**ДО АО «Банк ВТБ» (Казахстан)**

**г. Алматы**

**«14» октябрь 2020 год**

**Техническое задание**

**(к конкурсу по переходу от продукта Database Firewall (DBF) производителя Imperva на продукт DBF производителя Гарда)**

 В целях единого подхода к построению систем защиты информации группы ВТБ, переход от продукта Database Firewall (DBF) производителя Imperva на продукт DBF производителя Гарда.

**Описание системы**

Гарда БД - Аппаратно-программный комплекс класса DAM /DBF\* для обеспечения безопасности СУБД и независимого аудита операций с базами данных и бизнес-приложениями. Ведет непрерывный мониторинг обращений к базам данных и выявляет подозрительные операции в режиме реального времени.

**Требования к поставщику**

1. Техническая спецификация указана в приложении №1.

Поставщик обязуется поставить и передать Заказчику в собственность аппаратно-программный комплекс класса DAM /DBF\* для обеспечения безопасности СУБД и независимого аудита операций с базами данных и бизнес-приложениями.

1. Аппаратно-программный комплекс Гарда ДБ (Лицензия бессрочная, продление технической поддержки продукта).
2. Поставщик обязуется:
3. Осуществить поставку аппаратно-программного комплекса класса DAM /DBF.
4. произвести установку и настройку поставляемого оборудования.
5. предоставить гарантийную техническую поддержку от производителя 24х7 сроком на 12 месяцев, начиная с даты заключения договора.
6. предпринять все возможные усилия в разумных пределах для быстрого исправления ошибок в Продукте.
7. предоставить техническую поддержку и помощь ДО АО Банк ВТБ (Казахстан) в отношении Продукта, включающую в себя номер телефона для техподдержки, номер факса и/или адрес электронной почты, доступные только Техническому Контактному Лицу.
8. предоставлять Заказчику исправления ошибок, новые версии, обновления, расширения продукта и улучшения.
9. предпринимать в разумных объемах все необходимые меры для исправления Ошибок в соответствии с расписанием, приведенным ниже. Поставщик так же должен предоставить техническую поддержку и помощь по соответствующим Продуктам, включающую в себя:

1) разъяснения функций и возможностей;

2) разъяснения Документации;

3) помощь в использовании Продукта.

1. Наличие не менее 2-х сертифицированных инженеров в компании.
2. В коммерческом предложении **необходимо указать следующие данные**:
3. Условия оплаты - по умолчанию 50% предоплата, 50 после подписания актов приёма-передачи оборудования;
4. Техническая поддержка – 1 год.
5. Срок поставки оборудования – не более 45 календарных дней.
6. Установка и настройка поставляемого оборудования – 22 рабочих дней с даты поставки оборудования.
7. Совместное функционирование продукта с действующим ПАК DBF Imperva.
8. Обучение 1 работника по администрированию продукта.
9. Готовность подписать договор - по умолчанию 10 календарных дней с момента объявления победителя.

Приложение 1

**Техническая спецификация**

**Общие требования:**

1. Разработка схемы интеграции в сети заказчика;
2. Аппаратно-программный комплекс (сервер физический 2 шт.) класса DAM /DBF должен сохранять свою работоспособность после отказа одной или нескольких её составных частей (отказоустойчивость);
3. Защита от утечек хранящейся в БД информации;
4. Контроль действий привилегированных пользователей;
5. Выявление и предотвращение попыток внешнего вторжения;
6. Аудит всех операций с БД в режиме реального времени;
7. Анализ сетевого трафика с возможностью мониторинга или блокировки нелегитимных запросов пользователей и получаемых данных из СУБД;
8. Обработка данных и долгосрочное хранение всех запросов и ответов для ретроспективного анализа;
9. Автоматический поиск новых СУБД, не стоящих на контроле, классификация их по типу хранимых данных;
10. Сканирование баз данных, находящихся под контролем;
11. Аналитическая отчетность и поведенческий анализ (UBA), выявление нарушений политик безопасности;
12. Система оповещения уведомляет о событиях по электронной почте, передает данные во внешние SIEM-системы, отображает отчёты на главном экране;
13. Возможность ретроспективного анализа по сохраненным данным объёмом свыше 100 ТБ;
14. Аудит доступа к БД всех филиалов компании из единого центра.
15. Интеграция со всеми популярными SIEM;
16. Возможность анализа трафика на скорости более 10 Гбит/с;
17. Полноценная работа с трёхзвенной архитектурой взаимодействия с БД;
18. Минимальное влияние на производительность сети и серверов СУБД;
19. Интерактивные отчеты и понятная аналитика на основе всех запросов и ответов БД, статистика инцидентов;
20. Хранение всех ответов и запросов пользователей и приложений с возможностью ретроспективного анализа за любой период времени;
21. Встроенная система выявления аномалий и поведенческого анализа действий пользователей;
22. Отсутствие стороннего лицензирования.