



The **Future** of **Secrets** Management

WHITE PAPER

Doppler



Contents

Executive Summary	2
The Current State Of Secrets Management	3
The Cost of Inefficient Secrets Management	6
Doppler: A Modern Approach to Secrets Management	10
Secrets Management with Doppler	14
Secrets Automation with Doppler	16
Secrets Rotation with Doppler	17
Governance with Doppler	18
Local Development	19
Doppler Fact Sheet	20
Summary	21



Executive Summary

To embrace the future requires a willingness to exchange old ideas for new ones—to know the risks of failing to change, the opportunities for innovation, and the benefits that will follow.

This ebook aims to clarify the risks and costs associated with traditional approaches to secrets management and explain why a multi-cloud holistic strategy that maximizes automation is the future.

You'll learn what's possible and how a whole raft of problems you may have accepted as a given can be eliminated entirely.

We'll start by identifying the growing complexity and secrets management challenges companies of all sizes face, as well as address common misconceptions that keep companies stuck using traditional methods.

Next, we'll quantify the cost of poor secrets management practices, the risks facing businesses that fail to innovate, and the cost-saving benefits from companies that are embracing the future of secrets management.

We'll then use Doppler to illustrate modern secrets management in action, the key elements of a modern secrets management strategy, and why developer productivity is a crucial metric to consider when evaluating secrets managers.

With that, let's dive in!

The Current State Of Secrets Management

There's no shortage of examples of security breaches resulting from secrets found in git repositories, .env file usage, and a lack of secrets rotation. Secrets continue to fall into the hands of attackers due to a lack of awareness of effective secrets management practices or organizations' inability to implement them at scale.

With the proliferation of microservices, the number of secrets organizations must manage continues to grow rapidly. Coupled with the diversity in application deployment targets—from modern serverless platforms to CI/CD, Kubernetes, and virtual machines—secrets sprawl has become one of the biggest challenges for Engineering, DevOps, and Security teams to tackle in 2024.

Standard Approaches Cannot Mitigate Secrets Sprawl

Secrets sprawl occurs because, without a modern holistic strategy, secrets management is siloed within each platform and environment. This causes inconsistency in how secrets are managed between teams and makes organization-level governance and oversight difficult, if not impossible.

Without consistency and oversight in how each application manages secrets, risky and insecure practices, such as storing secrets in source code and .env files, become difficult to detect and are, therefore, likely to emerge.

Some organizations have invested in a single cross-platform secrets manager as a cure for secrets sprawl, mandating its usage across the organization. While the goal of having a single source of truth for managing application secrets is the right one, it's destined to fail without widespread adoption and secrets orchestration capabilities.

A Secrets Manager Is Only As Useful As Its Rate of Adoption








Because application teams are evaluated on their ability to ship features and add business value, a secrets manager that improves security at the cost of productivity will mainly be adopted by force—not by choice.

Unfortunately, traditional secrets managers don't offer development teams incentives beyond security as:

1. They are generic solutions for key-value storage of sensitive data—not designed for managing application secrets.
2. They were created for security professionals, not developers.
3. They weren't designed for a multi-cloud and microservices world.

Traditional Secrets Managers Have Failed to Adapt to Modern Needs

Because traditional secrets managers aren't purpose-built for managing application secrets, they're unable to provide the time-saving and automated workflows developers and DevOps teams need, such as:

 <p>Structured secrets storage by application with a list of customizable environments</p>	 <p>Synchronizing secret updates between environments to remove copy and pasting</p>	 <p>Missing secrets notifications for detecting drift between environments</p>	
 <p>Secrets referencing to reduce secrets duplication</p>	 <p>Secrets diff for comparing secrets between environments</p>	 <p>Lookup by value to find all instances of a secret</p>	 <p>Providing secrets during local development</p>

These example workflows touch on a theme we'll continue exploring throughout this ebook—that secrets management is not difficult or time-consuming as long as you have the right tools and workflows.

The Benefits Of Change

There is much to gain from stepping into the modern era of secrets management. We'll quantify the costs and benefits in the next section, but at a high level, this is what awaits businesses who take the leap:



The key to improvement is automation and streamlined workflows. When the right way is also the most accessible and most efficient, best practices naturally follow.

A secrets manager is only as valuable as its rate of adoption. To be future-proof and deliver sufficient ROI, it must improve both security and productivity while satisfying the needs of developers, DevOps, and security teams. Traditional secrets managers simply don't meet these modern demands.

Let's now quantify the cost of inefficient secrets management practices and the financial benefits of adopting a new operating model.

The Cost of Inefficient Secrets Management

The advent of Agile practices, cloud infrastructure, DevOps, and Infrastructure as code revolutionized the speed, quality, and ease with which applications could be developed, built, tested, and deployed.

The software industry woke up to the realization that software development and infrastructure management would benefit from the same fundamental automation principles that had been driving cost efficiency in other industries for decades.

But secrets management was left out of this transformation because:

- Secrets management was viewed as unavoidably complex, manual, and time-consuming.
- Secrets were treated as code add-ons, not infrastructure with a lifecycle of their own.

The cost and impact of poor secrets management practices stem from a lack of expectations around efficiency, which has a domino effect with negative consequences:



According to [IBM's Cost of a Data Breach Report 2023](#), “the global average cost of a data breach in 2023 was USD 4.45 million—a 15% increase over 3 years.”



Examples of breaches resulting from poor secrets management practices include:

Credentials stored in repositories	Uber , Dropbox , and Drizly suffered data breaches as a result of credentials stolen from Git repositories.
Failure to rotate secrets	49% of data breaches involved the use of stolen credentials, highlighting the need for regular rotation. Source
Unencrypted secrets in .env files	CISA security advisory for the Androxxgh0st Malware, targeting Laravel sites to download .env files. Source

Cost Benefits Of Modern Secrets Management

While a data breach poses the threat of potential cost, time wasted on inefficient secrets management by developers, DevOps, and security teams is immediate and recurring.

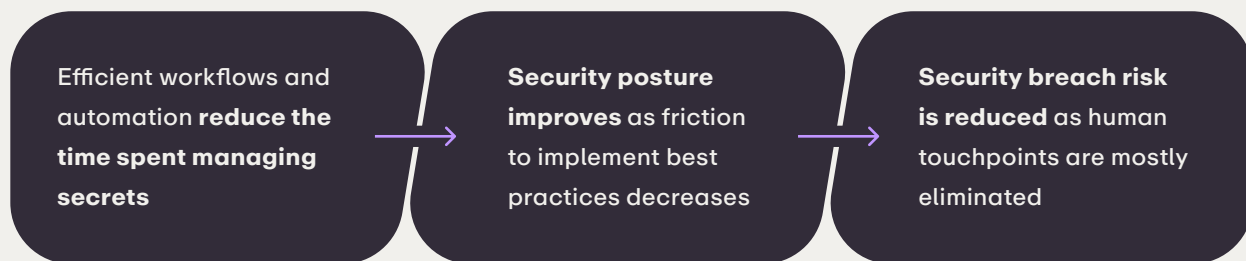
With a mindset shift towards automation and ruthlessly eliminating inefficiencies—secrets management can enter a new era—where the limitations and assumptions of old are exchanged for new possibilities.

Let’s compare some traditional secrets management workflows with their modern alternatives, using Doppler’s features as an example:

Traditional	Modern
Secrets sprawled across clouds, serverless, CI/CD, and Kubernetes	Secrets orchestration to sync secrets to any platform from a single source of truth
No predefined secrets structure	Projects and customizable list of environments
Confusing access control policy language	Access controls with intuitive UI
Synchronize changes to multiple environments using copy and paste	Apply updates to multiple environments in one UI operation
Missing secret detected through application deployment failure	Missing secrets notifications
Secrets duplicated across environments	Secrets referencing to eliminate duplication
Developers manually copy and merge secrets to development machines	Dedicated Development environment using the Doppler CLI for dynamic secrets injection



The benefits of implementing a modern and future-proof secrets management strategy have a domino effect that's the opposite of what we saw earlier.



Incremental improvements through slight enhancements to current processes won't get us to the future of secrets management. Transformational change is required to achieve security and productivity benefits while lowering the costs of managing secrets organization-wide.

Our customer success stories prove the time and cost savings you could expect from a next-generation secrets manager such as Doppler.



75% Faster Secrets Management

“Before Doppler, our engineers were spending roughly 5 hours every week managing secrets. Now, it's down to 5 hours or less per month.”



200% ROI

“With 20 developers, implementing a change in a .env file used to require 8 hours of work for all parties involved and occurred approximately twice a month. Now, this process is instant and failsafe.”



80% Faster Secret Management

“We reduced the sprawl of secrets, locked down access to secrets, streamlined the deployment of secrets, and improved developer onboarding and offboarding.”



Secret Audit Times Reduced By Over 90%

“Managing the lifecycle and versioning of thousands of secrets with Doppler has been magical. My time spent auditing our secrets portfolio has dropped drastically from one whole day to less than an hour.”



Quantifying The Potential

The benefits of modern secrets management are compelling. But how do you assess the potential cost savings in your own organization? It's a simple three-step process:

1. Research

Identify inefficient processes that have modern solutions (e.g., no manually managed secrets in local development)

2. Measure

Survey a selection of teams to get a representative sample of time spent managing secrets per week.

3. Summarize

Calculate the potential to be saved by using an estimated 70%-80% reduction in time spent managing secrets for the number of developers, DevOps, and security staff per month.

This process will provide you with a vital summary of your organization's current state of secrets management, enabling you to make data-informed decisions about evolving your secrets management strategy.

Before change, there must be awareness. By understanding the risks and unnecessary costs associated with traditional secrets management, businesses are empowered to make transformational changes, improving security and productivity.

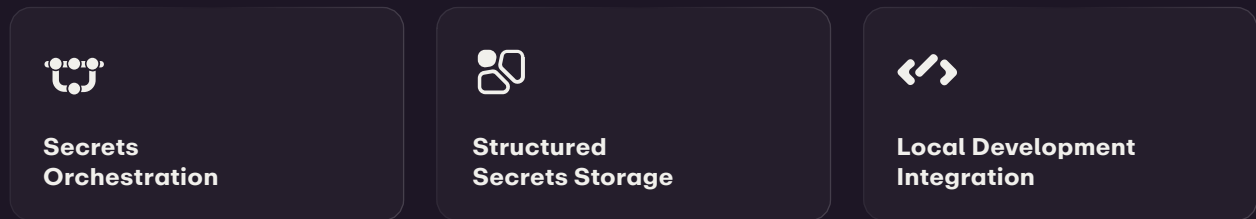
We'll now look at why Doppler is succeeding where other secrets managers have failed by understanding its modern and application-specific approach that meets the requirements of developers, DevOps, and security teams.



Doppler: A Modern Approach to Secrets Management

A modern secrets management strategy must deliver increased security and productivity while lowering costs. Doppler meets these requirements by removing all sources of friction in how secrets are managed and accessed.

At a high-level, Doppler has three unique capabilities which set it apart from traditional secrets managers:



Secrets Orchestration

Doppler’s key point of difference is its secrets orchestration model—providing a centralized hub for management and storage, with integrations for syncing secrets to where applications and infrastructure can most easily access them.

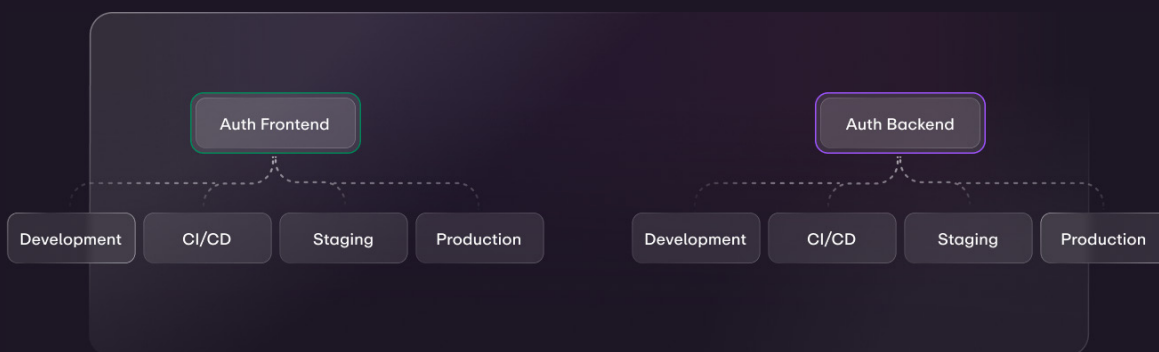




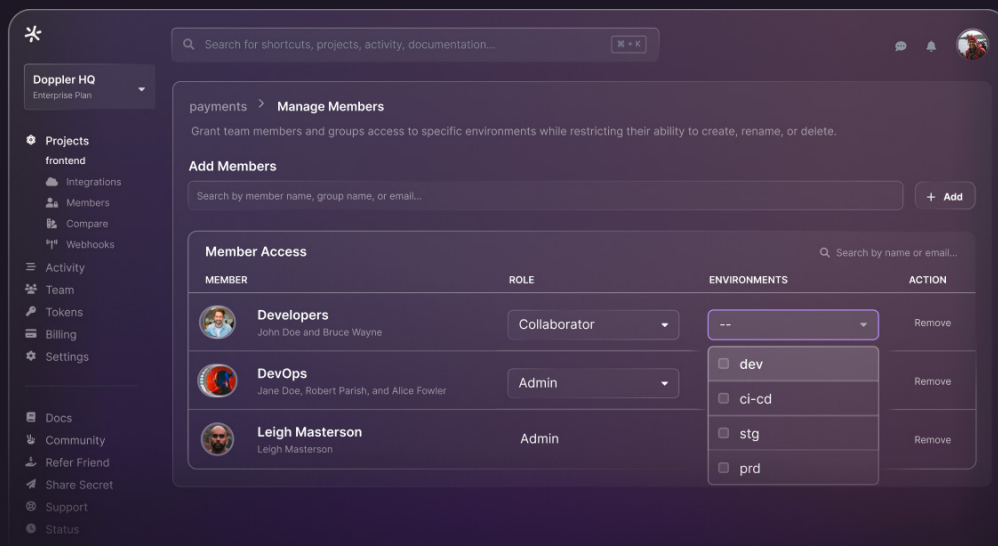
This provides teams with flexibility in how secrets are delivered to their applications and infrastructure, whether it's using integrations or Doppler's CLI, SDK, and API for injecting secrets at run time.

Structured Secrets Storage

Doppler provides isolated secrets storage for different applications through Projects, each with a customizable list of environments.



Because Projects standardize secrets storage, fine-grained access permissions per project and environment can be managed via the Doppler dashboard with no confusing policy language to learn.



Local Development Integration

Doppler Projects provide a dedicated Development environment—solving the time-consuming and manual chore of keeping locally maintained `.env` files in sync with upstream environments.

Traditional secrets managers are unable to provide secrets during local development as they're siloed within the confines of their respective cloud or platform. This is why, despite the pain and security risk of locally maintained `.env` files, they're still commonplace today.

The Development environment within each Doppler Project eliminates the need for hard-coded secrets. The Doppler CLI provides dynamic secrets access by injecting secrets into applications when launched via the command line or debug configuration within an editor or IDE.

The screenshot shows the Visual Studio Code interface. On the left, the 'DOPPLER' sidebar is open, showing a tree view of project files: address-validator, backend, frontend, payments, queues-manager, and shared. The main editor area is split into two panes. The left pane shows a file named 'dev_personal.x' with the following content:

```

1 #####
2 ## This file was generated by Doppler. When you make ##
3 ## changes to this file, they will be saved to your ##
4 ## config in Doppler as well. ##
5 ## ##
6 ## a 'null' value indicates that the secret is restricted ##
7 ## Restricted secrets may be overwritten, but cannot be read. ##
8 #####
9
10 DATABASE_URL: postgres://postgres@local/payments
11 FEATURE_FLAGS: |-
12   {
13     "Stripe": true,
14     "Braintree": false,
15     "ChargeBee": true;
16   }
17 LOGGING: dev
18 PORT: "3030"
19 PRIVATE_KEY: |-
20 ----BEGIN EC PRIVATE KEY-----
21 MHQCAOEETFp3mjgrvPQcDYu1MdeB8bqG8+94t2zomAw/EKUYvAcGBSjRBBAAK
22 oIQ00gEiUj7w0u5bpD00J/HkKzje2JjQ8Fde840NySjZFTQRzYFvESRc3Pvnu
23 wLzJMS1ppk28PFA3DAMAcTYvoAEYmg==
24 ----END EC PRIVATE KEY-----
25 SENDGRID_ID: Bxyy88DnX6an872UqW1zQ
26 SENDGRID_NAME: Doppler-payments-dev_personal_SENDRID-1697840221355
27 SENDGRID_SECRET:
28 SENDGRID_USERNAME:
29 SENDGRID_PASSWORD:

```

The right pane shows a file named 'index.js' with the following content:

```

1 const express = require('express');
2 const app = express();
3 const endpoints = require('./endpoints');
4
5 app.use(endpoints);
6
7 console.log('Starting server on port
8 ${process.env.PORT}');
9
10 app.listen(process.env.PORT);

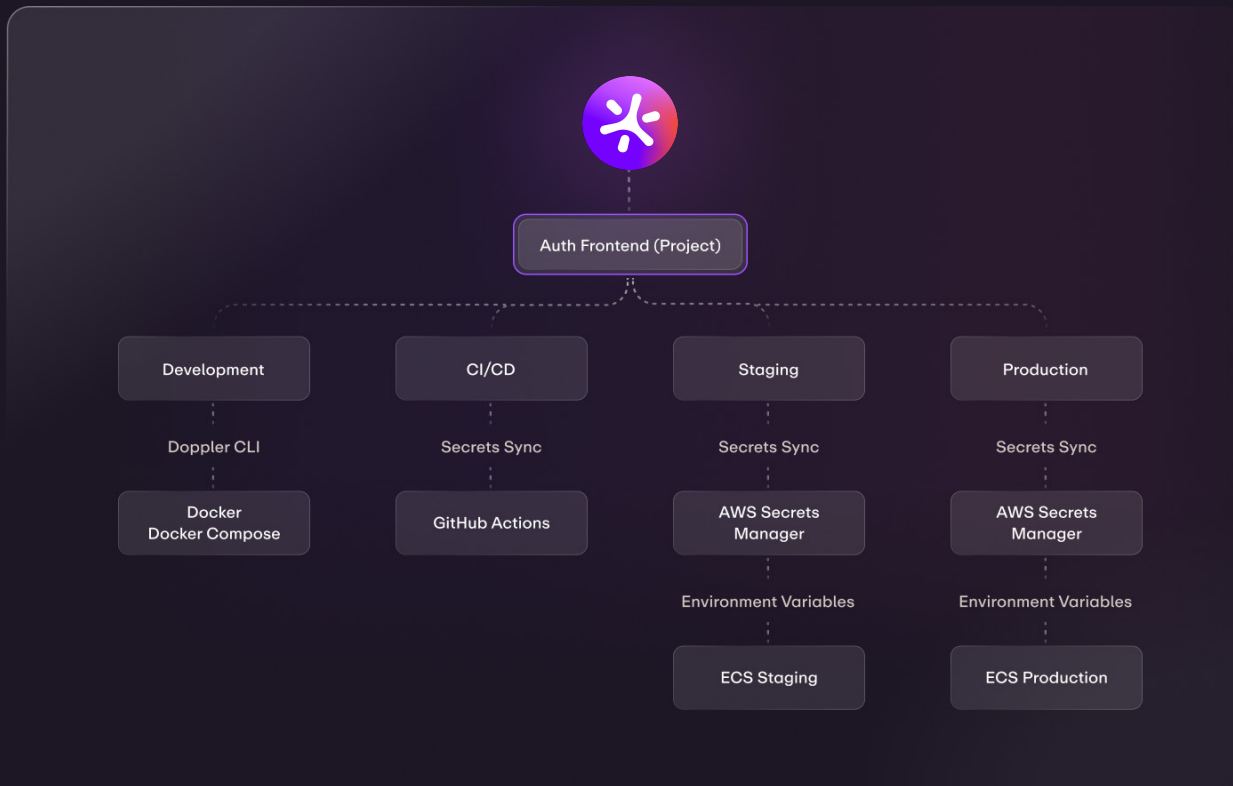
```




Bringing It All Together

Doppler’s secrets orchestration, structured secrets storage, and local development support combine to provide a consistent yet flexible methodology for managing secrets across an organization.


For example, a Project for a containerized application running in AWS ECS and integrated with AWS Secrets Manager to inject secrets as environment variables at runtime could look like the following.




That’s Doppler at a high-level. Now let’s explore Doppler’s features within the categories of:




Secrets Management



Automation



Governance



Local Development



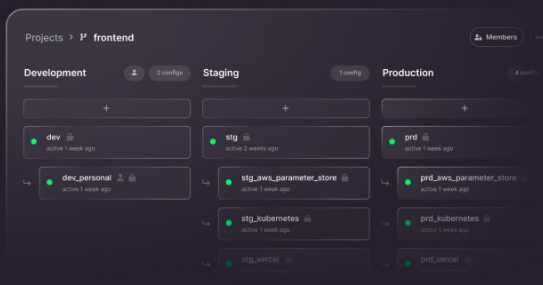
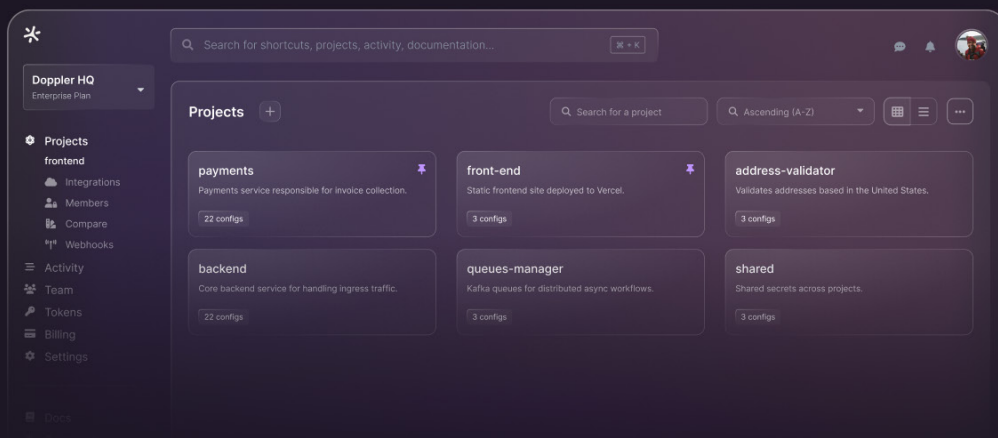
Secrets Management with Doppler

Empower teams with the tools and workflows to radically reduce the time spent managing secrets.

A Dashboard For DevOps and Developers

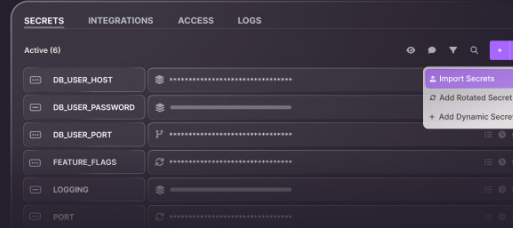
Onboarding is fast and effortless thanks to Doppler’s user-friendly dashboard.

Manage every secret from a single source of truth.



Sensible Structuring

Secrets are structured by Projects with a customizable set of environments—providing a mental model that makes sense for Developers and DevOps teams.



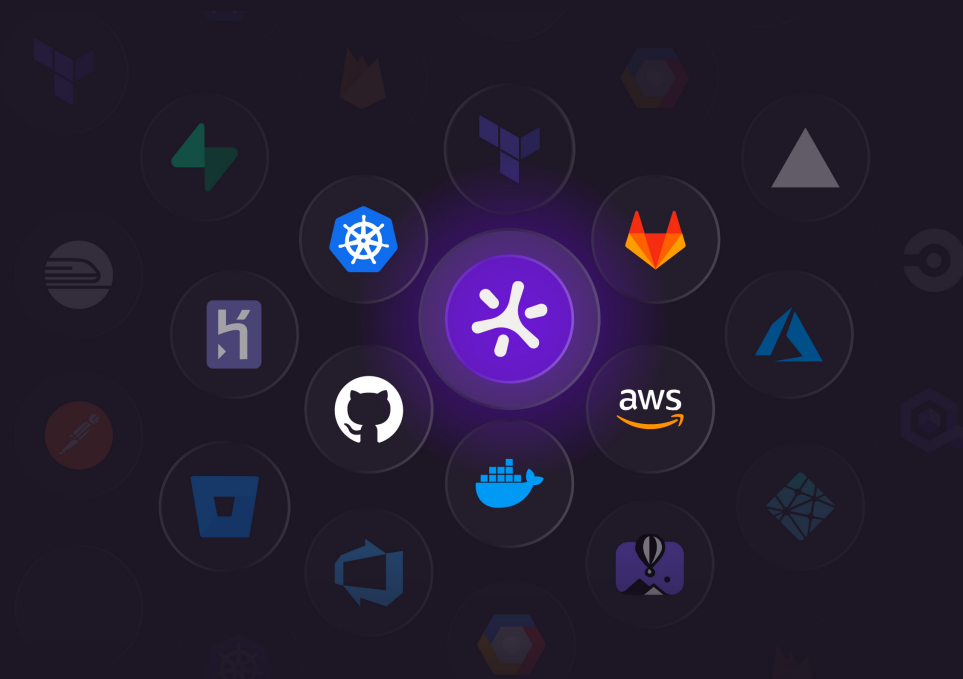
Editing Made Easy

The secrets edit page provides fast and intuitive workflows for managing every aspect of the secrets management lifecycle—including bulk importing, secrets sync integrations, versioning and access logs, one-click rollbacks, rotation and dynamic secrets.



A Single Source Of Truth To End Secret Sprawl

Secrets sprawl is now a solved problem thanks to Doppler's integrations that provide automated secrets sync to cloud secrets managers, CI/CD, serverless platforms, and Kubernetes.



Secrets Access Your Way

When you need additional flexibility for managing and accessing secrets beyond the Dashboard and integrations, Doppler has you covered.

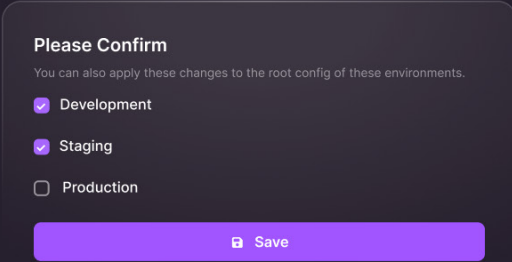
No More Missing Secrets

Get notified of configuration drift before misconfiguration occurs with missing secrets notifications in the dashboard.



Secrets Automation with Doppler

Automation is the key to maximizing efficiency and minimizing misconfiguration by removing all possible human touchpoints.



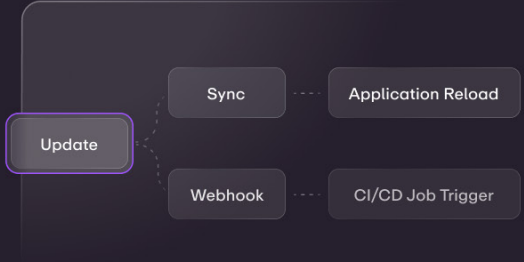
Please Confirm
You can also apply these changes to the root config of these environments.

- Development
- Staging
- Production

Save

Synchronize Secret Changes

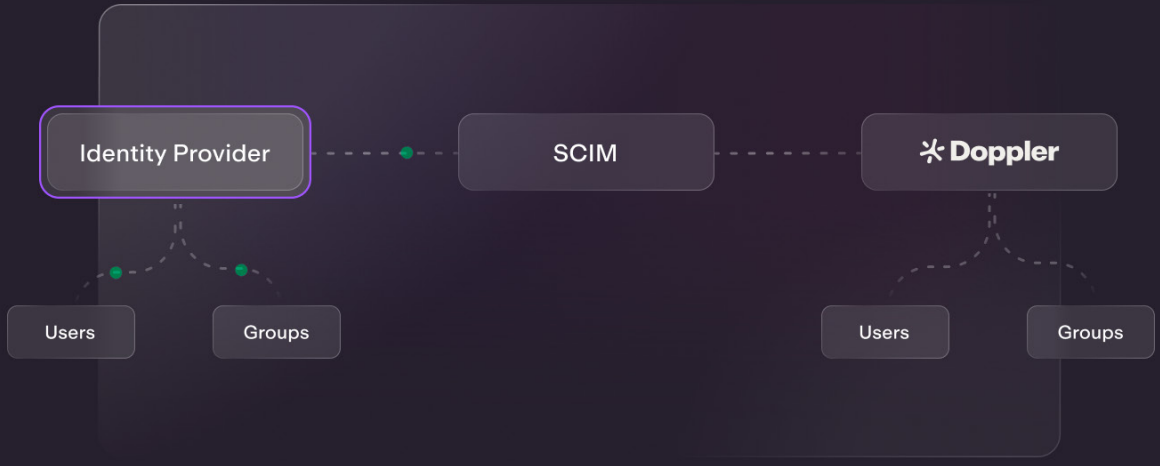
No more sending secrets over messaging platforms and error-prone copying and pasting.



```
graph LR; Update[Update] -.-> Sync[Sync]; Update -.-> Webhook[Webhook]; Sync -.-> Reload[Application Reload]; Webhook -.-> Trigger[CI/CD Job Trigger];
```

Automated Application Refresh

Deliver secrets to applications instantly with optional reloading on secrets sync, plus webhooks for event-driven workflows.



```
graph LR; IP[Identity Provider] -.-> SCIM[SCIM]; SCIM -.-> Doppler[Doppler]; IP -.-> U1[Users]; IP -.-> G1[Groups]; Doppler -.-> U2[Users]; Doppler -.-> G2[Groups];
```

Automated Principle Of Least Privilege

Automate team management and fine-grained secrets access from your identity provider using SCIM and groups to sync project and environment access within Doppler.

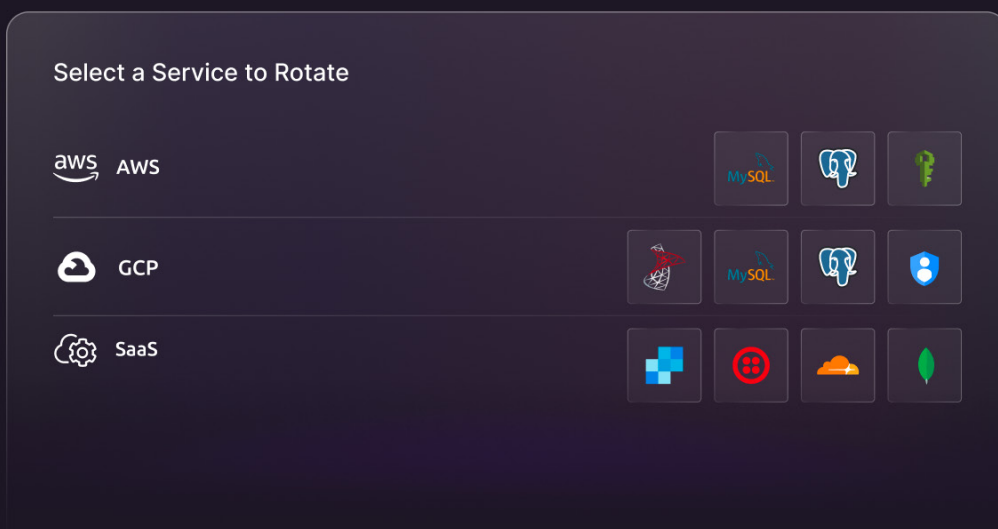


Secrets Rotation with Doppler

Remove the complexity of cloud-specific secrets rotation by centrally managing all rotations within the Doppler dashboard.

Secrets Rotation You Can Scale

Make multi-cloud secrets rotation possible for every team through Doppler's easy and streamlined configuration process.



Search by Secret Value
Supports only exact matches (ignoring all whitespace) for raw for secret values.

Search

SECRET NAME	PROJECT	CONFIG
OPEN_API_KEY	arch-bot	prd
OPEN_API_KEY	art-create	prd
OPEN_API_KEY	chalgpt-webapp	prd
OPEN_API_KEY	dash-qa	prd

Revoke, Find, Replace

Enable the rapid updating of revoked or ad-hoc rotated secrets with search by secret value.

Recurring Reminder

Reminder

Every days, starting

Cancel Create Reminder

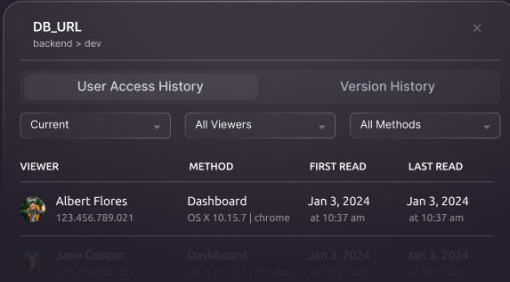
Rotation Reminders

Ensure secrets requiring manual rotation are updated as scheduled by notifying teams via email.



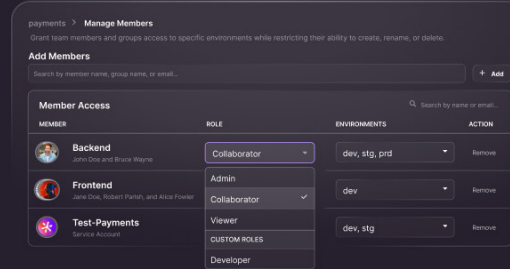
Governance with Doppler

Transform your secrets governance and audit capabilities with Doppler's enterprise-grade suite of access and observability solutions.



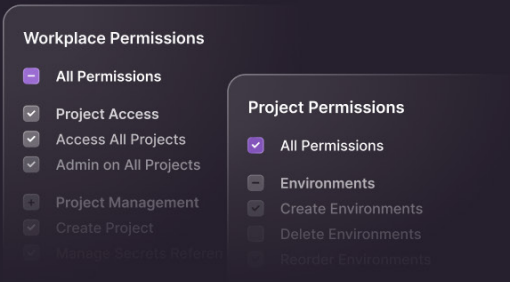
Single Source of Secrets Governance and Auditability

With increased productivity driving wide-spread adoption, Doppler provides you with a complete picture of all secrets activity, access, and version history across your organization.



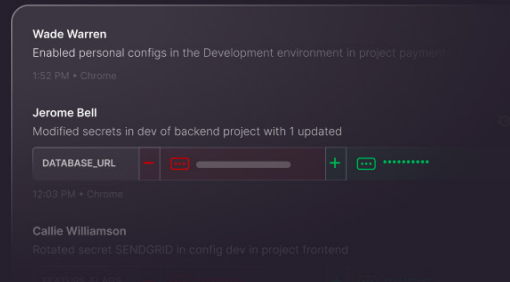
Increased Access Awareness

Manage and review member access and permissions for each Project from a single screen.



Fine-Grained Permissions Without The Pain

Replace confusing policy configuration languages with Doppler's customizable role-based access controls.



Simplified Secrets Observability

Gain instant visibility into all secrets operations in real-time through the Doppler dashboard, messaging platforms, and event-ingestion platforms.



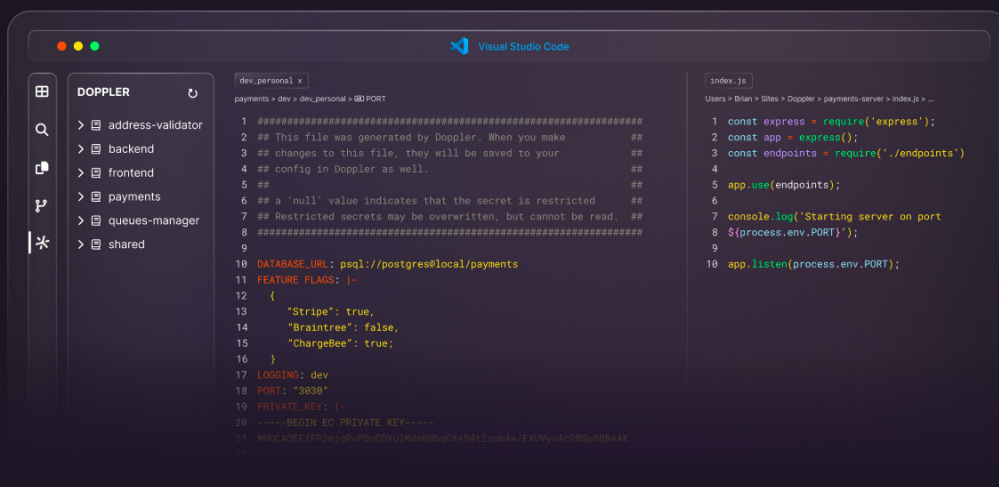
Local Development

Doppler’s first-class support for local development environments eliminates a whole host of productivity and security issues. With developers being the largest cohort of secret consumers, organizations have the most to gain in terms of cost reduction by streamlining inefficient processes affecting them.

Less Interruptions. More Flow.

The constant interruptions caused by breaking local development environments due to outdated .env files can be eliminated as the Development environment within each Project is now the shared source of truth for all team members.

Doppler also helps developers stay in flow, enabling secrets management tasks to be performed inside their development environment through editor integrations or the Doppler CLI.



No Secrets on Developer Machines

Hard-coded secrets are no longer needed during local development. The Doppler CLI dynamically injects the latest version of secrets into the application process via the command line or editor debug configurations.

```
temp - node doppler run -- node - 120x39

/tmp (*, backend.dev)$ doppler secrets
```

NAME	VALUE
DOPPLER_CONFIG	dev
DOPPLER_ENVIRONMENT	dev
DOPPLER_PROJECT	backend
PLUTO_TEST_KEY	sk_11ve_UR2UsZZgyPtbt0fV0jQXkvI1YAUBjCvoJ10bh3ntG2AxEWUqMzFa3BfMTD85k7kcl

```
/tmp (*, backend.dev)$ doppler run -- node
Welcome to Node.js v19.8.1.
Type ".help" for more information.
> process.env.PLUTO_TEST_KEY
sk_11ve_UR2UsZZgyPtbt0fV0jQXkvI1YAUBjCvoJ10bh3ntG2AxEWUqMzFa3BfMTD85k7kcl
```

Developer-Specific Secret Overrides

Secret overrides during local development are also available through user-specific Personal configs and shareable Branch Configs.

```
DATABASE_URL: ${common.dev.personal.D |
common.dev.personal.D ATABASE_URL
common.stg.personal.D ATABASE
common.stg.personal.D B_USER_HOST

FEATURE_FLAG:

LOGGING:

PRIVATE_KEY:
```



Doppler Fact Sheet

Managing secrets is a mission critical function. Here's why our customers trust us with their most sensitive data.



Industry Standard AES 256 GCM Encryption



SOC 2 Type 2 Compliant



Bring Your Own Key Encryption



3M+ Secrets Under Management



30+ Billion Secrets Read Every Month



49% of breaches involve credentials



99.99% Historical Annual Uptime



Doppler does not utilize AI technologies



Summary

The cost and security implications for organizations that fail to innovate cannot be overstated. The risks of security breaches from secrets sprawled throughout git repositories, .env files and other insecure methods can now be eliminated once a scalable and holistic approach is adopted.

The hallmark of modern secret strategy is a single source of truth for management and storage. With a centralized hub, secrets orchestration provides the means for syncing secrets to where applications and infrastructure can most easily access them—from local development to CI/CD, staging, and production.

Automation is the key to replacing all sources of inefficiency, friction, and unnecessary human touchpoints. By streamlining previously manual workflows, productivity increases—driving widespread adoption and, as a result, providing greater observability, auditability, and governance.

This is what an application-specific secrets manager delivers—meeting the operational needs of developers, DevOps, and security teams in a diverse multi-cloud world. This is what Doppler delivers.

Experience the future of secrets management by scheduling a demo with one of our solution engineers or sign up for a free trial today.



Enter the **new era** of secrets management.

Doppler's developer-first secrets management platform empowers teams to seamlessly orchestrate, govern, and control secrets across any environment at scale.

[Get a Demo →](#)

[Learn More](#)

Doppler