harness

eBook 2022

Security & Privacy

Within the Harness Software Delivery Platform

Table of Contents

Introduction

The need for reliable and efficient Software Delivery and DevOps processes continues to become a necessity amongst engineering teams. This rings true across all industries and sectors. However, it's not all about the teams themselves. Their tools and services must also be reliable and secure, in order to ensure related activities execute without a hitch.

Harness provides the industry's first Software Delivery Platform-as-a-Service that leverages Artificial Intelligence to simplify DevOps processes. We empower engineering teams to deploy on demand, build and test code safely and efficiently, make cloud cost management decisions easier with intelligence, ensure reliability and stability in production environments, and make DevSecOps effortless with intelligent security testing orchestration. Our platform and operations are designed to put the developer first, all while establishing trust within the business.

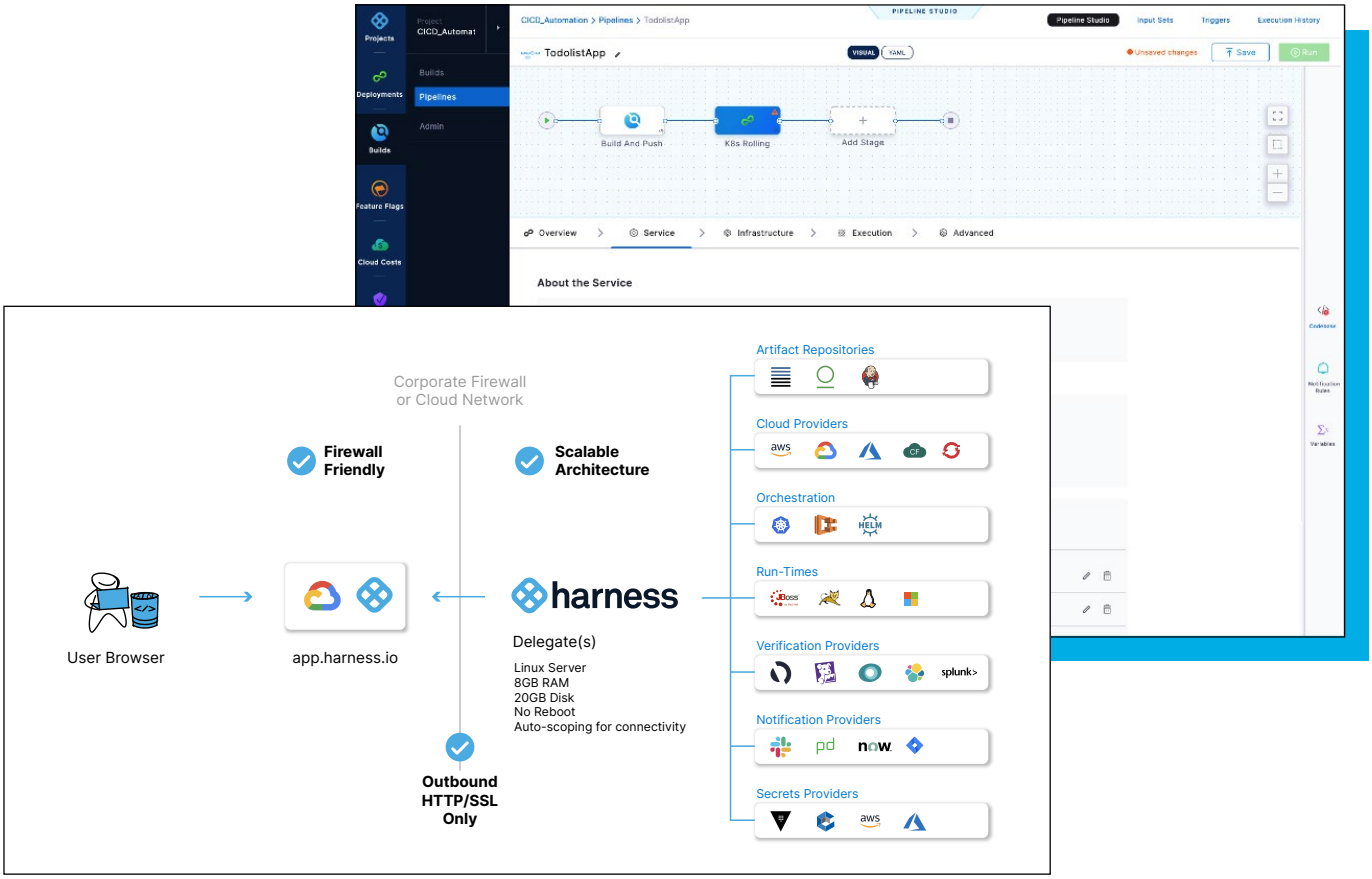
> At Harness, data security and privacy are top of mind when designing our platform, network, and business processes.

At Harness, data security and privacy are top of mind when designing our platform, network, and business processes. Within both our platform and how it interacts with our customers' environments, we have built enterprise features to support the security and privacy requirements of our customers. Additionally, we employ best-of-breed technologies and stringent operational processes to ensure that customer data is safe at all times.

Harness Architecture

Harness SaaS

Harness SaaS leverages the cloud (Google Cloud Platform) for its computing and processing components. These include the Harness Manager, Microservices, UI, Database, and Load Balancer & Proxy components. The client components (called Delegates) are installed on-premises behind the customer's firewall. Their purpose is to execute tasks fetched from the Harness Manager, and to communicate and integrate with different third party tools (Connectors) determined by the customer.



Delegate Overview
Delegate Requirements and Limitations

Network and Communication

There are four types of communication between different Harness components:

- User to Harness UI: This is a secure communication over HTTPS.
- User or Service Account to Harness API: This is authenticated through an API Key and Personal Access Token or Service Account Token.
- Delegate to Harness Manager: This is an outbound only call over HTTPS from the Delegate to the Harness Manager, which resides in the cloud and requires no inbound ports to be opened in any firewall.
- Delegate to Connectors: The Delegate integrates with Connectors such as cloud providers, APM tools, Log Analyzers, Artifact Repositories, etc. These connections can be secured using SSH or TLS/SSL.

Data Storage, Segregation, and Retention

Harness uses MongoDB Atlas managed service as its main database storage provider. Data is kept logically separate on various layers throughout the entire Harness platform. Each customer organization has a unique identifier (Account ID) that is attached to every transaction type performed in Harness, allowing for a complete segregation between the organizations.

This restriction applies to all data and all processes/threads, both in memory and on disk, and is strictly enforced throughout our system. In addition, secrets (passwords, keys, etc.) leveraging the built-in secrets manager are encrypted using envelope encryption and can only be decrypted within the customer's Delegate.

Customers are responsible for scrubbing any prohibited or sensitive data within their logs before sharing with the Harness platform. Customer execution data, such as deployment logs, are retained for six (6) months, however, they can be exported via API for additional retention or SIEM ingestion. Platform audit trails and cloud cost data ingested and processed by Harness are retained for two (2) years. Customer data such as pipelines are retained for the duration of the service. If Harness service is terminated, customer data will be deleted automatically within 90 days.

Platform Security

Security is a critical part of the software delivery lifecycle, which is why the Harness platform was designed from the ground up with built-in security measures.

Platform Authentication

Harness can integrate with your company's Single Sign-On solution so that users can log into the platform using their SSO credentials. This eliminates the need for users to have separate Harness credentials. Additionally, this enables our customers to apply the same authentication policies to Harness as they do for other enterprise applications.

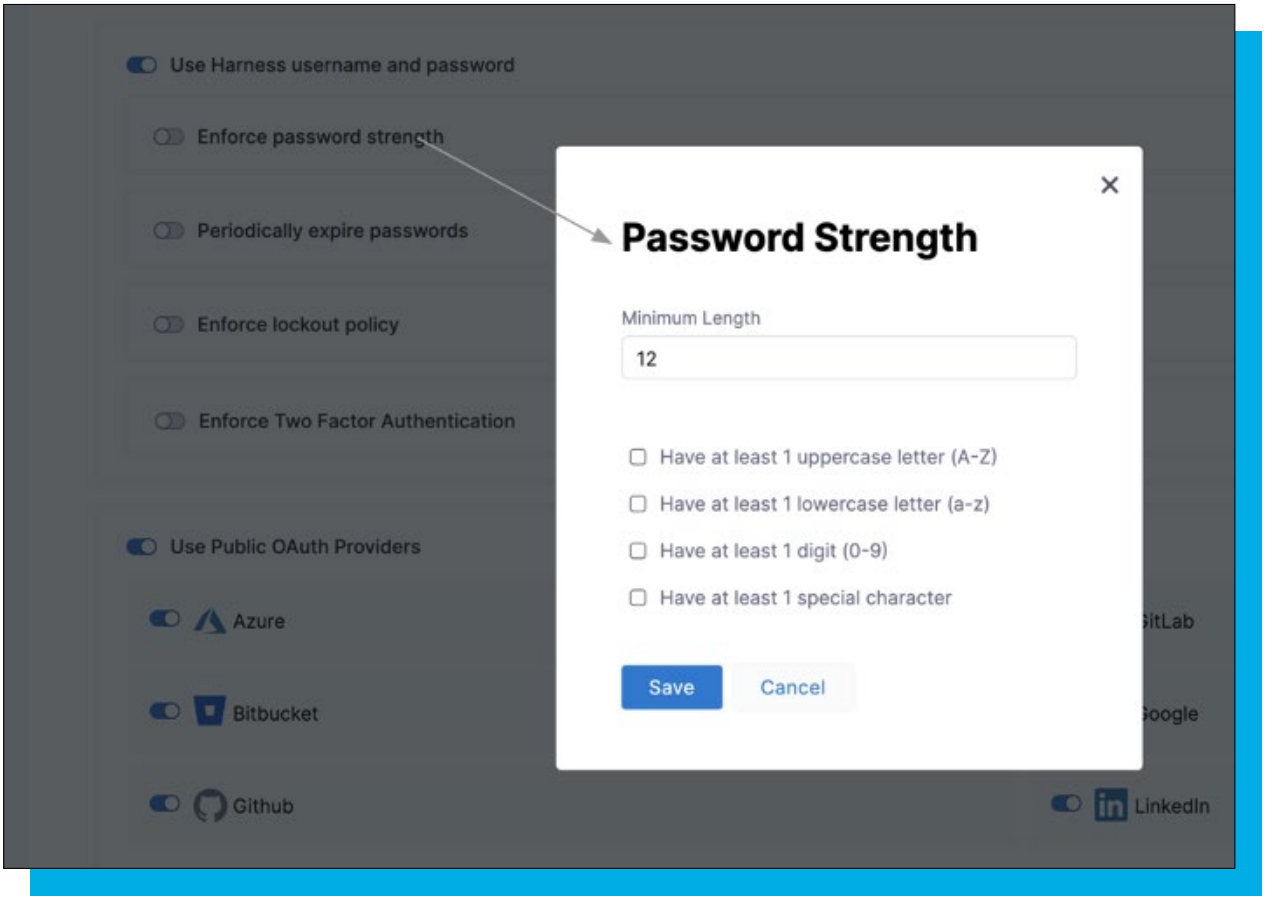
We offer Single Sign-On (SSO) via the following methods:

- SAML (Okta, OneLogin, etc.)
- LDAP*
- Public OAuth (Google, GitHub, Azure, etc.)
- SCIM (Okta, Azure AD, OneLogin)

*Only for CurrentGen

> Password policies can be configured to comply with company password policies.

If SSO is not required, or a secondary authentication method is required for backup, a Harness username and password can be utilized. Password policies can be configured to comply with company password policies. This includes password strength, expiration, and failed login attempts.



CurrentGen Authentication Settings
NextGen Authentication Settings

Harness also supports 2FA through authentication apps such as the Google Authenticator and Authy, as well as domain restriction so that customers can whitelist approved domains as usable in login credentials. IP Whitelisting and Restricted Access/Temporary Access settings (behind a feature flag) are also available to CurrentGen customers to add fine-grained access controls for specific users.

Platform Authorization

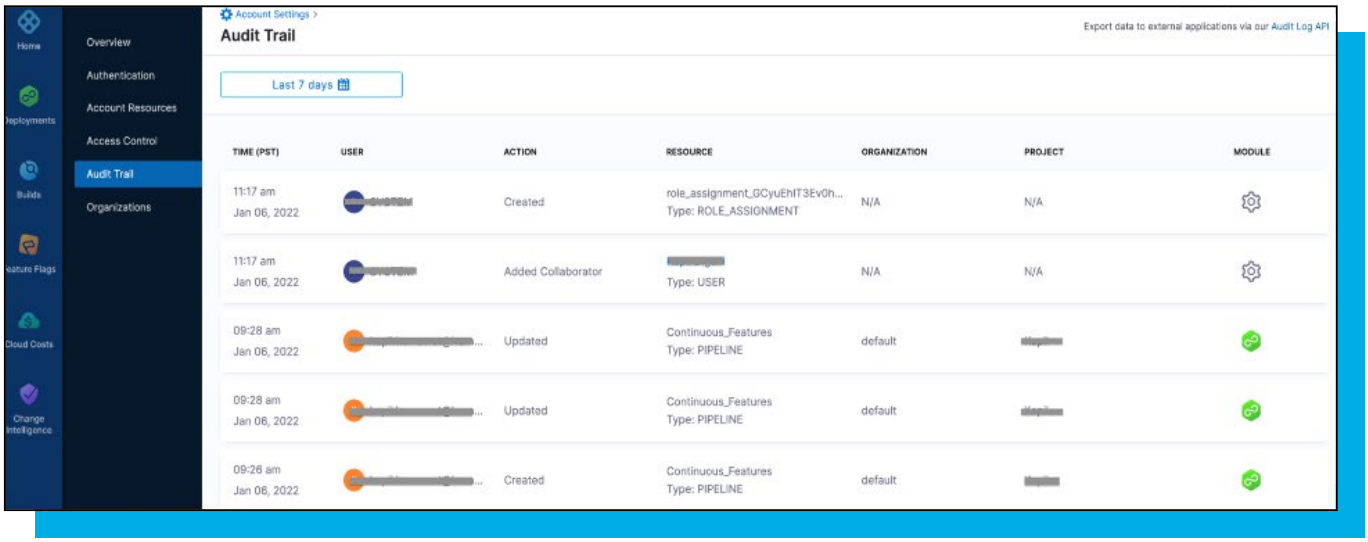
To ensure that a user's access can be configured to follow the principle of least privilege for security and compliance requirements and still satisfy job responsibilities and business needs, Harness boasts advanced Role-Based Access Control (RBAC) functionality, which allows for granular control over what users and service accounts can and cannot do in the platform.

Permissions can be configured for the following:

- Applications – logical group of services
- Services – artifacts
- Environments – infrastructure
- Triggers – condition to execute pipelines/workflows
- Pipelines – set of stages/workflows
- Workflows – deploys service(s) to an environment
- Deployments – execution of a pipeline/workflow

Audit Trails

Harness offers comprehensive Audit Trails for events and changes that take place in the platform. This allows customers to validate user activities and trace back changes made within the application. The Audit Trail includes a detailed description of the action, resource affected, and a timestamp. Data can be exported via the Audit Log API for further retention and analysis.



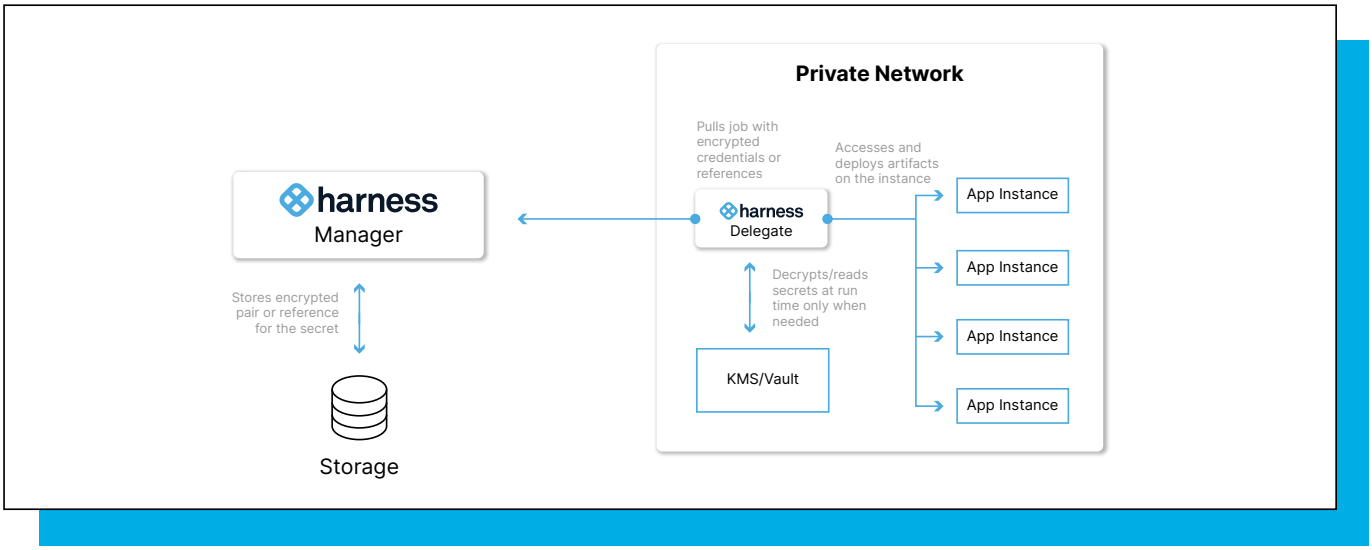
Harness Governance

Harness provides a governance feature using Open Policy Agent (OPA), Policy Management, and Rego policies. Customers can use Harness Governance to ensure that Harness entities like Pipelines meet specific compliance requirements when certain events happen. Policies can be centrally defined, stored, and selected where and when they should apply. The Harness OPA server is managed by Harness. Please reach out to Harness Support to request access to this feature.

> Policies can be centrally defined, stored, and selected where and when they should apply.

Secrets Management

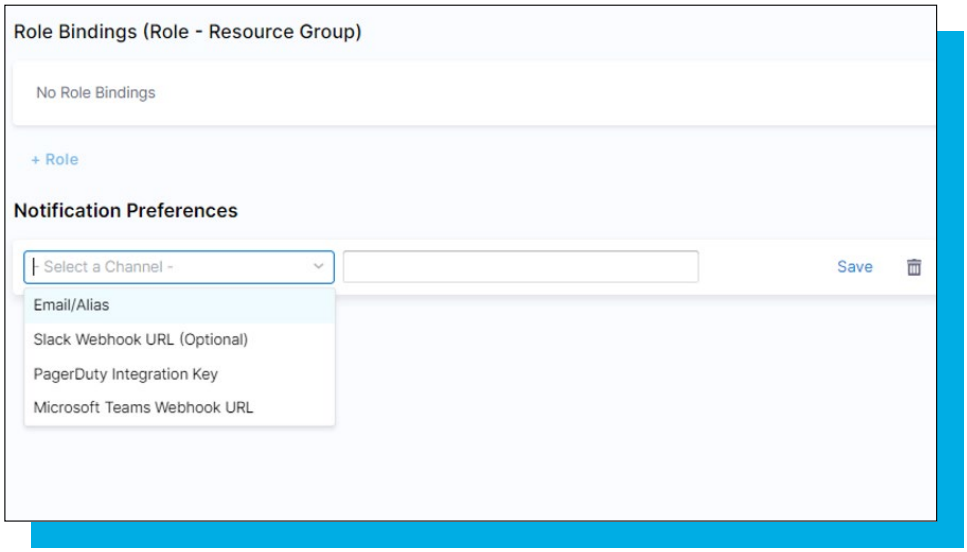
Harness has a built-in Secrets Management solution built on top of the GCP KMS service. This allows customers to maintain and store secrets (keys, tokens, credentials, variables, etc.) used in their Harness account, pipelines, and connectors in a secure and convenient way. Secrets are only accessed and decrypted at the time when they are needed. In addition, Harness supports customers who want to store their secrets in their environment and control the encryption keys used to encrypt the secrets by integrating with existing third-party secret management tools, such as AWS Secrets Manager or HashiCorp Vault.



Notifications

The Harness platform provides notification features that allow customers to create alert conditions for specific users and groups across their account and in individual workflows.

Notifications provide users with real-time alerts when certain activities have occurred, as well as their status, supporting timely confirmation or response needs. These notifications can be wired into platforms like Slack for your convenience.



There are three major notification features:

- **Notification Settings for User Groups** – Set the notification channels for User Group members. These include group or individual email addresses, as well as PagerDuty groups and Microsoft Teams or Slack channels. When User Groups are used in an Alert Notification Rule or in a Workflow Notification Strategy, these channels will be used to notify the group members.
- **Alert Notification Rules** – Set which types of alerts are sent to different User Groups. You can also set up a default Catch-All Notification User Group to receive all alerts.
- **Workflows Notification Strategy** – Set notification conditions in a Workflow or Workflow Phase, and the User Groups that need to be notified when these conditions are met.

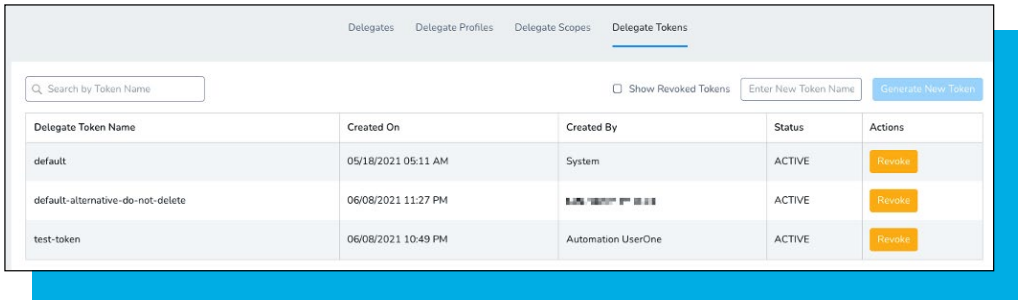
Delegate Security

The Delegate is a service you run in your local network or VPC to connect all of your artifact repositories, infrastructure, collaboration and verification tools, and other service providers. It is the worker in your environment that performs tasks initiated by the Harness Manager. The Delegate connects to the Harness Manager via outbound HTTPS, Websocket over TLS, and gRPC connections.

Securing the Delegate Connection to the Harness Manager

The Harness Manager identifies Delegates by the Harness account ID and token. When a new Harness account is created, Delegates associated with that account are propagated with a token through the configuration file in order to authenticate and secure the Delegates to the Harness Manager.

This token is encrypted via AES-GCM and used in every call between the Delegate and Harness Manager. Customers can further secure the Delegates by revoking and replacing the default token with new tokens.



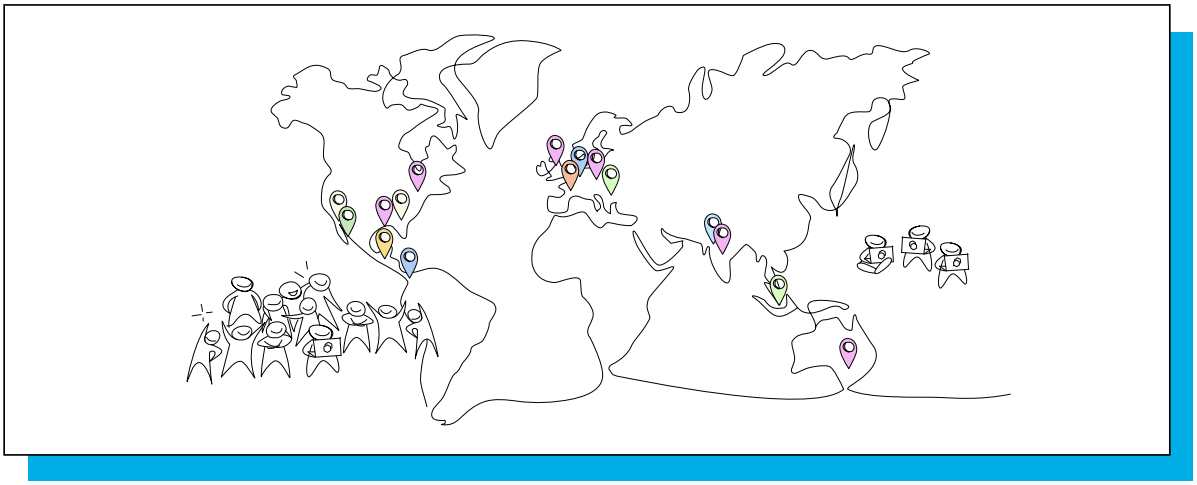
Delegate Scoping

The Harness platform performs tasks using any available Delegates. However, specific Delegates can be prioritized to perform specific tasks if mapped to a Tag. This allows customers to define boundaries and association of a specific Delegate and task with a chosen application, environment, environment type, and service infrastructure.

This is useful if, for example, you need to restrict access to an environment (e.g. production), or if you'd like to dedicate a Delegate to an application or task.

High Availability & Disaster Recovery

The Harness platform is designed to provide high availability and reliable uptime by utilizing autoscaling, load balancing, and task queues. Multi-region architecture for the Harness platform is in place in a separate geographic location to ensure the platform and its services can be rapidly scaled up in the event of a disaster to its primary location. This architecture is tested by Harness at least annually to validate the failover procedures and recovery technologies.



In addition, Harness leverages existing DR capabilities built into its cloud computing and database managed services, which includes validating that each provider has a DR plan, performs annual testing, and for our databases, leveraging 'replica set' functionality for clusters. Harness also performs frequent backups of its database to ensure that data is backed up and can be restored at a point in time in the event of an incident or data corruption.

Delegate high availability can also be set up in the customer's environment, allowing one Delegate to go down without impacting the Harness platform's ability to queue tasks for execution.

Attestations & Certifications

Harness holds certifications in both ISO 27001 and 27017, which are international certifications for information security and cloud security. These certifications demonstrate that Harness' internal Information Security Management System (ISMS) program meets those security baselines.

Harness must annually ensure that its ISMS program includes all of the required elements for certification, including but not limited to: Information Security Policies & Procedures, Access Controls, Cryptography, Vulnerability Management, Secure SDLC/Change Management, Vendor Risk Management, and IT Security Incident Response.

In addition to both ISO certifications, the Harness platform also holds a SOC 2 Type II attestation report. This report provides assurance over the Security, Availability, and Confidentiality of the platform, its supporting processes, and the internal controls of the organization.

Harness also engages with trusted third parties to complete network and application penetration tests at least annually. Results from those tests and copies of Harness' latest ISO certifications and SOC 2 Type II reports can be found here.

Data Privacy

Harness is committed to protecting the privacy of our customers and their data.

Encryption

All data that traverses from a customer's environment to the Harness platform and UI is encrypted in transit utilizing TLS 1.2+. This provides assurance that the confidentiality of the data remains intact from the Delegate or browser through to the Harness platform.

All data at rest within the Harness platform and MongoDB Atlas is AES-256 encrypted, adding a protection layer to guarantee customer data is only visible once decrypted by an authorized process.

Personally Identifiable Information

Harness respects your privacy and seeks to limit our collection of PII. We must collect name, user ID, and email to enable platform access, support administrative purposes, and provide technical support. Harness is committed to ensuring the security and protection of personal information that is processed, and to provide a compliant and consistent approach to data protection which complies with existing laws (including GDPR and CCPA) and abides by data protection principles. For more information about how Harness collects, stores, and processes PII, please see our privacy policy at www.harness.io/privacy.

Harness recommends that customers scrub their log data (prior to being transferred to Harness) to prevent any data considered "prohibited" by the customer from being shared with Harness.

Conclusion

A world class DevOps experience should not be restricted to only certain organizations with large budgets and resources. Harness is here to provide the best Software Delivery platform for all organizations to utilize, while also ensuring that customers don't sacrifice their security and privacy requirements. We are committed to being the go-to platform for developers, while providing a secure and safe solution for businesses.

If you'd like to learn more about how Harness can support your business, please request your demo today.

Have additional security or privacy questions or concerns? Email us at security@harness.io.

Author Appendix

Written By	**Kevin Moy** Staff Security Analyst	Kevin is a member of the GRC team at Harness, and is responsible for supporting the company's compliance and IT risk management initiatives. He enjoys cold brew coffee, city biking, and techno music.
Reviewed By	**Peter Gregg** Security Analyst	Peter has always been interested in both physical and digital security. He is currently working to complete his Masters in Information Security Engineering at Sans Technical Institute. Outside of work and studying, he enjoys playing retro amiga games and locksports.
	Roxanne Williams Senior Content Strategy Manager	Roxanne is a lover of all things DevOps, devoting a large portion of her time at Harness to competitive research, CI/CD as a whole, and Security. She is passionate about pugs, plants, and writing.