



**DerScanner против Micro Focus  
Fortify, Checkmarx, HCL AppScan  
Source, Veracode, Synopsys.**

**Сравнение с конкурентами**

## Оглавление

<b>ИСПОЛНИТЕЛЬНОЕ РЕЗЮМЕ.....</b>	<b>3</b>
DERSCANNER .....	3
MICRO FOCUS FORTIFY .....	3
CHECKMARX.....	4
HCL (EX. IBM) APPSCAN SOURCE .....	5
VERACODE .....	5
SYNOPSIS COVERITY CODE ADVISOR.....	6
<b>ПОДРОБНОСТИ ОЦЕНКИ .....</b>	<b>7</b>

## Исполнительное резюме

### DerScanner

#### Основные моменты

- **Комплексная платформа безопасности приложений:** Единое решение, объединяющее SAST, DAST, SCA, MAST и бинарный анализ для устранения как известных, так и неизвестных угроз для кода на протяжении всего жизненного цикла разработки программного обеспечения (SDLC).
- **Лидирующее на рынке покрытие стека разработчиков в SAST:** Поддерживает 43 языка программирования, что является самым высоким показателем на рынке, включая популярные и развивающиеся языки, с эксклюзивной поддержкой Delphi, Perl, ABAP и Solidity в смарт-контрактах на базе Ethereum.
- **Двухэтапное тестирование мобильной безопасности:** обеспечивает полную защиту за счет тщательного тестирования мобильных приложений во время разработки (исходный код) и после их запуска в Google Play и App Store (бинарный анализ), гарантируя отсутствие уязвимостей в производстве, защищая и ваше приложение, и ваших пользователей.
- **Минимизация ложных срабатываний:** Используется собственный движок Confi AI, работающий на основе искусственного интеллекта, для снижения количества ложных срабатываний, фильтрации уязвимостей и предоставления действенных рекомендаций после проверки.
- **Расширенный анализ двоичных файлов:** Возможность статического анализа исполняемых файлов без отладочной информации, что очень важно для оценки мобильных приложений и устаревшего программного обеспечения без исходных кодов.
- **Интерактивный анализ (IAST):** объединяет возможности DAST и усиливает результаты SAST путем перекрестного сопоставления и корреляции обнаруженных уязвимостей, предлагая единое решение для выявления и устранения уязвимостей в реальных веб-приложениях.
- **Унифицированный анализ состава программного обеспечения:** Встроенный генератор SBOM и визуальный график дерева зависимостей позволяют получить максимальную видимость компонентов и зависимостей проекта с открытым исходным кодом. Этот единый подход позволяет проактивно обнаруживать уязвимости, снижать риски цепочки поставок, такие как typosquatting и starjacking, обеспечивать соответствие лицензиям и выбирать безопасные пакеты с высокими показателями здоровья, защищая ваш проект от потенциальных угроз и юридических проблем.
- **Разработано для сотрудников службы безопасности:** Удобный интерфейс и отчеты, разработанные специально для сотрудников службы безопасности, исключают необходимость в навыках разработки.
- **Гибкие варианты развертывания:** Выбирайте между локальной установкой, обеспечивающей полный контроль над производительностью, безопасностью и конфиденциальностью в закрытых средах, и SaaS-решением с мгновенной доступностью. Развертывание на месте обеспечивает более быстрое сканирование и полный контроль, идеально подходит для сред без доступа в Интернет.
- **Гибкость и свобода ценообразования:** В отличие от традиционных поставщиков AppSec, использующих модели ценообразования, основанные на потреблении - тарификация по пользователям, разработчикам, строкам кода или сканированию приложений, - DerScanner предлагает единую политику лицензирования, обеспечивающую настоящую гибкость. С помощью одной лицензии вы можете подключить неограниченное количество разработчиков, сканировать неограниченное количество приложений и обрабатывать неограниченные объемы кода, что дает вам полную свободу без скрытых затрат.

### Micro Focus Fortify

#### Основные моменты

- **Поддержка языков программирования достойная:** Поддерживает 27 языков программирования.
- **Поддерживается анализ двоичного кода:** Статические оценки помогают разработчикам выявлять и устранять уязвимости в двоичном или байт-коде для создания более безопасного программного обеспечения.

- **Легкая интеграция с конвейером CI/CD:** Интегрируется с различными CI/CD, IDE, репозиториями
- **Выявление ошибок, уязвимостей и запахов кода:** Micro focus Fortify помогает проактивно улучшать кодовую базу, выявляя потенциальные проблемы до того, как они станут проблемами.

## Lowlights

- **Обнаружение недокументированных функций отсутствует:** Micro Focus Fortify не предназначен для выявления недокументированных функций.
- **Ложные положительные/отрицательные результаты:** Как и любой автоматизированный инструмент безопасности, Micro Focus Fortify может генерировать ложные срабатывания и отрицательные результаты, что требует ручной проверки и может отнимать много времени.
- **Поддержка языков:** Хотя Micro Focus Fortify поддерживает большое количество языков, он не охватывает Groovy, Rust и Scala.
- **Стоимость и модель ценообразования:** Для некоторых предприятий, особенно малых или начинающих, цена внедрения Micro Focus Fortify может представлять значительную проблему, учитывая ее потенциально высокую стоимость по сравнению с другими вариантами.
- **Модель поставки:** Развертывание SaaS предоставляет ограниченные возможности
- **Рекомендации по настройке WAF:** Micro Focus Fortify не предоставляет рекомендаций по настройке WAF.

## Checkmarx

### Основные моменты

- **Поддержка языков программирования достойная:** Поддерживается 27 различных языков программирования.
- **Интеграция с инструментами и практиками безопасности:** Этот статический анализатор исходного кода имеет богатую функциональность и множество коннекторов для интеграции с SDLC.
- **Доступ к CLI и API:** Интерфейс командной строки (CLI) и API доступны для упрощенного управления сценариями и автоматизации.
- **Управление ложными срабатываниями:** Инструмент позволяет управлять и фильтровать ложные срабатывания.

## Lowlights

- **Обнаружение недокументированных функций отсутствует:** Checkmarx не предназначен для выявления недокументированных особенностей.
- **Нет бинарного анализа:** Checkmarx не анализирует бинарные файлы. Это ограничивает вас в изучении сторонних компонентов или мониторинге кода на рабочих серверах.
- **Варианты развертывания:** SaaS-развертывание недоступно, есть только локальная установка.
- **Предназначен в первую очередь для разработчиков:** Checkmarx - инструмент, ориентированный на разработчиков, и может оказаться слишком сложным для использования сотрудниками службы кибербезопасности.
- **Стоимость и модель ценообразования:** Для некоторых предприятий, особенно малых или начинающих, цена внедрения Checkmarx может представлять значительную проблему, учитывая ее потенциально высокую стоимость по сравнению с другими вариантами.
- **Отсутствует корреляция между SAST и DAST:** Хотя Checkmarks предлагает DAST и SAST, эти методы не обеспечивают единой работы. Поэтому вы не можете соотнести результаты SAST и DAST и определить приоритетность уязвимостей, обнаруженных обоими методами.
- **Отсутствуют рекомендации по настройке WAF:** Checkmarks не дает рекомендаций по настройке WAF, что ограничивает ваши возможности по устранению последствий.

## HCL (ex. IBM) AppScan Source

### Основные моменты

- **Поддерживает множество языков:** Поддерживает 22 различных языка программирования, что выше среднего.
- **Легкая интеграция с конвейером CI/CD:** Интегрируется с различными CI/CD, IDE, репозиториями
- **Доступ к CLI и API:** Интерфейс командной строки (CLI) и API доступны для упрощенного управления сценариями и автоматизации.
- **Выявление ошибок, уязвимостей и запахов кода:** AppScan помогает проактивно улучшать кодовую базу, выявляя потенциальные проблемы до того, как они станут проблемами.

### Lowlights

- **Ценообразование:** Хотя HCL AppScan может показаться экономически выгодным на нижних уровнях, модель ценообразования имеет существенные ограничения. Плата взимается за каждого авторизованного пользователя, и эти лицензии не подлежат передаче. Если вам понадобится передать или использовать плавающие лицензии, расходы быстро возрастут. Кроме того, корпоративные лицензии без ограничений приводят к значительному повышению цены, что делает масштабирование дорогостоящим.
- **Обнаружение недокументированных функций отсутствует:** HCL не предназначена для обнаружения недокументированных функций.
- **Нет бинарного анализа:** HCL не анализирует бинарные файлы. Это ограничивает вас в изучении сторонних компонентов или мониторинге кода на рабочих серверах.
- **Варианты развертывания:** Решение может быть установлено на сервере заказчика или предоставляться по модели SaaS, но с ограниченной функциональностью.
- **Поддержка языков:** Хотя AppScan поддерживает большое количество языков, он не охватывает Groovy, Kotlin, Scala и Swift.
- **Ложные срабатывания:** HCL дает большое количество ложных срабатываний, которые необходимо перепроверять вручную.
- **Предназначен в первую очередь для разработчиков:** HCL - инструмент, ориентированный на разработчиков, и может оказаться слишком сложным для использования сотрудниками службы кибербезопасности.
- **Рекомендации по настройке WAF:** AppScan не дает рекомендаций по настройке WAF, что ограничивает возможности устранения последствий.
- **Стоимость и модель ценообразования:** Для некоторых предприятий, особенно малых или начинающих, цена внедрения AppScan может представлять значительную проблему, учитывая его потенциально высокую стоимость по сравнению с другими вариантами.

## Veracode

### Основные моменты

- **Поддерживает множество языков:** Поддерживает 25 различных языков программирования, что выше среднего.
- **Поддержка языка:** Veracode - единственный поставщик, поддерживающий язык программирования RPG.
- **Анализ исполняемых файлов:** Veracode - единственное решение, способное анализировать исполняемые файлы, но только при наличии отладочной информации и исходного кода. Это серьезное ограничение, которое практически сводит на нет это преимущество.

### Lowlights

- **Ценообразование:** Модель ценообразования Veracode - взимание платы за приложение в SAST, за URL в DAST и за проект в SCA - может быстро стать непомерно дорогой для крупных, динамичных проектов. В отличие от этого, DerScanner предлагает более экономичное решение с лицензиями Enterprise, которые обеспечивают

неограниченное сканирование для проектов любого размера и количества, обеспечивая большую гибкость и свободу.

- **Развертывание только по принципу SaaS:** Предложение облачного решения без возможности установки на месте. Несмотря на удобство, пользователи часто выражают недовольство медленным временем сканирования и ограниченным контролем над процессом.
- **Обнаружение недокументированных функций отсутствует:** Veracode не предназначен для обнаружения недокументированных функций.
- **Отсутствует тестирование мобильных приложений в магазине:** Veracode не способен протестировать мобильное приложение, используя URL-адрес приложения из Google Play или AppStore.

## Synopsys Coverity Code Advisor

### Основные моменты

- **Поддержка языков:** Однако это единственный анализатор, поддерживающий языки Fortran и Cuda.
- **Легкая интеграция с конвейером CI/CD:** Интегрируется с различными CI/CD, IDE, репозиториями
- **Доступ к CLI и API:** Интерфейс командной строки (CLI) и API доступны для упрощенного управления сценариями и автоматизации.

### Lowlights

- **Цены:** Synopsys взимает плату за каждого члена команды, что делает ее менее выгодным вариантом для больших команд. По мере роста команды растет и счет, что со временем может привести к значительным дополнительным расходам. В отличие от этого, DerScanner обеспечивает большую гибкость и свободу, предлагая лицензии Enterprise с неограниченным числом пользователей, что позволяет расширять команду без увеличения расходов.
- **Обнаружение недокументированных функций отсутствует:** Synopsys не предназначена для обнаружения недокументированных функций.
- **Нет бинарного анализа:** не анализирует бинарные файлы. Это ограничивает вас в изучении сторонних компонентов или мониторинге кода на рабочих серверах.
- **Поддержка языков:** анализатор Synopsys поддерживает относительно небольшое количество (19) языков программирования и не совместим с Delphi, ABAP или Groovy, которые становятся все более популярными.
- **Варианты развертывания:** SaaS-решение недоступно, возможна только локальная установка.
- **Решения Synopsys требуют масштабного обучения** и поддержки со стороны поставщика, поскольку конечные пользователи сталкиваются с трудностями при обучении работе с продуктом.
- **Synopsys не интегрирует отдельные продукты:** Synopsys предлагает различные продукты для защиты приложений, которые не объединены в единую платформу. Например, White Hat Dynamic позволяет проводить анализ DAST, а Black Duck - анализ SCA и SCS. Модуль SCS анализирует только целостность зависимостей, но не целостность исходного кода и сборки.
- **Доставка обновлений:** базы данных уязвимостей могут обновляться только автоматически.

## Подробности оценки

Нет.	Критерий	DerScanner	Micro Focus Fortify	Checkmarx	Источник HCL AppScan	Veracode	Synopsys Coverity Code Advisor (SAST) WhiteHat Dynamic (DAST) Black Duck (SCA)
<b>1. Технологии анализа уязвимостей и недокументированных возможностей</b>							
1.1.	Поиск уязвимостей	да	да	да	да	да	да
1.2.	Поиск недокументированных функций	да	нет	нет	нет	да	нет
1.3.	Анализ двоичного кода	да	да	нет	нет	Да, но только с отладочной информацией.	нет
1.4.	Проверка обфусцированного кода	да	да	нет	нет	нет	нет
1.5.	Проверка приложений, написанных более чем на одном языке	да	да	да	да	да	да
1.6.	Анализ состава программного обеспечения (SCA)	да	да	да	да	да	да
1.7.	Лексический анализ	да	да	да	да	да	да
1.8.	Анализ синтаксиса	да	да	да	да	да	да
1.9.	Семантический анализ	да	да	да	да	да	да
1.10.	Анализ пятен	да	да	да	да	да	да
1.11.	Анализ постоянного распространения	да	да	да	да	да	да
1.12.	Анализ распространения типов	да	да	да	да	да	да
1.13.	Анализ синонимов	да	да	да	да	да	да
1.14.	Анализ графа потока управления	да	да	да	да	да	да
1.15.	Подключение внешних инструментов сборки	да	нет	нет	нет	нет	нет
<b>2. Анализ исходного кода</b>							
2.1.	АВАР	да	да	да	нет	нет	нет
2.2.	Сценарий действия	нет	да	нет	нет	нет	нет
2.3.	Арех	да	да	да	да	нет	нет
2.4.	ASP	нет	да	да	да	да	да
2.5.	ASP.NET	да	да	да	да	Только из IDE	да
2.6.	C/C++	да	да	да	да	Только из IDE	да
2.7.	C#	да	да	да	да	Только из IDE	да
2.8.	Objective-C	да	да	да	да	Только из IDE	да
2.9.	COBOL	да	да	да	да	да	нет
2.10.	Холодный синтез	нет	да	нет	нет	Требуется предварительная компиляция в код Java	нет
2.11.	Куба	нет	нет	нет	нет	нет	да
2.12.	Delphi	да	нет	нет	нет	нет	нет
2.13.	Dart	да	нет	нет	нет	нет	нет
2.14.	Фортран	нет	нет	нет	нет	нет	да
2.15.	Перейти на сайт	да	да	да	да	да	да

Нет.	Критерий	DerScanner	Micro Focus Fortify	Checkmarx	Источник HCL AppScan	Veracode	Synopsys Coverity Code Advisor (SAST) WhiteHat Dynamic (DAST) Black Duck (SCA)
2.16.	Groovy	да	нет	да	нет	Только из IDE	нет
2.17.	HTML5	да	да	да	нет	нет	нет
2.18.	Java	да	да	да	да	Только из IDE	да
2.19.	Java для Android	да	да	да	да	Только из IDE	да
2.20.	JavaScript	да	да	да	да	да	да
2.21.	JSP	да	да	да	да	да	да
2.22.	Kotlin	да	да	да	нет	Только файл .apk	да
2.23.	Lotus Script	да	нет	нет	нет	нет	нет
2.24.	Паскаль	да	нет	нет	нет	нет	нет
2.25.	Perl	да	нет	да	да	да	нет
2.26.	PL/SQL	да	да	да	да	нет	нет
2.27.	T-SQL	да	да	нет	да	нет	нет
2.28.	PHP	да	да	да	да	да	да
2.29.	Python	да	да	да	да	да	да
2.30.	RPG	нет	нет	нет	нет	да	нет
2.31.	Руби	да	да	да	да	да	да
2.32.	Ржавчина	да	нет	нет	нет	нет	нет
2.33.	Scala	да	нет	да	нет	Только из IDE	да
2.34.	Солидность	да	нет	нет	нет	нет	нет
2.35.	Swift	да	да	да	нет	Только из IDE	да
2.36.	TypeScript	да	да	да	нет	да	да
2.37.	VBA	да	нет	нет	нет	нет	нет
2.38.	VB.NET	да	да	да	да	Только из IDE	да
2.39.	VBScript	да	да	да	да	нет	нет
2.40.	VisualBasic 6	да	да	да	да	да	нет
2.41.	Випер	да	нет	нет	нет	нет	нет
2.42.	Xamarin	нет	нет	нет	нет	Только из IDE	нет
2.43.	1С	да	нет	нет	нет	нет	нет
2.44.	Общее количество языков	36	27	27	22	25	20

### 3. Статический анализ бинарного кода (исполняемых файлов приложений)

3.1.	JAR/WAR/EAR/AAR (Java, Scala)	да	частично	нет	нет	да, но для корректного отображения результатов необходимо также передать исходный код	нет
3.2.	EXE/DLL (C/C++)	да	нет	нет	нет	да, но только с отладочной информацией и исходным кодом для корректного отображения результатов	нет
3.3.	APK (Google Android)	да	нет	нет	нет	да, но для корректного отображения результатов необходимо также передать исходный код	нет
3.4.	IPA (Apple iOS)	да	нет	нет	нет	нет	нет
3.5.	APP (Apple macOS)	да	частично	нет	нет	нет	нет

Нет.	Критерий	DerScanner	Micro Focus Fortify	Checkmarx	Источник HCL AppScan	Veracode	Synopsys Coverity Code Advisor (SAST) WhiteHat Dynamic (DAST) Black Duck (SCA)
3.6.	Проверка приложений в App Store или ссылке Google Play	да	нет	нет	нет	нет	нет
3.7.	Проверка устаревшего программного обеспечения без исходных кодов	да	нет	нет	нет	нет	нет
3.8.	Восстановление исходного кода приложения без отладочной информации	да	нет	нет	нет	нет	нет
3.9.	Обнаружение уязвимостей в компонентах сторонних разработчиков без исходных кодов	да	нет	нет	нет	нет	нет
<b>4. Динамический анализ</b>							
4.1.	Динамический анализ	да	да	да	да	да	да
4.2.	Корреляция результатов SAST и DAST	да	нет	нет	нет информации	да	нет информации
4.3.	Подробное описание уязвимостей	да	да	да	нет информации	да	нет информации
4.4.	Информация об ответе на запрос HTTP(s)	да	нет информации	да	да	да	нет информации
4.5.	Возможность вручную изменить степень серьезности записи	да	нет информации	нет информации	нет информации	нет информации	нет информации
4.6.	Гибкая настройка авторизации в приложении	да	да	да	да	да	нет информации
4.7.	Возможность исключить URL-адреса	да	да	да	да	да	нет информации
4.8.	Возможность указать схему открытого API во время анализа	да	нет информации	нет информации	нет информации	нет информации	нет информации
4.9.	Фильтрация триггеров по URL и имени уязвимости	да	нет информации	нет информации	нет информации	да	нет информации
4.10.	Возможность автоматического сканирования через пользовательский интерфейс	да	нет информации	нет информации	да	да	нет информации
<b>5. Анализ состава программного обеспечения</b>							
5.1.	Анализ состава программного обеспечения	да	да	да	да	да	да
5.2.	Анализ файлов SBOM	да	да	да	нет информации	да	да
5.3.	Анализ без файла SBOM	да	нет информации	нет информации	да	да	да
5.4.	Анализ переходных зависимостей	да	да	да	нет информации	да	да
5.5.	Рекомендации по замене компонентов	да	да	да	да	да	да
5.6.	Поддержка NVD	да	нет информации	да	да	да	да
5.7.	Собственная поддержка БД уязвимостей	да	нет информации	нет информации	нет информации	да	да
5.8.	Анализ известных уязвимостей	да	да	да	да	да	да
5.9.	Устаревший компонентный анализ	да	нет информации	нет информации	нет информации	нет информации	нет информации
5.10.	Покрытие лицензионных рисков	да	да	да	да	да	да
5.11.	Анализ безопасности цепочки поставок	да	нет	да	нет	нет	да
5.12.	Обеспечивает оценку достоверности каждого компонента	да	нет	нет	нет	нет	нет
5.13.	Указывает на популярность используемого компонента	да	нет	нет	нет	нет	нет
5.14.	Рассчитывает балл оценки авторства	да	нет	нет	нет	нет	нет
5.15.	Оценивает активность сообщества и скорость реагирования на возникающие проблемы	да	нет	нет	нет	нет	нет
5.16.	Указывает на интерес автора к безопасности	да	нет	нет	нет	нет	нет

Нет.	Критерий	DerScanner	Micro Focus Fortify	Checkmarx	Источник HCL AppScan	Veracode	Synopsys Coverity Code Advisor (SAST) WhiteHat Dynamic (DAST) Black Duck (SCA)
5.17.	Указывает, была ли библиотека создана недавно	да	нет	нет	нет	нет	нет
5.18.	Предупреждает, если первая версия библиотеки имеет подозрительно высокое значение	да	нет	нет	нет	нет	нет
5.19.	Сигналы, если у разработчика нет других известных проектов	да	нет	нет	нет	нет	нет
5.20.	Следит за соблюдением надлежащей практики написания кода	да	нет	нет	нет	нет	нет
5.21.	Гибридный анализ SCA и SAST с помощью трассировки вызовов	да	нет	нет	нет	нет	нет
5.22.	Дерево зависимостей для визуализации зависимостей и их уязвимостей в проекте	да	нет	нет	нет	нет	нет
<b>6. Интеграция с SDLC по принципу "из коробки"</b>							
6.1.	Интеграция с репозиториями	да	да	да	да	да	да
6.2.	Интеграция со сложными средами разработки	да	да	да	да	да	да
6.3.	Интеграция с серверами CI/CD	да	да	да	да	да	да
6.4.	Интеграция с системами отслеживания проблем	да	да	да	да	да	да
6.5.	Интеграция с SonarQube	да	да	да	нет	нет	нет
6.6.	Интерфейс командной строки (CLI)	да	да	да	да	да	да
6.7.	Открытый API	да	да	да	да	да	да
<b>7. Реагирование на уязвимости и недокументированные функции</b>							
7.1.	Назначение задач для разработчиков (JIRA)	да	да	да	да	да	да
7.2.	Рекомендации по настройке WAF	Imperva, ModSecurity и F5	нет	нет	нет	Imperva, ModSecurity (только для DAST)	нет
7.3.	Управление ложными срабатываниями	да	да	да	да	да	да
7.4.	Фильтрация выявленных уязвимостей по заданным критериям	да	нет	да	нет	да	нет
7.5.	Сравнение интегрированных отчетов	да	да	да	да	да	да
7.6.	Отслеживание истории сканирования приложений	да	да	да	да	да	да
7.7.	Сообщение о результатах сканирования по электронной почте	да	да	да	да	да	да
<b>8. Отчеты</b>							
8.1.	Отчет для разработчиков	да	да	да	да	да	да
8.2.	Отчет для сотрудников службы безопасности	да	да	да	да	да	да
8.3.	Поддержка форматов отчетов PDF	да	да	да	да	да	да
8.4.	Отчеты о соответствии требованиям: PCI DSS, OWASP Top 10, OWASP Mobile Top 10, HIPAA, CWE/SANS и др.	да	да	да	да	да	да
<b>9. Юзабилити</b>							
9.1.	Автоматическое определение языка программирования	да	да	да	да	да	да

Нет.	Критерий	DerScanner	Micro Focus Fortify	Checkmarx	Источник HCL AppScan	Veracode	Synopsys Coverity Code Advisor (SAST) WhiteHat Dynamic (DAST) Black Duck (SCA)
9.2.	Выделение обнаруженных уязвимостей и недокументированных функций	да	да	да	да	да	да
9.3.	Предоставление блок-схем путей выполнения	да	да	да	да	да	да
9.4.	Инкрементный анализ	да	да	да	да	да	да
9.5.	Поддержка Microsoft Active Directory	да	да	да	да	да	да
9.6.	Рейтинг безопасности приложений	да	нет	нет	нет	да	нет
9.7.	Быстрая установка	да	да	да	да	Только облачная версия	да
9.8.	Мастер установки	нет	да	да	да	нет	да
9.9.	Гибкая модель доступа на основе ролей	да	да	нет	нет	да	да
9.10.	Автоматическое обновление базы данных уязвимостей и недокументированных функций	Только для облачной версии	да	да	да	Только для облачной версии	да
9.11.	Ручное обновление базы данных уязвимостей и недокументированных функций	да	нет	нет	нет	Только для облачной версии	нет
9.12.	Интеграция с DefectDojo	нет	да	да	да	да	нет
9.13.	Интеграция с OpenDJ	да	нет	нет	нет	нет	нет
<b>10. Лицензирование</b>							
10.1.	SaaS	да	Ограниченная версия	нет	Ограниченная версия	да	нет
10.2.	On-Premise	да	да	да	да	нет	да

## О компании DerSecur

С 2011 года DerSecur находится на переднем крае безопасности приложений. Команда из 70 экспертов DerSecur продолжает расширять границы исследований и разработок в области безопасности приложений. DerSecur является надежным поставщиком в 45 странах мира, что свидетельствует о ее влиянии и стремлении к совершенству в области защиты приложений.

### Связаться с

[company@dersecur.com](mailto:company@dersecur.com)