GitGuardian

Are your secrets... truly secret?

GitGuardian helps organizations secure software development with automated secrets detection & remediation for private or public source code.

SECRETS ARE THE KEYS TO YOUR KINGDOM

Secrets tie together the building blocks of modern software by creating a secure connection between your cloud infrastructure, APIs, databases, microservices, and many other components.

This is why your secrets should be kept...secret. Unfortunately, this is often not the case. In 2021, GitGuardian found more than 6 million secrets exposed in public GitHub.

ATTACKERS DON'T HACK, THEY LOG IN.

Every day, we find 10,000 secrets on GitHub. Leaving secrets in source code gives attackers easy access to your systems. Even worse, you may never know they were there – or how they got in.

When valid credentials fall into the wrong hands, penetration, lateral movement across your IT systems and services, privilege escalation, turn into simple and unsophisticated operations.

```
database = aws_lib.connect("AKIAF6BAFJKR45SAWSZ5",
  "hjshnk5ex5u34565AWS654/JKGjhz545d89sjkja")
```

THERE'S MORE TO SECRETS THAN WHAT MEETS THE EYE

Secrets often strike the eye. The random sequences of characters are hard to miss, yet the human eye is not trained to scan thousands of lines of code and they often go unnoticed during code reviews.

THE GITGUARDIAN ADVANTAGE

GitGuardian has been monitoring every single commit on public GitHub since 2018. With over 3 billion commits scanned, our secrets detection engine has been trained for speed, accuracy and precision, it:

- supports 350+ types of secrets
- detects secrets in less than 4s on average
- delivers a True Positive rate of 91%

#1 SECURITY APP ON GITHUB MARKETPLACE

Trusted by security • Loved by developers

align · AUTOMOX · cloudbakers · DATADOG · orange · FRED HUTCH CURES START HERE · GENESYS · instacart · iress · Maven Wave · MIRANTIS · NOW: Pensions · SEEQUENT · stedi · talend

GITGUARDIAN INTERNAL MONITORING

APPSEC • DEVSECOPS

GitGuardian for Internal Monitoring secures your software development lifecycle from the first line of code to the last build. Enforce policies across your VCS, DevOps tools, and infra-as-code configurations to reduce the risk of secrets exposure.

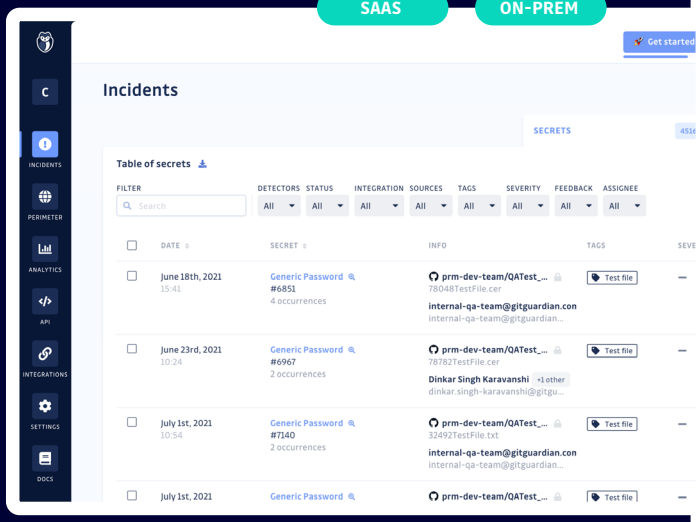
Monitoring
Scan your GitHub, GitLab, and Bitbucket repositories, CI pipelines and developer environments continuously for hardcoded secrets

Detection & Alerting
Get your alerts delivered wherever you are
PagerDuty splunk> slack DISCORD

Developer-driven remediation
Collaborate with your developers and empower them to remediate incidents by themselves

Shift Left
Shift security testing left with the GitGuardian CLI and API to prevent your secrets from getting exposed

SAAS ON-PREM



orange instacart GENESYS AUTOMOX SEEQUENT
iress stedi NOW: Pensions cloudbakers

GITGUARDIAN PUBLIC MONITORING

THREAT INTELLIGENCE • INCIDENT RESPONSE • RED TEAM

GitGuardian for Public Monitoring scans GitHub round the clock for your secrets and sensitive data. Keep an eye on your developers' activity, even on personal public GitHub repositories.

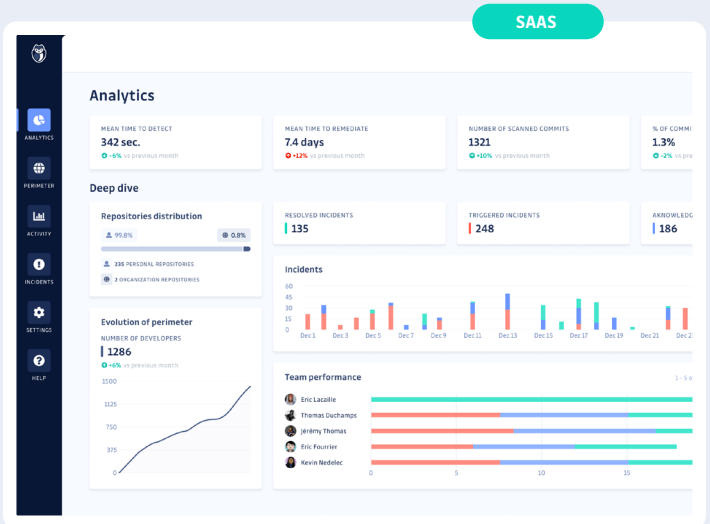
Monitoring
Map your attack surface on GitHub and monitor a perimeter including every developer related to your organization

Detection & Alerting
Get your alerts delivered in real-time, at the right place and never miss on a leak again
PagerDuty splunk> servicenow Jira

Remediation
Collaborate with the developers involved and collect their feedback to prioritize and remediate incidents faster

Threat hunting
Search public GitHub for your sensitive data (IP addresses, project codenames, licenses...)

SAAS



talend MIRANTIS align FRED HUTCH Maven Wave

Start your journey to secrets-free source code

Contact us at gitguardian.com/contact-us to talk to our experts
and to learn more about how GitGuardian can help you secure your code.

sales@gitguardian.com •