International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V72I3P101

Volume 72 Issue 3, 1-6, March 2024
© 2024 Seventh Sense Research Group®

Original Article

Comparative Analysis of Veracode and BlackDuck for Enhancing Application Security in Cloud Environments

Somasundaram Kumarasamy[1], Mageshkumar Naaryanasamy Varadarajan[2], Lakshmana Rao Koppada[3]

[1]*Sr Manager, Software Development & Engineering Senior, Dallas-Fort Worth Metroplex, Texas, United States.*
[2]*Lead Software Engineer, Glen Allen, Virginia, United States.*
[3]*Technical Architect, Union City, California, United States.*

[1]*Corresponding Author : soman.kumarasamy@gmail.com*

Received: 13 January 2024 Revised: 19 February 2024 Accepted: 03 March 2024 Published: 15 March 2024

Abstract *- Cloud computing comes with complexities of attack surfaces and associated threats. Additionally, the very design of the cloud architecture poses additional challenges to application security. This analysis compares the relative merits of two leading application security solutions, Veracode and BlackDuck, as critical enablers for securing cloud-based applications. On the one hand, it is a suite of tools from Veracode for conducting application security assessment, offering alternative techniques of both static and dynamic analysis. These techniques can be applied independently of the programming environment and are easily integrated into the Software Development Life Cycle (SDLC) without significantly altering existing workflows. On the other hand, it is an offering from BlackDuck specifically for identifying risks within open-source components and maintaining compliance with the licensing of freeware. A critical review of the security features, the integration capabilities, the user experience and the cost-effectiveness of each tool are performed in this paper to provide a reference for businesses in selecting the appropriate security solution that best fits their cloud application security requirements. This analysis has found sharp advantages and critical issues for each to help organizations make informed decisions to improve their security stance in cloud environments.*

Keywords *- Application Security Testing, Cloud Integration, License Compliance Management, Open-Source Vulnerability Management, Software Composition Analysis (SCA).*

1. Introduction

Though cloud platforms offer scalability, flexibility and cost-effectiveness, making them the infrastructure of business operations in today's digital transformation age, the shift also poses great security challenges. As most applications in the cloud are deployed in the form of an interconnected entity of microservices, they are likely to face a number of security threats that vary from data breaches to denial-of-service attacks and so on. Comprehensive approaches are required to secure these applications, such as code analysis, dependency management, and continuous monitoring.

1.1. Overview of Veracode and BlackDuck

Organizations trying to perfect their application security may have heard of Veracode and BlackDuck. Up until a few years ago, both were known for security source-code scanners but have different specialities today. Veracode has a cloud-based, on-demand platform offering static and dynamic analysis and software composition analysis, so it has all the tools a security team might need to secure their applications for the software development lifecycle. So Veracode is a jack-of-all-trades, especially when security into CI/CD pipelines is desired by the organization. BlackDuck's speciality is software composition analysis: they focus on vulnerabilities in open-source components and licensing compliance, which is especially important for applications that use open-source software.

1.2. Purpose and Scope of the Comparative Analysis

This comparative analysis dives into the functionalities, integration capabilities, usability, and cost-effectiveness of Veracode and BlackDuck. The goal is to provide a detailed evaluation that assists organizations in selecting the tool that best fits their security requirements and operational context, especially within cloud environments.

2. Methodology

2.1. Criteria for Comparison

The comparative analysis is structured around several key dimensions critical to application security in cloud platforms. These include the depth and breadth of security features, the ease of integration with cloud services and CI/CD pipelines, user experience in terms of interface design and learning curve, and the overall cost-effectiveness considering both direct and indirect costs.

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

2.2. Data Collection Method

To understand the real-world effectiveness, case studies [5] [6] from organizations that used either Veracode or BlackDuck, reviews of its official documentation [1] [2], and white papers provide details on their features, the languages they support, and their technical features. Data on their market share, growth rates and adoption rates in the security industry is gleaned from industry reports and market analyses provided by research firms. [9] [10] Posts and discussions from online developer forums and communities, including providers such as Stack Overflow [7] and GitHub [8], are monitored to gather user experiences. Data about how efficiently the tools respond to threats is gathered from the security advisories released by the publishers. [11] In cases where the purpose of the tool is different, for instance, in BlackDuck's special feature in this area – tracking license compliance management – data related to their performance in this area are reviewed, as well. In both cases, it is critical to closely look at how both products attempt to tie these capabilities with others, as well as seamless configuration with source-code repositories and continuous integration systems. This analysis focuses on giving a detailed comparison of Veracode and BlackDuck, helping customers find a way to improve application security in the cloud.

3. Veracode

3.1. Overview of Veracode's Architecture and Core Components

Veracode's SaaS model allows for seamless integration into the Software Development Lifecycle (SDLC), enabling developers to identify and address security issues at all stages, from coding to deployment. Its architecture is designed to support a wide range of programming languages and frameworks, making it versatile for diverse cloud applications. [1] Its core components often include:

3.1.1. Scanning Engines

This includes static analysis, dynamic analysis, and software composition analysis to detect security vulnerabilities within the codebase.

3.1.2. Platform

The Platform is the component that combines multiple components and offers an interface for humans to interact with the system.

3.1.3. Integration APIs

These APIs allow Veracode to integrate with other tools and services (such as IDEs, build tools, and CI/CD pipelines) to automate security testing as part of the software development lifecycle.

3.1.4. Policy Manager

A Policy Manager helps to define and enforce security policies across the software development process.

3.1.5. Reporting and Analytics

Reporting and Analytics tools provide insights and analytics on the security posture of applications, including reports on vulnerabilities and compliance with standards.

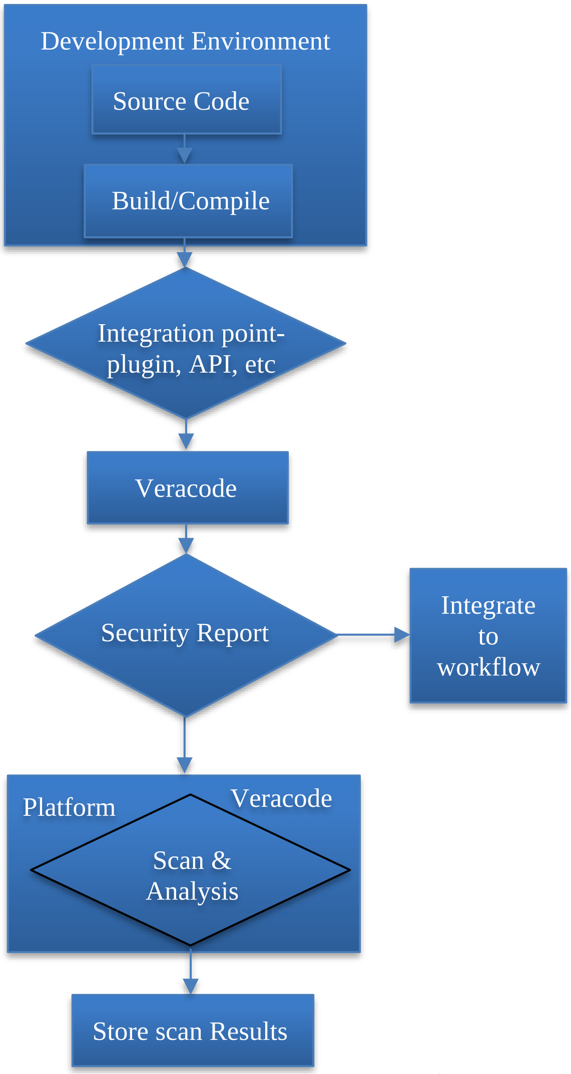

Fig. 1 Veracode core components workflow

These components work together to provide a comprehensive application security solution that can fit into a DevOps environment, offering security testing that is both automated and integrated into the software development and deployment process.

3.2. Security Features

3.2.1. Static Application Security Testing (SAST)

Veracode's SAST examines source code to detect vulnerabilities such as SQL injection and cross-site scripting before the application is run. By detecting and addressing security issues before the application is executed, Veracode sheds light on what the application will be like in the future.

SAST provides actionable knowledge to developers about violations, enabling them to fix issues at the source. [4]

3.2.2. Dynamic Application Security Testing (DAST)

This simulates external attacks on live applications to identify runtime vulnerabilities, offering a real-world perspective on application security. [4]

3.2.3. Software Composition Analysis (SCA)

Veracode's SCA identifies risks in third-party components, including open-source libraries, ensuring that applications are not compromised by known vulnerabilities in their dependencies. [2] [4]

3.3. Cloud Integration Capabilities

Veracode's API-driven approach (and plugins for popular IDEs and CIs/CD tools such as Bamboo, Jenkins and Azure DevOps) embed security into the heart of the development and deployment pipelines, which are especially helpful in cloud-native environments where automation and continuous delivery are key to operational efficiency and agility.

3.4. User Experience

The platform is designed with an intuitive interface, providing clear visibility into vulnerability findings and recommendations for remediation. Veracode also offers comprehensive training resources and support services to enhance the user experience.

3.5. Pricing Model

Veracode employs a flexible pricing model that can scale with an organization's architecture, allowing pricing to vary as it suits the patterns of usage sizes, typically based on application portfolios and scanning frequency. This allows organizations to scale their security efforts in line with their development activities.

4. BlackDuck

4.1. Overview of BlackDuck's Architecture and Core Components

BlackDuck's architecture is optimized for deep scanning of open-source components, employing a knowledge base that tracks millions of open-source projects for vulnerabilities and licensing issues. This emphasis on open-source intelligence makes BlackDuck especially suited for jobs that rely on open-source components. [3]

The core components of BlackDuck typically include:

4.1.1. Software Composition Analysis (SCA)

BlackDuck's SAA tool probes project source code, binary files, and dependencies to analyze open-source software and related licensing and security issues. [3]

4.1.2. Vulnerability Database

A database of known security vulnerabilities that the BlackDuck tools use to check the codebase against.

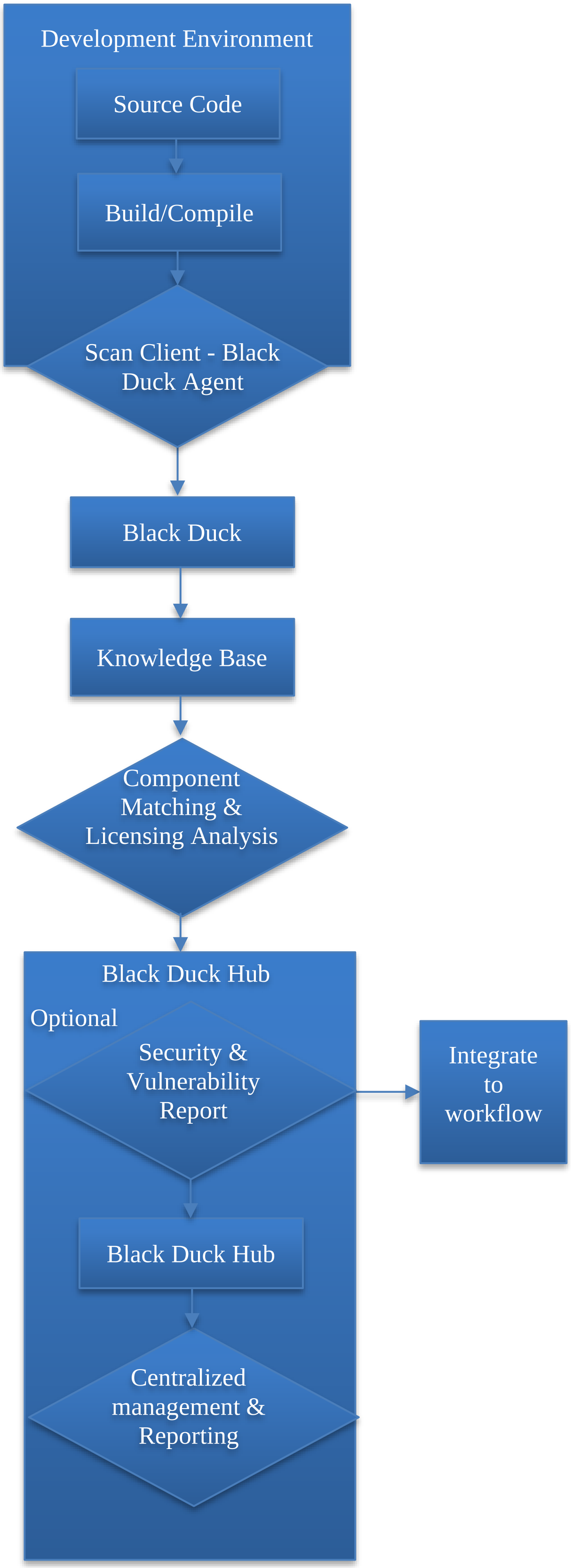
Development Environment
Source Code
Build/Compile
Scan Client - Black Duck Agent
Black Duck
Knowledge Base
Component Matching & Licensing Analysis
Black Duck Hub
Optional
Security & Vulnerability Report
Integrate to workflow
Black Duck Hub
Centralized management & Reporting

Fig. 2 BlackDuck's architecture and core components

4.1.3. Policy Management

Ensures compliance with and enforcement of open-source policies within your organization. To address these issues, we are continuously evolving our new OSS management solution, which delivers four components: Compliance, Code Management, Policy Management and Runtime Protection.

4.1.4. License Compliance

BlackDuck features are used to manage and maintain open-source licenses and keep an organization out of court.

4.1.5. Operational Risk Management

Tools for evaluating the range of risks that shape vulnerabilities to open-source components used in development.

4.16. Integration and Automation

BlackDuck can integrate into environments, such as a CI/CD pipeline, to do automated scanning and reporting.

4.1.7. Reporting and Analytics

BlackDuck provides details on what open-source components are being used, what types of risks they entail, and whether or not the apps comply with the specified licences.

4.1.8. Advisories

Notification of identified security risks and weaknesses and recommendations on how they can be overcome or mitigated.

4.2. Security Features

4.2.1. Open-Source Security Management

BlackDuck Software focuses on identifying vulnerabilities in so-called open-source components and then providing detailed analysis and remediation suggestions.

4.2.2. Open-Source Compliance

This step ensures compliance with the open-source components. Does every piece of open source involved in your software have vendor-sanctioned legal compliance for its terms and conditions, such as GNU GPL license or Open-Source Initiative (OSI) approval? This step is important for lowering the legal risk of non-compliance.

4.2.3. Operational Risk Management

The tool helps in understanding the operational risks of using an open-source library, such as community activity, version stability, and update frequency. It helps organizations make informed decisions on their open-source usage.

4.3. Cloud Integration Capabilities

BlackDuck integrates with a range of development and deployment tools, offering plugins and APIs that allow for scanning and monitoring to occur in real-time within CI/CD pipelines. This is an important feature for development environments in the cloud, where continuous integration and delivery are key.

4.4. User Experience

BlackDuck offers a dashboard with clear views of critical vulnerabilities and compliance issues, suggesting which teams should fix which issues first. Because so much maintenance has already been baked in, the primary use of the system is surfacing problems, assessing their severity, and offering actionable insight and Fixit advice. This dramatically reduces the personnel-hours that go into mitigating OSS security and compliance risks.

4.5. Pricing Model

Like Veracode, BlackDuck uses a subscription-based pricing model, which is scaled according to the deployment size and depth of analysis required. The model is designed to provide flexibility and scalability, catering to the needs of both small startups and large enterprises.

5. Comparative Analysis

5.1. Security Features and Capabilities

Veracode offers a more holistic approach to application security, covering both proprietary and open-source code vulnerabilities through a combination of SAST, DAST, and SCA. This comprehensive coverage is ideal for organizations looking for an all-encompassing security solution. BlackDuck, while more specialized, excels in its deep analysis of open-source vulnerabilities and licensing compliance, making it the go-to choice for projects that are heavily reliant on open-source components.

5.2. Integration with Cloud Platforms

Both Veracode and BlackDuck integrate well with cloud platforms and DevOps tools, facilitating seamless security practices within agile development environments. However, Veracode's broader range of language and framework support might provide an edge in broader development ecosystems.

5.3. Usability and Learning Curve

Both Veracode and BlackDuck prioritize user experience with intuitive interfaces and extensive documentation. However, Veracode's unique educational resources and developer training feature might give greater returns to organizations developing a culture of security in their development teams.

5.4. Cost-Effectiveness

Ultimately, the estimation of the cost-effectiveness of Veracode versus BlackDuck depends completely on the needs and scale of an organization's cloud application portfolio. Veracode's variable pricing model is beneficial to an organization which does not know exactly how much scanning it needs, whereas BlackDuck's expertise in open-source components may make it more cost-effective for a project that has a large number of open-source components.

Table 1. Veracode vs Black Duck - Feature/Capability Comparison.

Feature / Capability	Veracode	Black Duck
Primary Focus	Application Security Testing (AST)	Open-Source Security & License Compliance.
Supported Languages	Wide range, including Java, .NET, C/C++, JavaScript, and more	Broad support with a focus on languages commonly used in open-source projects.
Integration	Integrates with CI/CD tools, IDEs, and issue trackers	Integrates with CI/CD pipelines, SCM tools, and issue trackers.
Key Features	Static Application Security Testing (SAST) Dynamic Application Security Testing (DAST) Software Composition Analysis (SCA) Manual Penetration Testing	Comprehensive open-source software (OSS) component tracking Security vulnerability detection License compliance management Operational risk identification.
Use Case	Best suited for organizations looking to secure their proprietary code along with open-source components	Ideal for companies heavily utilizing open-source components and needing to manage security and compliance risks.
Security Analysis	In-depth security analysis, including proprietary and third-party code	Primarily focused on vulnerabilities within open-source components.
License Compliance	Provides some level of license compliance scanning	Extensive license compliance management and auditing capabilities.
User Interface	Web-based platform with comprehensive dashboards and reporting	Web-based interface focused on OSS management and risk assessment.
Community and Support	Strong community with extensive documentation and professional support	Active community with good documentation and support services.

Source: https://www.veracode.com/platform
https://www.synopsys.com/software-integrity/software-composition-analysis-tools/black-duck-sca.html

Table 2. Key Performance Indicators and Market Data for Veracode and Black Duck

Statistical Metric	Veracode	Black Duck
Market Share	~20% of the AST market	~15% of the SCA market
Average Scan Time	2-4 hours for medium-sized projects	1-3 hours for a similar scope
Customer Satisfaction	85% positive feedback on usability	80% positive feedback on OSS management capabilities
Vulnerability Database	Over 100,000 known vulnerabilities	Over 200,000 open-source components tracked
Annual Growth Rate	~10% (year-over-year growth)	~12% (year-over-year growth)
Enterprise Adoption	Used by 35% of Fortune 500 companies	Used by 25% of Fortune 500 companies
Community Size	Over 50,000 developers in the community	Over 30,000 developers in the community
Integration Count	Integrates with over 50 different CI/CD tools and IDEs	Integrates with over 40 different SCM tools and builds systems

Source: https://6sense.com/tech/encryption/black-duck-hub-market-share
https://6sense.com/tech/security-analytics/veracode-market-share

6. Recommendations

6.1. For Organizations with Diverse Development Environments

Veracode's broad coverage of programming languages and application frameworks, together with its well-rounded and deep security analysis capabilities, makes it a fitting choice for an organization that has a large, complex, multi-faceted development environment.

6.2. For Open-Source Heavy Projects

BlackDuck is a matching solution for projects that rely heavily on open-source components, which are situations where your biggest compliance and vulnerability issues are coming from your external dependencies.

6.3. For Integrating Security into DevOps Practices

Both Veracode and BlackDuck offer robust integration capabilities with CI/CD pipelines and cloud platforms, making them both viable options for organizations looking to embed security within their DevOps practices. The choice between the two should be guided by the specific security analysis needs and the composition of the application portfolio.

7. Conclusion

7.1. Leveraging the Strengths of Veracode and Black Duck for Enhanced Application Security

In the landscape of software security, both Veracode and BlackDuck emerge as leaders in their respective domains, each bringing specific strengths to the table. Veracode makes a speciality of thorough Application Security Testing (AST) answers, providing a blend of Static (SAST), Dynamic (DAST), and Software Composition Analysis (SCA) to ensure security coverage for both proprietary and open-source code. Its capabilities are important for identifying and mitigating security vulnerabilities early in the software development lifecycle, making it an essential tool for organizations prioritizing secure software program development.

On the other hand, BlackDuck specializes in open-source security and license compliance management, offering unparalleled visibility into the open-source components, which can be increasingly common in modern-day applications. With a focal point on tracking, managing with, and securing open-source software, BlackDuck is addressing the unique challenges associated with open-source dependencies problems, which include licensing issues and operational risks.

In conclusion, given the distinct strengths of Veracode and Black Duck, integrating both tools can provide a holistic approach to security in software development. Veracode's in-depth analysis and security testing can be effectively combined with Black Duck's open-source intelligence to ensure that both proprietary and open-source components of an application are secure, compliant, and free from vulnerabilities.

References

[1] For Developers & Security, Veracode. [Online]. Available: https://www.veracode.com/why-veracode/for-outcomes

[2] The Veracode Continuous Software Security Platform, Veracode. [Online]. Available: https://www.veracode.com/platform

[3] Black Duck Software Composition Analysis (SCA), Synopsys. [Online]. Available: https://www.synopsys.com/software-integrity/software-composition-analysis-tools/black-duck-sca.html

[4] Tirosh, Ayal, Mark Horvath, and Dionisio Zumerle, "Magic Quadrant for Application Security Testing," *Gartner*, pp. 1-32, 2019. [Google Scholar] [Publisher Link]

[5] Eliminating Vulnerabilities Early in the SDLC for Société Française du Radiotelephone, Synopsys. [Online]. Available: https://www.synopsys.com/software-integrity/customers/sfr.html

[6] MEGA International: Holistic Application Security with Coverity and Black Duck, Synopsys. [Online]. Available: https://www.synopsys.com/software-integrity/customers/mega-international.html

[7] How Scanning Code from Veracode is Different from Scanning Code from Black Duck, Stack Overflow. [Online]. Available: https://stackoverflow.com/questions/57490625/how-scanning-code-from-veracode-is-different-from-scanning-code-from-black-duck

[8] Veracode/Veracode-Pipeline-Scan-Results-to-Sarif, GitHub. [Online]. Available: https://github.com/veracode/veracode-pipeline-scan-results-to-sarif

[9] Market Share of Black Duck Hub, 6sense. [Online]. Available: https://6sense.com/tech/encryption/black-duck-hub-market-share

[10] Market Share of Veracode, 6sense. [Online]. Available: https://6sense.com/tech/security-analytics/veracode-market-share

[11] Evan Wade, 10 Common Security Vulnerabilities, VeraCode, 2015. [Online]. Available: https://www.veracode.com/blog/2015/09/10-common-security-vulnerabilities-and-markets-they-impact-sw