DATA SHEET

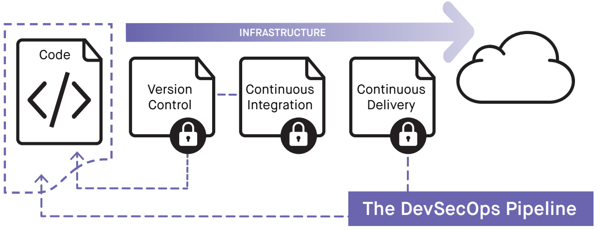
Integrate Security into Your DevOps Pipeline

DevOps tools and practices enable enterprises to save time and money in rapidly iterating on smart, fast software deployments. But security is often neglected or avoided because of the perception that adding security will dramatically slow the pace of development. With Fugue, you can bypass the unnecessary risks of this approach by integrating security directly into your DevOps pipeline.

DevSecOps Provides Agile Security

DevSecOps is established by placing security controls in every phase of your pipeline. Common best practices include:

- **Training:** Educate engineers to incorporate security best practices into code such as always validating inputs from untrusted data sources or enforcing the principle of least privilege
- **Access Control:** Limit permission for code commits to qualified developers
- **Infrastructure:** Create application infrastructure from pre-constructed templates using verified AMIs and containers
- **Continuous Integration:** After code is committed to version control, statically analyze code for vulnerabilities like buffer overflows or the unwanted inclusion of keys or passwords
- **Infrastructure:** Verify that logging and monitoring are always enabled
- **Continuous Deploy:** After deployments are complete, run risk or vulnerability assessment tools on applications and infrastructure



DEVSECOPS WITH FUGUE

- Easy API-driven integration with common CI/CD tools
- Infrastructure and compliance as code
- Automated remediation for all infrastructure security violations
- Use a single tool to access, trace, and manage accounts, users, and configurations

> *"When security becomes an integral part of DevOps, security engineers can build controls directly into the product rather than bolting them on top of it after the fact"*
>
> *Vehent —*
> *Securing Devops: Safe Services in the Cloud*

Fugue

www.fugue.co | hello@fugue.co | @FugueHQ

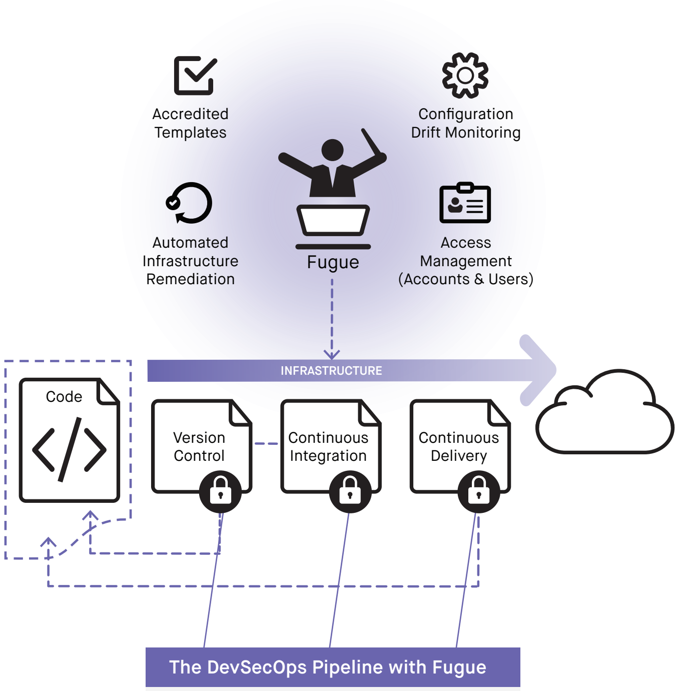
Fugue Integrates Security into DevOps Pipeline

Fugue enforces security controls for the infrastructure components of your CI/CD pipeline. It identifies risks in your cloud infrastructure and ensures they are never repeated. Other Fugue benefits include:

- **Enforce Accredited Templates:** Fugue protects infrastructure by making sure that only verified AMIs or containers can be deployed into the cloud. If any other AMIs or containers are used Fugue generates an error before provisioning.
- **Identify Policy Violations:** Fugue can enforce security controls based on regulatory standards such as NIST 800-53, HIPAA, CIS, or any unique internal security policies. Fugue generates errors when it detects policy violations such as not enabling encryption or logging. Fugue can analyze infrastructure for violations at two stages, when it is initially provisioned, or after application code is deployed.
- **Eliminate Configuration Drift:** Fugue also detects inadvertent changes to infrastructure, such as mistakenly opening an SSH port on production servers. Fugue automatically restores infrastructure to its known good state, saving both time and resources to prevent security violations.
- **Access Management:** Fugue uses Role-based Access Control (RBAC) to ensure that only authorized users are permitted to commit code. RBAC provides account and user management for permissions across groups/roles/levels for any complexity of resources. Fugue logs all actions, including RBAC, for accountability.

Smart, successful DevSecOps revolves around adding security controls throughout your CI/CD pipeline. Fugue enables you to do this for the infrastructure components of your pipeline, enforcing compliant infrastructure for all your applications.

INTEGRATED SECURITY WITH FUGUE


Accredited Templates
Configuration Drift Monitoring
Automated Infrastructure Remediation
Fugue
Access Management (Accounts & Users)
INFRASTRUCTURE
Code
Version Control
Continuous Integration
Continuous Delivery

The DevSecOps Pipeline with Fugue

Pipeline Security

- ✓ Scan for vulnerabilities
- ✓ Use accredited templates, AMIs and containers
- ✓ Verify compliance
- ✓ Monitor and remediate configuration drift

About Fugue

Fugue, a leader in cloud infrastructure automation and security, provides solutions to ensure that enterprise and public agencies cloud resources are always provisioned according to a single source of truth—and stay that way throughout the resources' lifetime. Fugue is privately held and headquartered in Maryland. Fugue was names a Cool Vendor in Cloud Computing 2017 by Gartner.

aws partner network Advanced Technology Partner