sonatype

Платформа Nexus

Software Supply Chain Security Platform
Анализ безопасности компонентов ПО (SCA)

Модули

sonatype nexus repository

- Проксирование и кэширование компонентов
- Хранение и управление компонентами
- Как Gitlab, только для компонентов
- Возможно уже есть у вас

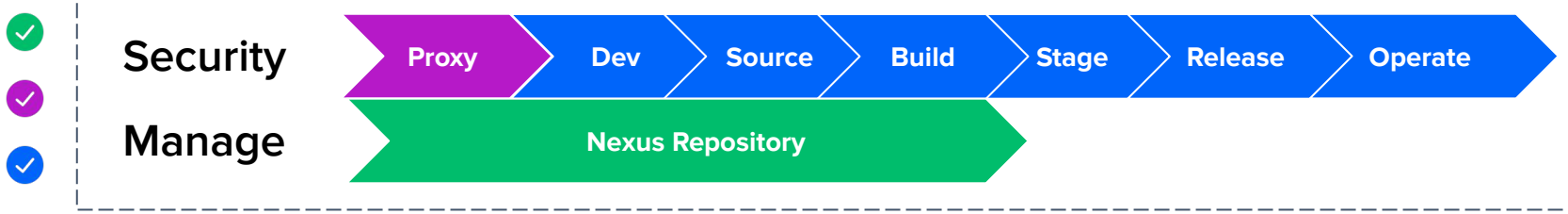
sonatype repository firewall

- Раннее обнаружение рисков
- Блокирование зловредных компонентов на точке входа

sonatype lifecycle

- Сканирование
- Отслеживание угроз
- Интеграции

- Автоматический Blocking и Warning уязвимостей по политикам ИБ



sonatype

Автоматическая работа Sonatype Platform в SDLC

Nexus Firewall
Автоматически предотвращает угрозы входящие в SDLC

Nexus Repository
Управление и проксирование компонентов

Jira

Создание задач

Docker

Проверка Application уровня контейнеров

Quality Gate

Dev

Раннее обнаружение уязвимостей
IDE, Chrome интеграции

Vcs

Мониторинг уязвимостей
Gitlab, BItbucket, Github

Build

Stage

Прохождение проверки на соответствие регламентам
Gitlab, Jenkins, Bamboo, Azure DevOps

Release

Прохождение проверки на регламенты

Operate

Мониторинг уязвимостей на production

Сравнение функционала

sonatype
nexus
repository

nexus repository oss

- Open-Source продукт
- Хранение и управление компонентами
- Основной функционал Nexus Repository
- Ограничен внутренней базой данных, не рассчитанной на большие нагрузки

nexus repository pro

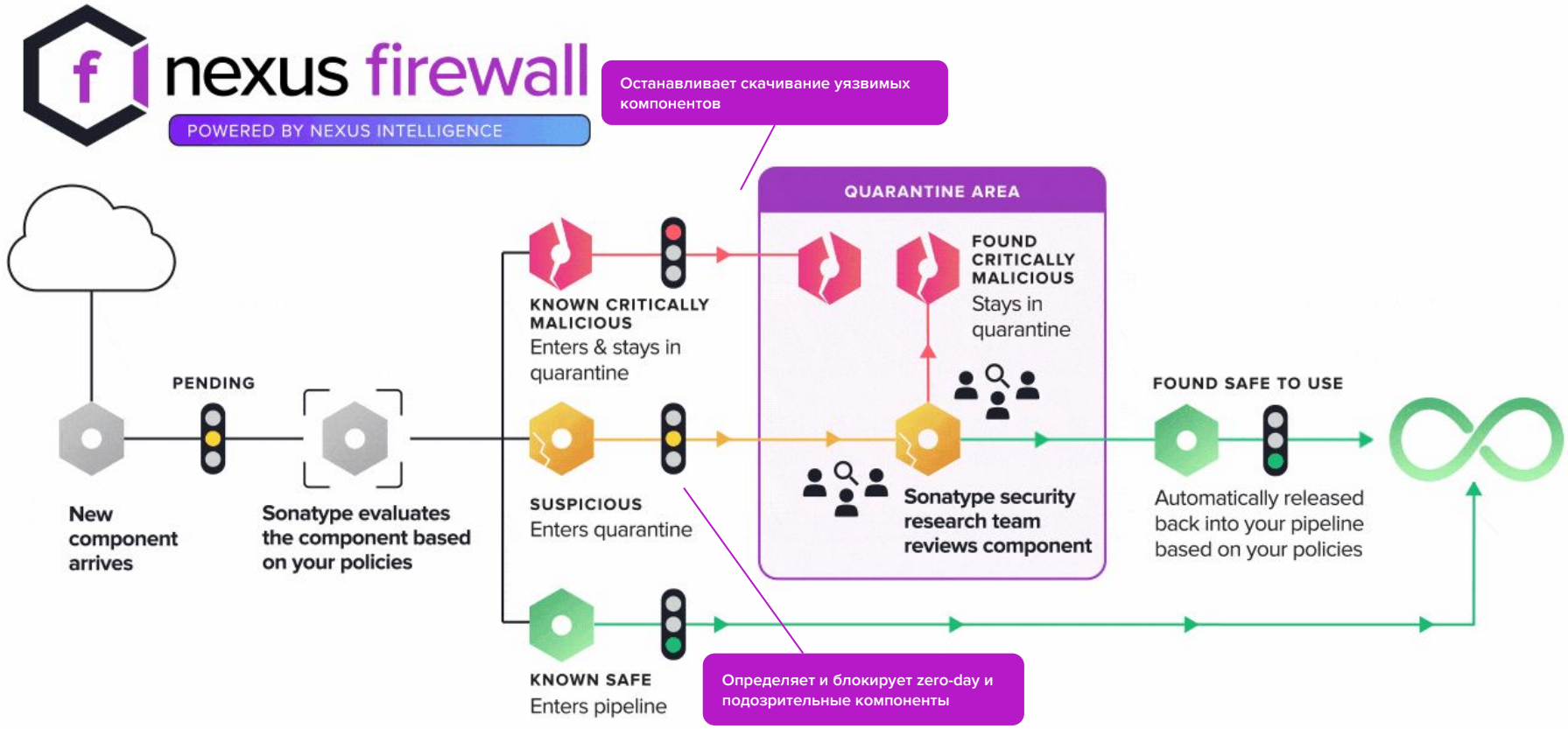
- Enterprise-level продукт
- SAML/SSO, Enterprise LDAP, Auth Tokens
- Интеграция с Nexus Firewall
- Tech Support

- Репликация Blob Store
- Возможность миграции на PostgreSQL
- Варианты отказоустойчивого развертывания
- Бэкапирование и восстановление

High Availability

Безопасность Периметра

sonatype
repository
firewall



- Описание причин блокировки компонентов
- Подробные рекомендации по исправлению/обновлению уязвимых компонентов
- Автоматизированный выпуск безопасных компонентов
- Конфигурация политик безопасности на основе вашего допустимого риска

Secure SDLC

sonatype lifecycle

- Интеграции
- Сканирование
- SBOM
- Транзитивные зависимости

Окружение разработчика

Интеграция с IDE's и VCS
Безопасность с ранних этапов ПО

Сканирование

Автоматическое сканирование и ручное через Web-интерфейс или CLI

Отсутствие False Positives

Самая крупная и корректная БДУ с использованием:
ИИ и 65+ профессионалов Research Team

Масштабирование

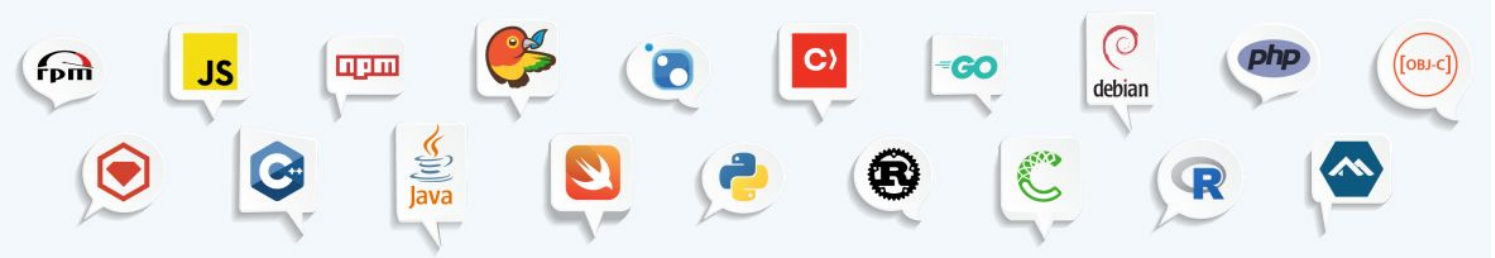
Кастомизация политик (Лицензия, Безопасность, Архитектура) под разные команды

Быстрое исправление

Подробные рекомендации чтобы быстро устранять угрозы

Мониторинг

Контроль рисков на всех этапах SSDLC



Sonatype Platform Сравнение

sonatype

Фундаментальные

- Наличие Бинарного Repository
- Firewall для компонентов
- SSDLC нативная интеграция

Казахстан

- >8/10 компаний в Казахстане уже используют Nexus Repository OSS (бесшовный переход на Pro)
- 48 Постановление Нацбанка
- Имеются внедрения в финтех компаниях

	Forrester's weighting	Checkmarx	FOSSA	GitLab*	JFrog	Revenera	Snyk	Sonatype	Synopsys	Veracode	WhiteSource
Current offering	50%	2.68	2.91	1.66	1.72	2.03	3.37	4.40	3.18	2.53	4.20
Vulnerability identification	22%	3.40	2.60	1.30	3.80	2.20	3.20	4.40	4.40	2.20	4.40
License risk management	13%	3.00	5.00	2.60	1.00	5.00	2.60	4.60	3.40	1.00	4.60
Software bill of materials	10%	1.00	5.00	1.00	1.00	1.00	3.00	5.00	3.00	3.00	3.00
Policy management	10%	1.40	2.80	0.80	1.20	1.40	2.40	4.80	4.00	1.20	3.80
SDLC integration	10%	1.40	1.70	1.90	1.80	2.40	3.60	3.50	2.30	1.70	3.50
Remediation	25%	3.70	2.50	2.20	1.00	1.10	4.00	4.50	2.60	4.10	4.90
Reporting	5%	1.90	1.30	1.60	1.30	1.50	4.70	3.80	1.00	3.60	3.50
Breadth of coverage	5%	2.80	1.05	0.75	0.75	1.30	3.90	3.80	2.80	2.50	4.10

Данные

- 10x Быстрее чем NVD NIST
- 70% больше уязвимостей чем в альтернативных БД
- 65+ профессионалов Research Team
- Определяет компоненты по Fingerprint а не по названиям
- Конкуренты используют данные Sonatype OSS Index
- На базе искусственного интеллекта и машинного обучения
- >130 млн проанализированных компонентов
- #1 в The Forrester Wave™: Software Composition Analysis, Q2 2023

Лицензирование

	sonatype nexus repository	sonatype repository firewall	sonatype lifecycle
Тип лицензирования: По пользователям	✓	✓	✓
Минимальное кол-во пользователей: 10	✓	✓	✓
Срок лицензирования: Подписка на год	✓	✓	✓
Sonatype IQ Server: Система, необходимая для работы Firewall и/или Lifecycle	✗	✓ Обязателен для работы продукта	✓ Обязателен для работы продукта
Метод подсчета пользователей	Кол-во пользователей которые скачивают через Nexus Repository Proxy	Должно быть идентичным Nexus Repository	Сканирующие, анализирующие, использующие продукт (Администраторы, ИБ, DevOps специалисты)
Развертывание: Cloud, On-Premise, Air-Gapped			