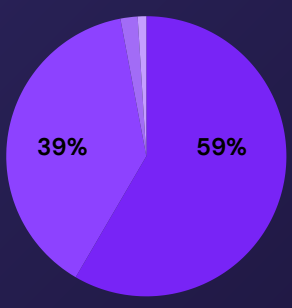
Nightfall AI

2024 State of Secrets Report

Do you know where your most sensitive secrets are shared across the cloud? Based on our findings, odds are that some have slipped through the cracks.

Read on to learn more about where your passwords and keys are sprawled—as well as what best practices you can implement to clean up your tech stack.

WHAT KINDS OF SECRETS DID WE LOOK FOR?

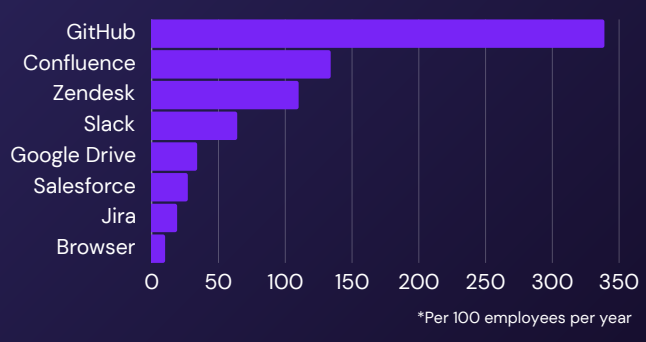


- Passwords
- API Keys
- Database Connection Strings
- Cryptographic Keys

171k+

Secrets discovered across SaaS apps and GenAI tools

WHERE DID WE FIND SECRETS?



HOW MANY SECRETS DID WE FIND?

API Keys — 7

Passwords — 8

7 API keys and 8 passwords discovered per 100 employees per week

WHERE DID WE FIND PASSWORDS?

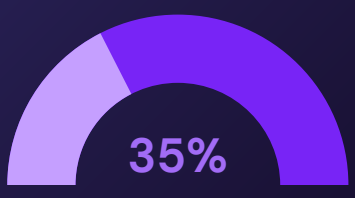
54% GitHub

23% Confluence

15% Zendesk

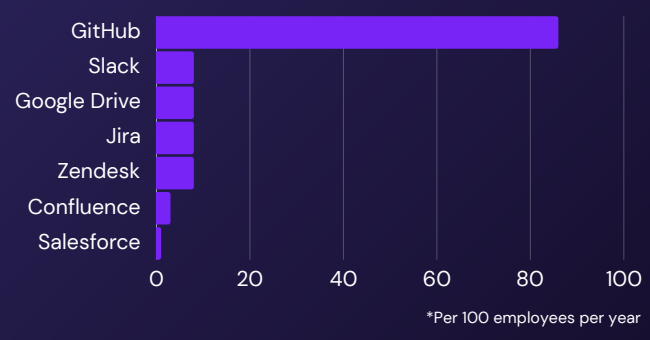
8% Slack

HOW MANY ACTIVE KEYS DID WE FIND?



2.3 active API keys detected per 100 employees per week

WHERE DID WE FIND ACTIVE API KEYS?



WHAT KINDS OF API KEYS DID WE FIND?

- AWS
- AZURE
- CONFLUENCE
- CONFLUENT
- DATADOG
- FACEBOOK
- GCP
- GITHUB
- GITLAB
- JIRA
- JWT
- OKTA
- PAYPAL
- PLAID
- SALESFORCE
- SENDGRID
- SLACK
- STRIPE
- TWILIO
- TWITTER

WHAT ARE BEST PRACTICES FOR SHARING SECRETS?

1. Scan for sprawled secrets

Conduct both historical and real-time scans to maintain visibility into where secrets are shared across SaaS and GenAI apps, as well as email and endpoints.

2. Automate remediation

Configure real-time notifications and automated workflows to immediately handle secrets through actions like deletion, redaction, rotation, or encryption.

3. Rotate API keys

Rotate API keys regularly and create a clear process for updating and distributing new keys.

4. Keep it all encrypted

Share secrets securely using password managers or end-to-end encryption solutions to encrypt information before it leaves the client side.

5. Coach employees

Implement real-time notifications to maintain year-round awareness of security policies and best practices.

6. Self-remediate violations

Empower employees to address their own policy violations so security teams can concentrate on building a stronger security culture.