**Security99 secures ANZ (Australia and New Zealand) Small Medium Businesses Market with CodeSecure.** *CodeSecure will help 2.1 million small to medium businesses with inhouse development team to analyse their code and provides security insights at the early stages of their product development to reduce their cyber risk.*

**Melbourne, Security Magazine, 20th August 2021** – Security99 announced the launch of CodeSecure to benefit small to medium businesses (SMBs) in building secure applications. It automates the analysis of code and saves precious business hours for growing businesses. It helps users identify vulnerable packages and recommends minor security fixes.

BullGuard 2020 Research states that around 43% of SMBs lack cybersecurity defense plans. The pandemic has urged the business community to shift online. Another report from Alliant Cybersecurity states that 20% of businesses possess cybersecurity risks as they lack prevention of cyber-attacks. The Chief Security Officer of Fastly, Window Synder, said, 'One vulnerability is all an attacker needs.' 60% of Small and Medium Businesses affected by cyber-attacks end up closing business within 6 months [1]. Two-thirds of the data breaches have been caused by third party vulnerabilities [1]. SMBs, in general, do not have the resources or the budget to spend on cybersecurity. Hence there is a need for a product that can solve this problem. SMBs can now access an affordable and reliable pipeline tool, provided by RMIT (Royal Melbourne Institute of Technology) Cloud Innovation Center (CIC) powered by Amazon Web Services, to help keep them secure from cyber-attacks.

CodeSecure does the work of mitigating vulnerabilities. It is an online code analyser feature integrated with AWS (Amazon Web Services) Code Pipeline that helps identify the vulnerabilities. It uses data based on issues identified in more than 100 open-source security tools. It identifies the static code and provides suggestions to handle the security fixes. The development team now has easy access to an overview of security misconfigurations in the solution.

Previously, developers had to spend long hours finding and fixing security issues. Now, they can instantly validate their code to discover security vulnerabilities by passing it through the CodeSecure. CodeSecure assists the developers in identifying the security issues in the initial stages of the product development and keeps them secure by notifying the developer about it. It discovers the packages with potential security threats and suggests fixes. The product addresses the unintentional security threat opened by an authorized user in the code. This is implemented by collecting data from various AWS service logs and sending alert notifications when anomalies are detected. As an added feature, this product suggests the security measures be implemented to mitigate the security vulnerabilities. The product makes the deployment process hassle-free, helps save company resources and business hours spent on security validation and redundant code reviews.

Mary, the owner of an online consulting and recruiting firm, said that "I feel like a huge burden has been lifted from my shoulders now that my team is using this product. I would recommend every SMBs to give this product a go, to experience an automatic information security review and a hassle-free and secure deployment." She added an experience from her team developer, who was quoted as saying, "Never found a better way to avoid vulnerable packages. Each resource is safe now as only the authorized personnel can handle it based on tags".

Visit [www.security99.com](http://www.security99.com/) to use this product.

**Reference**

[1] ID Agent. 2021. 10 SMB Cybersecurity Statistics That Every Business Owner Needs to See. [Online] Available: https://www.idagent.com/blog/10-smb-cybersecurity-statistics-that-every-business-owner-needs-to-see/

**FAQs**

**Genral Questions**

1. Why use CodeSecure?

CodeSecure adapts the Shift Left Security Approach and brings the advantage of discovering security vulnerabilities earlier in the stages of development. It runs behind the scenes and does not interfere with the developer's code until it is run through the service.

1. How will it help my business?

It helps the organization avoid security vulnerabilities and save business hours spent by the testing and quality assurance team.

1. Does it have a trial version?

The users can register with Amazon Web Services (AWS) and get a free trial version for a month for a single project.

1. How much does it cost?

The cost depends on the usage of the service. It varies from $10 a month to more than $99 a month as per the usage of CodeSecure.

1. Does it send notifications?

The user gets notified via pop up notification and email alert for both successful and failed completion of scans.

1. What level of code security does the product provide?

CodeSecure provides a superior level of security for the users' code. CodeSecure detects most vulnerabilities and suggests security measures to patch those vulnerabilities to secure the code. The product has been optimized.

1. Does this product send weekly reports?

 CodeSecure gives the user the privilege of selecting report alerts. The user can choose daily, weekly, biweekly, or monthly reports based on the company's requirements.

1. Do you have a user manual or training provision for the product?

Yes. CodeSecure documentation provides the user with all the information required to use the service. It includes information on interpreting the logs. There is also a provision for the customers to email us for help, and the support team will get back within 48 hours (about two days).

1. How can we get started?

The users can get started by following the documentation provided on the website or email us to get support.

1. How can you ensure the product's sustainability with modern technologies and ways to misuse those technologies growing every day?

The current release is up to date with the current technology, and with every release, newer technology support will be added to the product.

**Technical Questions**

1. How does it stand out from other products?

CodeSecure does a few more security checks which have not been implemented in similar products. It also sends success or failure notifications via pop up and email alerts. The feature to check anomalies through logs is also one of the advantages of CodeSecure.

1. Can we migrate from other pipelines?

The migration from various products has been made simple by CodeSecure. The detailed documentation of migration will help the user.

1. Does it support all languages?

The CodeSecure currently supports major programming languages like Java, Python and C#. Future updates will include the support of other languages as well.

1. How can we be sure that our company/customer information is not being misused?

Security99 follows strict security guidelines and ensures that the data used in their product CodeSecure is not compromised.

1. What permissions are needed for this service?

CodeSecure must be provided read access to the code repository for scanning purposes. For auto-remediation cases, additional write access might be required.

1. What is CI/CD?

CI/CD stands for continuous integration and continuous deployment. Continuous integration refers to automated build and test steps when code changes are merged to the repository. Continuous deployment refers to releasing the code changes in the repository to the production/live environment.

1. How does it work for codes in private repositories?

The user must provide access to the private repositories by allowing AWS CodePipeline to create a secure connection. It differs for different source control providers, and users can follow the documentation for further details.

1. How easy will it be to update to new versions?

CodeSecure provides the user with the option to upgrade to a newer version only if required. It has automated and manual update options with information about both mentioned in the documentation.

1. What kind of data analytics is used in CodeSecure?

It does the static code analysis of the application branch.

1. Will the option for code analysis be embedded in the pipeline, or will a plugin need to be installed in the channel?

Initially, it will be provided as a plugin to be installed in the pipeline. In further updates, CodeSecure will be embedded with the CodePipeline for code analysis to improve the security posture of the code.

1. Is there a possibility that this pipeline can slow down our deployment process?

CodeSecure is a part of CodePipeline, and it analyses the code to find vulnerabilities. The time required to analyze the code depends on the size of the repository.

12. **What risks does it look for in the code?** Does it do it natively, or leverage 3rd party tools/plugins?

CodeSecure uses third party tools to identify the vulnerabilities in the code.

13. Is there a way to enable/disable security checks, depending on the environment? (dev/test/prod)

The security checks are enabled by the end users. The user has the option to create a security check for the environment required and disable it when not required.

**14. How will you keep the product up to date with the latest vulnerabilities?**