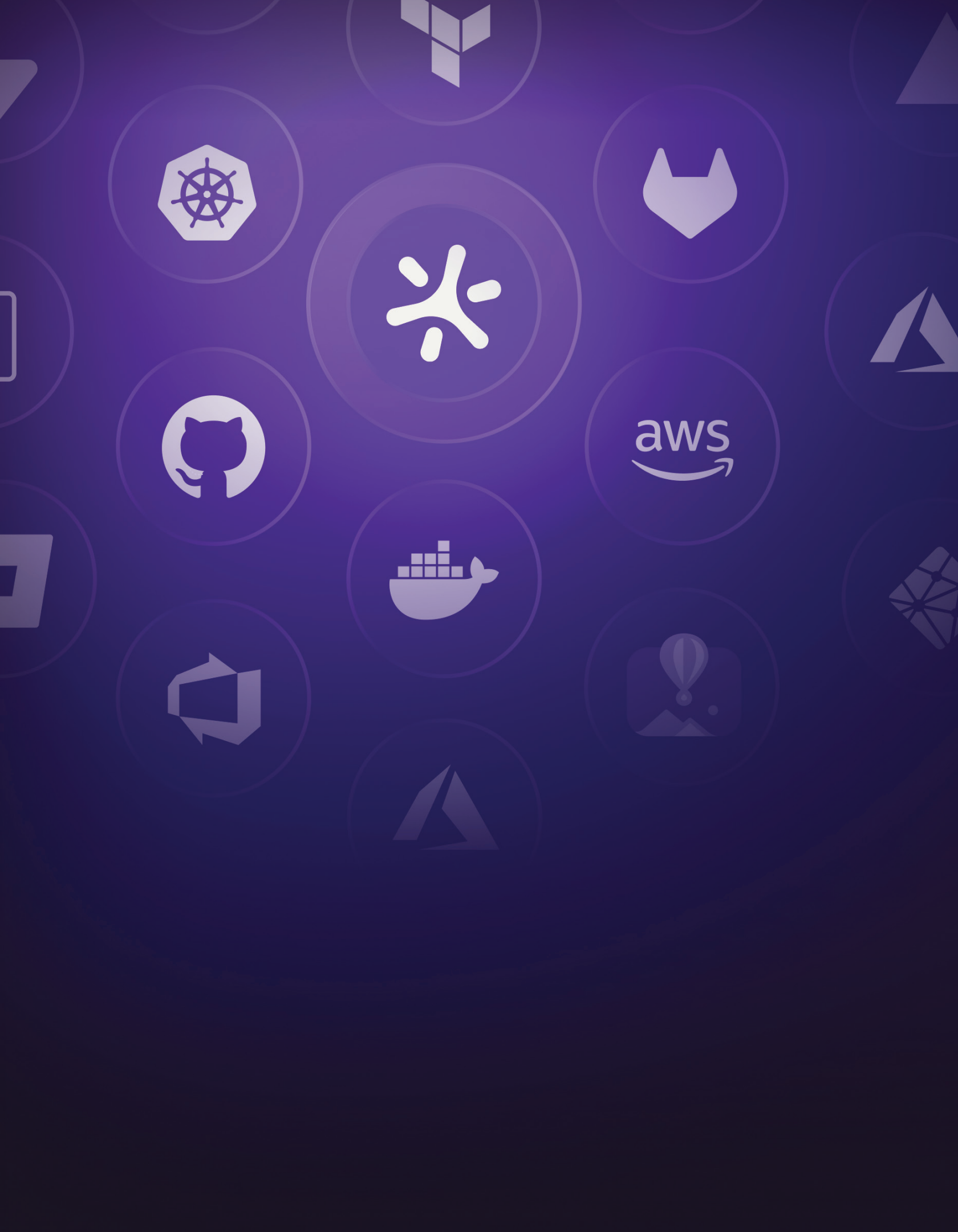
Doppler

Integrations, comparisons, & compliance made simple

Explore integrations, see comparisons, and learn why teams trust Doppler.




aws

CHAPTER 1

Endless integrations, one unified ecosystem

Leverage our partner ecosystem to integrate natively into your infrastructure, enhance security, and streamline operations.

Read on to learn more about a few of our most popular integrations



Integrating Doppler & Kubernetes

Optimize your Kubernetes deployments with Doppler's sophisticated integration. This partnership provides an advanced, streamlined approach to managing secrets in Kubernetes clusters, enhancing both security and operational efficiency.

Improve security with role-based access controls

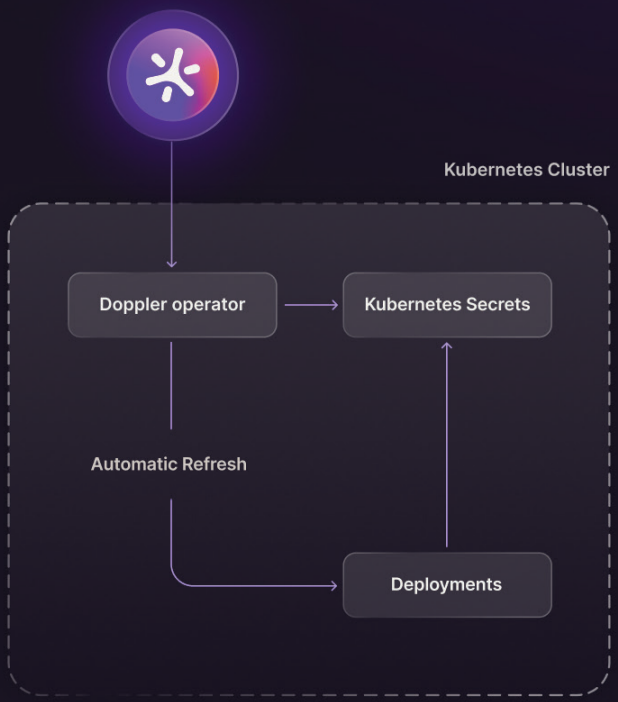
Continuously sync secrets from Doppler to Kubernetes across multiple namespaces and projects, streamlining management and reducing manual intervention.

Multi-cloud and hybrid support

No more long-lived tokens to sync secrets. OIDC authentication gives you short-lived, on-demand tokens linked to service accounts.

Optimize developer experience across environments

The Doppler Kubernetes Operator automatically reloads deployments that reference managed secrets, ensuring applications always use the latest version of secrets.



Getting started is simple and quick

1. Install Doppler Kubernetes Operator
2. Service account and role setup
3. Generate a Doppler token secret or use OIDC
4. Create DopplerSecret CRD
5. Deploy and automate

Secure your development pipeline with secrets management:

Integrating Doppler & AWS Secrets Manager

Integrating Doppler with AWS Secrets Manager extends your security beyond AWS, providing a unified source of truth for secrets across all your services and environments while enhancing local development capabilities.

AWS Secrets Manager & Doppler: Better together

Platform	Encryption	Automatic provisioning	Built-in auditing	Team management	Reference secrets across projects	Cloud-agnostic
AWS Secrets Manager	✓	✓				
AWS Secrets Manager + Doppler	✓	✓	✓	✓	✓	✓

Streamline access management

Centralizing secrets in Doppler provides a unified interface for developers, reducing the need for direct AWS access, and minimizing the risk of unauthorized changes.

Optimized developer experience across environments

Improve local development with Doppler's git-like environment. Inject secrets into any process and automate app restarts, eliminating .env files and manual setups.

Multi-cloud and hybrid support

Improve local development by directly injecting secrets into processes, triggering automatic app restarts, and eliminating .env files and manual configurations.

Comprehensive logging and auditing

Increase observability by combining Doppler's advanced audit logs and secrets visibility with AWS CloudTrail's detailed API call tracking for a robust auditing and logging solution.

Learn more about securing secrets with Doppler + AWS here:

Integrating Doppler with Azure Key Vault

Integrating Doppler with Azure Key Vault centralizes secrets management across your cloud infrastructure. Empower developers with role-based access to manage secrets updates, all within one intuitive UI and without cloud lock-in.

Azure Key Vault & Doppler: Better together

Platform	Encryption	Secure secrets storage	Built-in auditing	Reference secrets across projects	Cloud-agnostic
Azure Key Vault	✓	✓			
Azure Key Vault + Doppler	✓	✓	✓	✓	✓

Improve security with role-based access controls

The integration of Azure Key Vault with Doppler enhances access management by offering developers a single, unified interface for secrets, reducing reliance on direct Azure access, and lowering the chances of unauthorized changes.

Multi-cloud and hybrid support

Doppler's integration supports a multi-cloud approach, allowing secrets to move freely between Azure and other cloud environments without vendor lock-in.

Optimize developer experience across environments

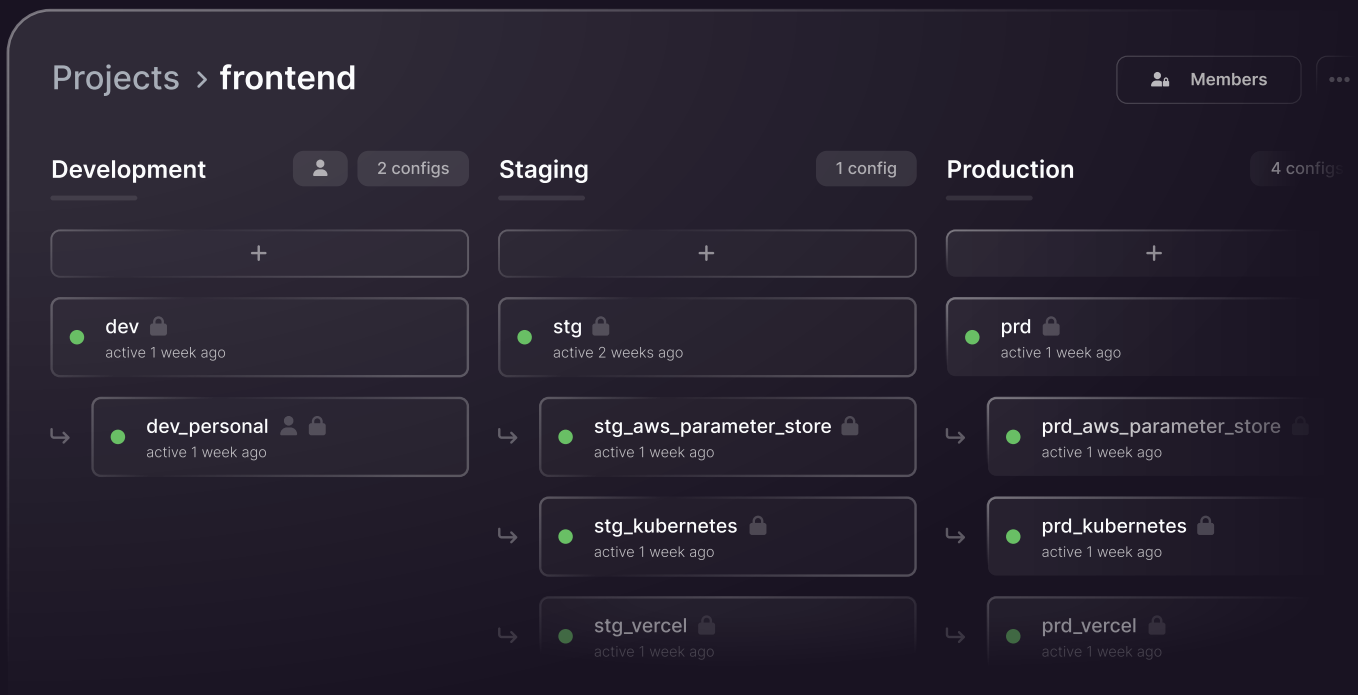
Improve local development by directly injecting secrets into processes, triggering automatic app restarts, and eliminating .env files and manual configurations.

Check out our other Azure integrations and setup guides here:

CHAPTER 2

Not all secrets managers are built for developers

Here's how Doppler stacks up against traditional and emerging tools, without the complexity, overhead, or lock-in.



Doppler vs. Vault: Headache-free secrets management

Out-of-the-box simplicity, best-in-class UX, and predictable pricing.
Doppler is the faster, more secure way to scale your secrets management.

Why companies are switching to Doppler

- Predictable, transparent pricing
- Secure and reliable architecture
- Scalable integrations
- Faster adoption across teams
- Build more. Manage less.

Doppler vs HashiCorp® Vault Enterprise

	Doppler™	HashiCorp® Vault Enterprise
Audit logs	✓	✓
User groups & custom roles	✓	✓
Encrypted storage	✓	✓
SAML SSO	✓	✓
SCIM	✓	×
Intuitive RBAC with security guarantees	✓	×
Predictable & transparent seat-based pricing	✓	×
Maintenance free	✓	×
Quick onboarding & migration	✓	×
40+ sync, rotation, and SIEM integrations	✓	×
Track every time a secret is read and by who	✓	×

"Solutions like Vault were too complicated. We needed something that didn't require a dedicated team to manage it."

Dan Steen,
VP of Infrastructure

PARADOX

Learn how to scale secrets securely without the Vault overhead:

Doppler vs Infisical: The enterprise-ready choice for secrets management

Secure your secrets with powerful integrations, enterprise-grade security, and a developer-friendly experience.

Why companies choose Doppler

- Enterprise-grade security & compliance
- Secrets management without the overhead
- Predictable & transparent seat-based pricing
- Powerful functionality & ease of use
- Integrate natively and reduce friction

Doppler vs Infisical

	Doppler™	Infisical
Approval / Change Requests	✓	✓
User groups & RBAC	✓	✓
SCIM	✓	✓
Audit Logs	✓	✓
Secret Access Reads	✓	✓
VS Code extension	✓	×
Predictable & transparent seat based pricing	✓	×
Maintenance free	✓	×
ISO 27001 Compliant	✓	×

"Doppler's pricing per developer seat is predictable and flexible, with unlimited service accounts. Infisical's pricing on service accounts didn't make sense. Even self-hosting Infisical should have been cheaper, but it wasn't."

Certified Cloud Security Engineer at an Information Services Company

Learn how to scale secrets securely without the Infisical limitations:

Doppler vs CyberArk:
Cut the complexity. Keep the security.

Doppler is a developer-first secrets management platform with no lengthy setup, on-premise overhead, or hidden costs.

Why companies choose Doppler

- Built for developers, not just compliance teams
- Fast, no-hassle setup
- Predictable & transparent seat-based pricing
- Enterprise-grade security made accessible
- Cloud-native and CI/CD integrations

Doppler vs CyberArk

	Doppler™	CyberArk®
Fine-grained access controls	✓	✓
Secret rotation & audit logs	✓	✓
RBAC	✓	✓
Developer-friendly UX	✓	×
Fully managed SaaS	✓	×
Quick time-to-value	✓	×
Predictable pricing	✓	×

Learn how to manage secrets securely, without the CyberArk complexity:



Secrets, secured

Doppler makes secrets management easy at every stage of growth. Whether you're an individual developer, a growing team, or an enterprise, there's a plan built to fit your needs.

Developer

Secure your solo projects or small team workflows. Includes unlimited projects, integrations, CLI access, and more. Free for up to 3 users.

Team

Unlock team productivity with advanced access controls, secret rotation, audit logs, and priority support. Free 14-day trial included.

Enterprise

Tailored for complex security and compliance needs. Gain customer roles, dynamic secrets, on-prem rotation, dedicated support, and more.

Scan the QR code to choose the plan that's right for you:


Doppler