КОД безопасности

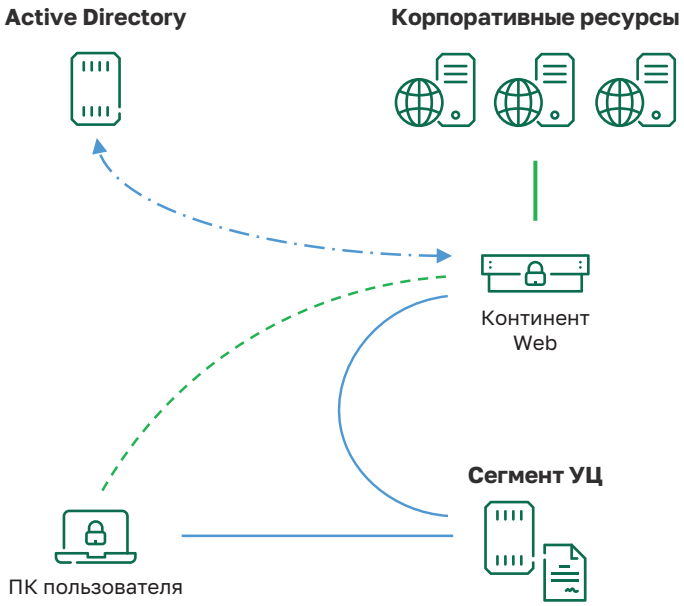
Континент Web

Система комплексной защиты веб-приложений (TLS-шлюз + WAF)

- Доступ только к разрешенным приложениям (TLS-шлюз)
- Разграничение прав доступа пользователей к веб-приложениям (TLS-шлюз)
- Поддержка различных программных клиентов (TLS-шлюз)
- Виртуальный патчинг и защита от атак 0-day (WAF)
- Автоматизированное изучение бизнес-логики приложений (WAF)
- Расширенные механизмы защиты от атак: собственные машинное обучение и сигнатурный анализатор (WAF)
- Single-Sign-On для доступа к приложениям

Сценарии применения

Удаленный доступ к корпоративным ресурсам



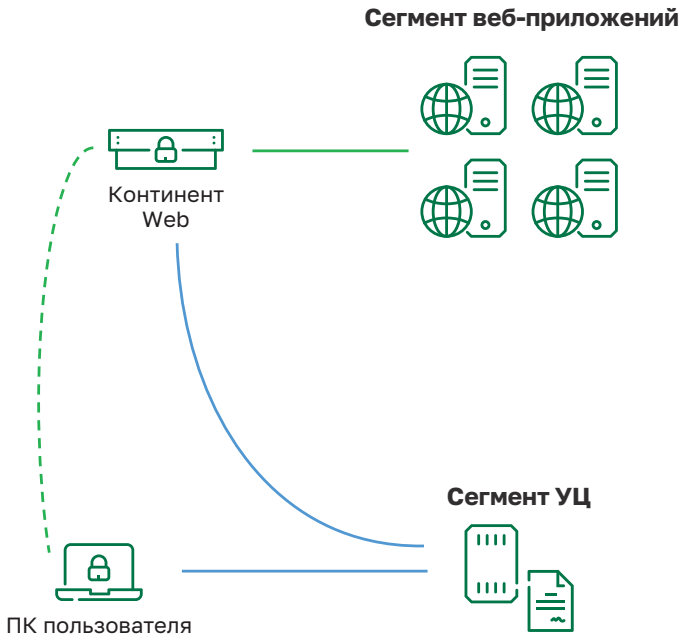
Компоненты

- Сервер: Континент Web.
- Лицензии для сервера: HTTPS-прокси и/или TLS-туннель.
- Клиент: Континент TLS Клиент, Континент ZTN Клиент или КриптоПРО CSP, Валидата CSP или браузер.
- Удостоверяющий центр.

Результат

- Организован доступ удаленных пользователей к внутренним веб-приложениям.
- Обеспечено разграничение доступа удаленных пользователей к различным веб-приложениям.
- Обеспечен доступ пользователей к корпоративным ресурсам с помощью «толстых» программных клиентов (терминалов, клиентов ERP-систем и т.д.).

Безопасный доступ к ведомственному веб-приложению



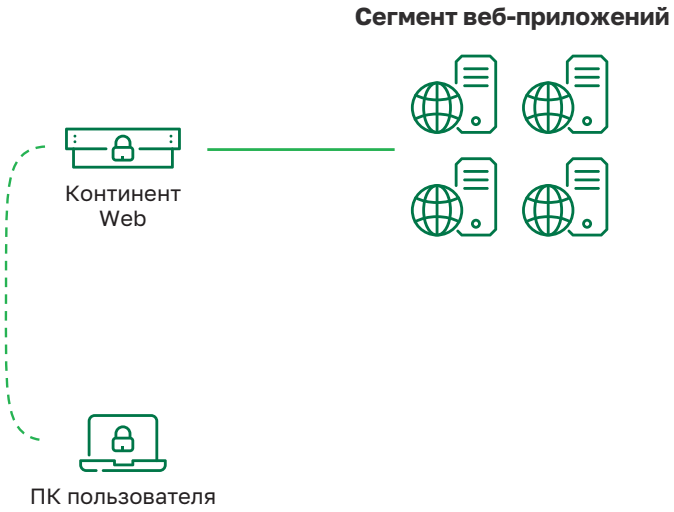
Компоненты

- Сервер: Континент Web.
- Лицензии для сервера: HTTPS-прокси и/или TLS-туннель.
- Клиент: Континент TLS Клиент, Континент ZTN Клиент или КриптоПРО CSP, Валидата CSP или браузер.
- Удостоверяющий центр.

Результат

- Организован доступ к ведомственному веб-приложению (для ГИС – обязателен).
- Создана система дистанционного банковского обслуживания.
- Обеспечен безопасный доступ к электронной торговой площадке.

Анонимный или идентифицированный доступ к веб-приложению



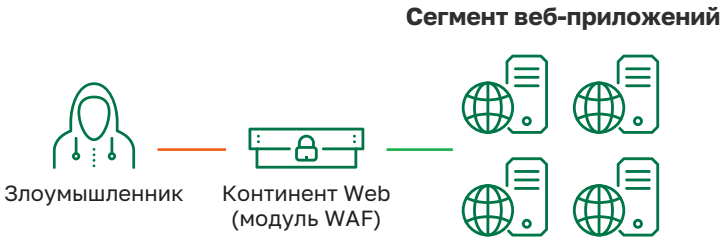
Компоненты

- Сервер: Континент Web.
- Лицензии для сервера: HTTPS-прокси.
- Клиент: браузер или Континент ZTN клиент.

Результат

- Организован анонимный доступ пользователей к веб-порталу.
- Организован идентифицированный доступ пользователей к веб-порталу.
- Реализован дополнительный контекст для проверки удаленных пользователей на соответствие комплаенсу.

Защита веб-приложений от атак



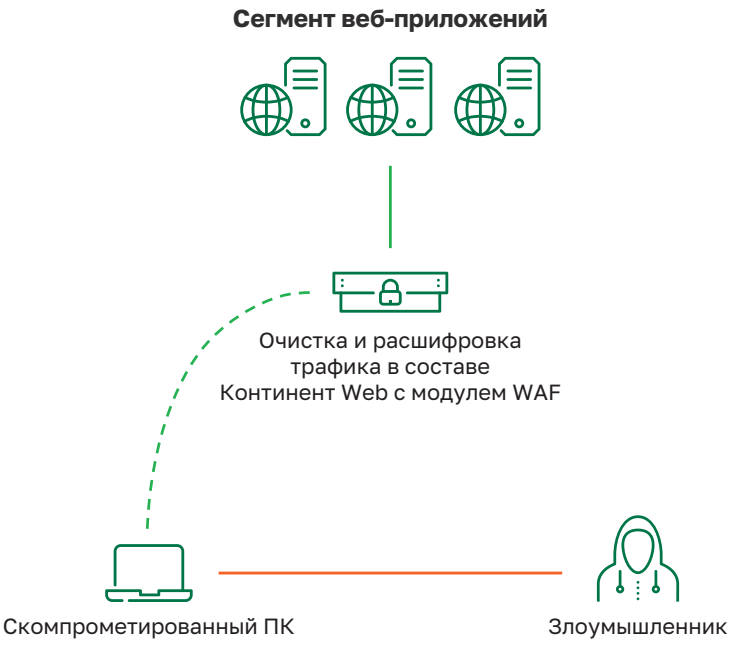
Компоненты

- Сервер: Континент Web.
- Лицензии для сервера: WAF.

Результат

- Обеспечена защита от атак:
  - Публичных веб-приложений;
  - Личного кабинета пользователя;
  - Систем межведомственного взаимодействия;
  - Мобильных приложений;
  - Веб-интерфейсов критичных систем.

Комплексная защита веб-приложений



Компоненты

- Сервер: Континент Web.
- Лицензии для сервера: HTTPS-прокси и WAF.
- Клиент: Континент TLS Клиент, Континент ZTN Клиент или КриптоПРО CSP, Валидата CSP или браузер.

Результат

- Обеспечен защищенный доступ пользователей к веб-приложению с разграничением прав.
- Обеспечена защита веб-приложений от атак.

Возможности

Управление и мониторинг

- Веб-интерфейс для управления и мониторинга.
- Интеграция в SIEM-систему по протоколу syslog.
- Регистрация событий информационной безопасности, связанных с работой Континент TLS Клиент.
- Поддержка утилит для сбора статистики.
- Графическое отображение модели разбора запросов и ответов веб-сервера.
- Мониторинг и управление защитой нескольких приложений из единой консоли.
- Графическое отображение и редактирование правил принятия решений.
- Вывод обобщенной статистики в режиме реального времени.
- Агрегирование и приоритизация данных о событиях ИБ.
- Автоматическое оповещение оператора о событиях ИБ.
- Ролевая модель доступа в консоль управления.
- Аудит действий оператора WAF в консоли управления.
- Обновление правил ModSecurity в соответствии с OWASP Top 10.
- Возможность создания списков объектов для дальнейшего использования в правилах.

Обнаружение атак на веб-приложения

- Обнаружение специфических для веб-приложений атак:
  - OWASP TOP 10;
  - Bruteforce-атаки;
  - DoS на уровне приложений;
  - Атаки на механизмы авторизации и аутентификации;
  - Автоматизированные атаки.
- Обнаружение аномалий в запросах и ответах веб-сервера.
- Обнаружение аномалий на основе модели работы приложения:
  - Совпадение с моделью;
  - Отклонение от модели.
- Обнаружение аномалий внутри вложенных данных, передаваемых по протоколу HTTP.

Шифрование

- Криптографическая защита HTTPS-трафика по протоколу TLS.
- Поддерживаемые российские криптоалгоритмы:
  - Алгоритм шифрования: ГОСТ 34.12-2018 («Магма» и «Кузнечик»);
  - Защита передаваемых данных от искажения: ГОСТ 34.12-2018 («Магма» и «Кузнечик»);
  - Расчет хэш-функции: ГОСТ Р 34.11-2012 (длина ключа 256 бит);
  - Формирование и проверка электронной подписи: ГОСТ Р 34.10-2012 (на основе кривых Эдвардса с длиной ключа 256 или 512 бит).
- Поддерживаемые иностранные криптоалгоритмы:
  - RSA/AES.
- Поддерживаемые протоколы:
  - TLS v1.0;
  - TLS v1.2.
- Возможность работы с различным клиентским ПО:
  - Континент TLS Клиент и ZTN Клиент:
    - Поддержка туннелирования TCP-трафика через протокол TLS.
  - КриптоПро CSP и Валидата CSP:
    - Работа пользователя в браузере Edge и Яндекс Браузер.
  - Любой другой клиент, соблюдающий спецификацию TLS.

Контроль доступа к защищаемым ресурсам

- Идентификация и аутентификация пользователей по сертификатам открытых ключей стандарта x.509v3 (ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012).
- Обоюдная аутентификация пользователя и сервера в процессе установки защищенного соединения.
- Проверка сертификатов ключей по спискам отозванных сертификатов (CRL).
- Автоматическая загрузка и обновление Trust-service Status List (TSL).
- Интеграция с Active Directory при работе сервера удаленного доступа в режиме портала приложений:
  - Аутентификация пользователя по имени и паролю AD;
  - Предоставление доступа к приложениям на основе принадлежности пользователя к структурному подразделению.
- NTLM аутентификация для ресурсов.
- Single-Sign-On в приложениях портала.
- Интеграция с сервисом auth.as и multifactor.ru
- Механизм просмотра и перевыпуска сертификатов кластера.
- Разграничение доступа к защищаемому ресурсу по корневому сертификату и по полям сертификата пользователя.
- Возможность управления списком разграничения доступа к ресурсам HTTPS-прокси с помощью текстового файла средствами веб-управления.

Сетевые возможности

- Сокрытие защищаемых серверов (обратный прокси-сервер):
  - К каждой сессии пользователя может быть добавлен произвольный идентификатор.
- Работа в режиме кластера с балансировкой нагрузки:
  - Неограниченное линейное масштабирование производительности.
- Блокировка неиспользуемых портов.

Анализ трафика

- Гибкая настройка моделей работы приложений:
  - Валидация HTTP, JSON, XML, GraphQL, HTML, MultiPart/Form-Data, YAML;
  - Синтаксический анализ запросов и ответов;
  - Определение бизнес-логики приложения;
  - Идентификация, аутентификация пользователей и контроль сессий.
- Автоматическое построение модели работы приложения.
- Анализ отклонений поведения пользователя от стандартного сценария.
- Анализ данных в SSL-туннеле.
- Пакет преднастроенных сигнатур.
- Поддержка правил формата ModSecurity и Suricata.
- Расширение доступных для разбора структур передаваемых данных.
- Возможность выбора различных объектов в качестве источника анализа данных (IP-адрес, сессионный идентификатор и т.д.).
- Проверка успешности действий пользователя и контроль последовательности действий (уровень бизнес-логики).

Сертификаты

Планируется сертификация по требованиям РД ФСТЭК России:

- 4-й уровень доверия
- 4-й класс защиты МЭ типа «Г»

Планируется сертификация по требованиям РД ФСБ России:

- СКЗИ класса КС2/КС3

Техническая поддержка

Техническая поддержка продуктов линейки «Континент» может осуществляться как напрямую, силами специалистов компании «Код Безопасности», так и через авторизованных партнеров.
В случае технической поддержки через партнера, партнер обеспечивает первую линию технической поддержки, а в случае сложных вопросов обращается в службу технической поддержки вендора.

Каталог услуг	Пакет поддержки			
	Базовый	Стандартный	Расширенный	VIP
Способ обращения в ТП	e-mail	веб-портал, e-mail	телефон, веб-портал, e-mail	
Приоритет	Низкий	Средний	Высокий	Наивысший
Консультирование по установке и использованию продукта	●	●	●	●
Доступ к Базе знаний	●	●	●	●
Доступ к пакетам обновлений	●	●	●	●
Прием предложений по улучшению продукта	●	●	●	●
Работа над инцидентами в режиме 8x5 (рабочие дни МСК 10:00–18:00)	●	●	●	●
Регистрация и контроль обращений на веб-портале		●	●	●
Работа над критичными инцидентами в режиме 24x7			●	●
Консультирование по дополнительному функционалу продукта			●	●
Выделенный инженер (для проведения работ)				●
Присутствие инженера на площадке заказчика				●

О компании «Код Безопасности»

Компания «Код Безопасности» – лидирующий российский разработчик сертифицированных программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов.

+7 (495) 982-30-20 (многоканальный) **info@securitycode.ru** **www.securitycode.ru**