

Secure your code from creation to release, with automated secrets detection

THE APPLICATION SECURITY AT THE SPEED OF DEVOPS CHALLENGE

01 Software development is running at the speed of DevOps

DevOps is slowly but surely becoming the gold-standard for software delivery. The speed and agility it enables makes it the obvious choice for successful organizations.

No matter where you are on the DevOps adoption curve, the speed at which code is delivered is adding to the risk of introducing vulnerabilities or misconfigurations with large-scale implications.

02 Turning developers into hackers' targets of choice

Unlike any other users in your organization, developers have privileged access to every component across your stack and own the keys to the house.

Protecting the credentials and secrets they use to securely connect the distributed components of your software is of paramount importance.

03 Secrets are out in the open

Developers write code with the best of intentions, but they still end up committing credentials and sensitive data in public and private repositories. With more than 2 million secrets* exposed on the public GitHub and heaps more in the private repositories, why should attackers look at anything else other than the developers' source code?

*Our research on the public GitHub, published in The State of Secrets Sprawl 2021, shows...



Enter GitGuardian

- GitGuardian Internal Monitoring is an automated secrets detection and remediation solution for your organization's git repositories and pipelines. Secure every step of the Software Development LifeCycle, from code creation to release.
- Complement your secrets management efforts with a final layer of automated detection.

GitGuardian for Internal Repositories Monitoring

Our commitments

Fits your tech stack like a glove

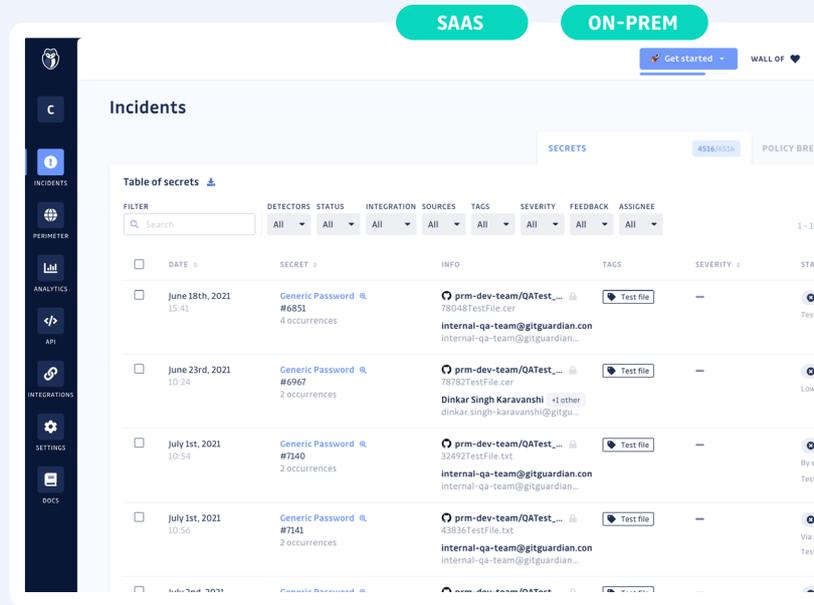
- Connect to your VCS with native GitHub, GitLab and Bitbucket integrations
- Harden your pipeline with native CI/CD integrations (Circle CI, Travis CI, GitHub Actions, and more...)
- Integrate the secrets detection engine across any tools in your stack with our REST API

All your previous leaks, and the next ones

- Run historical scans on all your repositories for a complete healthcheck
- Don't miss any leaks with detectors covering 250+ types of secrets
- Stay focused and reduce alert fatigue with a 91% True Positive rate

No falling through the cracks

- Bring every alert to your SIEMs and ITSMs (PagerDuty, Splunk, Sumo Logic, and more...)
- Automate incidents triage, assignment and resolution with templated playbooks
- Verify incidents resolution with on-the-fly secrets presence and validity checks



Shift left, and extend right

- Bring developers and AppSec together with collaboration features and feedback collection
- Empower your developers with the ability to resolve their own incidents
- Configure pre-commit git hooks to detect secrets locally before they enter the VCS

We're putting the Sec in DevSecOps...



Letting the authors solve their own problems before they get to the reviewer has significantly improved visibility and reduced the remediation time from multiple days to minutes or hours. Given how time-consuming code reviews can be, it saves some of our more scarce resources. There is easily a 30-hour improvement on time to remediation, which is about an 85% improvement.

Danny, Chief Software Architect

...and developers are loving it.

With a total of **110k** installs on the GitHub Marketplace, GitGuardian is the most popular security app used by developers.



GitGuardian
By GitGuardian
GitGuardian provides real time secrets detection and security policies enforcement across all your repositories
↓ 110k installs



Snyk
By snyk
Find, fix (and prevent!) known vulnerabilities in your code
↓ 49.3k installs



Start your journey to secrets-free source code

Contact sales at gitguardian.com/contact-us to schedule a demo or to learn more about how we can help you secure your code.

sales@gitguardian.com • [f](#) [in](#) [gh](#) [tw](#)