
Security is treated as an isolated function
Security
Plan
Code
Create
Test
Release
Deploy
Operate
DevSecOps Approach
Security is integrated to the entire application lifecycle
Security
Plan
Code
Create
Test
Release
Deploy
Operate

Cyberark Secrets Manager: Secrets Management at the Speed of Devops

CyberArk Secrets Manager lets organizations centrally secure and manage secrets and credentials used by the broadest range of applications, including COTS, RPA, automation platforms and CI/CD tools, running in hybrid, cloud-native and containerized environments. Mission-critical applications running at scale can securely access high-value resources, including databases and IT infrastructure, to improve business agility while reducing operational complexity.

CyberArk Conjur Secrets Manager Enterprise, part of the CyberArk Secrets Manager offering, is a secrets management solution for securing cloud-native applications, CI/CD pipelines and DevOps tool chains. Conjur Enterprise is specifically architected to centrally manage secrets and credentials used in containerized environments and can be deployed at massive scale to secure DevOps environments across the enterprise. The solution integrates seamlessly with widely used DevOps tools and platforms. It also integrates with existing identity security platforms to help organizations extend established security models and practices.

Moving from DevOps to DevSecOps with PwC

Understanding Business Agility, DevOps and DevSecOps

Business Agility

... is the ability of an organization to **sense, adapt, innovate, and change** to market and environment conditions in productive, cost effective ways

... focuses on **re-engineering the entirety of the business,** including:

- Business Strategy
- Governance and Leadership
- Team Structures and Operating Models
- Ways of Working
- Culture, Mindsets, and Behaviors

Better

DevOps

... is the ability of cultural philosophies, practices, and tools that increases an organization's ability to deliver applications and services at **high velocity;** evolving and improving products at a **faster pace than organizations using traditional software development** and infrastructure management processes.

...focuses on **transforming the technology** and infrastructure, specifically:

• **Rapid Development Cycles** with high frequency delivery

• **Elastic and scalable service**s through modernized cloud infrastructure

• **Accelerating the time-to-market** of digital products

Faster

DevSecOps

... is the **integration of security capabilities into DevOps** to create a "Security First" culture with shared accountability and flexible collaboration between developers, release engineers, and security teams.

...focuses on **making security an enabler** of DevOps and Business Agility by:

• **Changing cultural mindsets and behaviors** between DevOps and Security teams

• Reducing security friction and **providing a secure infrastructure** for a DevOps innitiative

• **Automating security services** so that DevOps teams dictate speed of delivery

Safer

PwC strongly believes delivery teams must build security into their development and operations practices to proactively identify and manage threats and code vulnerabilities. By shifting security left in the development process, organizations can accelerate the pace of innovation and reduce risk.

We provide the strategy through execution for organizations to help them successfully integrate security into DevOps deployment methodologies, serving as a trusted advisor to help accelerate transformation. PwC helps clients combine transformative organization design methodologies with secure development drivers to create a security-driven culture that unleashes business innovation.

Our deep cybersecurity experience enables us to effectively advise and assist in a successful transformation where security is fused into Agile delivery and modern technology platforms. PwC can help you develop a delivery model where security is organically integrated into business and development lifecycles, transforming security from an organizational tax into a competitive advantage.

Our team of experienced DevSecOps practitioners and business advisors can help you:

- Assess your current development environments and implications for the software supply chain.
- Formulate a detailed DevSecOps strategy for the entire enterprise, not just for individual projects.
- Conduct a thorough DevSecOps evaluation and proof of concept.
- Introduce effective DevSecOps practices, for development teams and across the organization.
- Integrate security into your development processes and underlying environments.

Overcome Complex DevSecOps Challenges with PwC

Standardize security architecture and product design

Accelerate the delivery of security at the scale and pace of business and DevOps

Automate the registration of risk, application of controls, testing of security requirements

Visualize across infrastructure, platforms, and applications to drive prioritized remediation actions

Embed security capabilities throughout business and development lifecycles

Build a security-driven culture that guides decisions

PwC And CyberArk Secrets Manager in Action

PwC helped a global corporation strengthen the security of its containerized applications with Conjur Enterprise Secrets Manager. The CyberArk solution helps the company reduce attack surfaces, mitigate risk and simplify operations by providing a common, automated framework for managing secrets used by various configuration management tools, CI/CD automation tools and container infrastructure.

PwC helped the company accelerate time-to-value by deploying, integrating and validating the CyberArk solution in two production environments. PwC professionals developed workflows and security policies, onboarded security credentials and accounts, and trained key stakeholders. The PwC team delivered well-documented, easily repeatable processes and an extensible framework that enabled the client to scale the CyberArk solution globally with less disruption.

Conclusion

Businesses around the world are using DevOps to unleash innovation and accelerate digital transformation. But fractured security systems and practices can hinder DevOps initiatives and expose the business to costly cyberattacks and data loss. Smart organizations are embedding security into DevOps workflows and using secrets management solutions like Conjur Secrets Manager to automate security controls, reduce vulnerabilities, and mitigate risk. DevSecOps helps development organizations and operations teams strengthen security, improve productivity, and accelerate time-to-market.

Together, PwC and CyberArk can help you jumpstart your DevSecOps journey and more quickly realize business value from your organization’s digital transformation initiatives and technology investments. PwC has an extensive business relationship with CyberArk and has deep experience architecting and implementing CyberArk solutions. In fact, CyberArk named PwC its Global Systems Integrator of the Year Americas four years running.

PwC and CyberArk can help your organization accelerate the pace of innovation, mitigate risk, and increase business agility by securing and streamlining DevOps initiatives and improving operational efficiencies.

Contacts

Sowvik Chakrabarty | Principal, PwC
sowvik.chakrabarty@pwc.com

Rich Kneeley | Managing Director, PwC
Richard.j.kneeley@pwc.com

Darren Orf | Principal, PwC
darren.c.orf@pwc.com

Clay Rogers | Director, CyberArk
clay.rogers@cyberark.com

Kurt Sand | General Manager - DevSecOps, CyberArk
kurt.sand@cyberark.com