Microsoft

Окончание поддержки SQL Server и Windows Server 2008 и 2008 R2 уже скоро

Как подготовиться к прекращению поставок обновлений безопасности?

Последний день поставки обновлений системы безопасности:

9 июля 2019 г.
SQL Server 2008 и 2008 R2

14 января 2020 г.
Windows Server 2008 и 2008 R2

Тысячи критически важных бизнес-приложений во всем мире, в том числе, возможно, и ваши, работают на SQL Server и Windows Server 2008 и 2008 R2.

Когда Microsoft прекратит осуществлять поддержку этих продуктов, системы, которые работают на их основе, могут остаться без защиты и перестанут соответствовать современным требованиям. Организации, не обновляющие регулярно свои системы информационной безопасности, более уязвимы для кибератак, способных привести к хищению клиентских и корпоративных данных, нанесению ущерба репутации компании и утрате доверия со стороны участников рынка.

Примите меры уже сейчас, чтобы сохранить соответствие требованиям, предотвратить утечки данных и избежать штрафных санкций. Используя текущие версии системного ПО, вы получаете преимущества благодаря самым новым возможностям, механизмам обеспечения производительности и надежности, а также регулярным обновлениям системы безопасности.

Избегайте риска для бизнеса и предотвращайте проблемы безопасности

Получая от Microsoft регулярные обновления системы безопасности, организации заботятся о защите своих приложений и данных, а также о соответствии законодательным требованиям.

Примеры рисков	Пояснение	Серьезность: ущерб
Программы-вымогатели (WannaCry, NotPetya, BadRabbit)	Такие программы блокируют доступ к вашим данным и требуют выкуп	Критически важная: блокирование доступа к системе, блокирование доступа к данным, уничтожение данных, остановка бизнес-процессов
Аппаратные уязвимости (Meltdown, Spectre)	Уязвимость ЦП, позволяющая злоумышленникам похищать конфиденциальные данные (устраняется с помощью обновлений безопасности для операционной системы).	Важная: получение контроля над системой и данными, раскрытие информации
Общие положения о защите данных (GDPR) ЕС. Акт о передаче и защите данных учреждений здравоохранения (HIPAA). Стандарт безопасности данных в сфере платежных карт (PCI DSS). Федеральный закон США об управлении информационной безопасностью (FISMA). FIPS (федеральный стандарт обработки информации). Служба регулирования отрасли финансовых услуг (FINRA). NIST 800-53 (MFA). Закон Сарбейнза — Оксли.	Без обновлений системы безопасности появляется риск уязвимости приложений и, как следствие, хищений данных и удостоверений. Для выполнения некоторых нормативно-правовых актов, в том числе GDPR, требуются возможности, которых в устаревших системах просто нет.	Важная: ущерб репутации, потеря конкурентной способности, потеря доверия клиентов, значительные штрафы со стороны контролирующих органов.

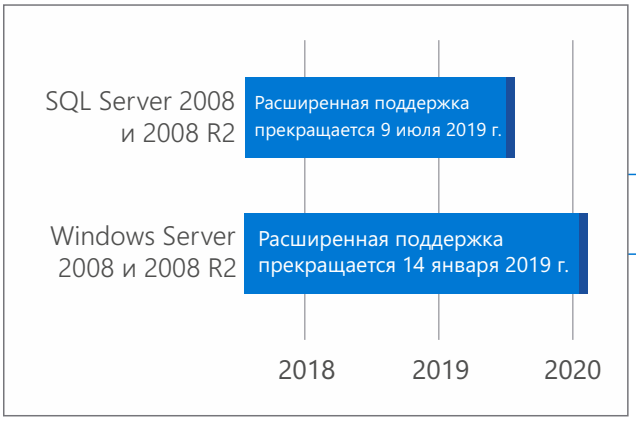
Новые решения упрощают соблюдение требований регуляторов

Последние версии SQL Server и Windows Server помогают соблюдать новые требования, в том числе самые строгие, такие как GDPR.
Вы можете использовать эти мощные программные продукты в Azure, локально или в гибридной среде.
Защититесь от хищения учетных данных и создайте более безопасную среду со встроенными средствами аутентификации и авторизации.
Упростите управление личными данными и их мониторинг, получите доступ к инструментам и ресурсам, помогающим соблюдать требования GDPR об отчетности и оценке.
Дополнительные сведения см. на сайте Microsoft Trust Center

Повышайте уровень защищенности

Примите меры по предотвращению проблем, связанных с обеспечением безопасности и соответствия требованиям регуляторов, установив новые версии ПО: SQL Server 2017 и Windows Server 2016 или 2019.
Текущие версии всегда сопровождаются обновлениями системы безопасности, что гарантирует защиту от новых угроз. Если вы не успеваете перейти на новую версию до наступления срока прекращения поддержки, защитите рабочие нагрузки с помощью расширенных обновлений, бесплатно предоставляемых при переходе на виртуальные машины Azure, или заплатите за обновления для ваших локальных серверов.

Продление поставки обновлений системы безопасности в Azure — бесплатно



Миграция в Azure

Продолжайте использовать локальные системы

Модернизируйте защиту согласно требованиям нового времени

Мощные механизмы безопасности, встроенные в Azure и последние версии SQL Server и Windows Server, повышают надежность вашей платформы и обеспечивают сквозную защиту всей среды — от компьютеров и серверов до облачных систем.

- Защититесь от хищения учетных данных, которое происходит в 63% случаев несанкционированного проникновения.
- Позаботьтесь о том, чтобы доступ к вашим ИТ-средам, данным и приложениям имели только те пользователи, у которых есть на это полномочия.
- Дополните все конечные точки мощными средствами обнаружения вторжений, расследования инцидентов и реагирования.

Переместите приложения

Переходите на виртуальные машины Azure, не меняя код приложений, и еще 3 года бесплатно получайте обновления системы безопасности. Установите новую версию, когда будете к этому готовы.

Защитите свои данные

Перенесите SQL Server в управляемый экземпляр базы данных SQL Azure (не требует учета номера версии, полностью управляемая служба, не нуждается в установке обновлений).

Установите последнюю версию Windows Server и SQL Server.

ИЛИ

Заплатите за продление на 3 года поставки обновлений безопасности, чтобы защитить серверы, пока выполняется миграция.

Приступайте

Приступайте к планированию, используя онлайн-ресурсы, перечисленные на сайте: www.microsoft.com/2008-eos

Расширенные обновления безопасности доступны только для Windows Server 2008 и 2008 R2 и SQL Server 2008 и 2008 R2.