

A thin white vertical line is positioned to the left of the main title.

# Secure Evolutive Application

защита без границ

# Актуальность

- Проблема обеспечения информационной безопасности актуальна уже много лет, и со временем масштаб угроз и финансовых потерь только увеличивается
- Большинство хостинг-провайдеров не обладают специализированными инструментами и компетентным персоналом, необходимым для обеспечения защиты своих клиентов, в связи с этим они не могут сделать адекватное предложение в этой области
- Проблемы информационной безопасности клиентов могут стать проблемами хостинг-провайдера. Примеры:
  - распределенная атака на отказ в обслуживании (DDoS) может парализовать целые ЦОДы провайдера
  - вредоносный трафик со стороны инфраструктуры клиента, ставшей частью ботнета, может привести к попаданию всего диапазона адресов провайдера в «черный список»



# Основные преимущества решения

Расширение списка услуг уникальным и универсальным сервисом по защите информации позволяет:

- быть на шаг впереди своих конкурентов
- получать дополнительный доход с каждого клиента за счет предоставления полезного сервиса
- заслужить репутацию надежного поставщика сервисов
- обеспечивать выполнение требований регуляторов

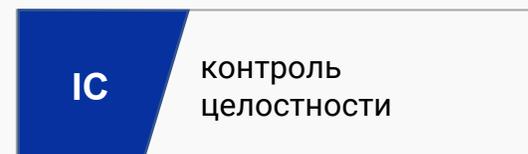
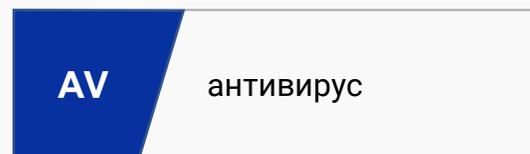
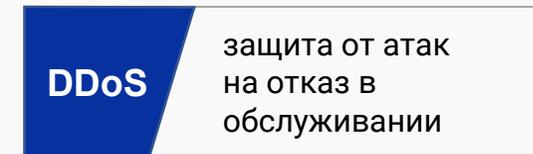
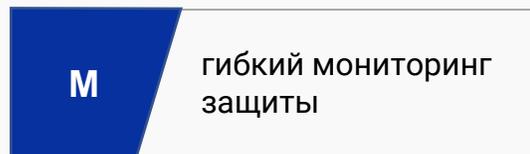
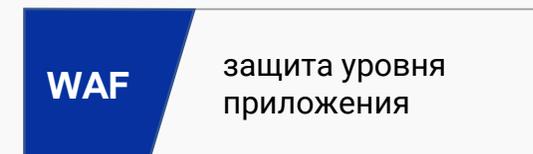
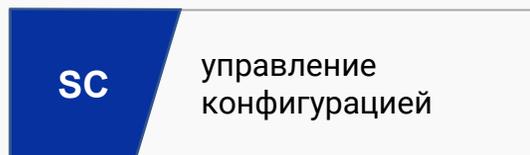
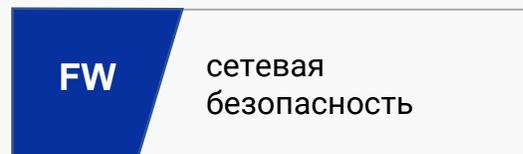
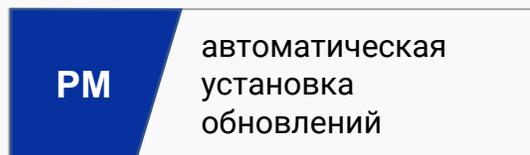
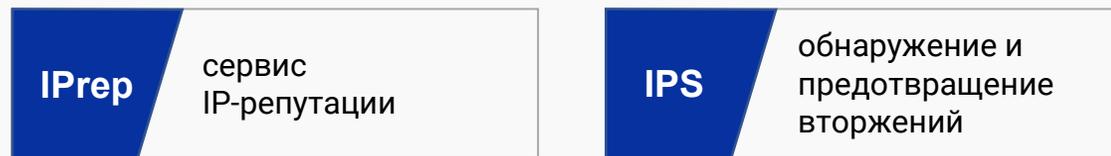
■ ~~судебные  
иски~~

■ ~~штрафы~~

■ ~~репутационные  
потери~~

# Как это работает?

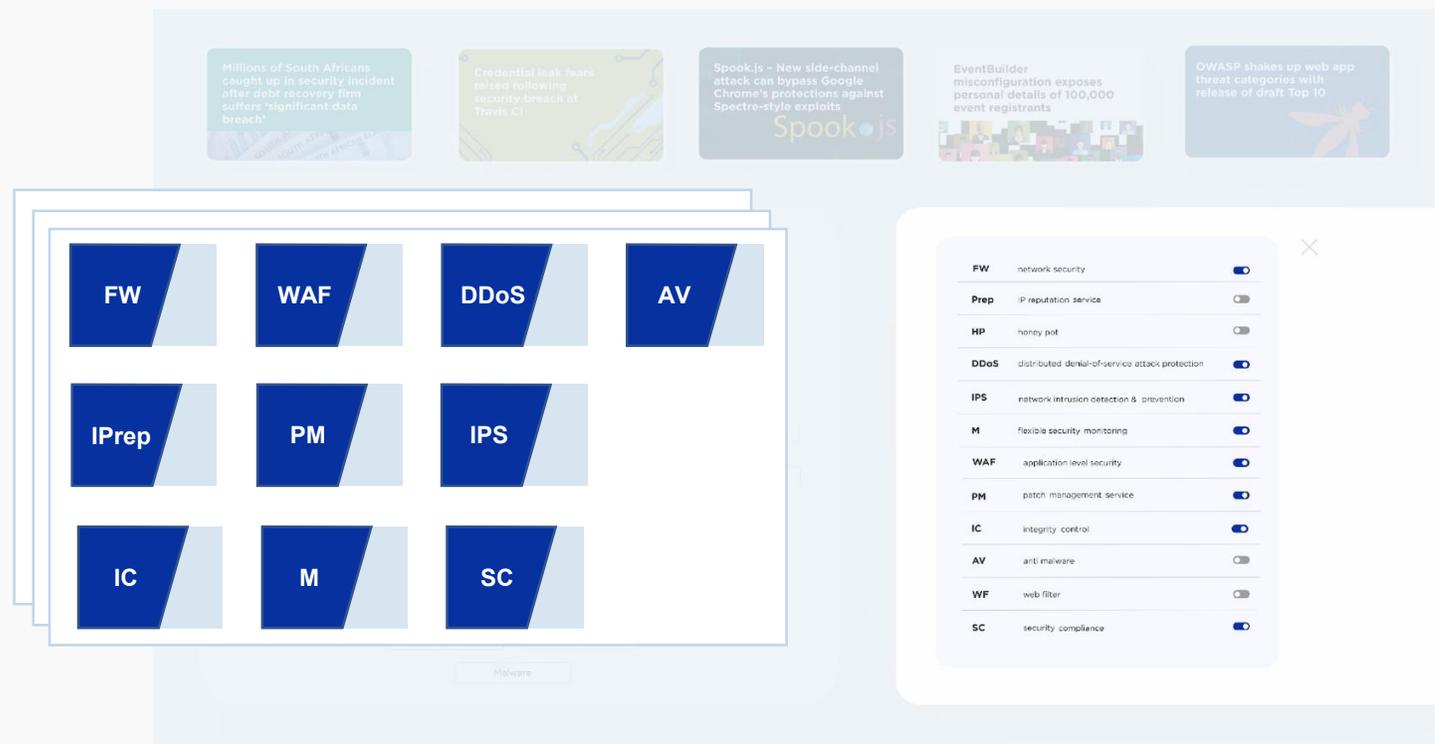
Набор активируемых модулей безопасности собственной разработки или в виде партнерского сервиса



# Как это работает?

Клиент активирует или отключает модули в любое время

Это позволяет эффективно выстроить персонализированную систему защиты. Клиенты платят абонентскую плату только за подключенные сервисы и получают информативные отчеты, отражающие эффективность их использования

The dashboard displays several security modules and their status:

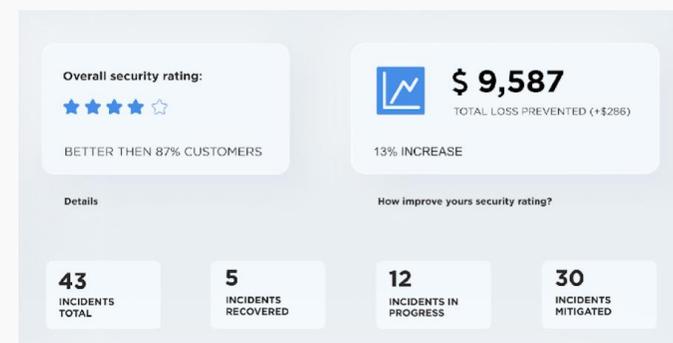
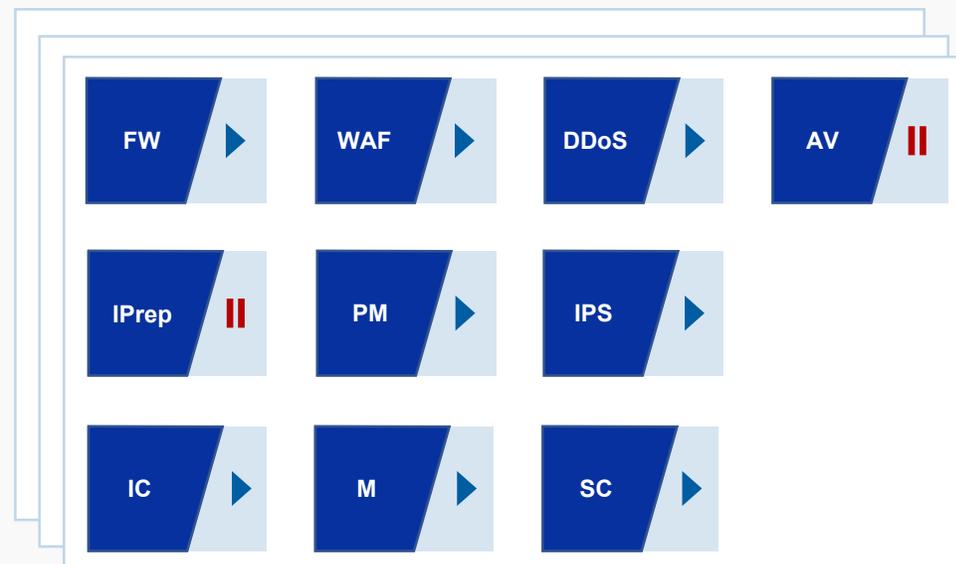
Module	Status
FW	On
WAF	On
DDoS	On
AV	On
IPrep	On
PM	On
IPS	On
IC	On
M	On
SC	On
Malware	On

Additional news items visible in the background:

- Millions of South Africans caught up in security incident after debt recovery firm suffers 'significant data breach'
- Credential leak fears raised following security breach at Travels CI
- Spook.js - New side-channel attack can bypass Google Chrome's protections against Spectre-style exploits
- EventBuilder misconfiguration exposes personal details of 100,000 event registrants
- OWASP shakes up web app threat categories with release of draft Top 10

# Как это работает?

У клиентов есть единая консоль управления, которая позволяет управлять подписками и создавать общие и подробные отчеты



# Пример интерфейса клиента

Millions of South Africans caught up in security incident after debt recovery firm suffers 'significant data breach'

Credential leak fears raised following security breach at Travis CI

Spook.js - New side-channel attack can bypass Google Chrome's protections against Spectre-style exploits

EventBuilder misconfiguration exposes personal details of 100,000 event registrants

OWASP shakes up web app threat categories with release of draft Top 10



The diagram shows a central server icon surrounded by four quadrants: Perimeter defense (top), Network Attack Protection (right), Core security (bottom), and Manageability (left). Each quadrant is connected to various security components: Authentication, Zero Day, SQL Injection (1), RCE (2), Encryption (5), Database security, Cloud security, DNS, Phishing, DDoS (8), RCE (2), Database security, Encryption (5), and Malware.

**Overall security rating:**  
★★★★☆  
BETTER THEN 87% CUSTOMERS

**Details**

**43**  
INCIDENTS TOTAL

**5**  
INCIDENTS RECOVERED

**12**  
INCIDENTS IN PROGRESS

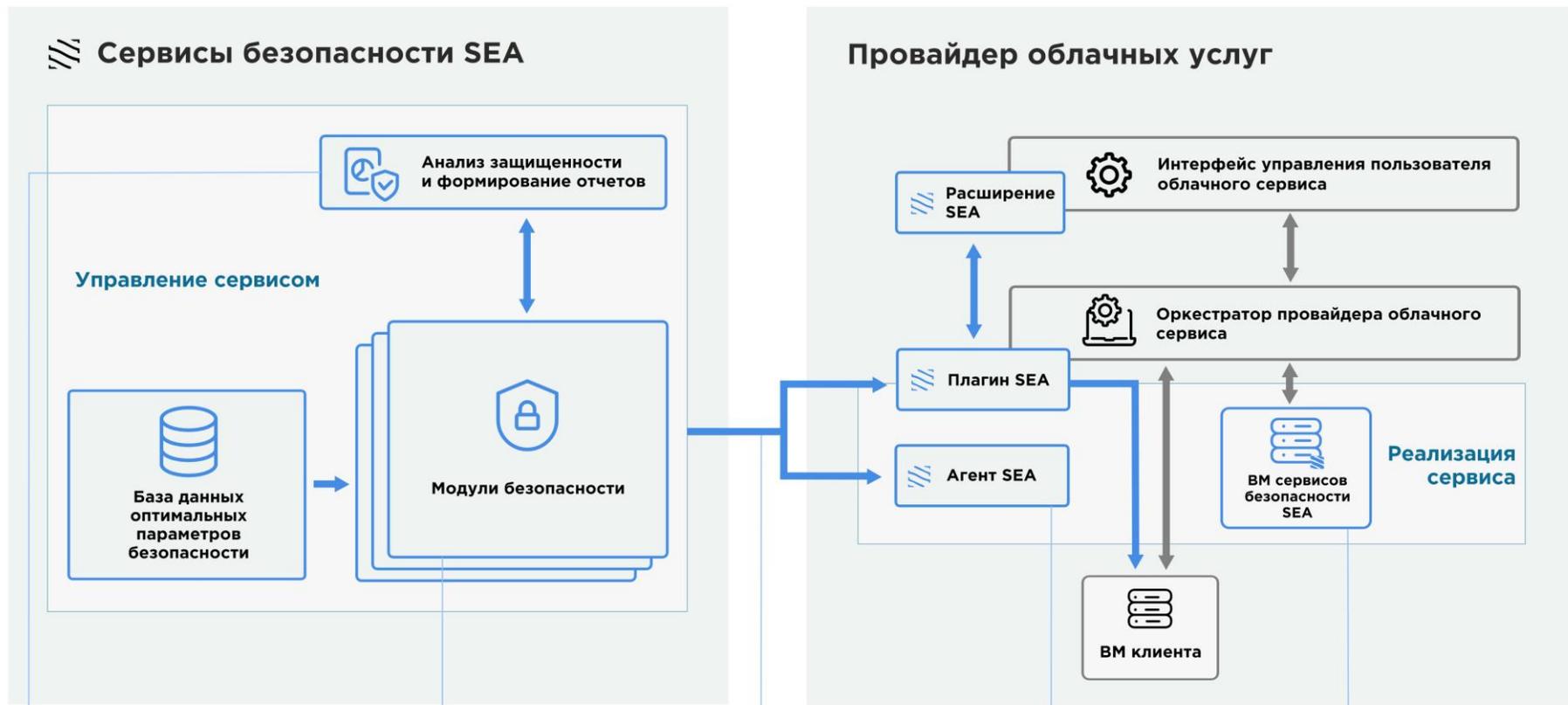
**30**  
INCIDENTS MITIGATED

Module	Data opened	Data closed	Description	Status	Efficiency
Integrity Control	01.03.2021	03.03.2021	.htaccess file changed unexpectedly	Mitigated	90%
AV	01.04.2021	01.04.2021	Generic.Trojan32 detected in file ascodebase.exe, file re...	Mitigated	100%
Ddos	26.06.2021	30.06.2021	Application level Ddos detected. Traffic cleaning mod...	Mitigated	100%

**\$ 9,587**  
TOTAL LOSS PREVENTED (+\$286)

13% INCREASE

**How improve yours security rating?**



Различные отчеты, формируемые по запросу, для провайдера и конечного пользователя:

- Биллинг
- Сведения об использовании сервисов SEA
- Сводка по инцидентам

- Распространение агентов SEA и конфигурации модулей
- Сбор журналов безопасности

Настройка параметров безопасности виртуальной машины клиента:

- Защиты удаленного доступа
- Безопасное хранение данных
- Активация Secure boot и vTPM
- Полное шифрование диска (по запросу)
- Автоматическое обновление модулей специальных компонентов платформы виртуализации
- Автоматическая установка агента SEA

Реализация функций безопасности:

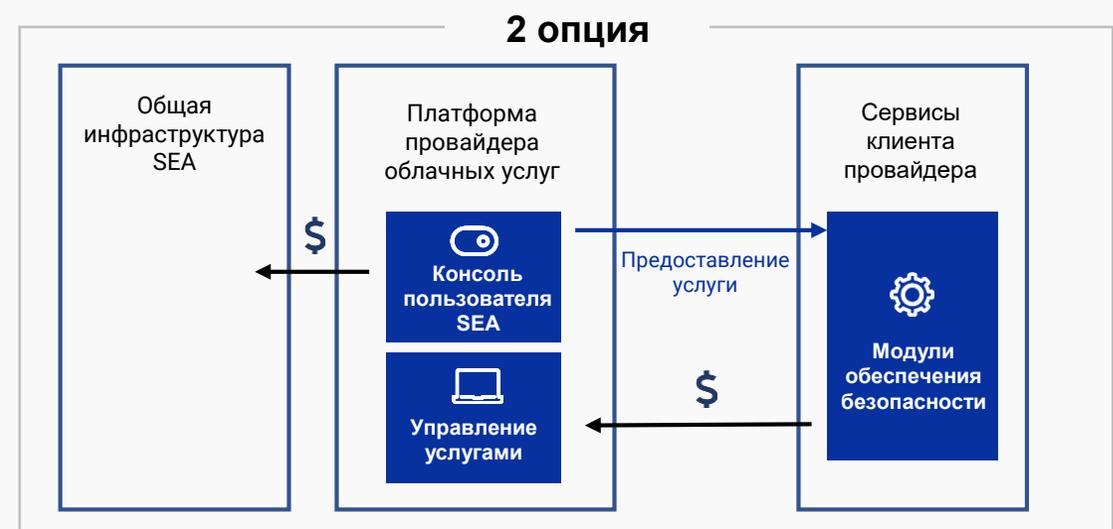
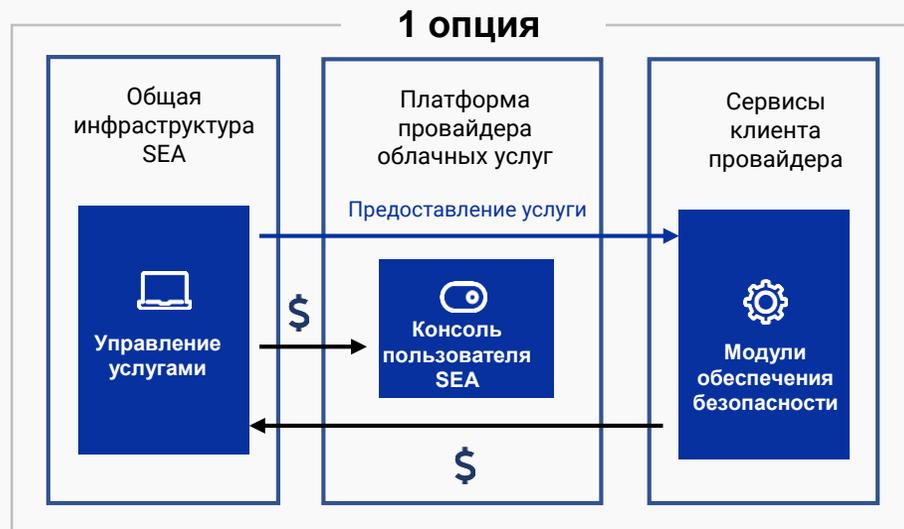
- Защита от вредоносного ПО
- Контроль целостности
- Управление обновлениями
- Мониторинг безопасности
- Проверка на наличие уязвимостей

Кэш правил/политик и сетевые сервисы безопасности:

- Правила МЭ
- Правила WAF
- Кэша БД репутации IP-адресов

# Бизнес модель

- Инвестиции оператора ограничиваются интеграцией с системой управления (в т.ч. личным кабинетом) и службой биллинга
- Оператор может сам взимать плату за использование сервиса, оплачивая базовый сервис, либо получать «агентское вознаграждение» с продаж (возможна тарификация по фактическому времени использования, по подписке, по отчетам, по серверам/контейнерам...) – может использоваться на стартовом (ознакомительном) периоде



# Преимущества

- Интеграция с биллингом и системой управления сервисами (личным кабинетом)
- Легкая установка, интеграция и администрирование
- Централизованное мультитенантное управление (гибкое, относительно потребности клиента)
- Полный набор инструментов защиты (не только от вирусов)
- Оценка полезности подписок (механизм отчетности). Доказательная безопасность (+механизм периодического тестирования и контроля)
- Подключение по мере необходимости
- Нулевое влияние на производительность
- Возможность тестового периода, различных бизнес-моделей использования
- Получение сертификатов, обеспечивающих доверие и соответствие законодательным требованиям, снижение юридических рисков