GitGuardian Platform

PeerSpot

Blessed Uyo

Product Security / DevSecOps at a media company with 10,001+ employees

GitGuardian's automated features enhance productivity by allowing us to delegate tasks and concentrate on governance.

Mar 06, 2024

What is our primary use case?

“We utilize GitGuardian to scan for secrets within our codebase. Our implementation includes pre-receive and pre-commit hooks, dashboard scans, and CI/CD integration within GitLab.”

How has it helped my organization?

“Secret detection is pivotal for development security, ensuring no secrets exist in packages, libraries, dependencies, or code. Even with a locked-down application, explicit permissions could grant easy access to the environment and connected resources. GitGuardian serves as an essential tool for every development team.

GitGuardian aids in prioritizing remediation efforts by promptly notifying us of reported issues. This informs our approach; we prioritize valid reports over invalid

ones or those that failed checks. Automation plays a significant role, swiftly addressing invalid reports and saving valuable time.

The solution aligns with our shift-left strategy, empowering developers with security responsibilities through pre-receive hooks that act as security controls. Developers can quickly identify secrets, enhancing security awareness at the development level.

GitGuardian significantly reduces manual work through automation, streamlining incident resolution processes and allowing proactive measures like permissions revocation. While not fully automated, leveraging automated solutions has notably increased productivity, enabling us to focus more on governance and essential tasks.

Our secret detection capabilities have improved dramatically with GitGuardian. Initially facing over 10,000 incidents, we reduced them to 2,700, marking a 60 to 70 percent increase in detection efficiency.

Validation features save considerable time by eliminating the need for manual verification, allowing us to focus on remediation. While accuracy varies based on use cases, we've encountered only a handful of false positives, with the false positive rate correlating strongly with the number of secrets present."

What is most valuable?

"GitGuardian offers a range of features that align perfectly with our requirements. With internal policies in place to prevent secret exposure, especially concerning our code hosted on GitLab, GitGuardian's pre-receive hook stands out as a crucial feature. By activating this hook on the remotes, it effectively blocks commits from being pushed to the repository, ensuring that secrets never reach GitLab and remain protected from exposure.

The tool provides comprehensive coverage, including classic technologies such as SMTP credentials, along with Slack tokens and AWS secrets in our specific use case. Its ability to manage various types of secrets, including database connections, APIs, and RSA keys, streamlines our workflow by consolidating

detection efforts. This consolidation saves us considerable time, eliminating the need for back-and-forth verification with the team. Once a valid issue is identified, we can promptly escalate it to the team for remediation”

What needs improvement?

“The GitGuardian hook and dashboard scanners are essential components that should seamlessly integrate to provide comprehensive security coverage. However, we've encountered instances where discrepancies arise, with the dashboard scan detecting issues not reflected on the hook. This inconsistency requires fine-tuning to ensure efficient detection and resolution, as we aim to avoid unnecessary time wastage.

Moreover, the historical scan feature could benefit from improvement. Occasionally, it fails to efficiently track changes in updated histories, leading to delays in data history updates. This can be frustrating, especially when the reported secret remains unchanged or changed in history. Addressing this issue is crucial to alleviate the burden on the team and streamline our workflow. We hope to see enhancements in this aspect from GitGuardian.”

For how long have I used the solution?

“I have used GitGaurdian for two years.”

What do I think about the stability of the solution?

“Earlier, we had some challenges and problems with the dashboard crashing, but there have been many improvements since then. We haven't seen any crashes lately. ”

What do I think about the scalability of the solution?

“The scalability depends on the deployment model. Our engineers understand how to deploy the solution directly. We have two environments: production and dev. We haven't seen any major hassles, and it doesn't impact the development workflow.”

How are customer service and support?

“I rate GitGuardian support nine out of ten. GitGuardian support has been great. They respond fast. If something requires investigation, they also resolve the issue quickly. Recently, we had to upgrade because of a bug. They were happy to help us.”

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

“I used Trufflehog at a previous company. It's hard to compare the two. Both have their strengths and weaknesses. I've used a couple of the other solutions, and GitGuardian stands out.”

How was the initial setup?

“It was straightforward. We had deployed it on EKS with nodes for dashboard and other aspects of the app.”

What about the implementation team?

“It was a joint effort. Their support engineers were very skillful and did provide all required help.”

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

“Every company has a budget to spend on security tools, so it depends on what you want to spend on security at each stage in their maturity walk. You can have a vulnerability in your code with a firewall in front, but you don't want an application exposing secrets. An attacker knows how to crawl your application and extract information. It depends on how much you want to prioritize the cleanness of your code from a secrets perspective. ”

Which other solutions did I evaluate?

“We looked at a few other products but primarily chose GitGuardian because of the price. It also has some advantages regarding dashboard maturity and the number of available integrations. We also like the auto-validation and the way the pre-commit hook works. It was also a lot easier to implement GitGuardian.

I recommend open source for other things but not secrets detection. There's an inherent vulnerability to an open source solution that could leave your secrets exposed.
”

What other advice do I have?

“I rate GitGuardian Internal Monitoring nine out of ten. Before deployment, it's crucial to thoroughly understand your environment. For users of public cloud services, ensuring compatibility with GitGuardian's features is essential to

maximize benefits. While the SaaS solution offers simplicity, our air-gapped internal deployment had minor restrictions on available features. Despite this, we opted to continue with GitGuardian as it satisfied our core needs.

Understanding your environment and version control system is paramount. Determine your implementation approach, considering options like starting with dashboard scans rather than hooks, which I don't recommend initially. Beginning with dashboard scans on your version control system, such as GitHub, and conducting historical scans is advisable. As teams become more acquainted with the tool, gradual implementation of more advanced features like hooks can be considered."

Which deployment model are you using for this solution?

On-premises

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