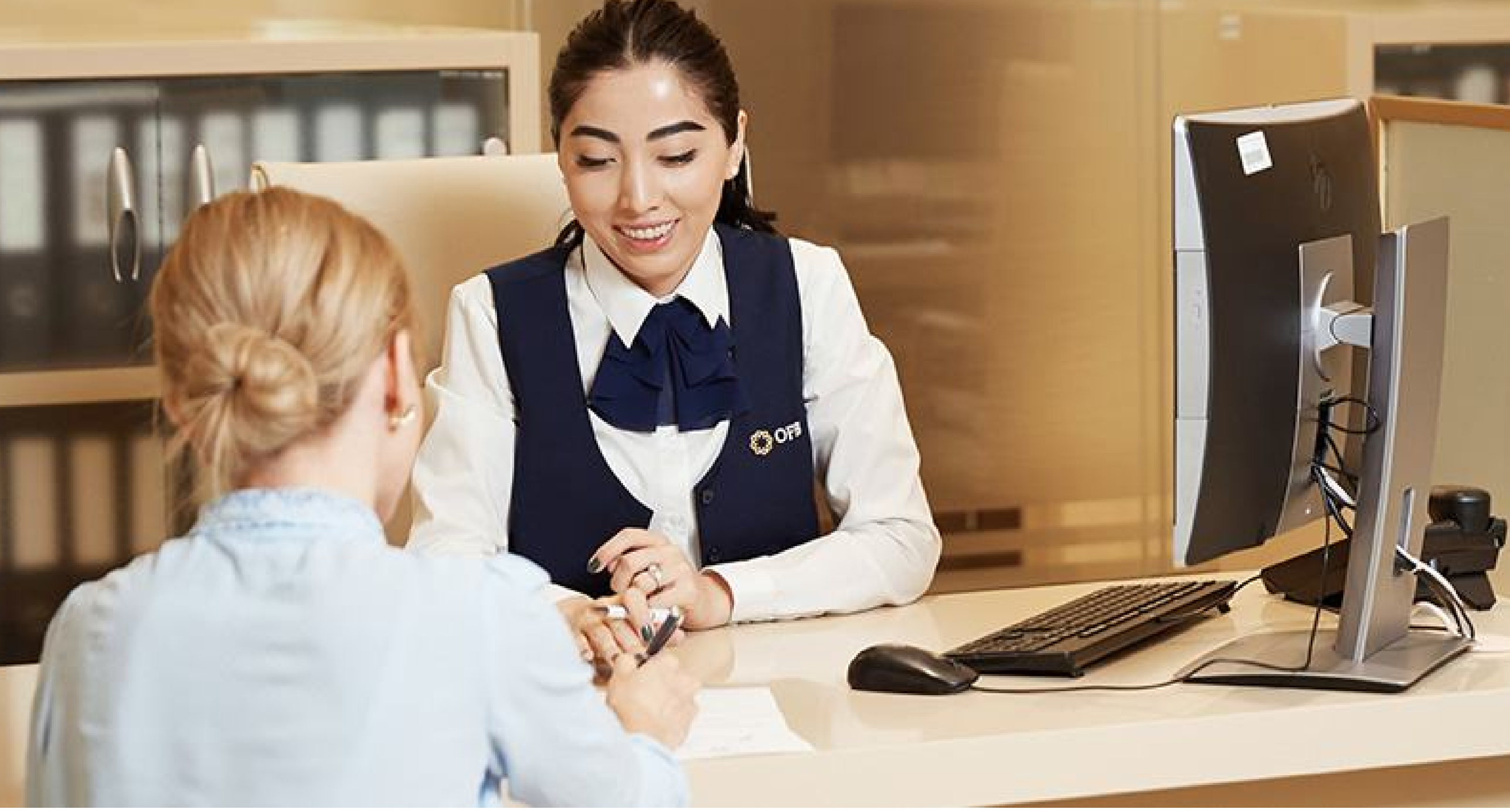
Банк «Ориент Финанс» перешёл на продвинутую защиту рабочих мест с помощью Kaspersky EDR для бизнеса Оптимальный

Банк «Ориент Финанс» из Республики Узбекистан перешел на решение Kaspersky EDR для бизнеса Оптимальный. Это позволило повысить защищенность рабочих мест от сложных угроз и тем самым сэкономить время специалистов банка, которые занимаются мониторингом ИБ- событий.

kaspersky



Предыстория

01.

Частный акционерный коммерческий банк «Ориент Финанс» работает в Узбекистане с 2010 года — сейчас в его активе 630 тыс. частных и более 20 тыс. корпоративных клиентов.

Надежность финансового положения банка подтверждают кредитные рейтинги международных и национальных рейтинговых агентств. Так, международное рейтинговое агентство S&P Global Ratings подтвердило долгосрочный кредитный рейтинг банка на уровне «B».

Сейчас «Ориент Финанс» — пример устойчивого развития и постоянной цифровизации. В условиях меняющегося ландшафта киберугроз банк повышает зрелость и эффективность внутренних процессов обеспечения безопасности. Поэтому ИБ — и ИТ-департаменты внедряют новые защитные технологии, оценивают безопасность применяемых ИТ-решений и развивают ИБ-процессы. Чтобы сотрудники могли эффективно выполнять эти задачи, в «Ориент Финанс» собирались сократить время, которое специалисты тратят на мониторинг киберинцидентов.

В итоге банк решил дополнить имеющуюся систему антивирусной защиты базовой функциональностью EDR (Endpoint Detection and Response). Решения класса Endpoint Detection & Response используются для обнаружения и изучения вредоносной активности на конечных точках: подключённых к сети компьютерах, серверах, устройствах интернета вещей и мобильных гаджетах. EDR-продукты ориентированы на выявление сложных атак, поэтому выступают в качестве дополнения к антивирусам, а не заменяют их. Пока антивирус борется с типовыми и массовыми угрозами в автоматическом режиме, EDR-решения помогают выявить более сложные атаки и оперативно на них отреагировать. Разные технологии — разные задачи.

630
тыс. частных
и более 20 тыс. корпоративных клиентов в активе банка «Ориент Финанс»

Решение

02.

Kaspersky EDR для бизнеса Оптимальный — это решение с расширенными возможностями обнаружения угроз, базового расследования инцидентов и автоматизированного реагирования.

Оно умеет идентифицировать, анализировать и нейтрализовывать даже маскирующиеся угрозы. При этом подойдет как для компаний с собственной ИБ-командой, так и для бизнеса, где задачи по киберзащите выполняют сотрудники ИТ-департамента.

Kaspersky EDR для бизнеса Оптимальный помогает компаниям противостоять сложным и изобретательным киберугрозам, которые способны причинить серьезный ущерб бизнесу. Продукт повышает видимость ИБ-событий в инфраструктуре, поскольку инструменты контроля программ, устройств и использования интернета снижают роль человеческого фактора и помогают сохранить устойчивость системы безопасности к интернет-угрозам, фишинговым рассылкам и социальной инженерии. Кроме того, перейти на Kaspersky EDR для бизнеса Оптимальный можно с любого решения «Лаборатории Касперского» по защите конечных точек — процесс пройдет быстро и бесшовно.

Преимущества Kaspersky EDR для бизнеса Оптимальный

- Содержит продвинутые технологии для защиты рабочих мест и их контроля; работает с разными типами конечных точек и всеми популярными платформами.
- Получает постоянные обновления базы данных об угрозах на основе глобальной облачно-репутационной платформы KSN и экспертных исследований «Лаборатории Касперского».
- Предоставляет детальную информацию об обнаруженной угрозе — открывает возможность анализа первопричин и всей цепочки развития киберинцидента.
- Удобно управляется — клиент получает единый агент для EPP и EDR, единую консоль управления защитой конечных устройств, процессами обнаружения и реагирования, а также единую карточку инцидента со сценариями, инструкциями по реагированию и простыми инструментами, не требующими экспертных знаний и долгого обучения.
- Экономит время сотрудников — решение позволяет автоматизировать реагирование на всех хостах при обнаружении угрозы, автоматизировать процесс сокращения поверхности атаки и настройки политик, а также создавать правила для блокирования аналогичных атак в будущем.

Результат и отзывы

03.

Переход на Kaspersky EDR для бизнеса Оптимальный позволил банку «Ориент Финанс» лучше выявлять сложные угрозы.

Функциональность реагирования помогает справляться с задачами по сдерживанию ИБ-инцидентов быстро и эффективно. Возможность сканирования с использованием индикаторов компрометации автоматизировала процесс проверки инфраструктуры на наличие новых угроз. В результате решение позволяет специалистам банка тратить меньше времени на ручные процедуры в рамках реагирования на инциденты.

Важно отметить, что инфраструктура банка уже была защищена решениями «Лаборатории Касперского» Kaspersky Security для бизнеса, Kaspersky Security для почтовых серверов и Kaspersky Embedded Systems Security. Решение поставлялось в рамках расширения функционала при ежегодном продлении пакета уже имевшихся ранее лицензий, поэтому миграцию на продвинутый продукт банк провел силами ИТ-департамента, и процесс отнял совсем немного времени.

«Внедрение EDR в “Ориент Финанс” поможет быстро выявлять атаки и эффективно реагировать на них, минимизируя потенциальный ущерб и значительно экономя время ИБ-специалистов банка. Это важный шаг в повышении ИБ-зрелости компании в целом. Существующий набор решений позволит банку создать прочный фундамент для защиты бизнеса от киберугроз и масштабировать защиту по мере роста и развития организации», — добавил Валерий Зубанов, управляющий директор «Лаборатории Касперского» по Центральной Азии и Монголии.

> «Новое решение позволяет нам бороться со сложными угрозами, которые умеют скрывать следы своей деятельности от классического антивируса. А за счет дополнительного контекста ИБ-инцидентов мы теперь можем точнее выявлять источник угрозы и определять её последствия, не прибегая к трудоемкому ручному анализу. Также решение позволяет выявлять первопричины возникновения киберинцидентов и проводить профилактику подобных событий в будущем, что важно для сохранения устойчивости бизнес-процессов».
>
> **Артем Норенко,** начальник Управления информационных технологий банка «Ориент Финанс».

Kaspersky EDR