GitGuardian Platform

PeerSpot

Joan Ging

Head of Development at Inhabit

It dramatically improved our ability to detect secrets, saved us time, and reduced our mean time to remediation

Mar 19, 2024

What is our primary use case?

“We use the GitGuardian Platform for internal security monitoring. Initially, we employed it to identify any secrets from our internal repositories that might have been accidentally exposed publicly and then expanded our use of GitGuardian to remove secrets from our private repositories, also.

Our company has grown through acquisitions. To address this complexity, we've integrated GitGuardian with our development teams. This allows them to identify secrets within any repository so they can be quickly remediated, ultimately enhancing the security of our codebase.”

How has it helped my organization?

“GitGuardian helps us prioritize remediation quickly. The alerting component is helpful because it lets people know immediately when something suspicious appears. Additionally, the code context feature is valuable as it shows developers

exactly where the issue occurs in their code. They can even click a link to jump directly to that location in GitHub. These features significantly speed up the process for developers to identify and remove vulnerabilities.

GitGuardian effectively supports a shift-left security strategy. This is because it integrates directly with the code repository, allowing for near real-time feedback on potential security issues before code is merged into production branches. This early detection is highly valuable. Furthermore, GitGuardian's command-line interface provides another layer of convenience. Developers can proactively search for and address security concerns before pushing their code.

GitGuardian improves collaboration between our developers and security teams on remediation efforts. The centralized dashboard is tremendously helpful for managing across a multitude of teams and hundreds of engineers. It allows me to see the progress of each team. This visibility makes it much easier to communicate with them. For instance, I can identify teams that might need assistance or recognize those that are successfully reducing vulnerabilities.

GitGuardian has dramatically improved our ability to detect secrets by shedding light on previously hidden vulnerabilities.

Our security productivity has increased significantly. Simply by making this information readily available to developers, we've empowered them to take action. Previously, this wasn't easy, especially when dealing with inherited legacy code. Developers often wouldn't know where these secrets were hidden within the codebase. This improved visibility has made security issues much more actionable for our developers.

With over 6,000 repositories, GitGuardian's automation capabilities have saved us many months of research.

GitGuardian has reduced our mean time to remediation. This ability to track security issues and communicate proactively with teams undoubtedly means we can also remediate them faster."

What is most valuable?

“Recently, a new feature was added that I had been requesting for a while, and I'm super excited about it! This feature allows us to filter incidents by team within the available filters. This is incredibly helpful because before, we could only search for individual repositories. Some of our teams have hundreds of repositories, so filtering by team saves a lot of time and effort.

The ability to create teams is also valuable for a large organization like ours. Some vendors struggle to provide enough user organization layers, but GitGuardian excels in this area.

The core incident management features are also fantastic. For example, alerting people via email about new incidents is crucial for staying on top of things. Additionally, the dashboard allows users to mark the status of secrets, providing a convenient location to review everything.

Another area where GitGuardian shines is the breadth of secret types it covers. They can identify a vast number of secrets out-of-the-box, with minimal false positives. This means they effectively distinguish real secrets from irrelevant data, saving us time and effort. I also appreciate the context provided for developers. When they investigate secrets, they can see exactly where those secrets reside in the code, allowing for quick fixes.”

What needs improvement?

“While they do offer some basic reporting, more comprehensive reporting would be beneficial in the long run. This would allow me to demonstrate the value of the product over time to continue to effectively budget for this subscription, especially as they add features that may come at an additional cost. I appreciate the improvements made to reporting over the past year, but continued development in this area will be appreciated.

We have encountered occasional difficulties with the Single Sign-On process. There is room for improvement in its current implementation. It works, but was not quite as smooth as the rest of the GitGuardian experience.”

For how long have I used the solution?

"I have been using the GitGuardian Platform for one year."

What do I think about the stability of the solution?

"GitGuardian is stable. I have not had any problems."

What do I think about the scalability of the solution?

"GitGuardian scales incredibly well. We bombarded them with a massive number of repositories, and they ingested everything much faster than I anticipated. This allowed for a swift evaluation process. Their ability to handle large deployments is evident, and I'm confident they support companies even bigger than ours."

How are customer service and support?

"The technical support team responded quickly and was able to resolve my issues the following day. There were no problems with their service."

Which solution did I use previously and why did I switch?

"Before implementing the GitGuardian platform, we lacked a solution to identify secrets in our code. This created a significant security blindspot for us."

How was the initial setup?

“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. ”

What about the implementation team?

“The implementation was completed in-house.”

What's my experience with pricing, setup cost, and licensing?

“GitGuardian is not inexpensive. It's one of the more expensive tools in our portfolio, especially considering its focused functionality. However, while it may not offer a wide range of features, it acts as a form of critical security insurance. It safeguards our most vulnerable points, and a data breach can lead to legal repercussions that can be very costly for years to come. In that light, the cost is warranted and rational.”

Which other solutions did I evaluate?

“After considering several options, we determined that GitGuardian was the most

robust solution for our organization's needs.

We evaluated several open-source solutions for secret detection. We also considered other security tools with similar capabilities but found that those not specifically focused on secret detection fell short. These tools often treated secret detection as an afterthought, resulting in limited effectiveness. While they might identify some basic secrets, they lacked the depth and comprehensiveness of GitGuardian. This is why we decided to invest in a dedicated secrets detection tool."

What other advice do I have?

"I would rate the GitGuardian Platform 10 out of 10.

Concerning maintenance, there may be a rare exception that we need to enter into the platform when new repos are added, but these have been very infrequent. The tool requires very little ongoing maintenance, beyond what teams need to triage.

While there are open-source secret detection tools available, they can be limited. GitGuardian, with its dedicated development team, offers a more comprehensive solution. Their support, including responsive sales reps and customer service, ensures you get the help you need to keep your system secure. Open-source solutions often lack this level of dedicated support, which can leave you troubleshooting issues on your own. For critical security needs, the additional features and support offered by GitGuardian are a worthwhile investment.

It's critical to our application development security program to have a robust secrets management solution. This is especially important when we have a large development team. In such an environment, the risk of human error increases, often due to unintentional mistakes. People might forget things, miss something during development due to time pressure, and so on. However, even a single mistake can have serious consequences. Therefore, careful management of secrets is essential. It safeguards our relationships with vendors, protects our internal data, and offers numerous other benefits.

My recommendation is to prioritize setting up SSO as first step, before onboarding

any other users, if you're planning to implement it. Do it first. That was the only real challenge we faced; trying to get it working later created some complications. The actual setup process of getting GitGuardian to scan our repositories was straightforward and fast."

Which deployment model are you using for this solution?

Public Cloud

GitGuardian Platform

For more in-depth insights from real user reviews

Download GitGuardian Platform Buyer's Guide

About PeerSpot

PeerSpot is the leading review site for software running on AWS and other platforms. 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