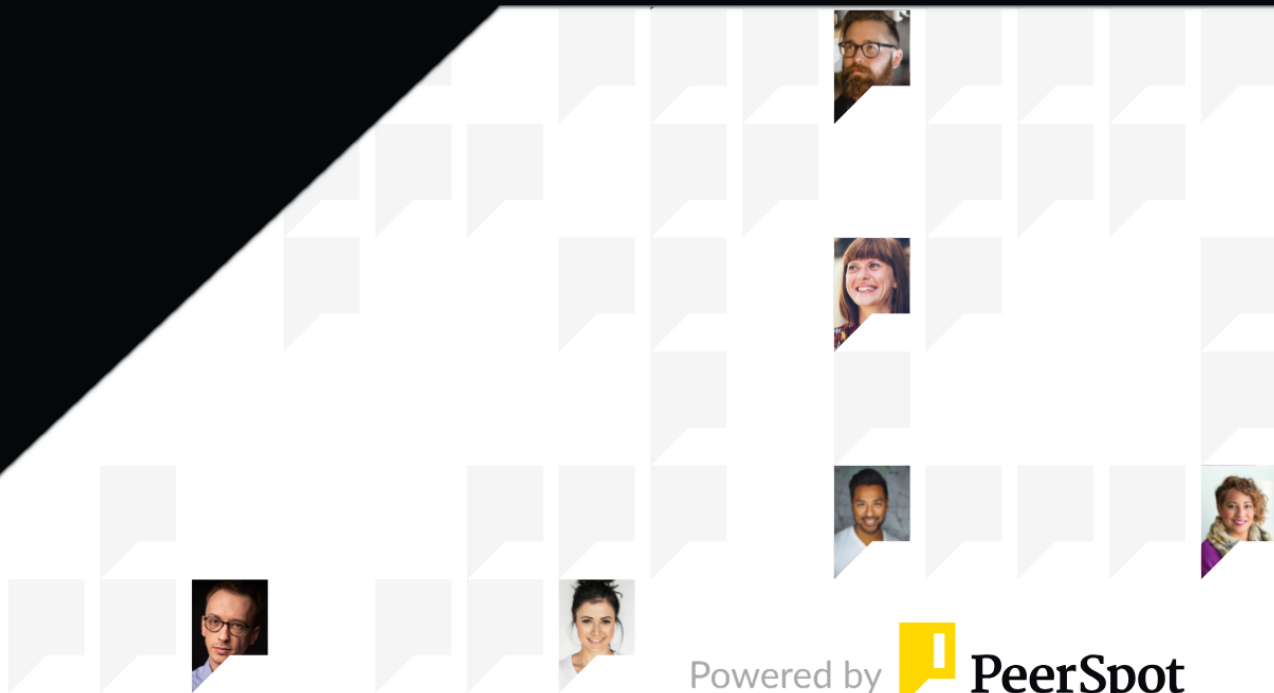


aws marketplace

GitGuardian Platform

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 13

Other Solutions Considered..... 14 - 16

ROI..... 17 - 19

Use Case..... 20 - 25

Setup..... 26 - 28

Customer Service and Support..... 29 - 31

Other Advice..... 32 - 35

Trends..... 36 - 37

About PeerSpot..... 38 - 39

Product Recap



GitGuardian Platform

GitGuardian Platform Recap

GitGuardian is the credential layer security platform for securing the secrets that let code, machines, and AI agents access systems and act as trusted identities. API keys, tokens, passwords, and other secrets carry real access. When they leak, attackers do not need to break in, they can log in. The scale of the problem keeps growing: 28.6 million new secrets were exposed on public GitHub in 2025, a 34% year-over-year increase and the largest jump on record.

GitGuardian finds the secrets that matter across an organization's entire secrets surface, inside and outside the perimeter. Internal Secrets Monitoring detects hardcoded credentials across private repositories, CI/CD pipelines, container images, cloud configs, and collaboration tools like Slack, Jira, Confluence, and Google Drive, using 550+ detectors with live validity checks that confirm each secret is active before it hits your queue. Public Secrets Monitoring scans public GitHub (1B+ commits per year) and DockerHub in real time for corporate secrets exposed online. Developer Endpoint Protection extends coverage to the developer machine itself: config files, shell history, MCP configs, and files persisted by AI coding agents like Claude Code, Cursor, and Copilot. AI Hooks add runtime guardrails inside the agents, checking prompts before they are sent.

For every secret it finds, GitGuardian reveals context and blast radius. NHI Governance supplies that identity layer, discovering every machine identity across repos, CI/CD, cloud, and collaboration tools, attributing ownership, scoring risk, helping configure rotation policies, and surfacing continuous compliance evidence for PCI-DSS v4.0, NYDFS, DORA, NIS 2, and NIST 800-53.

The detection surfaces find what's leaking. The identity layer connects each leak back to who owns it and what it accesses. One closed loop, from a developer's laptop to public GitHub. Honeytokens alert teams the moment an attacker uses a decoy credential.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“GitGuardian Platform has positively impacted our organization by improving our visibility into credential exposure and reducing the time it takes to identify and respond to leaked secrets; it also gives developers earlier feedback so security issues can be addressed closer to the source instead of becoming larger incidents later.”



Validated user

Consultant at a outsourcing company with 201-500 employees



“My impression of the GitGuardian Platform's capability to detect secrets in real time has been really amazing, because it lets us protect or block the pipelines in which we deploy new applications so we can acknowledge when a secret is hardcoded in a repository, or when we have already hardcoded secrets within templates in our repos.”



Ney Roman

DevOps Engineer at Deuna



“Our company has remained very safe in this regard because we need to secure our data effectively, being in the insurance reinsurance sector.”



Sanket-Shinde

Senior Engineer at a insurance company with 10,001+ employees



“A high number of our exposures are remediated by developers before security needs to step in, as the self-healing playbook process engages them automatically. This results in issues being resolved within minutes, saving significant effort from the security team in tracking down or communicating with developers.”



Ari Kalfus

Senior Manager, Product Security at DigitalOcean



“GitGuardian Platform has positively impacted our organization during the evaluation phase as this is a new realm.”



Brad Dyke

DSRE Director Of Dev Ops/Operations (Management Executive) at a outsourcing company with 51-200 employees



“GitGuardian Platform has impacted my organization positively by allowing us to identify usually exposed credentials earlier, reducing the time spent on manually checking repositories where credentials have been exposed, and it also gives better visibility into the status of security findings and their remediation.”



Validated user

Developer at a healthcare company with 1,001-5,000 employees



“The reduction of security leaks since we implemented GitGuardian Platform has been drastic and we have brought the indicator down to zero percent of secrets revealed within the code.”



Antonio Tirado Peña

Directo de TI at Instituto de Innovación Ciencia y Empresa

What users had to say about valuable features:

“In my experience, the best features of GitGuardian Platform include real-time secret detection, which is invaluable for catching credentials close to when they are introduced rather than finding them weeks later. The second feature is historical repository scanning. Additionally, it has CI/CD integration, can integrate with multiple Git platforms, offers custom detectors, provides context-aware detection, and allows for severity and prioritization of issues.

“The first three features have saved us considerably, particularly the real-time secret detection, while we initially also depended on historical repository scanning. As a DevOps professional, CI/CD integration is critically important to me..”

PrinceKumar7

Cloud Engineer at a computer software company with 501-1,000 employees

[Read full review](#) 

“The best features GitGuardian Platform offers that stand out most for me are the secret key detections and real-time alerts. I also find the incident tracking and remediation workflow useful because it makes it easier to understand, identify, investigate, and address exposed credentials.

“GitGuardian Platform has impacted my organization positively by allowing us to identify usually exposed credentials earlier, reducing the time spent on manually checking repositories where credentials have been exposed, and it also gives better visibility into the status of security findings and their remediation. GitGuardian Platform offers a more structured way, and we can quickly identify exposed secrets by this process, assign them to the right person, and track the remediation until it is resolved. It reduces the manual effort of coordinating and following up with the security findings..”

Validated user

Developer at a healthcare company with 1,001-5,000 employees

[Read full review](#) 

“The best features GitGuardian Platform offers are secret detection and real-time monitoring, which are probably the most useful for us; I also appreciate the alerting and incident investigation capabilities because they make it easier to trace when a secret was exposed and coordinate remediation with the development team.

“The real-time monitoring and alerting features of GitGuardian Platform have significantly helped my team respond to incidents; for example, the alerting has helped us catch exposed credentials shortly after they were committed rather than finding them during a later security review, and in one case, the team was notified the same day, allowing us to revoke the key, replace it, and clean up the repository before it caused any downstream impact.

“Another useful aspect of GitGuardian Platform is the visibility it provides to security and development teams into secret exposure across repositories; the remediation workflow and historical context around alerts are also helpful when investigating whether a credential is still active or when determining immediate action..”

Validated user

Consultant at a outsourcing company with 201-500 employees

[Read full review](#) 

“The best features for me are automated secret detection, repository monitoring, and clear alerts for exposed credentials. I also find the ability to prioritize findings and track remediation useful because it makes it easier to quickly identify high-risk secrets and ensure they are properly addressed.

“The feature I rely on most day-to-day is automated secret detection and repository monitoring. It continuously helps identify exposed API keys, tokens, passwords, and other credentials across repositories, so I do not have to manually review every change for potential leaks. It is especially important in my workflow because I work with security testing and code review, and catching a credential early allows me to investigate and remediate it before it becomes a larger security issue.

“GitGuardian Platform has improved our security posture by giving us better visibility into exposed secrets across repositories. It has also made my daily workflow more efficient because I can quickly identify, investigate, and remediate leaked credentials instead of relying entirely on manual code reviews. Overall, it has helped make secret detection a more consistent part of our deployment and security process..”

Validated user

[Read full review](#) 

Cyber Security Analyst at a tech vendor with 51-200 employees

“GitGuardian Platform's best features include automatically detecting issues in API keys, tokens, and passwords.

“The automatic detection feature helps my team and workflow tremendously by saving a lot of time because everything is automatic now and we don't need to scan manually. This has saved considerable time and makes it easy to scan the whole project and find whatever issues exist.

“Regarding additional features, the main focus was the ability to scan our project, CICD workflow, and other tools we are using to identify issues in the initial phases so that we can fix them easily and ensure our system has more comprehensive vulnerability scanning.

“GitGuardian Platform has positively impacted our organization by helping to scan issues in early stages so that we can make decisions and fix them easily. It aids in automatic deployment whenever there is no vulnerability, allowing us to deploy our services without any impact or additional checks, thus saving a lot of time.

“Earlier, when we had a security repository or CICD process, we were taking about four to five days to scan all those things and maintain documentation to reduce vulnerabilities and keys. However, with GitGuardian Platform, we have reduced that time to within a single day to perform all activities..”

Validated user

Senior Software Engineer at a consultancy with 51-200 employees

[Read full review](#) 

“GitGuardian Platform has good integration with Git. It works well with pull requests and Git actions. It does not have too much difficulty with Docker images, different CI/CD environments, Ansible, Puppet, and so on. The current integration to Confluence, Jira, and Slack for working with different environments is valuable for bringing the common form of tools into this particular style tool and having ease of work with those environments.

“All integrations including Git, Jira, Slack, and CI/CD environments add value for our team, but they have to happen in a specific process because the actions generate analytics. Those analytics drive up through Jira and Confluence and so on to generate analytic reporting. It is all important, and there is not just one tool.

“GitGuardian Platform meets the CDE security requirements guidelines specified for secops and infosec. I would describe the overall user experience and interface design of GitGuardian Platform as usable and functional..”

Brad Dyke

DSRE Director Of Dev Ops/Operations (Management Executive) at a outsourcing company with 51-200 employees

[Read full review](#) 

Other Solutions Considered

“We did not previously use a different solution. We used open source and manual processes. Now we are looking for a consolidation platform to do the same work..”

Brad Dyke

[Read full review](#) 

DSRE Director Of Dev Ops/Operations (Management Executive) at a outsourcing company with 51-200 employees

“Before choosing GitGuardian Platform, I did not evaluate other options. I was searching and found this platform to provide a better solution, which led me to utilize it..”

Validated user

[Read full review](#) 

Senior Software Engineer at a consultancy with 51-200 employees

“We previously relied more on built-in repository scanning and manual checks rather than a dedicated secret management monitoring platform, and we moved to GitGuardian Platform because we wanted centralized visibility, more consistent detection across repositories, and faster alerting and remediation workflows..”

Validated user

[Read full review](#) 

Consultant at a outsourcing company with 201-500 employees

“Earlier, we were using some Git-related cloud tools for scanning, such as SonarQube for finding issues and fixing vulnerabilities. However, now we are using GitGuardian Platform, which is quite helpful..”

Validated user

[Read full review](#) 

Senior Software Engineer at a consultancy with 51-200 employees

“Before choosing GitGuardian Platform, we looked at a few alternatives, mainly GitHub Advanced Security and GitLab's built-in security capabilities; we compared them based on secret detection coverage, alerting, integrations, and how easily the solution could fit into our existing development workflow..”

Validated user

[Read full review](#) 

Consultant at a outsourcing company with 201-500 employees

“The main factors that influenced my decision to evaluate GitGuardian Platform over other solutions include the need for a centralized single pane of glass of governance and compliance, which has been very fractured over the past three years. But now companies are starting to understand what these look like.

“Before choosing GitGuardian Platform, I am in evaluation of three different vendors. I cannot disclose those at this time due to NDA agreements, but GitGuardian Platform is and was actively being compared to two other vendors at this time..”

Brad Dyke

[Read full review](#) 

DSRE Director Of Dev Ops/Operations (Management Executive) at a outsourcing company with 51-200 employees

ROI

Real user quotes about their ROI:

“I would expect GitGuardian Platform to not require hiring additional resources, but to more effectively use the resources we have on hand now regarding return on investment..”

Brad Dyke

DSRE Director Of Dev Ops/Operations (Management Executive) at a outsourcing company with 51-200 employees

[Read full review](#) 

“I do not have quantified ROI figures because our team has not tracked them separately. For us, the return is more about reducing security risks and avoiding costs than achieving a direct, measurable financial benefit..”

Mir Shahzad Mubeen

CTO at Honeycomb AI

[Read full review](#) 

“It does not require any maintenance on our end as it has been working autonomously. I am unaware of new versions, but what we have been using has not required maintenance..”

Kingsley Zikora

Senior DevOps Engineer

[Read full review](#) 

“Regarding the return on investment, I do not have exact metrics, but in practice, it has reduced manual effort to check repositories and follow up on findings. The biggest improvement has been catching potential exposures earlier and shortening the remediation cycle..”

Validated user

Developer at a healthcare company with 1,001-5,000 employees

[Read full review](#) 

“We haven't calculated a formal dollar ROI or headcount reduction with GitGuardian Platform, so I would not want to put an artificial number on it; the main day-to-day benefit is that secret detection and initial investigation are automated, saving developers and security teams time and allowing them to focus on remediation instead of manually checking repositories..”

Validated user

Consultant at a outsourcing company with 201-500 employees

[Read full review](#) 

“I have seen a positive return on investment, mainly through time saved in identifying and investigating exposed credentials. GitGuardian Platform reduces the amount of manual effort required for secret detection and helps the security team respond to findings faster. I do not have a specific dollar amount or percentage to share, but the improved efficiency and earlier detection provide clear value in our security workflow..”

Validated user

Cyber Security Analyst at a tech vendor with 51-200 employees

[Read full review](#) 

Use Case

“I mainly use GitGuardian Platform to monitor source code and repositories for exposed secrets and credentials. I identify leaked API keys or tokens and help prioritize and remediate those findings before they can be misused.

“Recently, I used GitGuardian Platform to scan a repository, and it flagged an exposed API credential in the code. I reviewed the finding, verified where the credential was being used, removed it from the repository, rotated the affected credentials, and updated the code to use a secure secret management approach instead..”

Validated user

Cyber Security Analyst at a tech vendor with 51-200 employees

[Read full review](#) 

“One specific example of how my team has used GitGuardian Platform to catch an issue was when it detected an API key that had accidentally been committed to a repository; we were able to quickly identify the exposed credential, revoke and replace it, and then clean up the repository so that the secret wasn't left exposed.

“Day-to-day, we mainly use GitGuardian Platform as an additional security layer around our development workflow, helping us continuously monitor repositories, investigate alerts, and work with developers to remediate exposed secrets before they become larger security issues..”

Validated user

[Read full review](#) 

Consultant at a outsourcing company with 201-500 employees

“My main use case for GitGuardian Platform is for security purposes when scanning our source repository, deployment, and all configurations where we can have credentials that cannot be shared with end users or any third party. This is why we are using GitGuardian Platform for security purposes to store all credentials securely.

“In addition to the main use case, there are credentials we want to store for environment-related purposes. For production-related properties, we want to connect with Azure, Git, or some external APIs where we have secret API keys. We keep those in this secret management on Git so that we can secure our systems..”

Validated user

[Read full review](#) 

Senior Software Engineer at a consultancy with 51-200 employees

“My main use case for GitGuardian Platform is monitoring the repositories for exposed secrets and credentials and reviewing security alerts. I also use it to remediate any findings that come up.

“The majority of the time we are thinking about potential secret exposure across repositories and prioritizing the findings which need attention. GitGuardian Platform gives a good additional layer of security alongside our existing practices.

“A specific example of a time when GitGuardian Platform helped me catch and fix an exposed secret is when developers hardcode API credentials while developing. There is always a chance that a developer makes a mistake and hardens an API credential in a repository. We are able to identify and remove the credentials, rotating them before they could be misused. This is a quick specific example we have encountered, and it is usual for anyone..”

Validated user

Developer at a healthcare company with 1,001-5,000 employees

[Read full review](#) 

“We are leveraging GitGuardian Platform first to augment governance over security control mechanisms in relationship from the developer through the CI/CD process out to resources such as vaults and so on, so that we can get active control over how security is, what is security, and how we can improve it.

“For instance, we envision using GitGuardian Platform with developers using IDEs or APIs, AI tools, operating through the automated pipelines of CI/CD, up to a vault out there in the cloud environment that contains the security rules that we have in play. We want to watch that process, whether it be a container, an artifact, or a pipeline, and see how, first, what is it? And then secondly, how can we improve it? So that we can use security key template models versus access account models.

“We are also wanting to gravitate from the strategy of using traditional style security templates that require account access, ID/user password models, and use GitGuardian Platform to develop a strategy to use API keys and signature encryption keys instead. To do that, we need a tool that gives clear transparency for that requirement..”

Brad Dyke

[Read full review](#) 

DSRE Director Of Dev Ops/Operations (Management Executive) at a outsourcing company with 51-200 employees

“Our primary use case for GitGuardian Platform is preventing credentials and other sensitive secrets from being accidentally committed to source code or exposed through our development and CI/CD workflows. We experienced one or two incidents where our secrets were leaked through Git when developers accidentally committed them or they were exposed through the pipeline. This is crucial from an infrastructure perspective because our application interacts with many cloud services. For example, development and deployment environments can contain AWS access keys, API keys, database credentials, and JWT tokens. The problem is not always intentional credential exposure, as a developer can accidentally include credentials in a .env file, Terraform variable, Docker file, or CI/CD configuration and commit it to Git.

“GitGuardian Platform is designed to detect hardcoded secrets in both repositories and CI/CD workflows, including historical repositories and new contributions. It supports integrations with GitHub, GitLab, Bitbucket, and Azure DevOps, all of which we use in our organization. Our precise use case is to detect secrets before they become a production security issue.

“GitGuardian Platform fits into our workflow in many steps. The first step is repository secret scanning, the second is CI/CD pipeline production, the third is pull request scanning, and the fourth is historical scanning..”

PrinceKumar7[Read full review](#) 

Cloud Engineer at a computer software company with 501-1,000 employees

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

“My experience with GitGuardian Platform's pricing, setup cost, and licensing was straightforward. Everything mentioned in the document format was clear, and there were no issues..”

Validated user

[Read full review](#) 

Senior Software Engineer at a consultancy with 51-200 employees

“My experience with the pricing and licensing was generally positive. The setup was straightforward, and I found the licensing model relatively easy to understand. The overall cost felt reasonable for the visibility and security value provided, although pricing can vary depending on the organization's requirement and scale..”

Validated user

[Read full review](#) 

Cyber Security Analyst at a tech vendor with 51-200 employees

“We have one employee that primarily works on the deployment and configuration of GitGuardian Platform, and that took approximately a couple of weeks working directly with them. After that, she spends about an hour in there a week, so it requires minimal effort on our side.

GitGuardian Platform requires very little maintenance on our end—just making sure the keys are connected and ensuring people are following through..”

Validated user

[Read full review](#) 

Director, Corporate Security Operations at a tech vendor with 5,001-10,000 employees

“The initial setup of the self-hosted cluster was moderately complex. We faced some issues because of the environment we had. We had to fix some installation errors and bugs in their Helm configuration.

In terms of deployment model, we self-host a cluster out of necessity. We have an internal GitHub Enterprise server. We self-host GitGuardian Platform to connect to that environment. We also use their SaaS version for Slack and Atlassian integrations..”

Ari Kalfus

[Read full review](#) 

Senior Manager, Product Security at DigitalOcean

“For costs, we are on the free version for up to twenty-five developers, so we are totally covered. As for the implementation, it is super simple. You open GitHub, open the GitGuardian Platform connector, configure the repositories you want it to monitor, and it is running. The learning curve and monitoring are almost zero. We use GitGuardian Platform's SaaS. What we did was configure it with the GitHub connector, which took just a few clicks, and you just set it to work and notifications and responses start arriving about all your repositories that you share..”

Antonio Tirado Peña

[Read full review](#) 

Directo de TI at Instituto de Innovación Ciencia y Empresa

“GitGuardian Platform is deployed in a mixture, usually between a hybrid cloud and on-premise. For my hybrid cloud deployment, we use an on-premise localized cloud deployment.

“Integrating GitGuardian Platform with my existing tools and workflows during my evaluation has been fifty-fifty, because some of their APIs are custom made.

“The reason the learning curve for GitGuardian Platform is so high is because I am introducing a whole new platform to what we already know, and that process is nothing we are familiar with. So there is a learning curve..”

Brad Dyke

[Read full review](#) 

DSRE Director Of Dev Ops/Operations (Management Executive) at a outsourcing company with 51-200 employees

Customer Service and Support

“I have limited direct interaction with GitGuardian Platform's support, but the responses we received were helpful and reasonably quick. Most of the issues are dealt with through documentation and internal processes, so we did not go to support directly..”

Validated user

Developer at a healthcare company with 1,001-5,000 employees

[Read full review](#) 

“I have never contacted any technical support or customer support through phone or ticket system. We have never experienced any issues with it. It effectively helps us with credentials security and has been performing satisfactorily..”

Kingsley Zikora

Senior DevOps Engineer

[Read full review](#) 

“GitGuardian Platform's documentation has been helpful during my evaluation.

“GitGuardian Platform's customer support has been good so far.

“I rate GitGuardian Platform's customer support an eight on a scale of one to ten..”

Brad Dyke

[Read full review](#) 

DSRE Director Of Dev Ops/Operations (Management Executive) at a outsourcing company with 51-200 employees

“The customer support experience with GitGuardian Platform has been generally good for the issues and configuration questions we have raised; responses have been reasonably clear and helpful, though response times can vary depending on the complexity of the issue.

“I would rate customer support for GitGuardian Platform eight out of ten, as the team has generally been responsive and helpful, especially for configuration and troubleshooting questions; however, there is some room for faster responses on more complex issues..”

Validated user

[Read full review](#) 

Consultant at a outsourcing company with 201-500 employees

“I'm impressed with the technical support team. We have bi-weekly meetings where we discuss any issues, and whenever I need something, I've received a response within a few hours.

The customer success team is another group I truly value meeting with. Their focus aligns directly with the challenges we face. They are incredibly responsive, and if we ever need clarification on anything, they get back to us within a couple of days. Additionally, the onboarding documentation on their website, along with the videos they produce on YouTube, are more than sufficient for getting developers up to speed..”

Validated user

[Read full review](#) 

DevSecOps at a tech vendor with 51-200 employees

“Their technical support so far has been fantastic. Anytime I raise a ticket, it is resolved and answered very quickly. I am very impressed. Their support is incredibly knowledgeable. Whenever I have questions about detection or remediation, they are very detailed in their answers, and they clearly know a lot about the tool.

Our experience has been fantastic with the purchase, the onboarding, and the customer success team. Everything has been straightforward. Everyone so far has been nice, friendly, and helpful. When there were any hurdles, they helped me resolve them straight away. I would rate their support a ten out of ten..”

Validated user

[Read full review](#) 

Senior Application Security Engineer at Bazaarvoice

Other Advice

“I advise others considering GitGuardian Platform to proceed with it for integrating CICD tools, workflows, or source repositories, as it can help them in early development, ease their processes, and accelerate their workflow. I rate my overall experience with GitGuardian Platform as nine out of ten..”

Validated user

Senior Software Engineer at a consultancy with 51-200 employees

[Read full review](#) 

“My advice for others considering GitGuardian Platform is that for DevOps and cloud infrastructure teams, integrating secret detection into normal development and CI/CD workflows makes much more sense than relying entirely on manual security reviews. This tool is incredibly useful. I would rate this product a ten out of ten..”

PrinceKumar7

Cloud Engineer at a computer software company with 501-1,000 employees

[Read full review](#) 

“I would recommend evaluating GitGuardian Platform if secret detection and credential exposure are important concerns for your organization. It provides useful visibility into repositories, helps identify exposed credentials early, and makes investigation and remediation more efficient. I would suggest starting with the areas most relevant to your deployment workflow and then expanding coverage as needed. I gave this review a rating of 10..”

Validated user

Cyber Security Analyst at a tech vendor with 51-200 employees

[Read full review](#) 

“The most critical advice I would give to others looking into using GitGuardian Platform is to understand that it is brand new technology and a brand new standard, with nothing truly written in stone. The learning curve will be significant as an adaptation is put in place. The key thing is to fully know all of your key tools that you use in your CI/CD processes, as well as planning for future tools, so that you can properly map the right compliance tool that supports those tools you have picked and become part of your platform.

“I am not in it that much yet to get a full scope of its yearly add-ons or features and improvements regarding how satisfied I am with the pace of innovation and new features being released by GitGuardian Platform. But for now, they are adequate.

“I rate GitGuardian Platform a seven out of ten..”

Brad Dyke

DSRE Director Of Dev Ops/Operations (Management Executive) at a outsourcing company with 51-200 employees

[Read full review](#) 

“My advice for others looking into using GitGuardian Platform is to clearly define

your secret scanning and remediation workflow before implementing it. Also, make sure alerting and integrations are configured properly so the team can act on findings without creating too much noise.

“Regarding GitGuardian Platform's AI capabilities, I think its governance and security are useful for improving detection and investigation. While governance and security controls are important for keeping the process controlled, from my experience, GitGuardian Platform provides a good foundation, though clearer visibility into AI decision-making and configuration would be helpful.

“When it comes to the accuracy and reliability of output, from my experience, the AI-assisted detection is generally accurate and useful for identifying potential secrets and prioritizing findings. I would still validate important findings manually, especially when the context is ambiguous or there is a possibility of a false positive.

“I would rate this review an eight out of ten..”

Validated user

Developer at a healthcare company with 1,001-5,000 employees

[Read full review](#) 

“I would rate GitGuardian Platform eight out of ten; it has been reliable for secret detection and monitoring, with good visibility and useful alerting, although there is still room for improvement around integrations, customization, and alert management.

“Regarding the AI capabilities of GitGuardian Platform, I find them useful when they provide more context around detected secrets and reduce manual investigation; from a governance and security perspective, I still want clear controls around data access, privacy, auditability, and how AI-assisted analysis is used within our organization.

“I found the AI-assisted analysis of GitGuardian Platform generally useful for

adding context to security alerts and helping with investigations; however, I still treat the output as a supporting signal rather than the final decision, especially for higher-risk findings where we validate the details before taking action.

“We deploy GitGuardian Platform as a public cloud SaaS solution that integrates with our development and source control workflows, meaning there is no separate on-premise infrastructure required for the platform itself.

“We use GitGuardian Platform as a SaaS platform and do not directly manage or choose the underlying cloud provider for the deployment; from our side, we primarily interact with the GitGuardian hosted service and integrate it with our development tools.

“My advice for others looking into using GitGuardian Platform is to first identify which repositories, teams, and secret types you need to monitor, then set up the integrations and alert workflow around that; also, spending some time tuning notification and remediation processes early on makes the platform much more useful as your environment grows. I rate this product eight out of ten overall..”

Validated user

Consultant at a outsourcing company with 201-500 employees

[Read full review](#) 

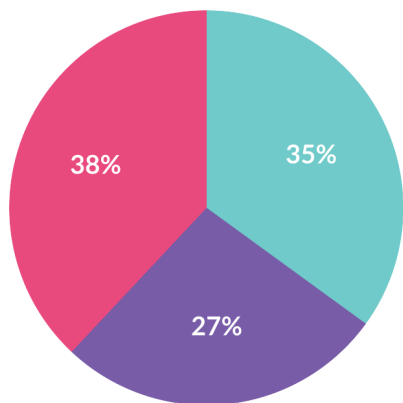
Top Industries

by visitors reading reviews

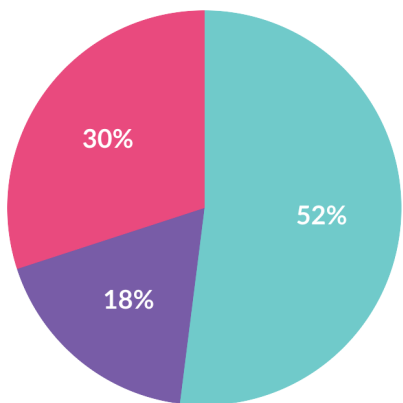


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a [customized report](#) of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.

[Get your personalized report here](#)

About PeerSpot

PeerSpot is the leading review site for cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944