

aws marketplace

Cycode

Reviews, tips, and advice from real users



Powered by  PeerSpot

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 8

Other Solutions Considered..... 9 - 10

ROI..... 11

Use Case..... 12 - 14

Setup..... 15 - 16

Customer Service and Support..... 17

Other Advice..... 18 - 20

Trends..... 21 - 22

About PeerSpot..... 23 - 24

Product Recap



Cycode

Cycode Recap

Cycode is a comprehensive security platform designed to protect the software development lifecycle by securing source code and detecting vulnerabilities early in the code distribution process.

Cycode integrates seamlessly into development workflows to ensure the integrity and security of code repositories. By automating secret detection and providing robust threat detection, Cycode builds a resilient security framework for code. It offers scanning capabilities that identify misconfigurations and tracks code leaks across distributed environments, allowing teams to act quickly and effectively. By leveraging advanced analytics, it provides insightful data to mitigate security threats proactively.

What are the key features of Cycode?

- **Secret Detection:** Automatically identifies confidential information hardcoded into the repository to prevent unauthorized access.
- **Misconfiguration Scanning:** Detects and alerts about potential configuration issues that can lead to security vulnerabilities.
- **Code Leak Detection:** Monitors and tracks unintentional source code exposure across environments.
- **Threat Detection:** Provides real-time alerts and insights on suspicious activities in the codebase.

How can Cycode improve your outcomes?

- **Enhanced Security Posture:** Helps maintain a secure development environment by stopping threats before they escalate.
- **Reduced Risk:** Minimizes the likelihood of data breaches by securing code practices.
- **Operational Efficiency:** Automates the detection process, saving time and resources for developers and security teams.
- **Comprehensive Visibility:** Offers detailed analytics to improve strategic decision-making regarding code security.

In industries such as finance, healthcare, and technology, Cycode is implemented to safeguard critical code infrastructure by providing proactive threat detection and code compliance features that meet stringent regulatory standards. It facilitates seamless security integration in cloud environments, enabling industries to maintain compliance and ensure the protection of sensitive data throughout development cycles.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“Cycode excels in secret scanning and is brilliant at finding and identifying secrets within code.”



Verified user

DevSecOps Security Engineer at a manufacturing company with 10,001+ employees



“In my experience as an integrator with Cycode, the biggest advantage is that it is platform agnostic and language agnostic.”



Mritunjay-Kumar

Principle Architect at Ford Motor Company



“Cycode has positively impacted the organization by saving time in the pipeline and providing one platform for secret scanning, SAST, and Infrastructure as Code facilities.”



Verified user

Cyber Security Engineer (DevSecOps) at a manufacturing company with 10,001+ employees

What users had to say about valuable features:

“Concerning the anomaly detection feature, I understand that it is related to detecting vulnerabilities and secrets. Cycode provides tools for detecting secrets, password vulnerabilities, and other issues in our continuous deployment environment, especially when using Docker. Since we use many dependencies, we need to detect vulnerabilities within them proactively, and Cycode assists us in identifying these vulnerabilities through its detection features.

“As for Cycode's continuous monitoring feature, I think it helps maintain code integrity. I manage almost one hundred ninety services and can maintain integrity, quality, and prevent any sort of data leaks or secret mismanagement early within the development environment. Our shift-left approach allows developers to address these issues during continuous integration, and Cycode provides extensive reports integrated into our pipeline..”

Mritunjay-Kumar

Principle Architect at Ford Motor Company

[Read full review](#) 

“Cycode has an extensive vulnerability list, great AI that helps obtain vulnerability resolution, and risk intelligence features. Additionally, Cycode has seamless integration with GitHub, which saves time in the pipeline. Other tools like Checkmarx require integration into the pipeline, which takes additional time. Cycode reduces pipeline time and saves development time. The developer community in the organization is happy with Cycode, specifically with the GitHub integration feature.

Cycode's AI helps with vulnerability resolution because, while other tools have AI for resolving vulnerabilities, the key difference is that Cycode has access to GitHub and can actually read the code to give more appropriate answers. It analyzes the code instead of just small snippets like other tools do. While it does not work one hundred percent of the time, it works most of the time, helping developers fix code quickly and providing examples of how to mitigate risk. For instance, if there is an SQL injection vulnerability, Cycode suggests sanitizing it beforehand. If the developer has not done it already, Cycode will analyze it and recommend how to fix the code, providing specific lines of code or a snippet on how it should look.

Cycode has positively impacted the organization by saving time in the pipeline and providing one platform for secret scanning, SAST, and Infrastructure as Code facilities. Cycode has a great ASPM solution feature that gives a dashboard and informs about vulnerabilities or risks in the application. Most notably, it has streamlined the experience for those waiting for pipeline results. After getting the result, developers see it in one tool and can simply go back to GitHub to view results without navigating through different tools. This saves considerable time, and when all information can be accessed in one application, it creates substantial value..”

Verified user[Read full review](#) 

Cyber Security Engineer (DevSecOps) at a manufacturing company with 10,001+ employees

“Cycode excels in secret scanning and is brilliant at finding and identifying secrets within code. The GitHub integration helps product teams run scans on their code during pull requests without requiring a task in their pipeline, allowing them to identify issues much earlier in the software development life cycle.

“The GitHub integration allows scanning to be performed as early as possible. Whenever product teams raise a pull request or commit to a GitHub repository, the integration identifies issues even before the scan runs in the pipeline. Since scanning happens in the version control system in GitHub rather than in the pipeline, it keeps the load on the pipeline simple and reduces the overall pipeline load.

“Measurable improvements and faster development are outcomes of using Cycode. Since it is integrated into GitHub as a GitHub app and performs PR scans, it makes the development process not just faster but more secure. It prohibits users from hard-coding secrets and pushes them to use secret vaults and managers, which is a much more secure method of handling credentials.

“Cycode helps with visibility into application security posture by having arguably the best dashboards and reporting among all the other tools in use, with different kinds of remediation funnels and MTTR data available in Cycode's dashboard that helps with overall application security posture management.

“Cycode helps prioritize vulnerabilities or findings with a custom risk score that can help prioritize findings. Even within secrets, it helps identify the severities associated with those secrets.

“Cycode supports collaboration between development and security teams well. The integration with GitHub makes it quite seamless..”

Verified user

DevSecOps Security Engineer at a manufacturing company with 10,001+ employees

[Read full review](#) 

Other Solutions Considered

“We chose Cycode because it has been in our enterprise for a long time, originally as an on-prem solution and then migrated to Cycode cloud. I did not compare it with other competitors in the market, as it was already integrated into our systems..”

Mritunjay-Kumar

Principle Architect at Ford Motor Company

[Read full review](#) 

“A proof of concept was conducted for multiple tools, including GitHub Actions, Checkmarx as the previous tool, and Cycode, along with considering additional tools..”

Verified user

Cyber Security Engineer (DevSecOps) at a manufacturing company with 10,001+ employees

[Read full review](#) 

“I was not part of the decision before choosing Cycode, so I am not aware of which options were evaluated. However, GitHub Advanced Security was believed to have been considered..”

Verified user

[Read full review](#) 

DevSecOps Security Engineer at a manufacturing company with 10,001+ employees

“Checkmarx was previously used as the solution. The reason for switching was convenience, as Cycode is more convenient due to its direct integration with GitHub, unlike the Checkmarx on-premises solution that was in place, which only provided SAST capability. For nearly the same pricing, although exact pricing cannot be confirmed, three services are now accessed with Cycode: SAST, Infrastructure as Code, and secret scanning..”

Verified user

[Read full review](#) 

Cyber Security Engineer (DevSecOps) at a manufacturing company with 10,001+ employees

ROI

Real user quotes about their ROI:

“A return on investment has been seen with Cycode. Overall, the security of assets and preventing the exposure of secret data is where Cycode excels. No specific metrics can be shared beyond that..”

Verified user

DevSecOps Security Engineer at a manufacturing company with 10,001+ employees

[Read full review](#) 

“Regarding the return on investment, I believe it provides value for money, especially for non-AI applications. We are still in the early stages of AI development, and while we are generating code and developing intelligent apps, I cannot comment on Cycode's effectiveness for AI applications yet because we have not evaluated it in that context..”

Mritunjay-Kumar

Principle Architect at Ford Motor Company

[Read full review](#) 

Use Case

“Cycode is used for our software development, maintaining clean code quality, and managing secrets within our enterprise. We write secure code by adhering to secure coding principles, ensuring that we do not embed secrets in our code. We utilize Dynatrace and other tools to manage these secrets, including certificates for connecting to memory stores and application configurations. Additionally, we have an API platform with complete API governance, where authentication happens through a client credential flow, involving unique client IDs and client secrets for API authorization. As part of our software development lifecycle, we promote a shift-left approach by testing locally and integrating with our development lifecycle, pushing our code to GitHub. Our GitHub code bases are enabled with Cycode to check for any secrets that may have been inadvertently committed, thus helping us uphold secure coding practices.

“In my experience as an integrator with Cycode, the biggest advantage is that it is platform agnostic and language agnostic. As a developer, I write Python and Kotlin programs, including Spring Web Flux and Spring Boot, and what I appreciate is that Cycode can be integrated with any software, services, or languages, whether it be TypeScript, React, or mobile apps built with React Native..”

Mritunjay-Kumar

Principle Architect at Ford Motor Company

[Read full review](#) 

“Cycode is used for multiple types of scanning including secrets, SAST scanning, and IAC misconfiguration scanning. Secret scanning was one of the first services launched using Cycode and is integrated into product teams' CI/CD pipelines for identifying hard-coded secrets within the code.

“Cycode is used for infrastructure as code misconfiguration scanning and SAST scanning to find code weaknesses. Both engines are solid with no complaints.

“As a policy, hard-coding secrets is prohibited. Cycode helps identify pieces of code that might be out of compliance. When the organization pivoted to GitHub Enterprise Cloud, this became a strong requirement for all product teams to comply with, and Cycode definitely assisted in that process.

“Cycode is used for secret scanning, IAC misconfiguration scanning, and SAST. Other tools are used for software composition analysis and container image scanning..”

Verified user

[Read full review](#) 

DevSecOps Security Engineer at a manufacturing company with 10,001+ employees

“I use Cycode for SAST scanning, Infrastructure as Code, and secret scanning, with a current proof of concept underway for containers.

Cycode scans all items when code is pushed into the Git repository, including secrets in that repository or in pull requests. This allows visibility into whether any secret tokens, email IDs, or data that should not be present are included before production deployment. The recommendation is to use vaults to save token secrets for application use. If someone has not adhered to this practice or accidentally used a token during development and forgot to change it before production, Cycode helps catch these violations. In the event of a code leak or cyber attack where code is exploited by vulnerabilities, tokens and secret information are not lost and cannot be further used to elevate application privileges.

Cycode results are integrated into the homegrown ASPM solution called Scout by using its APIs. Cycode has a valuable feature called risk intelligence that informs when there is a leak regardless of its source and provides a list of affected repositories. This helps in taking action and preparing an action plan. It becomes easier to resolve issues when the exact repositories are identified, and if a package is found vulnerable, it is possible to check which applications are using it. Cycode provides that repository information, so affected repository owners can be contacted to resolve issues, thus protecting against attacks or allowing countermeasures to be taken against tokens..”

Verified user[Read full review](#) 

Cyber Security Engineer (DevSecOps) at a manufacturing company with 10,001+ 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.

“Adoption and initial use of Cycode was fairly simple for the team. The GitHub integration made the process quite smooth as all assets in GitHub had to be bulk on-boarded to Cycode. Although the on-boarding and adoption were smooth and Cycode was scanning everything in GitHub, as a DevSecOps team, assets had to be mapped individually in order to perform application security posture management (ASPM), which took a good amount of time and remains an ongoing challenge..”

Verified user[Read full review](#) 

DevSecOps Security Engineer at a manufacturing company with 10,001+ employees

“An automated onboarding process is not currently in place, but a script or solution for developers organization-wide is being developed. Cycode has a pretty good onboarding page that is excellent. The significant advantage experienced with Cycode is that multiple services are leveraged; when a project or team is onboarded onto Cycode, it covers three services, highlighting that benefit. Beyond that, there is nothing remarkable that distinguishes it compared to other tools in the industry.

Cycode is utilized as a SaaS solution hosted on a private cloud..”

Verified user

[Read full review](#) 

Cyber Security Engineer (DevSecOps) at a manufacturing company with 10,001+ employees

Customer Service and Support

“Customer support has been excellent. While there has not been frequent direct interaction with customer support, from what has been heard during meetings, the rating would be nine out of ten..”

Verified user

Cyber Security Engineer (DevSecOps) at a manufacturing company with 10,001+ employees

[Read full review](#) 

Other Advice

“Cycode excels mainly in secret scanning, and if CLI was available in other types of scans like container scanning, the overall experience would have been better. Cycode's governance and security are good, and the AI remediation abilities through integrations like Secure Code Warrior are beneficial.

“The accuracy and reliability of Cycode's AI capabilities have not been fully tested. Others looking into using Cycode should move forward with it. It is a strong and robust tool for secret scanning.

“Overall, I rate Cycode a 7.5 out of 10. The rating reflects limitations such as the lack of a CLI for container scanning and some concerns about forced secret scanning, balanced against Cycode's excellence in secret scanning capabilities..”

Verified user

DevSecOps Security Engineer at a manufacturing company with 10,001+ employees

[Read full review](#) 

“Regarding machine learning algorithms, they help to detect open source dependency risks. Although we are still in the early stages of utilizing machine learning, I can state that fine-tuning the model during training is crucial, especially to avoid using PII or SPII data. I have not used the supervised fine-tuning capabilities of Cycode yet, so I'm unsure of how extensively it detects PII and SPII data or supports anomaly detection in these cases.

“Access governance and source control are very important in the DevSecOps workflow. Access control involves both coarse-grained and fine-grained authorization, which are crucial at every level of the architecture, whether it be application, infrastructure, or the software development lifecycle. In our enterprise, each team has their own Enterprise Management System (EMS), under

which all GCP native applications and projects are maintained. Access control is managed through Azure SSO and service accounts associated with every project. Each service that an application needs, such as Cloud Run, BigQuery, or Cloud SQL, requires specific permissions, forming a fine-grained access control structure based on the involved services and the infrastructure as code that each GCP team maintains with Terraform.

“The risk reduction and preventive measures we have taken since implementing Cycode are reflected in the extensive reports generated by every pipeline run. These reports detail the number of files scanned, including those from our object store and application configurations like secrets and Docker images used for deployment. The reports provide valuable information to the enablement and cybersecurity teams, making it accessible to executives across various EMS and GCP projects.

“I would rate this product a seven overall..”

Mritunjay-Kumar

Principle Architect at Ford Motor Company

[Read full review](#) 

“In the organization, sub-organizations have a regulatory compliance requirement to perform a SAST scan or security scan before going into production. Cycode helps adhere to these requirements well; while Cycode did not support Rust previously, it has now included the Rust language. However, support for legacy applications is still lacking, which presents a challenge since Cycode's vendor team has mentioned they do not plan to address this issue. Although it posed a challenge when transitioning from Checkmarx to Cycode, the experience has been beneficial overall as it delivers exact data and allows developers to see which repositories contain vulnerabilities. It even provides options to archive repositories that are no longer in use or required.

Cycode allows marking something as a false positive, giving the power to manage

security findings effectively. This access is restricted to only the team admin for that specific project, enabling them to mark items as false positives as needed.

Cycode is not being used as a medium to create tickets or anything of that nature in the organization.

Cycode provides an extensive dashboard that aids in prioritizing vulnerabilities and security issues that need addressing first, and it also features a customized risk score that can be utilized for prioritization.

For others looking into using Cycode, if they seek a tool with multiple services, excluding container services, Cycode is a solid option. It is a solid option for at least SAST and secret scanning, despite the non-use of [SCA](#). Cycode offers excellent secret scanning capabilities, and there does not appear to be another solution at the same pricing level that provides an equally good secret scanning tool like Cycode does.

Overall, Cycode receives a rating of eight out of ten..”

Verified user

Cyber Security Engineer (DevSecOps) at a manufacturing company with 10,001+ employees

[Read full review](#) 

Top Industries

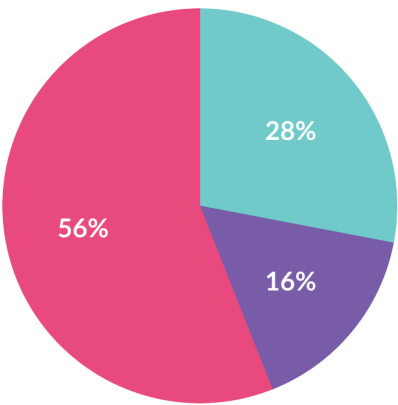
by visitors reading reviews



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