

//onboardbase

# App secret infrastructure for cloud-native dev teams



# Cloud-native engineering teams are facing a devops security crisis

- **Secret permissioning is complex** - More dev teams are remote and async, with many contract and junior devs
- **Dev tool stacks are growing rapidly** - The average cloud-native dev team uses **100+** different tools, including cloud providers and apps - all with their own set of app secrets.
- **Secret leakage is increasing, mostly via human vectors, not machine** - dev teams lack tools that are flexible enough to be used properly, and lack tools to mitigate mistakes.

**“Secret Chaos” is  
costly - both in  
security risks and  
developer  
productivity**

- **47%** of data breaches come from insecure app secret sharing.
- **37%** of engineering teams have experienced a breach due to improper sharing.
- **\$3.92m** is the average cost of a data breach.
- **55%** of engineers have had to delay the rollout of a new application due to poorly shared secrets.

# Onboardbase tames Secret Chaos

**Onboardbase is the single source of shared truth for app secrets and usage.**

It helps dev teams securely share and work with environment-specific configs at every development stage, synced across infrastructure without compromising security.

- **Automatic Sync** – Secrets are kept up to date across your environments and infrastructure, with 50+ integrations and growing
- **Great for Teams** – create, share, and clone configurations for easier collaboration.
- **Security** – Your secrets are end-to-end encrypted – your master keys are created on your devices, and never leave.

# Store. Sync. Collaborate. Securely and effectively.

Sync across teammates  
or cloud servers

Dante Lex  
Last seen 1 day ago · Karlistas-MacBook-Pro.local

Downloading secrets from onboardbase servers...  
Decrypting secrets using RSA Encryption...  
Decrypting secrets using AES Encryption...  
Creating a 24hrs Fallback Secrets file  
Injecting Environment Variables...  
Injected Environment Variables successfully  
Completely closed CLI process with status code of 0

Onboardbase dev

desktop-keys

Environment configs

desktop-keys

New Test

Env

Jobs

Merge Request

Activity

Integrations

People

Compare

Webhooks

List

Code

prod

2 environment(s)

4 variable(s)

+

↑

⚙

AZURE_CLIENT_ID	VALUE
Added Aug 23, 2022 by Dante Lex	.....
AWS_PG	VALUE
Added Aug 01, 2022 by Dante Lex	.....
AWS secret	

Project  
environments

prod

2 environment(s)

+ Add new environment

prod ✓

stag

Push requests  
from teammates

Ej to local

✓

🗑

STRIPE_SECRET_KEY	VALUE
Added Sep 06, 2022	.....
STRIPE_ENDPOINT_SECRET	VALUE

# What makes Onboardbase unique?

- **Designed for today's mixed-role, remote and async teams** – Fine-grained push-and-pull secret requests enables right kind of sharing across all environments and team roles
- **Robust automation and sharing** – secrets are kept automatically up to date with rotation and policy control; and create, share, and clone configurations for easier collaboration.
- **Assumes humans will make mistakes** – Ongoing codebase scanning for leakage with pre-deployment detection and automated

# Existing solutions force dev teams to trade off risk and productivity

## “Post-it Note” World

- Sharing notes insecurely in Slack, email or text message, or even Google Docs
- No centralized source of truth; no automation, secret rotation, or oversight
- Depends on synronous comms (tough for async team) - and bad for productivity

## Existing Secret Management Tools

- Older tools (Vault, etc) require dedicated security engineering team and overhead
- Newer platforms (Doppler, etc) aren't built for complex team types and lack important ongoing security measures

Still in beta

**\$ 3,000 MRR**

**👤 410 users**

**👥 260 teams**

**📈 75% increase in productivity**

*reported by our customers due to time saved  
sharing and securing secrets.*



Michael, *Intelliculture*

Onboardbase is collaborative secure project development.



Basile, *Embarque*

Onboardbase makes it easy to secure dev secrets across the entire organization, no matter the tech stack or tool we're using.



Varun, *Ad Auris*

I love the ease of use. My favourite is the ability to upload a .env and it automatically parses the file and inputs them into fields



Every dev team needs secret management

26 million devs in the world  $\times$  25% at SMB  $\times$  \$6/user/mo  
**= \$468 million annually TAM**

---

5 million devs in the US  $\times$  25% at SMB  $\times$  \$6/user/mo  
**= \$90 million annually SOM**

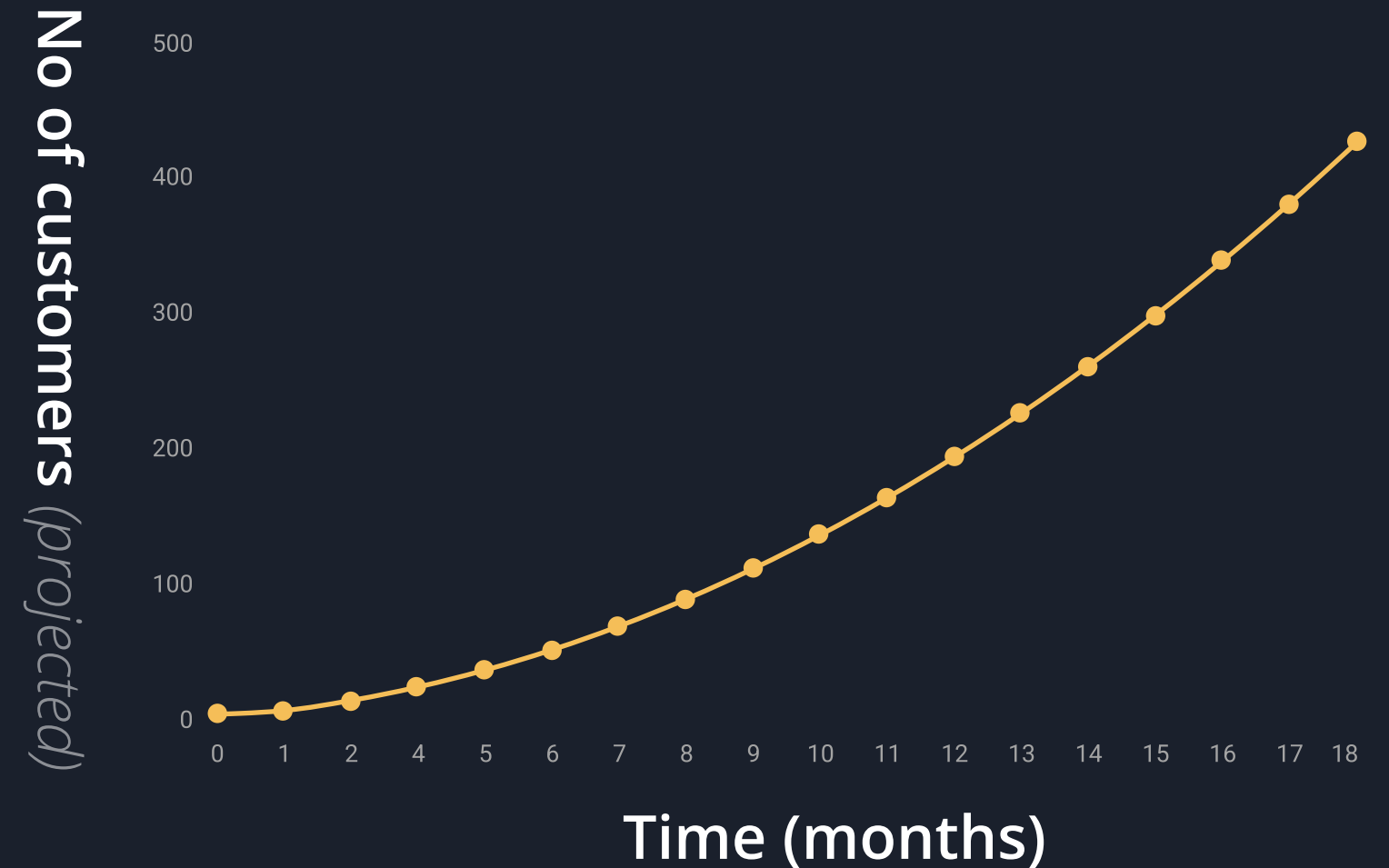
---



- I'm Dante; a software engineer and product designer
- 10+ years building and designing developer tools to improve productivity for thousands of devs.
- Part of 🏠 ODX, 📄 Pioneer, 🍄 Magic.do and XX. Worked with companies like Pitchly, Summitech and Tribe
- Led and joined teams, both as a FTE and a contractor.
- Leading a team of 5 at Onboardbase. 4 Engineers, and myself.

## Raising \$1m to invest in

- **Product development:**  
*focus groups with respected devs*
- **Talent:** *developers and customer success*
- **Customer acquisition:**  
*500 paying customers over the next 18 months*



**Our vision is to eliminate the tradeoff between developer productivity and security to usher in a new era of secure-by-default, seamless development.**

As security has "shifted-left" earlier into the development lifecycle, individual developers have taken on the burden of security practices – human security is the primary risk factor, not machine security. A critical vector in developer security is secret and environment management.

Phase one of this is building secret management, followed by a broader "git pull security" environment synchronization product, followed by a complete cloud development environment and deployment

Thank you!

//onboardbase

dante@onboardbase.com