Защита от DDOS-атак крупного регионального банка на базе отечественного Qrator Labs

КЕЙС CORTEL В ФИНАНСОВОМ СЕКТОРЕ

Заказчик – крупный региональный банк, имеющий 13 отделений в СФО и 1 филиал в Москве.

Заказчик предлагает своим клиентам финансовые услуги для физических и юридических лиц: кредиты, вклады, ипотека, обмен валюты.

CORTEL

В марте 2022 года банк столкнулся с циклом DDOS-атак, которые привели к перебоям в работе основного сайта, медленной работе веб-ресурсов, и обратился в Cortel за помощью. Благодаря сотрудничеству с которым **бизнес** получил **результат**:

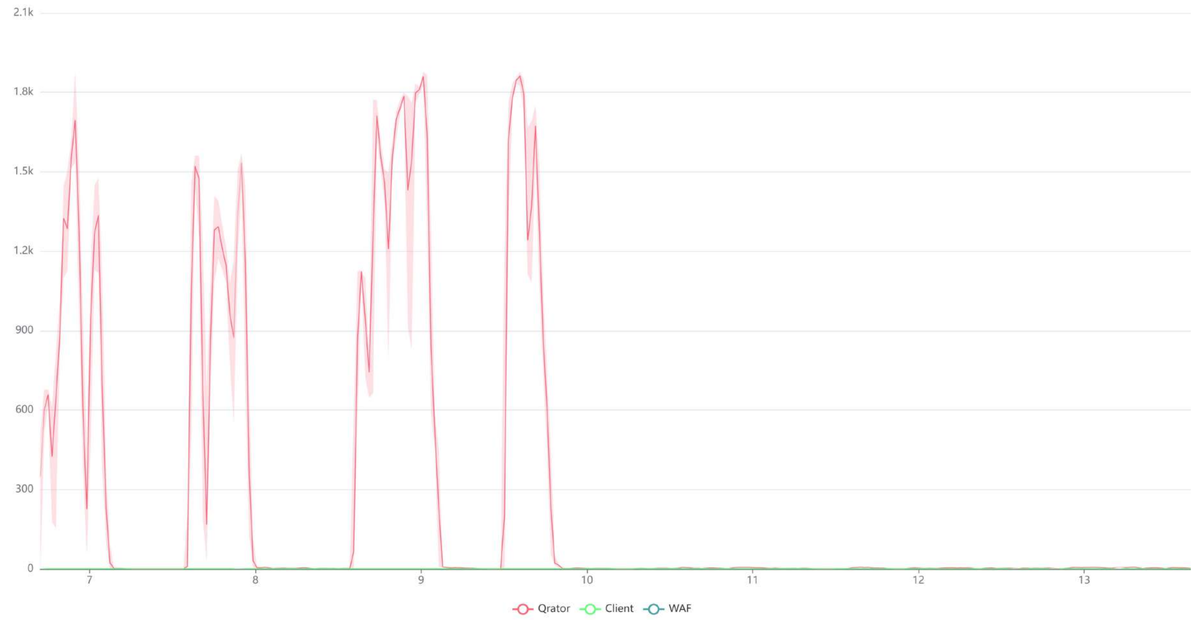
97% ⟶ доступность бизнес-критичных веб-сервисов в месяц

21 час ⟶ максимальное время возможной недоступности в месяц

Что было сделано?

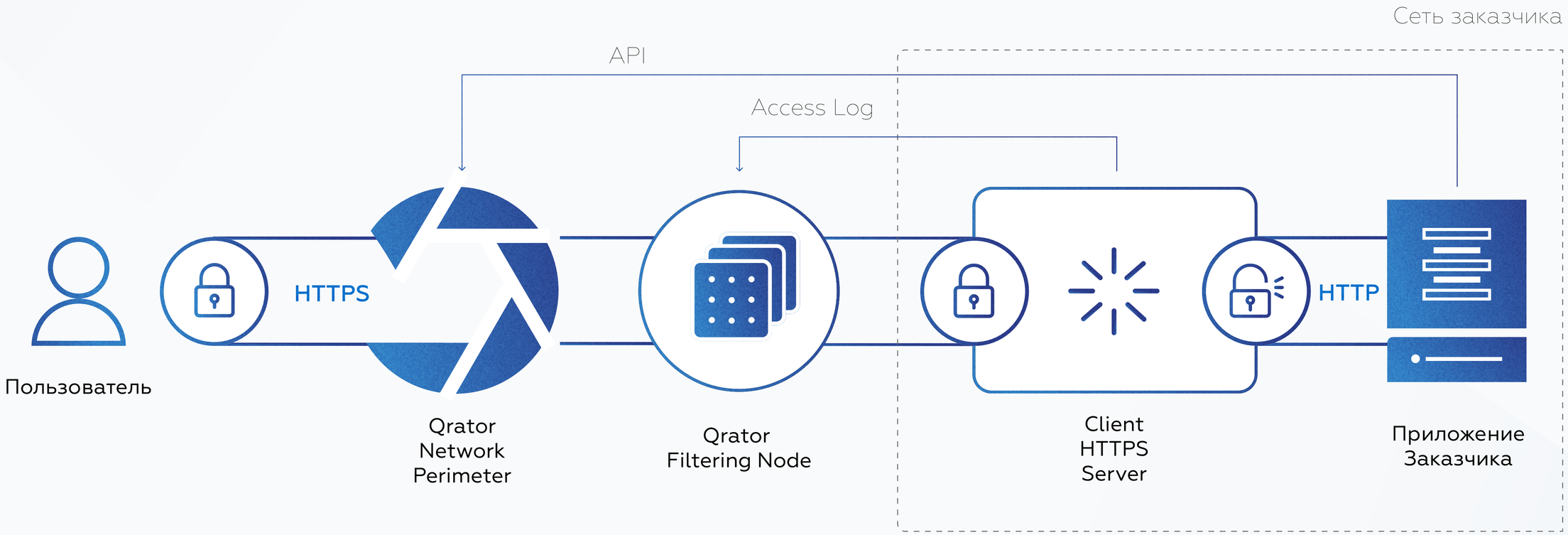
Обеспечили защиту сайта от всех видов DDoS-атак вне зависимости от полосы и сложности в день обращения, с учётом высоких требований к безопасности банковской ИТ-инфраструктуры.

Это стало возможным **благодаря внедрению технологии очистки трафика** через распределенные центры фильтрации, расположенные на всех континентах.

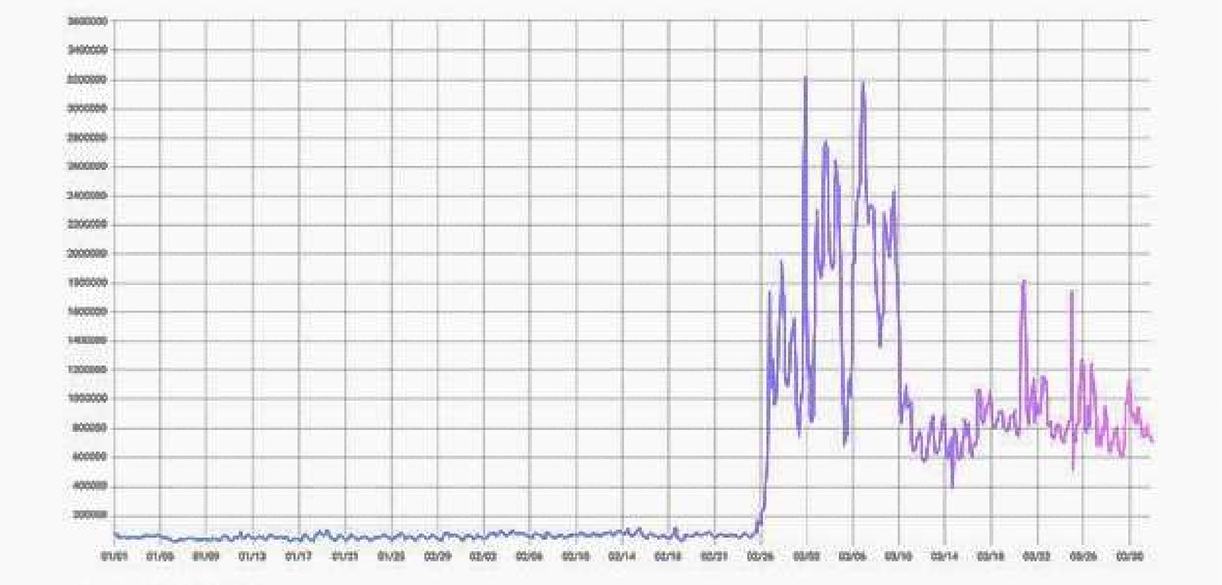


Количество IP-адресов, занесённых в чёрный список с 06 по 13 декабря 2022

Какая архитектура получилась?



По данным исследования ICT Online, 2022 год оказался рекордным с точки зрения DDoS-активности. В России выявили инцидент с участием **901 600** устройств. Средняя продолжительность атак - 29,5 часов, а самая долгая - 145 часов, чего не было **за всю историю наблюдений**.



Количество IP-адресов, занесённых в чёрный список с 06 по 13 декабря 2022

Статистика DDoS в 2022 году

DDoS-атака – распределенная атака типа «отказ в обслуживании». Цель – выведение веб-ресурса из строя. Злоумышленники направляют **постоянный поток запросов с** зараженных компьютеров, размещённых по всему миру.

Риски при DDoS-атаках

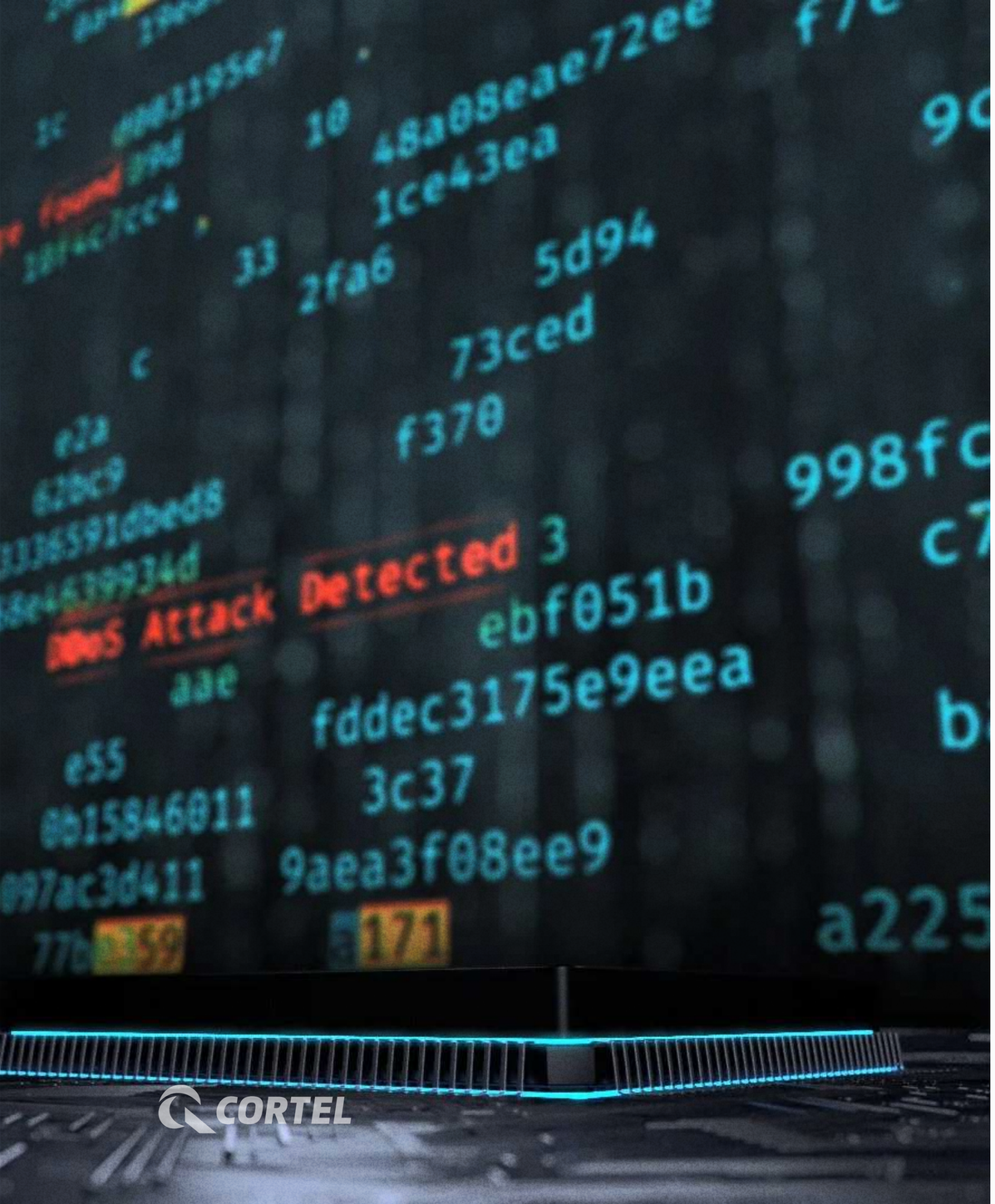
Репутационные риски
Надежность и удобство – часть имиджа банков. Длительные перебои в работе приводят к потере доверия клиентов.

Технические издержки
Устранение последствий требует дополнительного времени сотрудников, ресурсов на обеспечение безопасности, разработки плана обновления ПО, модернизации оборудования и т.д.

Финансовые потери
Простой в работе, утрата узнаваемости компании – и это не все. Убытки от атак с нарушением доступности оценивают в 85 тыс.$ для небольших организаций и почти в 790 тыс.$ для крупных предприятий.

“Какой бы мощной не была инфраструктура, обслуживающая приложения, она не выдержит нагрузку на несколько порядков выше нормы и выйдет из строя. Это, как правило, приводит к весьма критичным последствиям в виде финансовых и репутационных потерь. ”

- отметил коммерческий директор компании Cortel.



Зачем это заказчику?

Главной целью DDoS стал финансовый сектор. Доля атак в нем варьировалась от 70% в марте до 37% в июне.

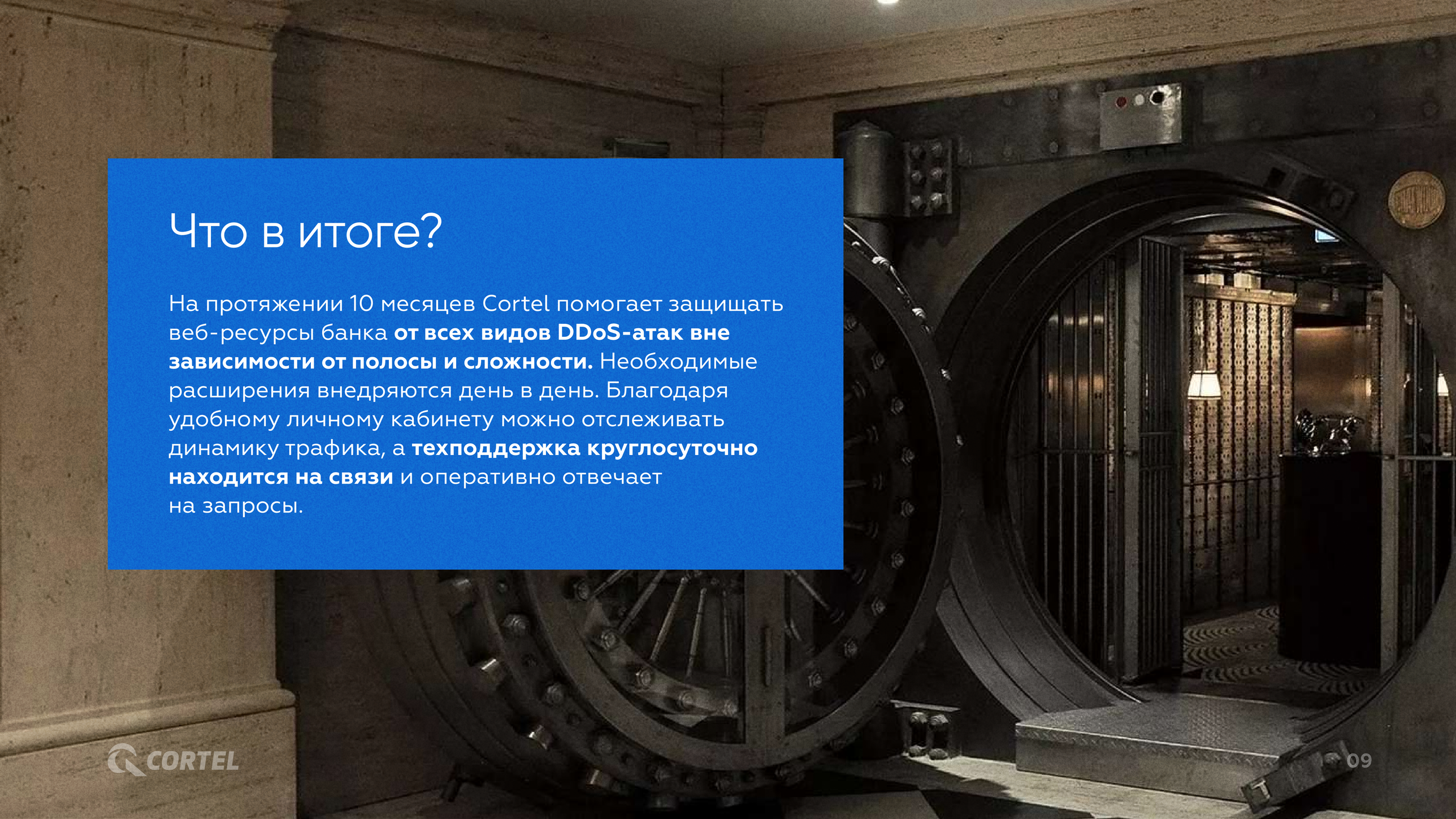
В марте 2022 года банк столкнулся с циклом DDoS-атак, которые привели к сбоям в работе основного сайта. Представители решили обратиться к подрядчику, который обеспечит **защиту от атак любой сложности на базе отечественных решений**.

Руководству банка **порекомендовали Cortel,** как **надёжного** поставщика услуг.
Защиту подключили в тот же день.

Что получил заказчик?

- Оказание услуги в день обращения, до подписания договора
- Сервис, гарантированный SLA
- Гибкие условия подрядчика
- Высокую экспертную помощь
- Персонального менеджера, круглосуточную техподдержку

CORTEL



Что в итоге?

На протяжении 10 месяцев Cortel помогает защищать веб-ресурсы банка **от всех видов DDoS-атак 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.