

Комплексная информационная безопасность для российского пищевого холдинга

Заказчик – пищевой холдинг с оборотом более 20 млрд рублей в год. Компания управляет десятком онлайн-ресурсов, представленных в 75+ доменных зонах. Простой любого ресурса ведёт к финансовым потерям и сбоям в логистике.

Заказчик столкнулся с ростом интенсивности атак и понял, что стандартные меры защиты не справляются. Чтобы обеспечить непрерывную работу и свести простой сервисов к минимуму, компания обратилась в CORTEL за комплексной защитой ИТ-инфраструктуры.



Бизнес результат



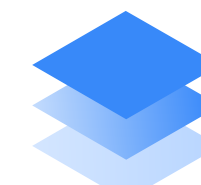
2 часа в год

максимально возможное
время недоступности онлайн
ресурсов под SLA 99,97%



4 уровня защиты

от DDoS, ботов, уязвимостей
в веб-приложениях
и атак на DNS



76 защищённых DNS-зон

отказоустойчивый DNS защищает
внешние и внутренние сервисы

Что было реализовано?

ЗАЩИТА ОТ DDOS-АТАК

- Первый реализованный уровень – это защита от DDoS на уровне приложения (L7).

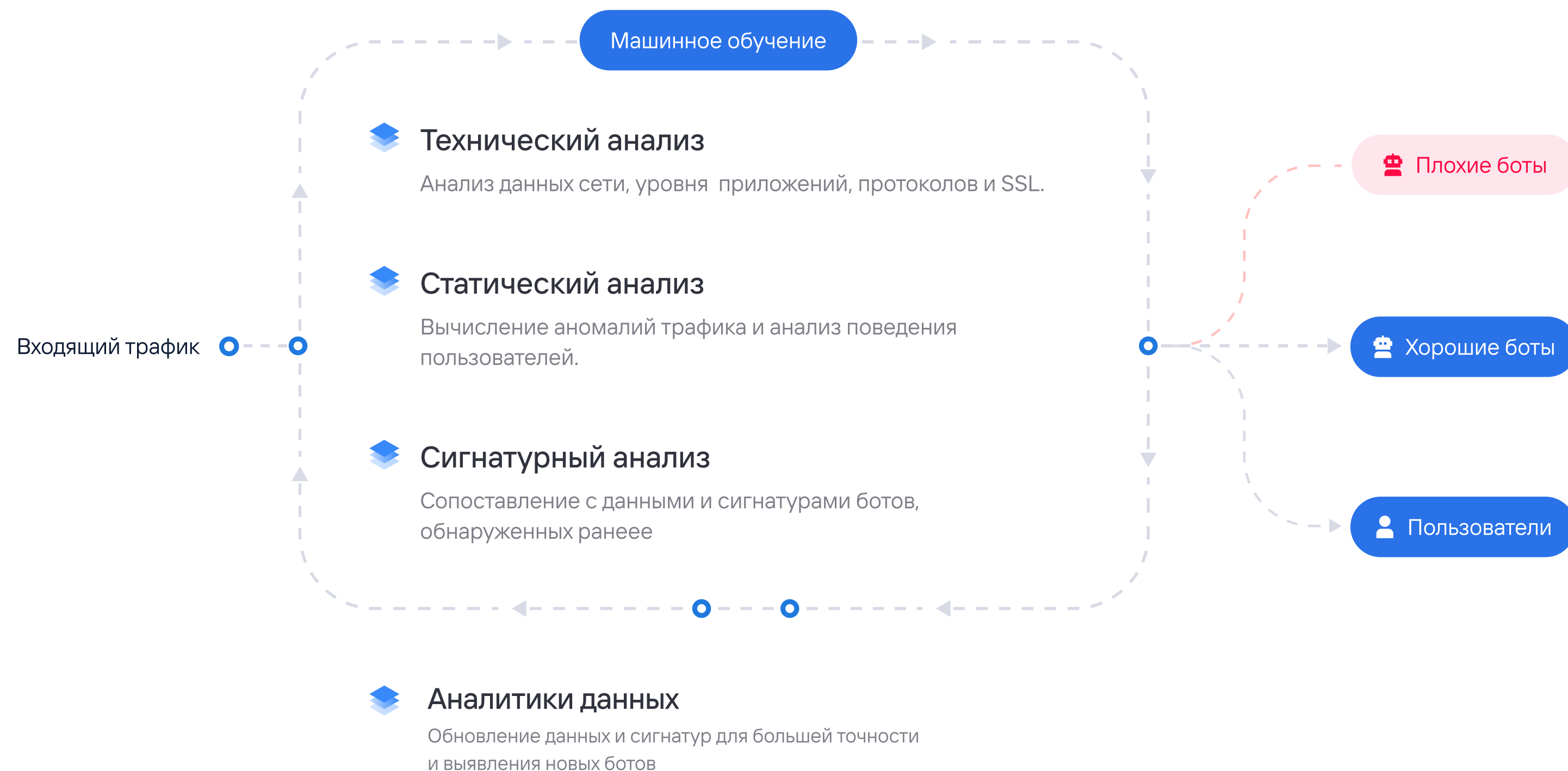
«У нас более десяти онлайн-сервисов. Мы убедились, что простой любого из них приводит к потерям в миллионы рублей и сбоям в логистике. Сетевой и транспортный уровни мы обезопасили сами, однако защита веба для нас критична, поэтому мы доверили её подрядчику, который гарантирует высокий уровень доступности» — прокомментировал директор по ИБ заказчика.



Что было реализовано?

ЗАЩИТА ОТ DDOS-АТАК

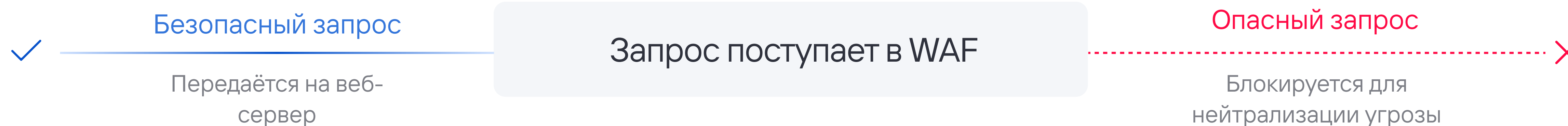
Под угрозой ботов любой онлайн-бизнес. Стандартная защита может их пропустить. Антибот-система фильтрует вредоносные боты и пропускает только легитимный трафик.



«Наши ресурсы – одни из крупнейших в России, и интерес к тому, чтобы нарушить работу онлайн-сервисов есть не только у злоумышленников, но и у конкурентов. Антибот – это дополнительный “фильтр”, который защищает наши ресурсы»
— прокомментировал директор по ИБ заказчика.

Что было реализовано?

WAF (WEB APPLICATION FIREWALL)

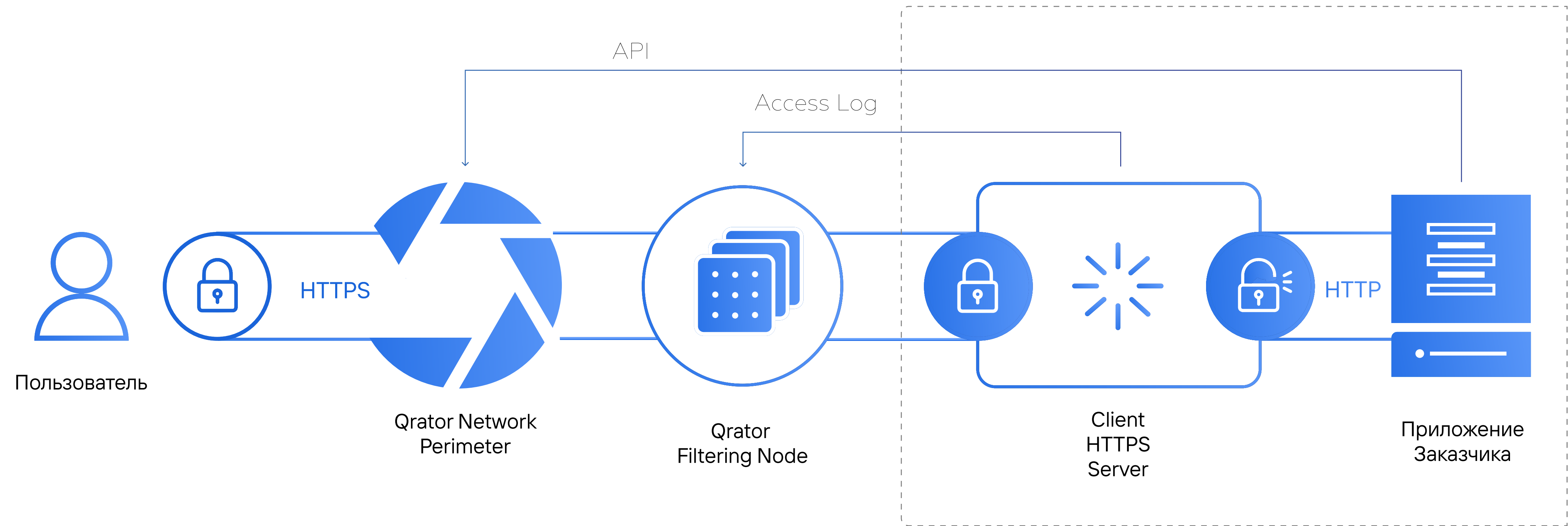


WAF – это средство фильтрации трафика, которое стоит между пользователем и веб-сервером. Оно анализирует HTTP(S)-запросы и блокирует подозрительную активность до того, как она нанесёт вред.

Технология не замедляет подключение пользователей к бизнес-приложениям. Для запуска не требуется обучение сотрудников, отдельная инфраструктура, закупка и установка дорогостоящего оборудования и ПО.

Архитектура решения

Сеть заказчика



Три уровня в комплексе – DDOS – Antibot – WAF – обеспечивают надёжную защиту и отказоустойчивость под SLA 99,97%.

Что было реализовано?

ДОПОЛНИТЕЛЬНЫЙ УРОВЕНЬ:
ОТКАЗОУСТОЙЧИВЫЙ ЗАЩИЩЕННЫЙ DNS

Заказчик разместил 76 DNS-зон на отказоустойчивом защищенном DNS.

Сайты, мобильные приложения, API и внутренние сервисы работают через доменные имена (DNS). Взлом DNS-сервера приведёт к тому, что пользователи не смогут попасть на веб-страницу компании.

Зачем это заказчику?

- В 2024 году ритейл стал одной из главных целей для киберпреступников. Только за IV квартал количество DDoS-атак на отрасль выросло на 26% год к году.
- Кибератаки на ритейл часто нацелены не просто на сбои в работе сайта, а на подрыв всей ИТ-инфраструктуры компании. В 2024-2025 годах DDoS – лишь прикрытие, за которым стоят целевые попытки взлома.
- Компания столкнулась с подобными прецедентами и решила обратиться в CORTEL для реализации комплексной защиты.

«Некоторые меры защиты, например, защиту от атак на сетевом и транспортном уровнях мы способны организовать самостоятельно, однако этого недостаточно в современных реалиях. Меры, которые работали раньше, теперь легко обходят. Поэтому мы решили обратиться к подрядчику, который не только обеспечит защиту, но и даст гарантии доступности всех веб-сервисов»
— прокомментировал директор по ИБ заказчика.



Как искали подрядчика

«По рекомендациям. Многие коллеги из сферы ритейла уже давно сотрудничают с CORTEL и полностью удовлетворены качеством услуг. Мы не можем позволить себе рисковать — цена ошибки слишком высока. Причём речь не только о финансовых потерях. Во-первых, регуляторы достаточно пристально следят за крупными холдингами. Во-вторых, всё больше покупателей переходят в онлайн. Если хотя бы один сервис будет недоступен, клиенты уйдут к конкурентам. К тому же, мы не можем допустить утечек данных. К тому же, мы не можем допустить утечек данных. Любой сбой критичен, по опыту гораздо эффективнее делегировать»
– прокомментировал директор по ИБ заказчика.



Что получил заказчик?

✓ Непрерывную работу веб-сервисов

✓ Надежную защиту от кибератак

✓ Гибкие условия подрячика

✓ Высокую экспертную помощь

✓ Персонального менеджера, круглосуточную техподдержку

✓ Сервис, гарантированный SLA



Директор по ИБ заказчика

«Некоторые меры защиты, например, защиту от атак на сетевом и транспортном уровнях мы способны организовать самостоятельно, однако этого недостаточно в современных реалиях. Меры, которые работали раньше, теперь легко обходят. Поэтому мы решили обратиться к подрядчику, который не только обеспечит защиту, но и даст гарантии доступности всех веб-сервисов»

Что в итоге

На протяжении года CORTEL помогает защищать веб-ресурсы заказчика от всех видов кибератак вне зависимости от масштабов и сложности.

Благодаря удобному личному кабинету можно отслеживать динамику трафика, а техподдержка круглосуточно находится на связи и оперативно отвечает на запросы.

Необходимые расширения внедряются день в день.

Количество пользователей растёт,
качество предоставляемых услуг остаётся неизменным.

