PLATFORM V

Принципы безопасности API

Дмитрий Вандышев,
владелец продукта
Platform V SOWA

Почему API подвергаются атакам?

83%

всего интернет трафика приходится на API

Akamai

#1

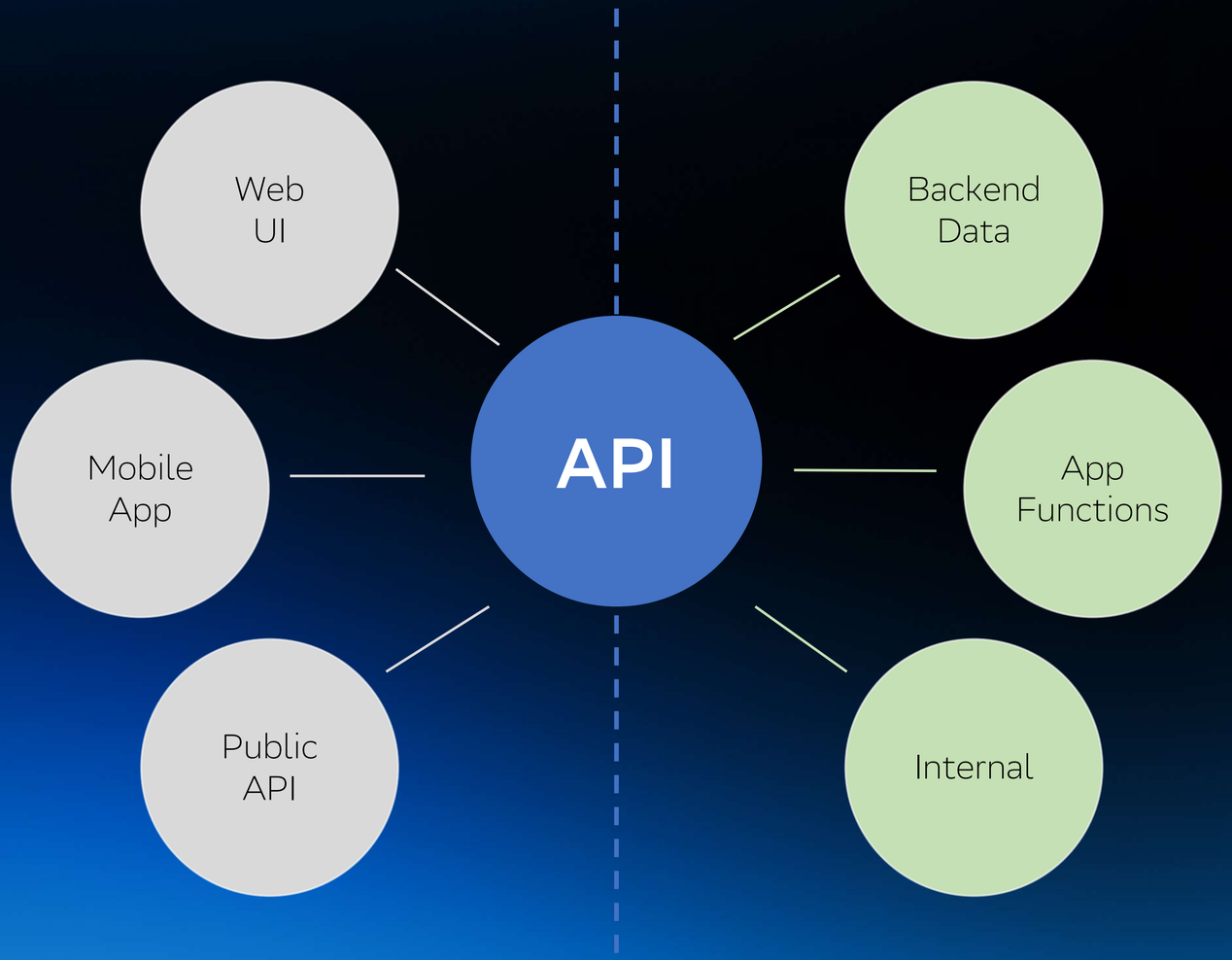
Атаки на API станут наиболее частым направлением атак

Gartner

92%

Специалистов КБ столкнулись по крайней мере с одним инцидентом, связанным с безопасностью API, за последние 12 месяцев

Что делает API главной целью атак



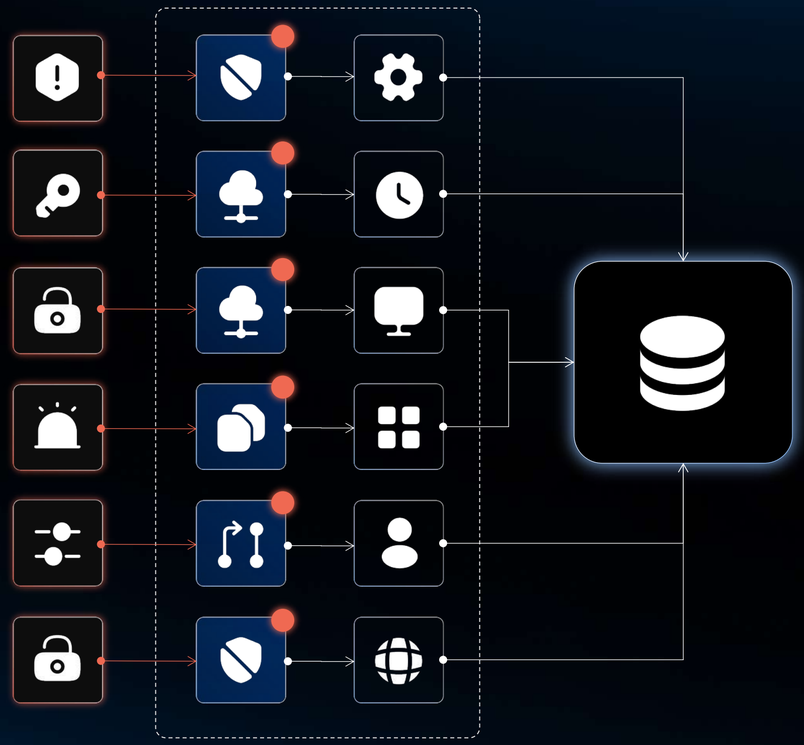
API:

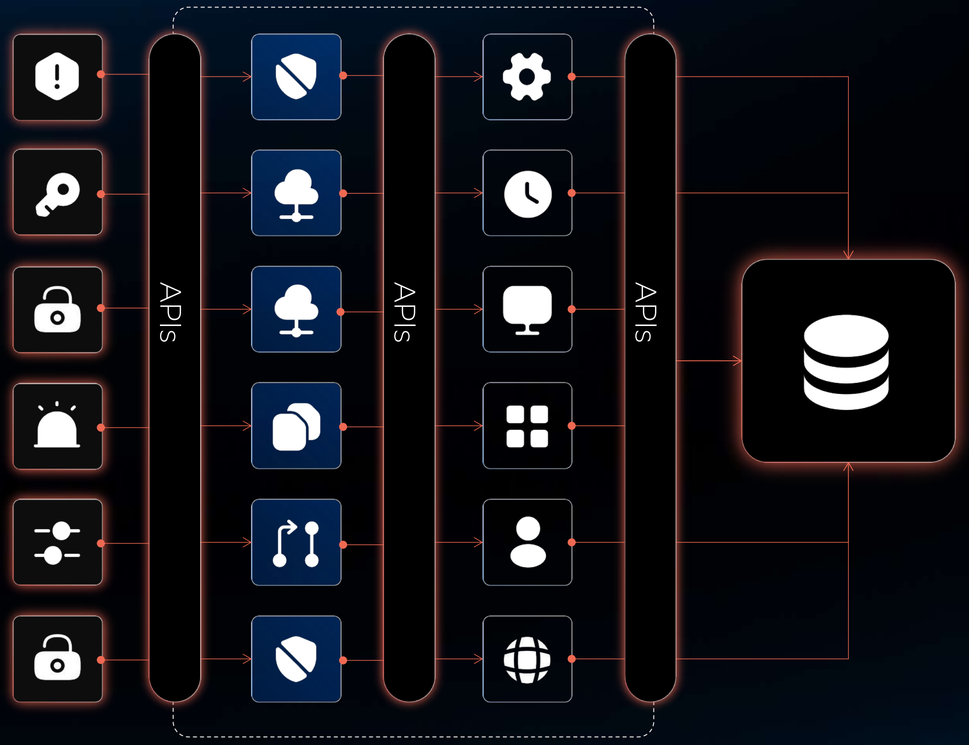
Соединяют UI и backend

Обеспечивают прямой доступ к данным

Легко обнаружить, даже если они явно не опубликованы

API – универсальный вектор атаки





Вектор атаки до использования API

Раньше хакерам приходилось учиться атаковать каждый уровень. Искать способы обойти WAF, DLP, API Gateway и т. д.

Вектор атаки после использования API

Хакеры могут просто атаковать API и получать доступ к конфиденциальным данным

2023 OWASP API Security Top 10 — отправная точка безопасности API

API1	Broken Object Level Authorization
API2	Broken Authentication
API3	Broken Object Property Level Authorization
API4	Unrestricted Resource Consumption
API5	Broken Function Level Authorization
API6	Unrestricted Access to Sensitive Business Flows
API7	Server Side Request Forgery
API8	Security Misconfiguration
API9	Improper Inventory Management
API10	Unsafe Consumption of APIs

Примеры атак на API в 2024 году

Trello

>15 млн

учетных записей скомпрометировал Trello API, связав частные адреса электронной почты с учетными записями Trello

GitHub

>13 млн

секретов просочились через публичные репозитории GitHub

Dell

>49 млн

учетных записей клиентов подверглись утечке данных из-за уязвимости API

Mercedes-Benz Twilio Dropbox Siemens NVIDIA ...

Использование OWASP API Top 10 для взлома Dell

Вот как произошел взлом:

01

Фейковый партнер, реальный доступ

Хакеры запросили учетную запись партнера на партнерском портале Dell. Без каких-либо проверок они получили учетную запись партнера на портале

02

Доступ к конечной точке API

Злоумышленники нашли API, который возвращал данные о клиенте, включая адрес, имя и т.д., после получения сервисного тега Dell

03

Масштабирование взлома

Как только хакеры узнали, что служебные теги представляют собой 7-символьные буквенно-цифровые коды, злоумышленник создал скрипт, который генерировал и отправлял эти коды в API со скоростью тысячи запросов в минуту

04

Учетка клиентских данных

В API не было ограничения скорости, чтобы предотвратить такие чрезмерные запросы. Это позволило злоумышленнику извлечь 49 миллионов записей о клиентах

Какие угрозы из OWASP API Top 10 использовали:
API1:2023 – Broken Object Level Authorization
API2:2023 – Broken Authentication
API9:2023 – Improper Inventory Management

PLATFORM V

Как обеспечить безопасность API

Фокус на защите OWASP API Top 10

- ✓ API1 Broken Object Level Authorization
- ✓ API2 Broken Authentication
- ✓ API3 Broken Object Property Level Authorization
- ✓ API4 Unrestricted Resource Consumption
- ✓ API5 Broken Function Level Authorization
- ✓ API6 Unrestricted Access to Sensitive Business Flows
- ✓ API7 Server Side Request Forgery
- ✓ API8 Security Misconfiguration
- ✓ API9 Improper Inventory Management
- ✓ API10 Unsafe Consumption of APIs

Обеспечение безопасности API на протяжении всего жизненного цикла

API Definition	API Development	Testing	Deployment	Monitoring	Retirement
Governance	Code reviews	DAST	Web server	WAF	Governance
Functionality	Static code analysis	Pen-testing	API Gateway	SIEM	Versioning
Policies	Composition analysis	Bug bounty			

Инструменты защиты API и почему их недостаточно

01

WAF

негативная модель безопасности блокирует только заведомо плохое

- Инструмент ориентирован на поиск инъекций, а не на анализ внутренней структуры передаваемых данных и вызовов
- Не заточен под валидацию схем
- В случае проверки ответов в основном ориентирован на проявление потенциальной реализации атаки
- WAF был создан для конкретной цели – защиты веб-приложений – и концентрируется на OWASP TOP 10
- В целом не фокусируется на рисках OWASP TOP 10 API
- Нужна отдельная команда сопровождения

02

API Gateway

позитивная модель безопасности допускает только заведомо хорошее

- В первую очередь это интеграционный инструмент
- Обеспечивает единую точку публикации и контроля API. А также применение единой политики безопасности
- Частично закрывает функции безопасности, но не является полноценным инструментом обеспечения безопасности. Например, не отслеживает SQL и другие инъекции
- Частично покрывает отдельные риски OWASP TOP 10 API
- Нужна отдельная команда сопровождения

03

Open API Specification Schema Validation

позитивная модель безопасности допускает только заведомо хорошее

- Инструмент проверки запросов и ответов на соответствие схеме
- Отсутствие или неполнота спецификации
- Рассинхронизация спецификации и реализации
- В целом не может защитить от наиболее распространенных и критически важных угроз API OWASP TOP 10 API
- Нужна отдельная команда сопровождения

Инструменты vs OWASP API Security Top 10

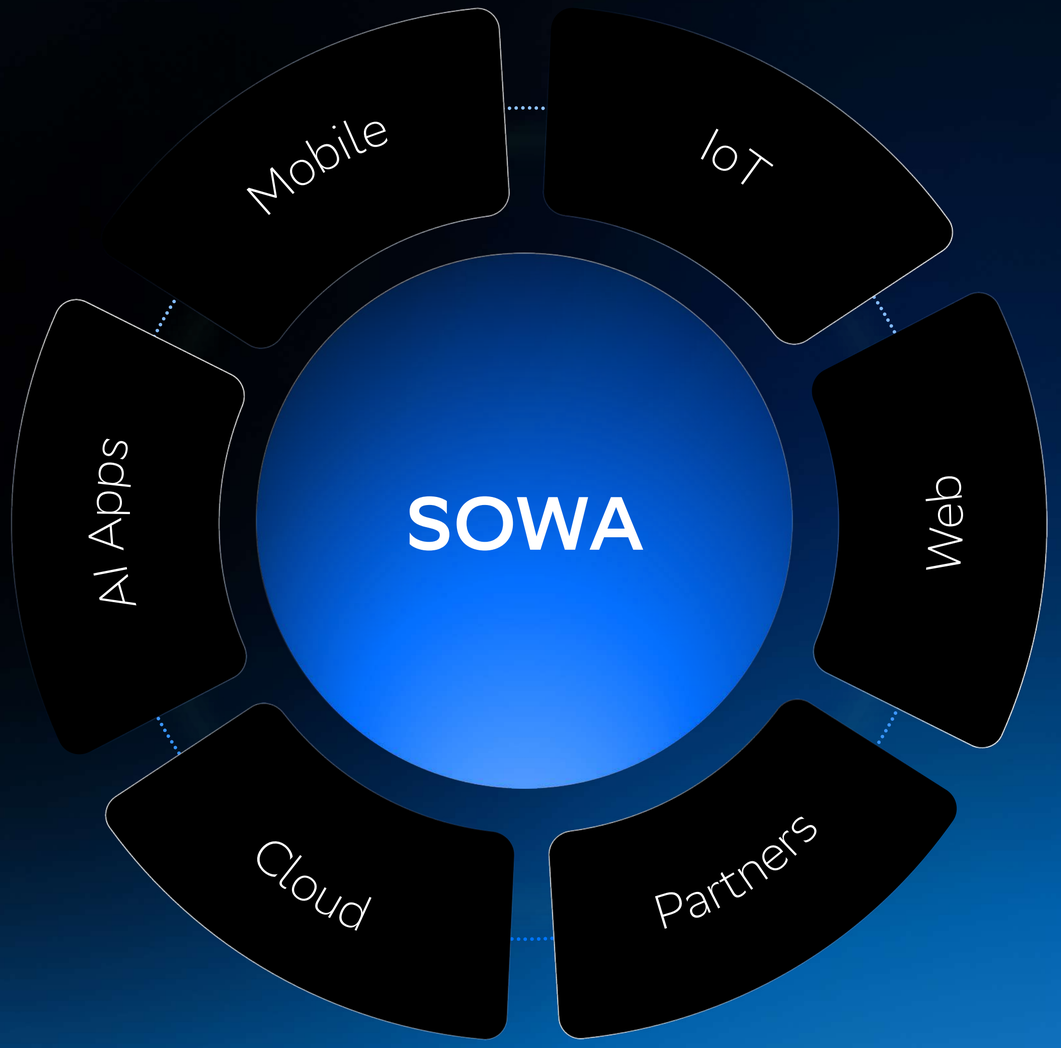
OWASP	API Security Top 10	WAF	API Gateway	OAS Scheme Validation
API 1:2023 –	Broken Object Level Authorization	нет	нет	нет
API 2:2023 –	Broken Authentication	да	да	нет
API 3:2023 –	Broken Object Property Level Authorization	нет	да	да
API 4:2023 –	Unrestricted Resource Consumption	нет	нет	да
API 5:2023 –	Broken Function Level Authorization	нет	да	нет
API 6:2023 –	Unrestricted Access to Sensitive Business Flows	да	нет	нет
API 7:2023 –	Server Side Request Forgery	да	нет	да
API 8:2023 –	Security Misconfiguration	да	нет	да
API 9:2023 –	Improper Inventory Management	нет	да	нет
API 10:2023 –	Unsafe Consumption of APIs	да	да	да

PLATFORM V

Platform V SOWA

Platform V SOWA

API Security Gateway, который обеспечивает безопасность и интеграцию API в различных сегментах сети и каналах обслуживания



SOWA API Security Gateway

с 2017 года
в промышленной эксплуатации

99,99%
отказоустойчивость*

17 000+
Постоянно действующих виртуальных машин

50 000
Транзакций в секунду в рамках одной инсталляции

24/7
без перерыва на обслуживание

Безопасность корпоративного уровня

Ключевые сервисы Сбера уже более 7 лет используют Platform V SOWA для обеспечения безопасности API и защиты критичной информации

- Сбербанк Онлайн
- sberbank.ru
- СБЕР Бизнес
- Кредитный конвейер

РРПО

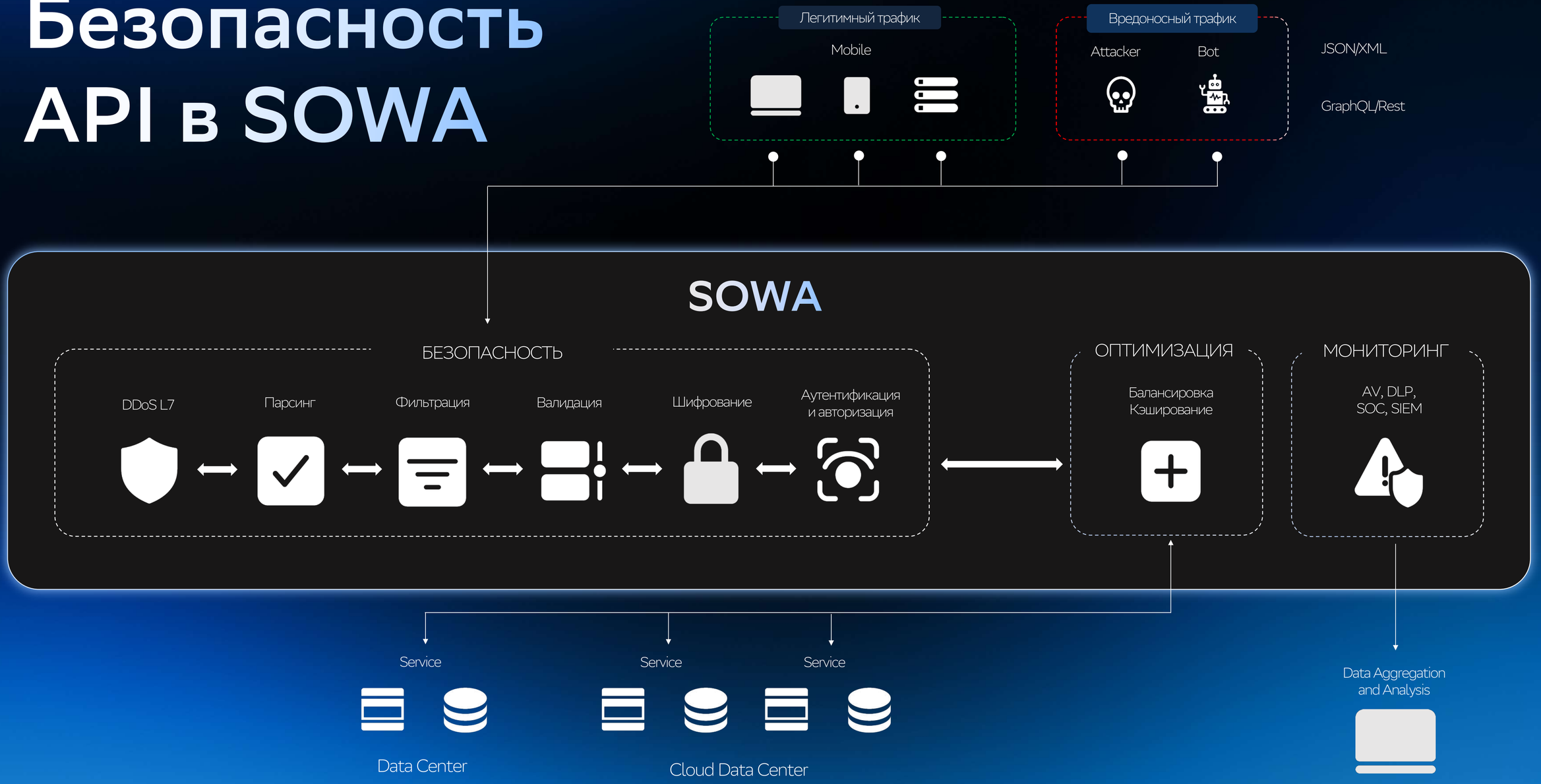
Platform V SOWA включен в РРПО и не использует в составе коммерческих лицензий

Проверено профессионалами

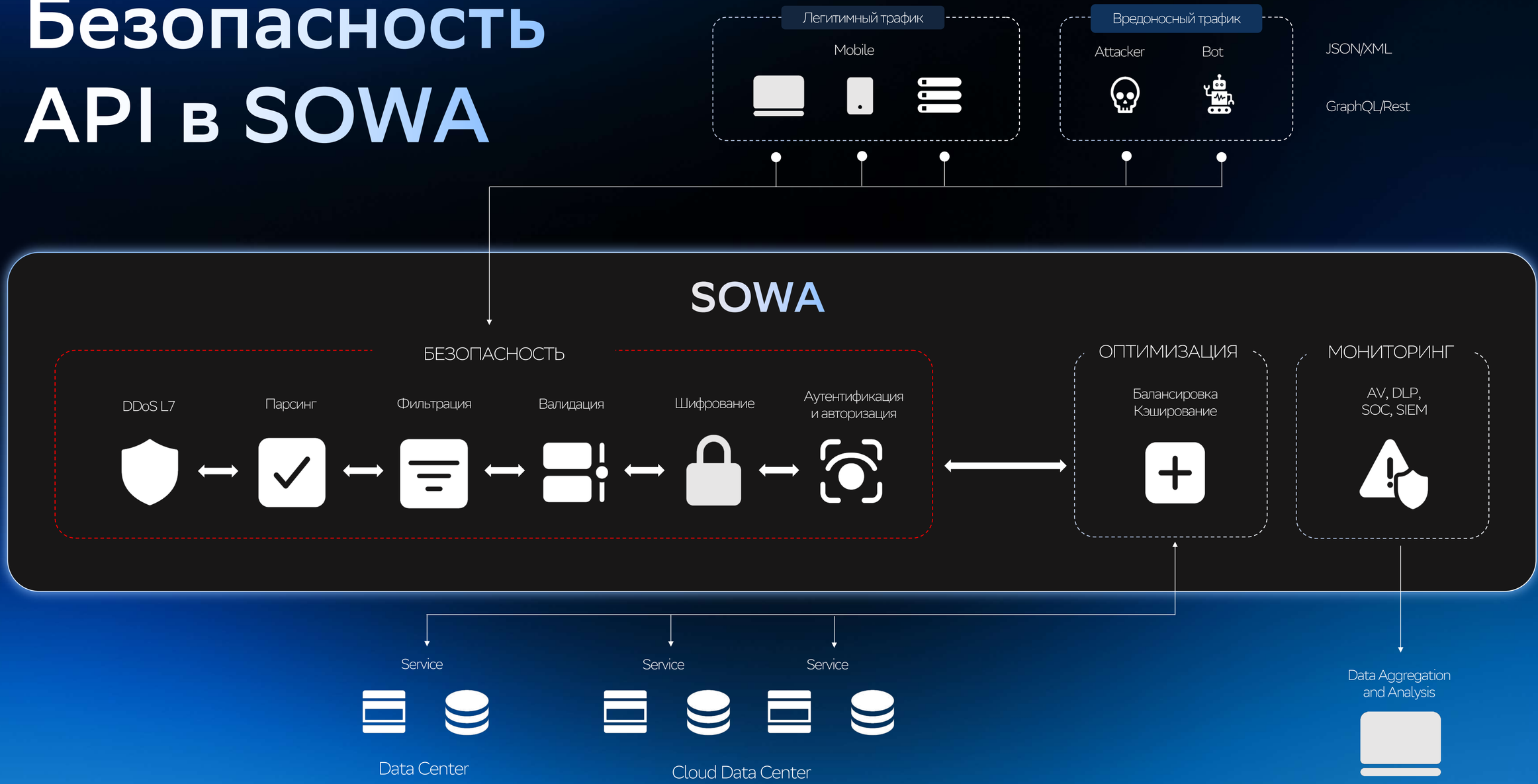
Тестирование на проникновение RedTeam компании Bi.Zone

*Максимальная доступность клиентских систем на уровне программного обеспечения, достигаемая в зависимости от используемой инфраструктуры развертывания платформы

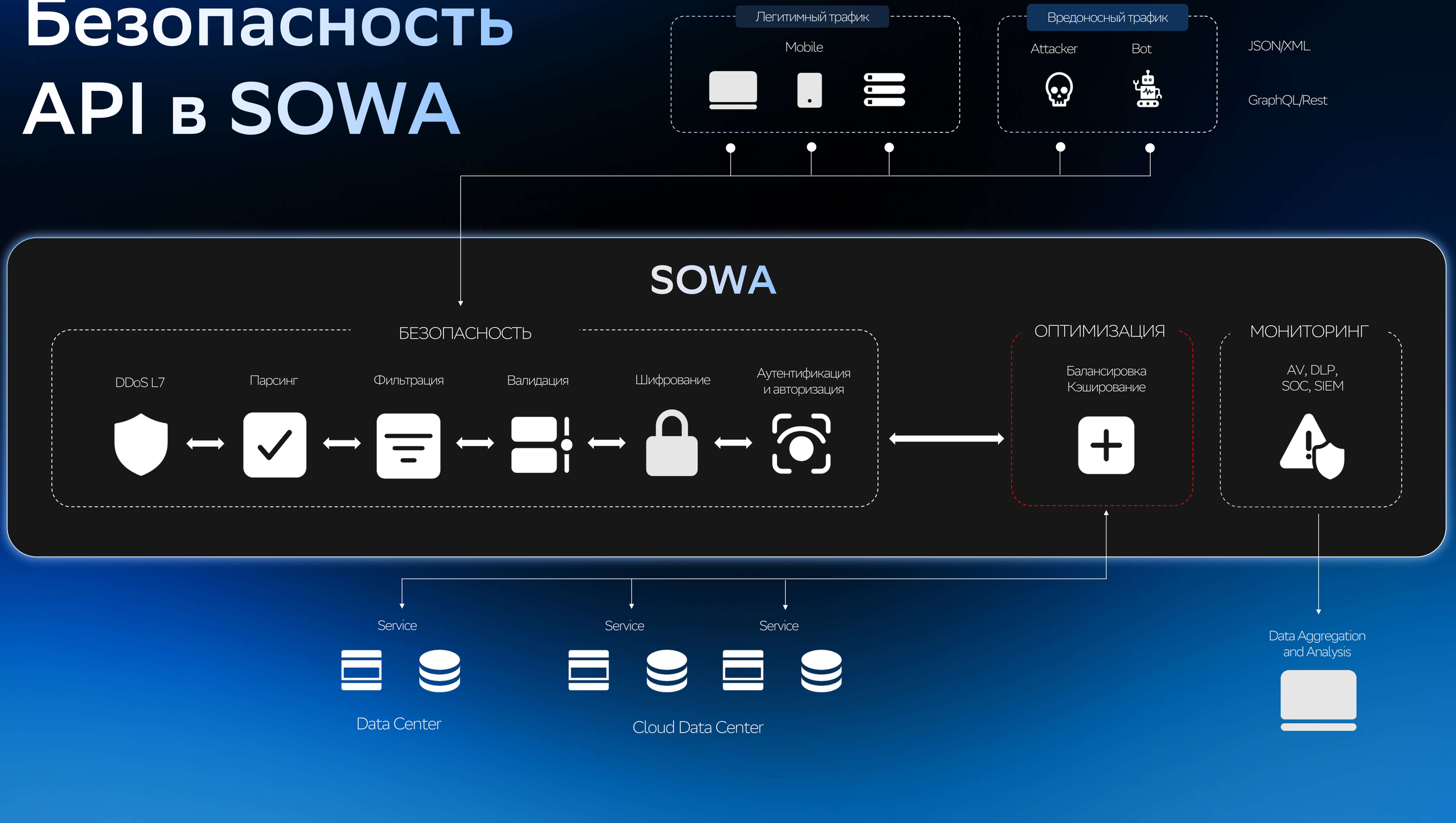
Безопасность API в SOWA



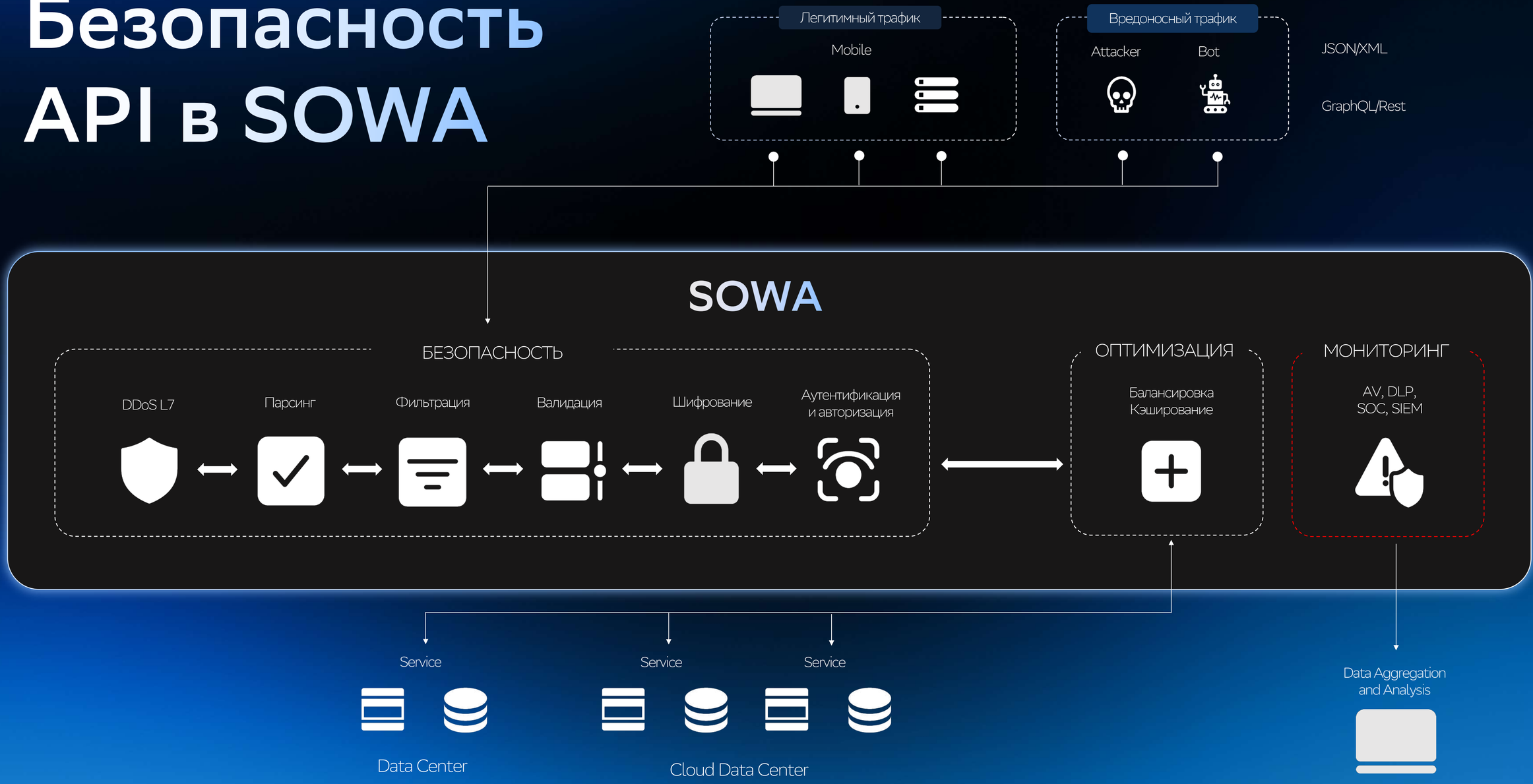
Безопасность API в SOWA



Безопасность API в SOWA



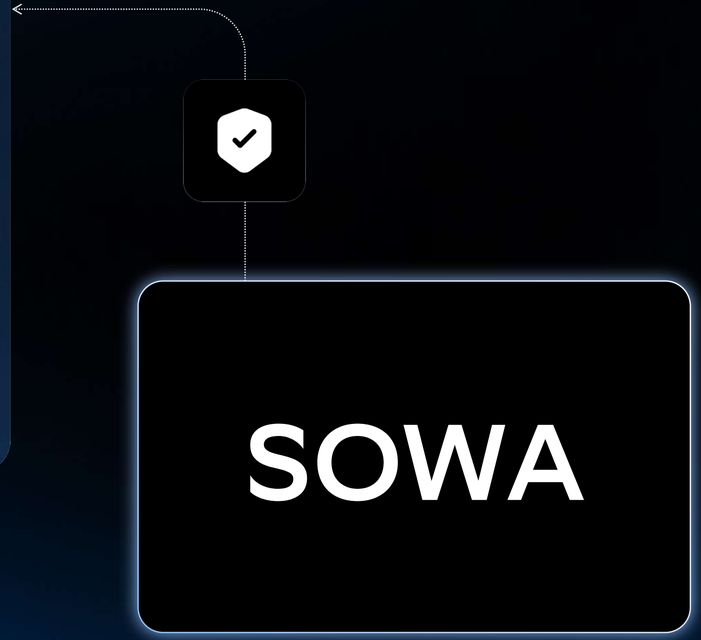
Безопасность API в SOWA



Функции Platform V SOWA

Безопасность

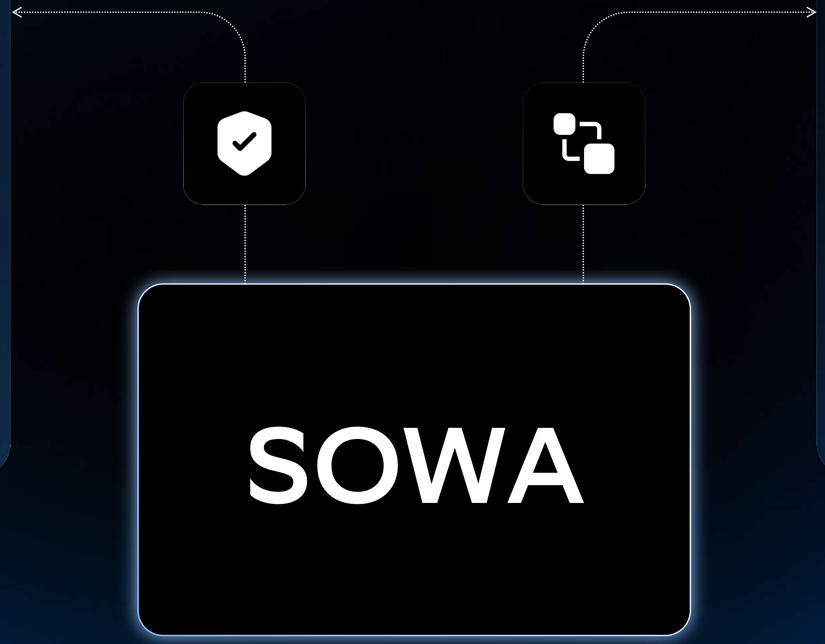
- Аутентификация, авторизация
- Трансляция токенов безопасности
- Валидация сообщений по схеме
- Фильтрация сообщений
- Шифрование канала
- Интеграция с антивирусным ПО, DLP, SOC/SIEM
- Отражение атак с помощью AI



Функции Platform V SOWA

Безопасность

- Аутентификация, авторизация
- Трансляция токенов безопасности
- Валидация сообщений по схеме
- Фильтрация сообщений
- Шифрование канала
- Интеграция с антивирусным ПО, DLP, SOC/SIEM
- Отражение атак с помощью AI



Интеграция

- Поддержка множества прикладных протоколов (включая IoT-протоколы)
- Конвертация прикладных протоколов
- Подключение протокола, разработанного клиентом
- Реализация концепции Open API
- Интеграция с облачными сервисами

Функции Platform V SOWA

Безопасность

- Аутентификация, авторизация
- Трансляция токенов безопасности
- Валидация сообщений по схеме
- Фильтрация сообщений
- Шифрование канала
- Интеграция с антивирусным ПО, DLP, SOC/SIEM
- Отражение атак с помощью AI

Интеграция

- Поддержка множества прикладных протоколов (включая IoT-протоколы)
- Конвертация прикладных протоколов
- Подключение протокола, разработанного клиентом
- Реализация концепции Open API
- Интеграция с облачными сервисами

Контроль

- Лимитирование запросов
- Whitelist/Blacklist
- Логирование и аудит
- Трассировка OpenTelemetry
- Маршрутизация контента
- Интеграция с системами мониторинга Zabbix, Prometheus и др.

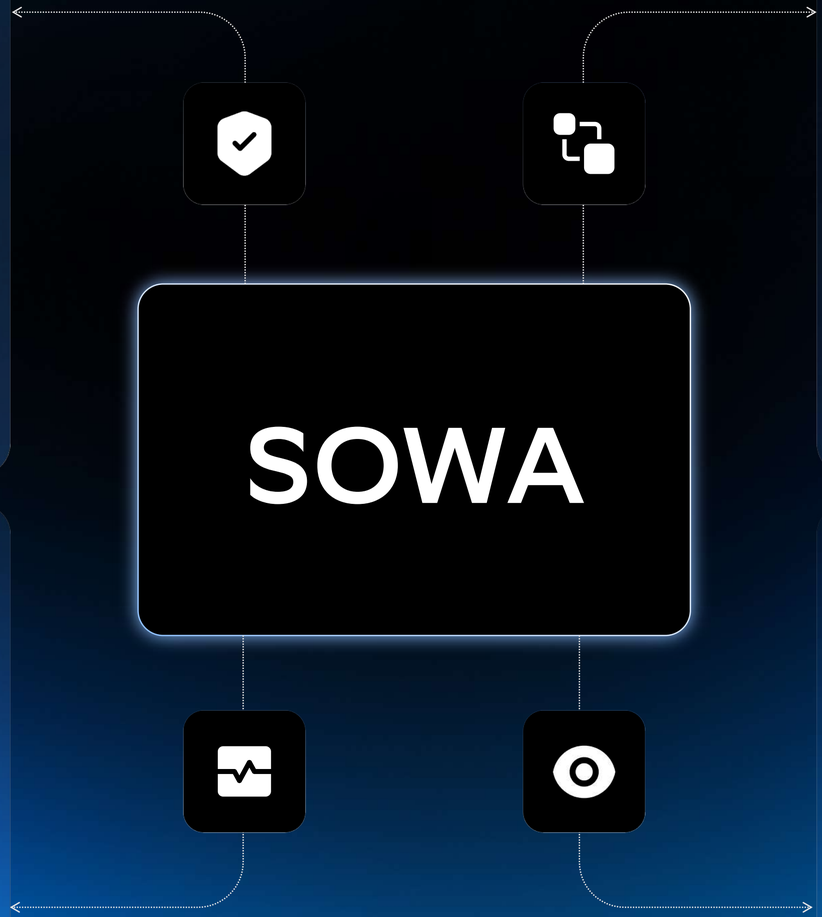
Функции Platform V SOWA

Безопасность

- Аутентификация, авторизация
- Трансляция токенов безопасности
- Валидация сообщений по схеме
- Фильтрация сообщений
- Шифрование канала
- Интеграция с антивирусным ПО, DLP, SOC/SIEM
- Отражение атак с помощью AI

Интеграция

- Поддержка множества прикладных протоколов (включая IoT-протоколы)
- Конвертация прикладных протоколов
- Подключение протокола, разработанного клиентом
- Реализация концепции Open API
- Интеграция с облачными сервисами



Оптимизация

- Терминация SSL-/TLS-сессий
- Кеширование данных
- Различные стратегии балансировки нагрузки, Sticky-session, Dynamic resolve DNS

Контроль

- Лимитирование запросов
- Whitelist/Blacklist
- Логирование и аудит
- Трассировка OpenTelemetry
- Маршрутизация контента
- Интеграция с системами мониторинга Zabbix, Prometheus и др.

SOWA — фокусная защита ваших API

OWASP	API Security top 10	WAF	API Gateway	OAS Scheme Validation	Platform V SOWA
API 1:2023 –	Broken Object Level Authorization	нет	нет	нет	да
API 2:2023 –	Broken Authentication	да	да	нет	да
API 3:2023 –	Broken Object Property Level Authorization	нет	да	да	да
API 4:2023 –	Unrestricted Resource Consumption	нет	нет	да	да
API 5:2023 –	Broken Function Level Authorization	нет	да	нет	да
API 6:2023 –	Unrestricted Access to Sensitive Business Flows	да	нет	нет	да
API 7:2023 –	Server Side Request Forgery	да	нет	да	да
API 8:2023 –	Security Misconfiguration	да	нет	да	да
API 9:2023 –	Improper Inventory Management	нет	да	нет	да
API 10:2023 –	Unsafe Consumption of APIs	да	да	да	да

Кейс применения

Финтех

Задачи

- Обеспечить безопасный доступ партнеров к API с использованием протоколов HTTP, Kafka и ArtemisMQ
- Выполнять преобразование Kafka в ArtemisMQ и наоборот
- Обеспечить безопасность API и конфиденциальность данных
- Интегрировать новые и legacy-приложения

Кейс применения

Финтех

Задачи

- Обеспечить безопасный доступ партнеров к API с использованием протоколов HTTP, Kafka и ArtemisMQ
- Выполнять преобразование Kafka в ArtemisMQ и наоборот
- Обеспечить безопасность API и конфиденциальность данных
- Интегрировать новые и legacy-приложения

Описание решения

- Проведен пилот совместно с заказчиком
- Функционал Platform V SOWA полностью удовлетворил потребности клиента
- Использованные технологии:
  - TLS Transport Security
  - Аутентификация и авторизация
  - Валидация схем SOAP/XML/JSON
  - Контроль методов HTTP
  - Фильтрация вредоносного контента
  - Конвертация протоколов Kafka-ArtemisMQ-HTTP
  - Лимитирование запросов
  - Отбрасывание событий безопасности в SIEM

Кейс применения

Финтех

Задачи

- Обеспечить безопасный доступ партнеров к API с использованием протоколов HTTP, Kafka и ArtemisMQ
- Выполнять преобразование Kafka в ArtemisMQ и наоборот
- Обеспечить безопасность API и конфиденциальность данных
- Интегрировать новые и legacy-приложения

Описание решения

- Проведен пилот совместно с заказчиком
- Функционал Platform V SOWA полностью удовлетворил потребности клиента
- Использованные технологии:
  - TLS Transport Security
  - Аутентификация и авторизация
  - Валидация схем SOAP/XML/JSON
  - Контроль методов HTTP
  - Фильтрация вредоносного контента
  - Конвертация протоколов Kafka-ArtemisMQ-HTTP
  - Лимитирование запросов
  - Отбрасывание событий безопасности в SIEM

Принципы безопасности API

01 Ведите полный перечень всех API в вашей организации

02 Используйте дополнительные механизмы аутентификации

03 Применяйте TLS для шифрования данных при передаче между клиентами и API

04 Используйте строгую проверку формата сообщения, чтобы гарантировать, что входящие данные безопасны и правильно отформатированы

05 Ограничивайте размер сообщения и количество запросов, которые клиент может сделать в течение указанного периода времени

06 Внедряйте методы журналирования и мониторинга событий безопасности для обнаружения подозрительных действий в режиме реального времени

07 Разрабатывайте API с учетом безопасности с самого начала

08 Убедитесь, что сообщения об ошибках, возвращаемые API, не раскрывают конфиденциальную информацию или детали реализации

09 Внедряйте Zero Trust архитектуру, где по умолчанию ни один объект не пользуется доверием, независимо от его местоположения в пределах или за пределами периметра сети

10 Проводите регулярные тесты безопасности, включая автоматическое сканирование уязвимостей и тестирование на проникновение

Чек-лист безопасности API

Остались вопросы?

Свяжитесь с нами любым удобным для вас способом:

Дмитрий Вандышев

Владелец продукта
Platform V SOWA

Мой telegram

Наш сайт