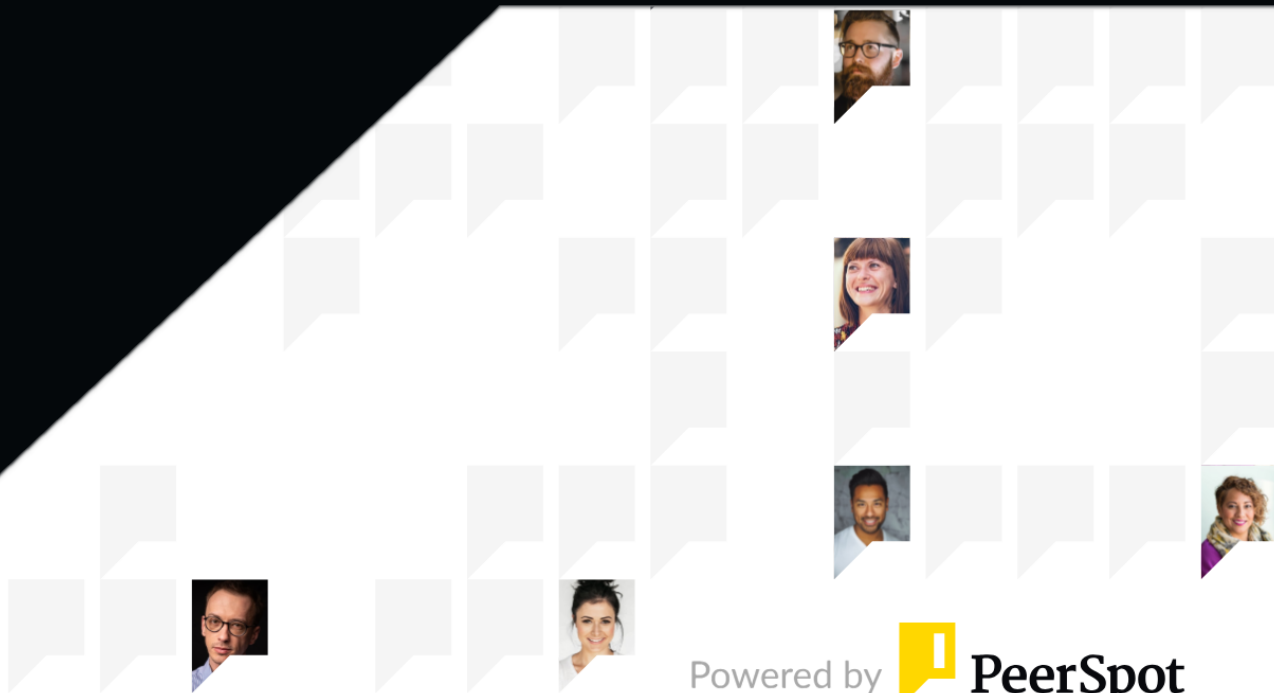


aws marketplace

GitGuardian Platform

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 11

Other Solutions Considered..... 12 - 14

ROI..... 15 - 17

Use Case..... 18 - 21

Setup..... 22 - 24

Customer Service and Support..... 25 - 27

Other Advice..... 28 - 31

Trends..... 32 - 33

About PeerSpot..... 34 - 35

Product Recap



GitGuardian Platform

GitGuardian Platform Recap

GitGuardian is an end-to-end NHI security platform designed to help organizations strengthen their Non-Human Identity (NHI) security posture and address compliance standards and regulations. As attackers increasingly target NHIs, such as service accounts, service principals, and applications, protecting and managing these critical assets has become paramount. NHIs rely on “secrets” like API keys and certificates for authentication, and their rapid proliferation has led to significant secrets sprawl.

GitGuardian's platform is built on two core pillars: **Secrets Security** and **NHI Governance**, delivering a holistic approach to NHI security.

With **Secrets Security**, GitGuardian aims to eliminate leaks and sprawl, detecting compromised or misused secrets across both public and internal environments. This foundation of NHI security is strengthened by monitoring for incidents, policy violations, and illegitimate use of secrets. GitGuardian offers three powerful products under its **Secrets Security** umbrella.

GitGuardian's **Secrets Detection** tackles internal secrets sprawl by identifying sensitive data in source code and developer productivity tools. The platform supports over 420 types of secrets, including API keys, private keys, and database credentials. With a robust policy engine, security teams can enforce rules across major version control systems (VCSs) like GitHub, GitLab, BitBucket, and Azure DevOps, CI/CD tools such as Jenkins, Travis CI as well as tools like Slack, Jira, container registries, and more.

GitGuardian Public Monitoring scans public GitHub repositories, detecting sensitive information in both organizational and developers' public personal repos. This is crucial, as 80% of corporate secrets leaked on public GitHub stem from personal accounts.

GitGuardian Honeytoken deploys decoy secrets that lure attackers looking for active secrets across your assets. Any unauthorized access attempts will trigger immediate alerts, enabling rapid detection and response during the software development lifecycle.

With **NHI Governance**, GitGuardian offers a centralized inventory of secrets, tracking their context and usage. This enables teams to detect high-risk secrets, manage their rotation, and leverage analytics to enhance the overall NHI security posture. Together, **Secrets Security** and **NHI Governance** work symmetrically: one track focuses on detecting compromised secrets, while the other manages legitimate usages of secrets and their lifecycle.

Trusted by over 600,000 developers and recognized as the top security app on GitHub Marketplace, GitGuardian is the choice of leading organizations like Snowflake, ING, BASF, and Bouygues Telecom, ensuring robust protection for their sensitive secrets.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “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



“Since we have this feature, we have peace of mind that our credentials will not be leaked or pushed somewhere by an employee.”



Dev Mittal

Cloud Engineer at Belinnov Solutions Pvt. Ltd.



“It's fantastic. We have checked a couple of other vendors and seen their results, which are quite inferior to the amount of detail that the GitGuardian Platform provides. With instantaneous notifications connected to our Slack platform, it allows us to deal quickly with incidents.”



Glenn McDonald

Head of Engineering Services at IRESS



“GitGuardian Platform has positively impacted our organization as it helps us reduce the number of secrets that we would accidentally commit into source code.”



PeterHenggeler

Security Engineer at Recidiviz



“The newest addition that we appreciate about GitGuardian Platform is the ability to create a custom detector, which we built and worked with the team, and that works very effectively.”



Verified user

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

What users had to say about valuable features:

“What I appreciate the most about GitGuardian Platform is its efficiency when triggering our pipeline and notifying us if secrets have been exposed, such as APIs, variables, our database, or anything being exposed. Currently, we have numerous repositories and pushes that happen in our repo. It would be humanly impossible for us to manually search for these secrets. GitGuardian Platform can do this automatically. All we need to do is wait for an email notification that indicates a secret has been exposed. It points out the repository that has the secret exposed, and we can fix it. This saves us the time of manual review..”

Kingsley Zikora

Senior DevOps Engineer

[Read full review](#) 

“The public leakage detection feature of GitGuardian Platform influences my data security positively. This addresses a problem that could happen to anyone. Since we have this feature, we have peace of mind that our credentials will not be leaked or pushed somewhere by an employee.

Sometimes, I have faced a specific problem. I work in the cloud and have cloud credentials. Our developers asked me to give them credentials for debugging on their local devices. If they push credentials somewhere and cannot communicate with me since I am the admin, that time gap becomes dangerous. GitGuardian Platform provides a good security measure for any company using it, though you cannot give it a specific percentage impact on the company..”

Dev Mittal

Cloud Engineer at Belinnov Solutions Pvt. Ltd.

[Read full review](#) 

“The best features GitGuardian Platform offers include notification directly to the engineer who created the pull request.

The direct notification feature has helped my engineers and my workflow overall by being effective. It is nice to know that no matter what happens, day or night, if someone puts up a change, they will get an alert, and the security team will get an alert.

GitGuardian Platform has positively impacted our organization as it helps us reduce the number of secrets that we would accidentally commit into source code. We have definitely saved time, as we do not have to go clean out Git history because we can just rotate the secret quickly..”

PeterHenggeler

Security Engineer at Recidiviz

[Read full review](#) 

“The best features of GitGuardian Platform are that it detects everything being pushed through the repository and scans everything comprehensively. It checks the possibility of exposure, so if there are API keys or database passwords being used, it warns us to either remove, rotate, or replace them, ensuring they should not be present in a GitGuardian Platform scan.

“Our company has seen many benefits from using GitGuardian Platform, especially since there have been numerous cyber attacks and security threats in the last two to three years. Our company has remained very safe in this regard because we need to secure our data effectively, being in the insurance reinsurance sector. GitGuardian Platform ensures our data is protected by regularly scanning the repositories and sending us reports on how to fix vulnerabilities, keeping us safe from cyber attacks..”

Sanket-Shinde

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

[Read full review](#) 

“My impression of the GitGuardian Platform's capability to detect secrets in real time is actually 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.

We adopted it a year ago, and it has been doing great in our teams, especially for developers. The impression so far has been good.

The severity scoring has helped us in incident management because it is doing the correct job. We got many secrets leaked within our platform and it was making the correct warnings regarding that particular secret, as we had a hardcoded Google Cloud API key. It was marked as a critical severity, so we had the chance to correct it, regenerate that secret and work again on not hardcoding secrets within our code.

GitGuardian's public leak detection significantly enhances our organization's data security by continuously monitoring public repositories. It allows us to proactively identify accidental exposures of sensitive credentials or secrets..”

Ney Roman

DevOps Engineer at Deuna

[Read full review](#) 

“The best features of the GitGuardian Platform are that it finds many different secrets, more than other competitors, and the support from the colleagues is also very good.

The GitGuardian Platform helps in monitoring and protecting our code repositories from leakage. It helps significantly because we connected our vulnerability management process to this, and the colleagues from vulnerability management have much easier work since we have the GitGuardian Platform installation due to the dedicated incidents or issues which are opened automatically.

The alerting capabilities and threat intelligence features of the GitGuardian Platform are managed by another team; we only host the platform.

The audit logs and compliance reports from GitGuardian are very helpful because, in the past, we needed to do it manually by scanning the repos. Now with GitGuardian Platform, we have a really good overview of what is open, what is closed, and how critical the issues are..”

Verified user

[Read full review](#) 

DevOps Engineer at a manufacturing company with 10,001+ employees

Other Solutions Considered

“We did not use any similar solution before. It was a manual process. We did not monitor anything. We just occasionally noticed things to be resolved. It was a manual process..”

Verified user

Senior Application Security Engineer at Bazaarvoice

[Read full review](#) 

“I have not ever used any similar solutions to GitGuardian Platform that I can compare it with. We simply use it and it is working well for us, so we did not switch from another solution..”

Dev Mittal

Cloud Engineer at Belinnov Solutions Pvt. Ltd.

[Read full review](#) 

“We created a technical evaluation and checked against other providers, though I don't remember the names. The GitGuardian Platform has the best technical capabilities, and our procurement handles the pricing part..”

Verified user

DevOps Engineer at a manufacturing company with 10,001+ employees

[Read full review](#) 

“I have not compared GitGuardian Platform with any alternatives in my organization. For GitHub repositories credentials, we use GitGuardian Platform. For AWS, we use Amazon Macie because we run our infrastructure on Amazon Web Services. We use Macie to protect our credentials from being exposed..”

Kingsley Zikora

Senior DevOps Engineer

[Read full review](#) 

“I have not compared GitGuardian Platform with any alternatives in my organization. For GitHub repositories credentials, we use GitGuardian Platform. For AWS, we use Amazon Macie because we run our infrastructure on Amazon Web Services. We use Macie to protect our credentials from being exposed..”

Kingsley Zikora

Senior DevOps Engineer

[Read full review](#) 

“There are many tools in our organization for similar purposes, but GitGuardian Platform is specifically for exposing secrets. We also use Snyk for vulnerability scanning, among others, though I cannot recall all of them.

“The decision was made by my organization, not me, so I am not sure about the parameters they considered before choosing GitGuardian Platform..”

Sanket-Shinde

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

[Read full review](#) 

ROI

Real user quotes about their ROI:

“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](#) 

“It's challenging to quantify, but it has saved us from a bit of panic because we know the state of our source code. It's hard to determine what savings might come from having the tooling or not..”

Glenn McDonald

Head of Engineering Services at IRESS

[Read full review](#) 

“It has definitely saved us a lot of time. To be able to view everything important and narrow our focus to resolve issues has sped up our development process and decreased our security risk..”

Verified user

[Read full review](#) 

Senior Application Security Engineer at Bazaarvoice

“We have only used GitGuardian for four months, so it's hard to calculate a return. However, it will save us a lot of headaches with the new EU regulations in the long run. .”

Mikkel Østergaard Eriksen

[Read full review](#) 

IT-Security Consultant at a energy/utilities company with 201-500 employees

“Regarding return on investment, we have actually saved time and resources because before having GitGuardian Platform, we had two or three people working in every repository looking for secrets with open-source tools. It took a long time to find secrets or many patterns, and at the time, we had to configure our own patterns to find them. I cannot specify the exact return on investment, but I can surely say that we have saved significant time and resources, particularly in terms of people and automation..”

Ney Roman

[Read full review](#) 

DevOps Engineer at Deuna

“The majority of our incidents for critical detectors and important secret types are remediated automatically or proactively by developers through GitGuardian's notification system, without security team involvement. It saves a lot of time for the security teams and the developers. It probably saves approximately 10 hours per week. Previously, we needed an extra 20% of our time focused on this subject area, which has now been saved because of this platform..”

Ari Kalfus

Senior Manager, Product Security at DigitalOcean

[Read full review](#) 

Use Case

“GitGuardian Platform is a security tool preventing the exposure of secrets. It is particularly valuable as a tool because it doesn't just identify exposed security issues, but works as a platform that gives developers an intuitive and easy way of reacting to and fixing the issues..”

Ari Kalfus

Senior Manager, Product Security at DigitalOcean

[Read full review](#) 

“My main use case for GitGuardian Platform is secret detection.

Every time we open a pull request, it scans the pull request and ensures that we did not accidentally put a database password in a pull request. That process has worked very well for my team as it has caught several things, it is very helpful, and it is easy to use..”

PeterHenggeler

Security Engineer at Recidiviz

[Read full review](#) 

“Our current use cases for GitGuardian Platform involve monitoring external and internal GitHub and GitLab, Bitbucket, and other code repositories that it supports for secrets..”

Verified user

[Read full review](#) 

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

“I use GitGuardian Platform to ensure that there are no secrets committed, such as hardcoded values, database credentials, API keys, or any secrets that could be exposed to external users of our application. To maintain security and data accuracy, confidential data should not be shared with other platforms. GitGuardian Platform checks our local code first, then it passes through our CI/CD pipeline as well. When we push code to GitHub, it scans and sends a report via Gmail, so we have to fix those security vulnerabilities..”

Sanket-Shinde

[Read full review](#) 

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

“We initially integrated GitGuardian Platform into our organization in 2023 into our GitHub repository. We implemented it because we did not want our secret credentials to be exposed to the internet or to a third party such as GitHub. It flags when credentials have been exposed so we can remediate and fix them. GitGuardian Platform was what my tech lead suggested we use, and we had to incorporate it into our repositories. We use the Platform version..”

Kingsley Zikora

Senior DevOps Engineer

[Read full review](#) 

“GitGuardian Platform serves as a security shield for our organization to prevent API keys and database credentials from being pushed to GitHub. Although we know we should not push credentials, anyone can make mistakes. GitGuardian Platform has a CLI tool called gg shield, which we have set up on our laptops. Since we already use Git version control with GitHub, the process is straightforward. Whenever we push code to GitHub, it scans the code and checks for API keys and database credentials. Even if credentials are commented out, GitGuardian Platform flags them because commented credentials remain readable on GitHub and can still be caught by bad actors.

The most problematic situation occurs when a developer pushes credentials to GitHub and then attempts to remove them by pushing again. The issue is that Git does not work that way. The credential still remains in our GitHub repository history. GitGuardian Platform rescans our GitHub repositories for API keys to address this situation.

I also use GitGuardian Platform in my CI/CD pipelines with GitHub Actions. Although we store credentials in GitHub secrets, sometimes people hardcode credentials by mistake. Once the CI/CD pipeline is working properly, we do not edit it much, so if someone hardcoded credentials and everything is functioning well, no one may even review it. That credential could remain exposed for months. Even though our GitHub repositories are private, we still use GitGuardian Platform as a security measure. As a backend engineer, DevOps engineer, and AWS cloud engineer at my small company, I understand what situations could occur and these are real scenarios we face. We must use this solution even though we all know we should not do these things. However, no one knows what can happen in the future..”

Dev Mittal

Cloud Engineer at Belinnov Solutions Pvt. Ltd.

[Read full review](#) 

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.

“The initial deployment of GitGuardian Platform is pretty easy. GitGuardian Platform has a YouTube channel with three to four-minute introduction videos that show step-by-step how to install it. They also have documentation, so the setup is simple and easy..”

Dev Mittal

Cloud Engineer at Belinnov Solutions Pvt. Ltd.

[Read full review](#) 

“We didn't have to do much. They manage all of the backend for us. All we have to do is integrate it into our GitHub organizations, and doing that is straightforward.

The solution does not require any maintenance. .”

Glenn McDonald

Head of Engineering Services at IRESS

[Read full review](#) 

“To implement it, the only thing required from our side was having someone with admin permissions to enable the installation. It was minimal from our side.

It does not require any maintenance from our side..”

Verified user

[Read full review](#) 

Senior Application Security Engineer at Bazaarvoice

“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..”

Verified 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

Senior Manager, Product Security at DigitalOcean

[Read full review](#) 

“The initial setup was straightforward. However, we did need to establish the initial connection between the repositories. This process went fairly smoothly overall. While connecting the repositories on GitHub was easy, it was a bit trickier on the Azure side. So, some preparatory work was required there. Once that was done, the internal monitoring setup was complete and went quickly. Additionally, we had to set up teams and invite members, but this also went quickly.

The deployment took a couple of days. The repository connections (6,000+ repositories) took an hour or two to fully populate. One person was required for the deployment. .”

Joan Ging

Head of Development at Inhabit

[Read full review](#) 

Customer Service and Support

“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](#) 

“I have not ever contacted the technical support or customer support for GitGuardian Platform. We do not need to contact them since the platform is simple to install. It is just there for precaution. We do not need it every day since it is simply for the rare chance that someone will accidentally push credentials and then it flags them..”

Dev Mittal

Cloud Engineer at Belinnov Solutions Pvt. Ltd.

[Read full review](#) 

“I rate GitGuardian support ten out of ten. We had some issues with GitGuardian failing to detect some secrets. We contacted support. They resolved the problem swiftly and kept us informed throughout the process. They started the process of creating a new detection, and it's a new feature that they're working on. .”

Mikkel Østergaard Eriksen

[Read full review](#) 

IT-Security Consultant at a energy/utilities 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..”

Verified 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..”

Verified user

Senior Application Security Engineer at Bazaarvoice

[Read full review](#) 

“The customer support has been very responsive to our requests and inquiries. They are very quick to take action, and I learn more about the product each time I reach out to them. They have been great to work with.

The technical support team is very responsive and thorough. Whenever I have a question, I simply email them. Even if I don't send it to the right person initially, they'll be sure to forward it to the appropriate support agent. When I receive a response, it's often more detailed than I expect. They explain not only how to solve my specific issue, but also provide additional information that helps me better understand and utilize the tool. This feedback allows me to learn a lot and improve my skills..”

Mary Loup

Application Security Engineer at a energy/utilities company with 10,001+ employees

[Read full review](#) 

Other Advice

“My advice to others looking into using GitGuardian Platform is that it is a very quick win to set up and very easy to configure. I would rate this review a 10..”

PeterHenggeler

Security Engineer at Recidiviz

[Read full review](#) 

“I will rate GitGuardian Platform a seven out of ten. The reason for this rating is that I wish they could have an agent embedded into their system that helps to identify real credentials from mock credentials, as this sometimes causes false alarms.

We are users of the product with no partnerships with GitGuardian Platform. They can contact me regarding any questions about this review. I am open to anything that benefits the community and makes everything better..”

Kingsley Zikora

Senior DevOps Engineer

[Read full review](#) 

“The effectiveness of GitGuardian Platform's automated severity scoring in incident management is good. When an incident happens, the incident manager receives an automated severity score based on the credential type. In my case, we mostly have development environment credentials, so the severity is not much, perhaps around six or seven.

I did not use the automated playbooks of GitGuardian Platform.

GitGuardian Platform does not require any maintenance on our end.

I rate this review an 8 out of 10..”

Dev Mittal

Cloud Engineer at Belinnov Solutions Pvt. Ltd.

[Read full review](#) 

“We are customers in our company's relationship with the vendor.

I work primarily with the CLI, focusing on pipelines and automations rather than the platform itself. The platform has remained almost the same within the year that we have been working with it.

We are not utilizing the automated playbooks yet.

I cannot determine if the pricing is cost-effective.

The vendor can contact me if they have any questions or comments about my review.

I have rated the GitGuardian Platform a 10 out of 10..”

Ney Roman

DevOps Engineer at Deuna

[Read full review](#) 

“The GitGuardian Platform is used worldwide in our environment.

Currently, we have approximately 1,300 licenses for the GitGuardian Platform, but we will increase to 2,000 next year.

The solution requires maintenance from our side only for user management, which is normal for each application.

I cannot quantify how much time or resources the GitGuardian Platform saves us because this is spread across all teams worldwide.

I would recommend the GitGuardian Platform to other users because the integration with [GitHub](#) and [Azure DevOps](#) is very easy, and you also have the possibility to use it locally on your [IDE](#). This is a very good solution.

I rate the GitGuardian Platform a nine out of ten because room for improvement is always possible, but it's really good..”

Verified user

DevOps Engineer at a manufacturing company with 10,001+ employees

[Read full review](#) 

“GitGuardian Platform prioritizes incidents in our workflow through automated validity checks. There are high risk, low risk, and medium risk incidents raised, and the infosec team prioritizes them and approaches us, the developers who pushed those changes, to fix them accordingly.

“GitGuardian Platform's public leakage detection influences our company's data security as a precaution. We are not sure if data might be exposed, but taking this precaution by scanning the repositories is crucial. A cyber attacker just needs one piece of data, so we ensure at least that one thing is secured. It is about cyber attack prevention, ensuring all our data remains safe.

“It rates the effectiveness of severity in incident management based on the severity of the change. This allows us to address the most important ones first. It

checks what has been pushed from the code, raising a high-level vulnerability if database-related passwords are involved and reports it urgently. For low-level issues like hardcoded values for APIs, it is reported accordingly based on priority.

“I use GitGuardian Platform's automated playbooks for scanning. Productivity-wise, these playbooks help me know if I am going to push code with secrets. I am aware now, so I intentionally avoid that, ensuring I write good code. It increases my productivity by helping me fix issues proactively. If GitGuardian Platform were not here and vulnerabilities were discovered later, there could be severe consequences. Currently, that impact has been reduced, minimizing our efforts significantly through early precautions.

“Our organization is currently innovating on the AI side, which includes creating a custom agent to fix vulnerabilities, similar to [GitHub](#) Copilot. This agent automates changes required based on GitGuardian Platform scanning, closing incidents directly. This support reduces our efforts and timelines.

“Fixing vulnerabilities now takes approximately 60% less time. If fixing took ten days, I now do it in six. I am not sure about multi-vault integration because I am just a developer using it to fix my code changes. I am not sure if I am using GitGuardian Platform's Honey Tokens feature. I would rate this product an 8.5 overall..”

Sanket-Shinde

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

[Read full review](#) 

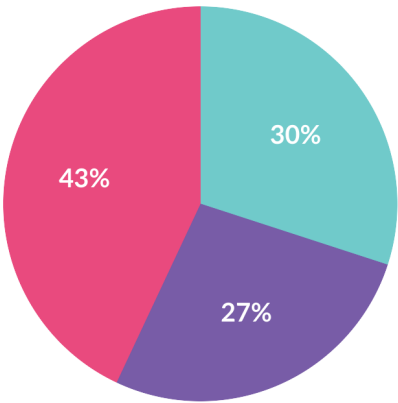
Top Industries

by visitors reading reviews

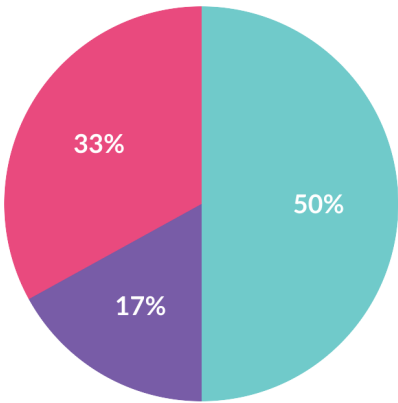


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsized 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