

# Защита от кибератак финансового онлайн-сервиса

## КЕЙС CORTEL И ВЕБЗАЙМ

Онлайн-сервис предоставляет услуги кредитования. Находится в рейтинге 10 крупнейших МФО по итогам 2022 года.

Все бизнес-процессы заказчика проходят онлайн 24/7, поэтому непрерывность – ключевое требование организации.





2022 год стал рекордным по количеству кибератак, направленных на российские организации. Одной из главных мишеней для злоумышленников был финансовый сектор. Благодаря внедрению WAF, компания получила **бизнес-результат:**

**0 минут**



простоя бизнес-критичных сервисов от атак различного уровня за 2022 год

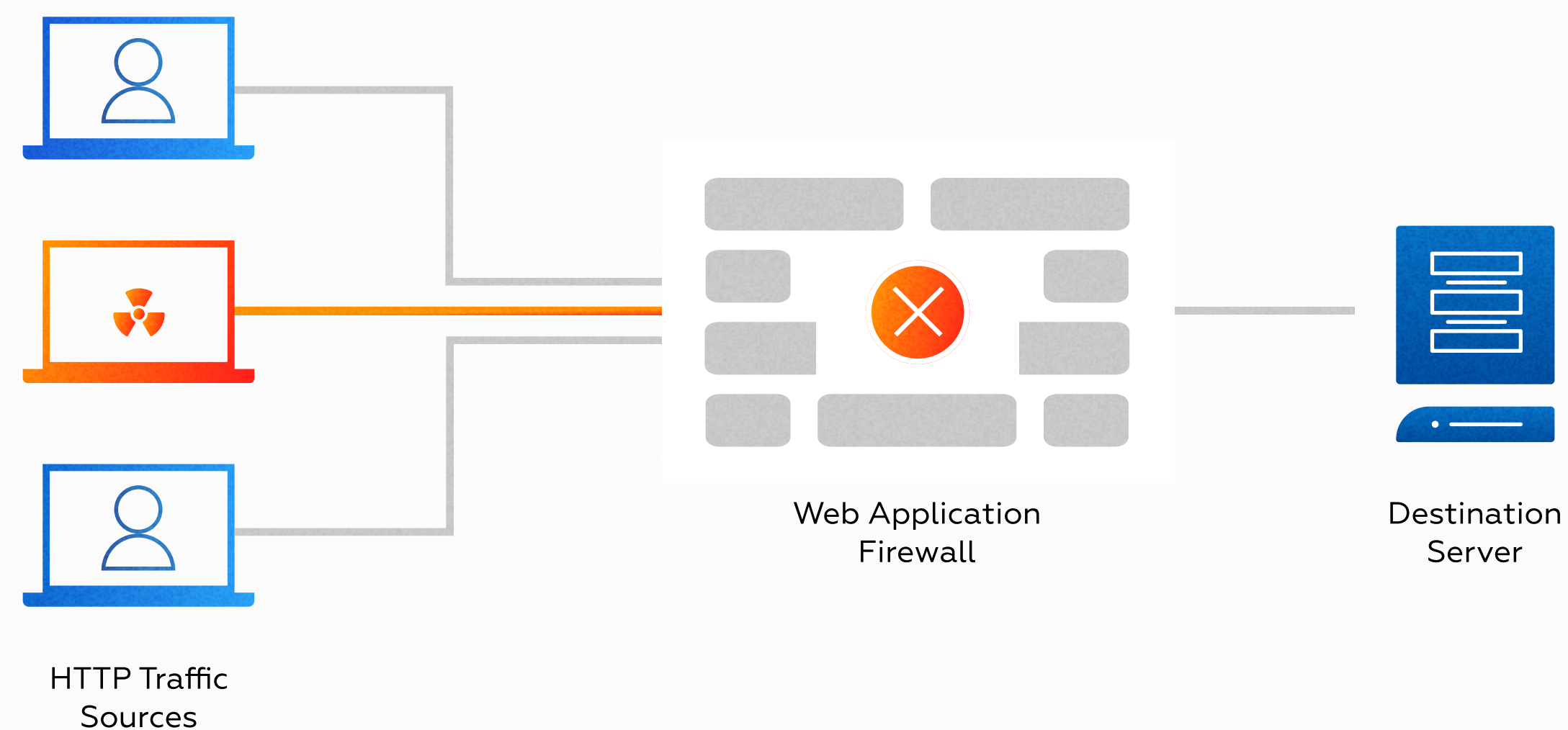
**100%**



доступ легитимных пользователей к сайту компании



# Что сделали?



**Внедрили межсетевой экран**  
(Web application firewall, WAF).

Это совокупность мониторов и фильтров, предназначенных для тонкого обнаружения и блокирования уязвимостей на любых уровнях полосы и сложности.

Технология реализована через облачный сервис, который не замедляет подключение пользователей к бизнес-приложениям.

**Для запуска не требуется обучение сотрудников, отдельная инфраструктура, закупка и установка дорогостоящего оборудования и ПО.**



# Зачем это заказчику?

CORTEL предоставлял клиенту базовую защиту от DDoS с 2019 года. На протяжении 3 лет она успешно справлялась с поставленной задачей, однако в 2022 году веб-сервис столкнулся с резким ростом интенсивности и длительности кибератак.

**Так как базовая защита не предназначена для отражения целенаправленных и сложных угроз, компания решила укрепить периметр.**



«В прошлом году произошло очень много кибератак по финансовому сектору. Мы не стали исключением, столкнувшись, в том числе, со сложными целенаправленными атаками. Мы и раньше встречались с DDoS, однако в этот раз сильно выросла необходимость в защите от более высокоорганизованных вторжений»

- директор по информационной безопасности «ВебЗайм»



# Какие были риски?

99% бизнес-процессов компании осуществляется на веб-площадках.

Любой сбой является критичным и влечёт за собой:

- потерю значительной части прибыли;
- репутационные риски;
- риски утечек персональных данных клиентов;
- регуляторные риски.



«Риски, связанные с непрерывностью, являются для нас критичными. Сбой в работе сервиса ведёт к остановке бизнес-процессов, рискам утечек персональных данных клиентов и, соответственно, регуляторным рискам»

- директор по информационной безопасности «ВебЗайм»



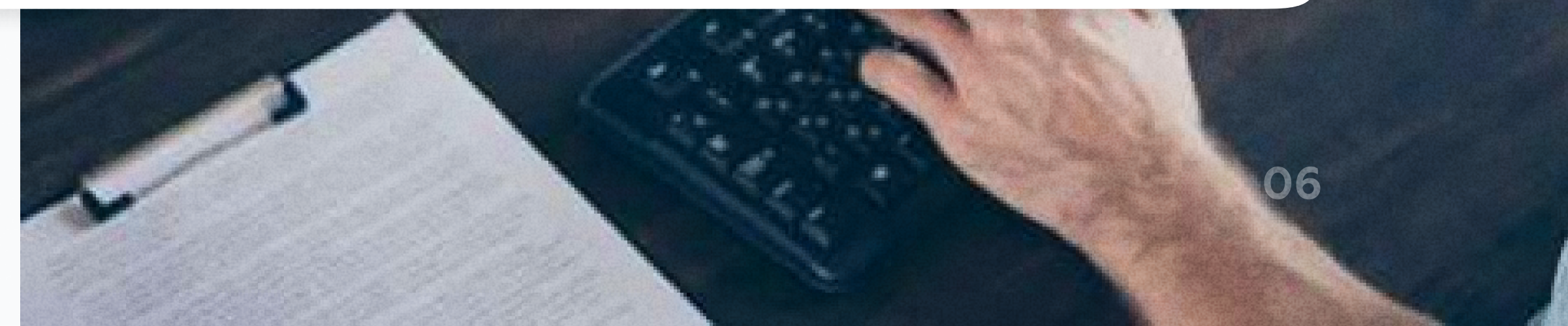
Как правило, **веб-приложения собственной разработки** обладают сложной архитектурой и множеством заимствованных компонентов. Зачастую, при выпуске обновлений и новых продуктов, разработчики не уделяют защите должного внимания.

**Такие уязвимости и становятся основной мишенью** злоумышленников и удобной точкой входа для проведения атак.



«Благодаря WAF от CORTEL мы стали увереннее в нашей стабильности. Знаем, что постоянно работает решение, которое может защитить не только от старых и текущих уязвимостей, но и в случаях выпуска нового продукта. Если разработчики оставят открытые уязвимости, WAF найдёт и заблокирует их, что гарантирует страховку от ошибок»

*- директор по информационной безопасности «ВебЗайм»*





# Как искали подрядчика

Заказчик на протяжении 3 лет использовал защиту от DDoS-атак, внедрённую CORTEL.

Компанию удовлетворяло качество предоставляемых услуг, поэтому **приняли решение укрепить ИТ ландшафт с проверенным партнёром.**



«Выбор подрядчика не занял много времени – мы давно работаем с облачными сервисами и не хотим, особенно сейчас, нести затраты на собственную ИТ-инфраструктуру, используем её только там, где в приоритете не стоит непрерывность – например, в тестовых средах, и привыкли бережливо относиться к финансовым и временным ресурсам. Поэтому сразу понимали, что решение должно находиться в облаке»

*- директор по информационной безопасности «ВебЗайм»*



# Что получил заказчик?



Сервис, гарантированный SLA



Надежную защиту от кибератак любой полосы и сложности



Гибкие условия подрячика



Непрерывную работу веб-сервисов



Высокую экспертную помощь



Персонального менеджера, круглосуточную техподдержку



«Разумеется, у нас был опыт взаимодействия с другими подрядчиками. CORTEL выгодно выделяется на фоне более крупных поставщиков оперативностью реакции на запросы и скоростью внедрения решений – WAF был установлен значительно быстрее, чем ожидали; и качеством предоставляемых услуг – в процессе тестирования было намного меньше ложных срабатываний, чем обычно при установке подобных решений»

*- директор по информационной безопасности «ВебЗайм»*



# Что в итоге?

На протяжении года Cortel помогает защищать портал ВебЗайм от всех видов кибератак вне зависимости от полосы и сложности. Необходимые расширения внедряются день в день. Благодаря удобному личному кабинету можно отслеживать динамику трафика, а техподдержка круглосуточно находится на связи и оперативно отвечает на запросы.

«Хотелось бы отдельно отметить “адекватность” команды Cortel. Для нас критически важна непрерывность и доступность нашего веб-сервиса. Мы являемся достаточно требовательными клиентами, детально изучаем все технические аспекты и требуем конкретного прогнозируемого результата в цифрах. Техподдержка помогает обеспечить необходимые условия и внимательно относится к качеству оказываемых услуг»

*- директор по информационной безопасности «ВебЗайм»*

