Ebook

The Modern Approach to a Legacy Challenge

Five Federal Use Cases that Point to the Path Ahead for DevSecOps Success

harness

Envision your path forward with DevSecOps

Find clarity and direction by studying these top challenges—and their solutions. The promise of DevSecOps is alluring to Federal agencies. **Speed. Efficiency. Automation. Security.** All four topics are at the top of mind for federal agencies, but in reality are extremely difficult to implement at scale.

Over and over, Federal agencies hit the same common roadblocks when it comes to applying DevSecOps policies to their current processes and, therefore, fail to see the same results as commercial organizations.

It's not surprising—the environment is different, the security needs are different, and operations are different. So, a different approach is needed to get there.

The Cost of Not Fixing the SDLC

40%
Developer time spent on non-coding toil

85%
Production incidents caused by change failures

60%
Production applications exploited through code vulnerabilities

$180B
Cloud cost wasted

As you read through the five most common challenges that Federal agencies experience around DevSecOps, you'll see that a solution does exist to accelerate results, embed agility, and smooth the way forward while building upon the progress you've already made: **Harness.**

We’re stuck waiting and waiting.

The time-consuming process of manual approvals

The Challenge

Every major Federal agency and its departments find themselves facing increasing demand when implementing resilient, enterprise-grade IT to utilize comprehensive Change Management and Service Management frameworks. At the heart of the issue are holdover policies that rely on manual approvals. Having to involve a developer to hand-document every step and push each approval forward negates the gains in efficiency and speed Federal agencies need.

The Industry’s Answer

IT management platforms like ServiceNow and Atlassian have gained significant popularity for streamlining various IT processes, enhancing collaboration, and improving overall operational efficiency, as well as complying with the frameworks and policies set forth in the Federal market. Despite their advanced capabilities, these platforms still rely on manual updating, introducing:

- Risk of errors, inconsistencies, and inaccuracies in the data stored within IT management platforms
- Time-consuming processes
- Dependency on human input
- Delays in reflecting real-time changes and updates
- Compliance and reporting issues crop up due to lagging data updates
- Learning curves necessitating employee training
- Manual updating and maintenance becoming more complex with scaling

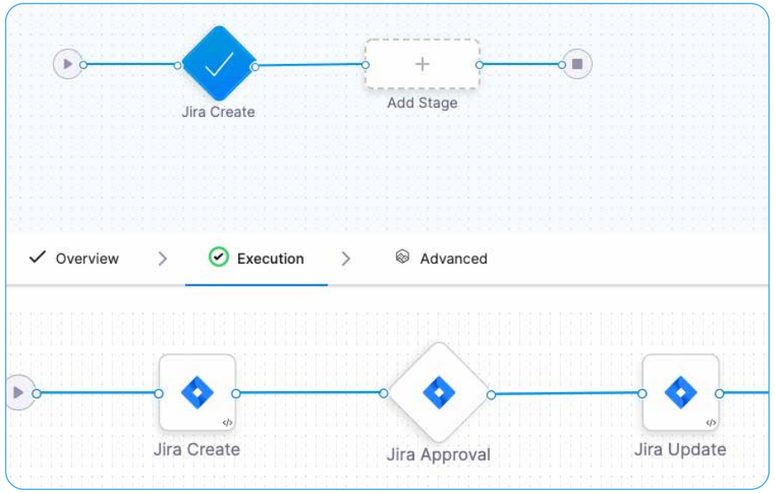
The Harness Solution

Automating change management

To solve this pain point, Harness automates change management, providing a streamlined and efficient way to manage the software delivery process.

Harness is a Software Delivery platform that automates the entire application delivery process, from code commit to production deployment. With integrations for popular tools like ServiceNow and Jira, and the ability to add gated approval steps to pipelines, development teams can ensure that all changes are properly tracked, approved, and deployed.

Harness's automation capabilities drive faster and more reliable software releases while minimizing the risks and toil associated with manual change management processes.



Federal Use Case

Our productivity is hindered by manual policies and compliance.

Painful policy management

The Challenge

Federal IT shops face unimaginable complexity in implementing, governing, and enforcing all of the required frameworks and policies. For most agencies, much of it is done manually by teams of expensive IT specialists who read up and dig in. Their approaches fall into two categories:

1. Lock everything down. This leaves DevOps staff to painstakingly plan, request, and attain manual approval for all necessary resources, identity and access management (IAM) permissions and dependencies just to implement a pipeline. If a new requirement is introduced, the process starts all over again.
2. Leave everything open. DevOps staff need to constantly recreate their pipelines and manually reference and apply long compliance checklist documents. When errors do occur, tedious discovery and post-mortem exercises must be conducted to attribute which actions and which personnel were responsible.

The Industry's Answer

Efforts are underway to reduce the toil around policy management. Tools like **Gamechanger** are in development to utilize AI to organize and sift through the mountain of policy information. While these efforts are important, they still demand massive amounts of manual tasks, supplemented with an optimized information retrieval system. And costs are prohibitive.

Agencies with high IT operations maturity have moved towards automated policy compliance, such as scripted checks and tests. While this is a trend in the right direction, this approach still requires manual toil to create compliance tests for every pipeline and every change.

The Harness Solution

Ease the process with policy-as-code

Since we can't reduce the number of policies or eliminate the conflicts among them, a good solution is to implement policy-as-code.

Policy-as-code (an idea popularized by the CNCF's Open Policy Agent (OPA) project), allows DevSecOps staff to retain development and deployment flexibility without making trade-offs in security and compliance. It does this by allowing teams to write policies that define what operations the organization cannot have, as well as what they must have and in what order. Agencies can then implement these policies in either an advisory mode that informs users what policies they are not in compliance with or an enforcing mode that actively prohibits non-compliant operations.

Harness incorporates Policy-as-Code as a centralized policy management and rules service that helps organizations create and enforce policies on deployments, infrastructure, and more, providing developer velocity without sacrificing compliance and standards.

Policy-as-code addresses the IT drudgery directly:

- IT specialists no longer need to assess every new software adoption or deployment manually. Instead, they can write a policy once and enforce its implementation on the front end of development.
- When an IT specialist is offboarded from a project or organization, their expertise is captured and reused in the policy agents, effectively codifying that tribal knowledge and allowing for seamless continuation of policy compliance operations.
- Developers have guardrails, giving them the flexibility to implement and utilize software and infrastructure assets available to them safely by ensuring policy compliance.

Federal Use Case

Why aren't our release cycles on par with commercial applications?

Balancing the risks and rewards of releases

The Challenge

As consumers, we barely notice the updates, bug fixes, and patches of commercial apps like Amazon or Gmail. Their parent companies, like other enterprise-grade commercial organizations, push out deployments at a frequency measured in minutes and hours every single day to maintain quality without any recognizable downtime. How can Federal agencies do that?

The Industry's Answer

Commercial organizations use two deployment approaches focused on risk reduction:

1. Canary deployments involve gradually rolling out a new version of an application to a small subset of users or servers before deploying it to the entire infrastructure. By exposing only a small number of users to the new version, any issues or bugs can be identified and addressed before a full rollout, and rollbacks only involve a limited group.
2. Blue/Green deployments maintain two separate environments (blue and green). At any given time, one environment hosts the production version of the application while the other is held in reserve for testing a new release, switching all users over to a new release at once minimizes service disruption.

Federal organizations looking to adopt these modern methodologies are hit with uniquely "government" challenges. They include:

- Legacy Systems that may be outdated, inflexible, or unable to support the required infrastructure or deployment processes
- The technical complexity of managing multiple environments, coordinating deployments, and handling traffic routing is more than they can handle
- Finding or developing the talent and expertise to implement and manage these modern rollout methodologies
- Security and compliance requirements complicate the rollout process
- A lack of interoperability between different systems, components, or vendors
- A reliance on manual deployment monitoring

The Harness Solution

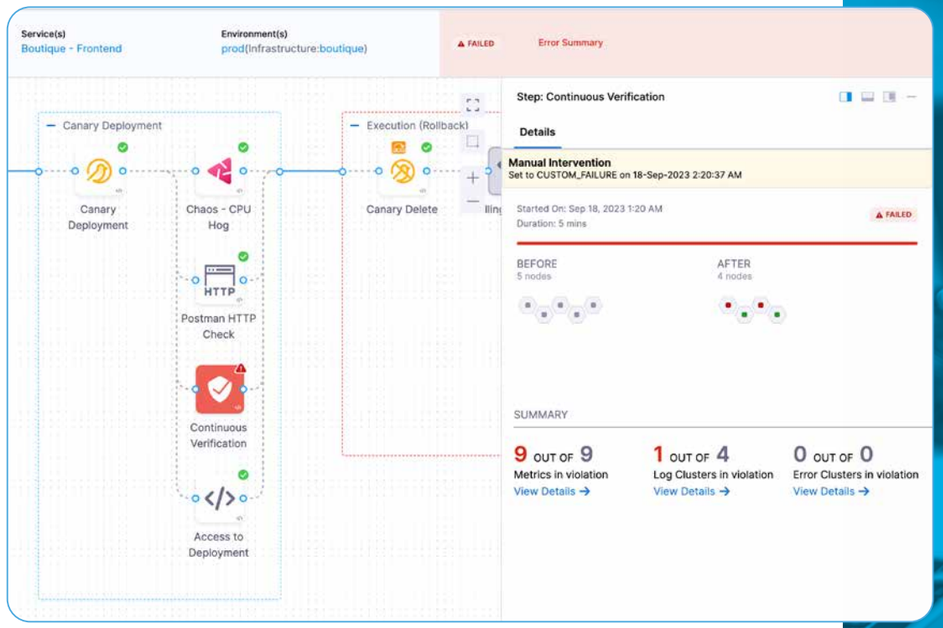
Rollout automation

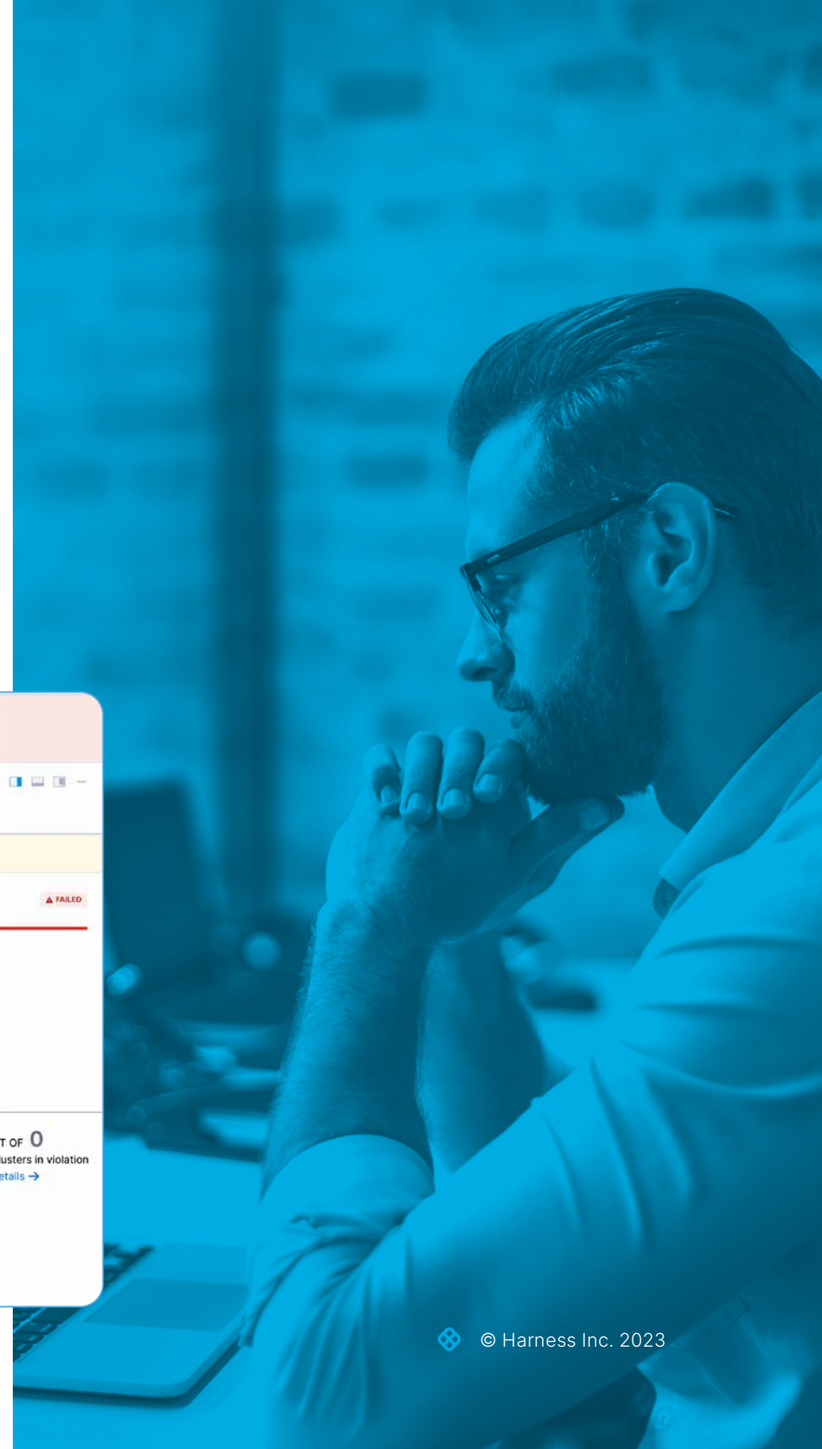
Harness offers pre-made rollout methodologies for Canary and Blue/Green deployments designed for flexibility and ease of use for DevOps teams. These rollout strategies are designed to ensure smooth and reliable software deployments while minimizing downtime and risks.

Harness also incorporates continuous verification to enhance the software delivery process by using Machine Learning to find anomalous behavior of services. This allows for faster, proactive monitoring and detection of anomalies or issues during deployments and reduces the manual effort required for verification.

When severe anomalies are detected, pre-made rollback methodologies are initiated, providing a more proactive approach to ensure the quality and reliability of software releases, mirroring commercial deployments with improved stakeholder experiences.

Pre-made rollouts, combined with automated rollback methodologies, allow developers to have the confidence to continuously and frequently deploy new features and patches without requiring a war room of IT Operations personnel to babysit deployments.





Federal Use Case

We’re stretched thin and can’t take on more.

The exponential growth of maintenance and overhead

The Challenge

According to an industry survey, more than 60 percent of government organizations believe they are not keeping pace with the private sector in terms of technology adoption. While they embrace the goals of digital transformation, managing the complexity—and the strain on IT resources—continues to be an issue.

As more DevSecOps projects are launched, there’s exponential growth in the resources needed. So, many Federal IT shops have turned to enterprise teams to build trusted templates that can be shared for more efficient adoption without adding significant overhead.

The Industry’s Answer

Using existing legacy tools such as Jenkins and Gitlab to run scripts and maintain the software development lifecycle (SDLC) linearly increases complexity as agencies adopt more technology, as the scripts need to be updated for every application change that occurs. All new security scanners, application performance monitoring tools (APMs), must be implemented within existing pipelines and operations—with major impacts:

- DevOps and platform teams are stretched thin as they “school up” on each new technology
- Maintenance and technical costs jump
- Applying industry-grade best practices becomes dependent on staffing, leading to inconsistent quality
- Risk of errors, inconsistencies, and inaccuracies in the data stored within IT management platforms

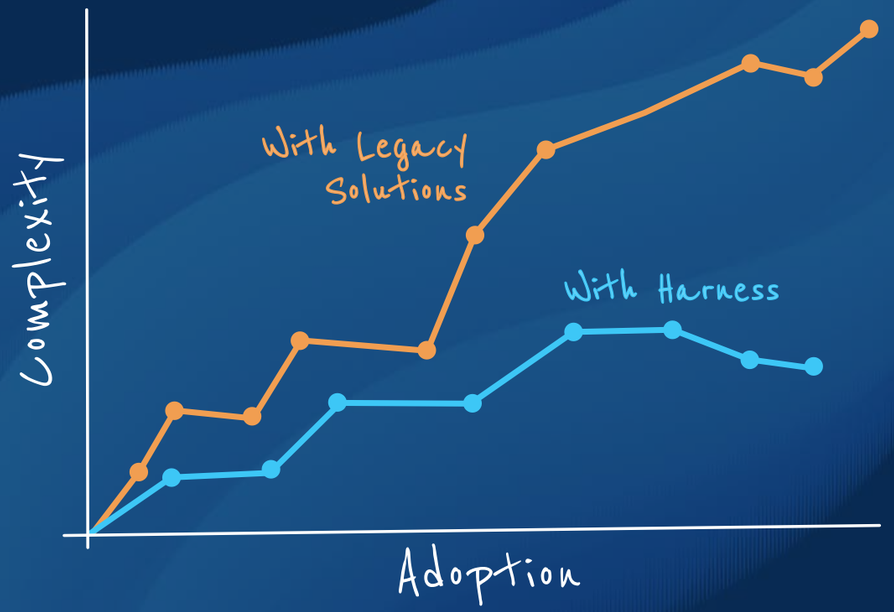
The Harness Solution

Solving the complexity/adoption problem

Harness was built to solve the complexity + adoption problem using distinct architecture and best practices:

First-Class Connectors and Step Library: DevOps and platform staff are tasked with the work necessary to implement the third-party platforms and tools required to deliver the software by wiring up connections. Harness eliminates the heavy lift, providing integration connectors for all major platforms and products throughout the SDLC. Once a connector is set up, provisioning access to these connections is simple using built-in Role-Based Access Management.

Step/Stage/Pipeline Templating: Harness maintains a growing library of pre-built steps that covers a majority of requirements throughout the SDLC. These steps make it incredibly easy for teams to adopt best practices and optimizations by dragging and dropping the steps into the pipeline editor and configure them using pre-built connectors. For those organization-specific steps not included in the library, teams can build, store, and access these complex steps in the Harness template library with full version control.



Federal Use Case

Ballooning costs are blowing our budget.

The quest for cost-conscious cloud migration

The Challenge

Federal agencies are moving to the cloud in record numbers. A **survey from SAIC** found that most use at least one cloud provider, and 70 percent use two or more. While the move improves software delivery velocity, it comes with challenges, chiefly increasing costs.

The problem becomes exacerbated when combined with an increased adoption of microservice architectures deployed through Kubernetes. Because Kubernetes is designed to be highly dynamic, with containers being created and destroyed on demand, it's difficult to predict and manage costs or even understand all the cost factors involved.

The Industry's Answer

Many in the industry are trying to use built-in cloud cost tools or business intelligence tools to gain observability into costs—while finding a lot of unnecessary work and inconsistencies.

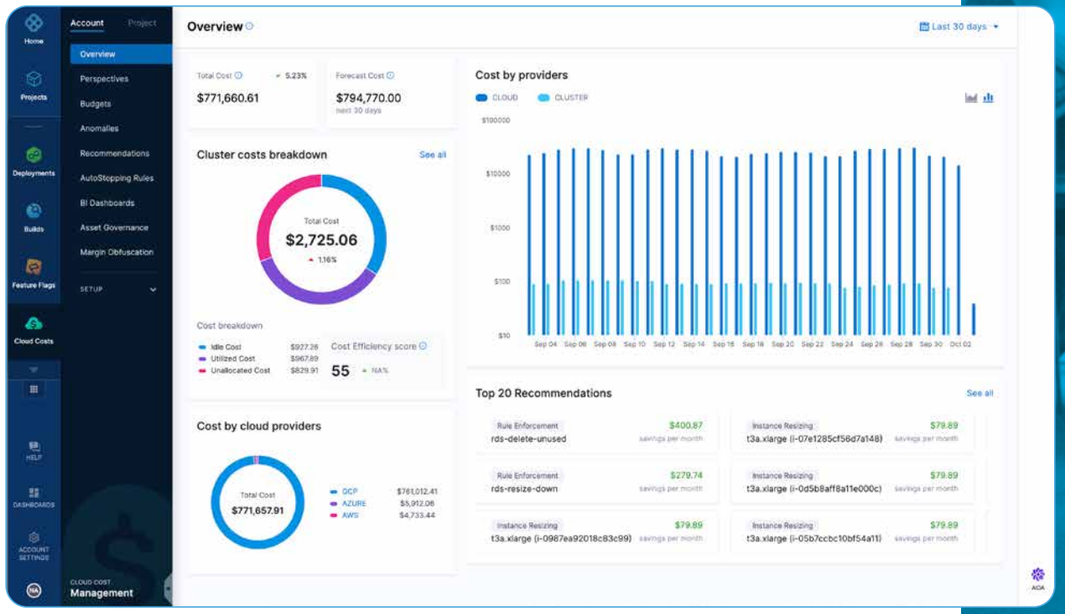
Harness has solved cloud cost management by introducing connectors for all three major U.S. cloud providers, including their Government Cloud offerings, as well as any Kubernetes cluster. These connectors are incredibly easy to configure and become assets that can be provisioned and managed, giving granular access to FinOps teams and Dev team stakeholders. Features for forecasting, auto-stopping rules, and dashboards further help organizations gain visibility into and control cloud costs.

The Harness Solution

Minimize spend from Day 1

Too often, Federal agencies feel stuck with the cost of cloud migration and become reactive when costs soar. Harness, however, has made it possible to use Cost Cloud Management to ensure cost efficiency and control from Day 1.

Harness even solves splitting up shared costs by attributing cloud costs to individual teams or projects. The powerful Perspectives tool provides a simple interface for FinOps teams to use metadata and billing labels to slice and dice the cloud costs into individual teams, projects, or initiatives—and ***even down to the individual Kubernetes service or application.***



Can you see your organization in these use cases?

Take action: Redefine your future with DevSecOps

Federal agencies find themselves at a critical crossroads on the road to modernization. While commercial companies provide an exciting model of what's possible, the realities of the public sector environment demand precision—there's no room for missteps or costly trial-and-error when it comes to optimizing the SDLC.

Accelerate, optimize and secure your agency's DevOps processes with the industry's first Intelligent Software Delivery Platform using AI/ML.

Determine if modernizing your software delivery process is the right solution.

DevSecOps Acceleration Modules

- **Continuous Integration**
- **Continuous Delivery**
- **Security Testing Orchestration**
- **Software Supply Chain Assurance**
- **Cloud Cost Management**

Identify a strong partner.

- Engage with federal IT partners who understand your specific challenges and tech stack
- Work with contractors and resellers who specialize in emerging technologies and are knowledgeable about best-in-class capabilities coming into the market.
- Leverage partners with a history of providing ROI through best-in-class commercial off-the-shelf products.
- Find a partner who understands DevSecOps and the complexities of processes at an enterprise level

Consider your ROI.

ancestry

50%

Ancestry eliminates 50% of major production incidents

UNITED

75%

United accelerates deployments & reduces toil by 75%

CARVANA

$1.4M

Carvana saves $1.4 Million in cloud costs

deluxe

95%

Deluxe decreases security risk by 95%

Choose your solution:
We recommend purpose-built Harness

End-to-end continuous integration/ continuous delivery pipeline

Harness builds 4x faster

AI-infused DevOps

Enhanced developer experience

Do more with less

Accelerate Speed-to-Mission

Schedule a demo for your team. Visit **www.harness.io/contact-sales/a**

About Harness

Harness provides a reliable, safe, and secure way for government enterprises to release applications to production across their respective mission-based architectures. By implementing the Harness software delivery platform, agencies can empower developers to be more productive while maintaining compliance and security through our OPA-based governance engine, custom pipeline policies, fine-grained RBAC, and versioned template library.

To learn more about the products Harness offers, or to request a demo, visit **www.harness.io**