

Какая платформа безопасности лучше всего вам подходит?

Задавайте правильные вопросы. Получите правильные ответы.



Выбор правильной платформы безопасности

Поиск платформы безопасности для вашей организации может оказаться непростой задачей. В контексте кибербезопасности термин “платформа” слишком перегружен – не всегда просто пробиться сквозь шум и понять, какие факторы следует учитывать при выборе оптимального варианта для вашего бизнеса. К выбору платформы следует подходить с особой тщательностью, поскольку она будет выполнять роль фундамента вашей системы обеспечения безопасности в течение следующих нескольких лет.

Специалисты по безопасности сталкиваются с огромными объемами данных, множеством инструментов и ограниченными ресурсами. Пришло время новых способов унификации данных, инструментов и команд, связанных с безопасностью – существует острая необходимость объединить всё это в одной интегрированной платформе для обеспечения безопасности.

Какими качествами должна обладать платформа безопасности

Для того чтобы найти комплексную, интегрированную платформу кибербезопасности с прицелом на будущее, вам необходимо принять во внимание:



Соображения по поводу перемещения данных



Варианты развертывания



Взаимодействие с другими инструментами



Открытость и адаптивность платформы



Поддерживаемые функции и службы

Следующие ключевые вопросы помогут лучше понять доступные варианты при выборе оптимальной платформы для вашей организации.

1 Требуется ли перемещение данных?

Многие платформы безопасности требуют перемещения в них всех данных, чтобы обеспечить доступ к ним. Несмотря на то что размещение всех данных в одном месте может показаться хорошей идеей, это может быть сложным и дорогостоящим процессом. Более того, для этого может потребоваться решить важные проблемы, связанные с местом хранения и конфиденциальностью данных.

С точки зрения стоимости и сложности может оказаться более целесообразным обеспечить доступ платформы к данным, там где они уже расположены – без необходимости их перемещения. Такой подход может дополнить существующие инструменты и получить максимальную отдачу от существующих инвестиций, предоставив централизованное представление и доступ к данным, которые уже распределены между разными инструментами.

2 Можно ли для развертывания платформы выбрать локальную среду, общедоступное облако или частное облако?

Многие платформы безопасности доступны только как решения SaaS (программное обеспечение в качестве услуги). Однако, полностью облачные решения подходят далеко не всем организациям – многие отдают предпочтение гибридной мультиоблачной архитектуре, которая отличается высокой гибкостью. Учитывая, что многие организации по-прежнему используют преимущественно локальные приложения, платформа безопасности с поддержкой не только локальной среды, но и общедоступного или частного облака может оказаться полезной. Вместо того, чтобы ограничивать себя только одним вариантом развертывания, ищите гибкую архитектуру, которую можно развернуть в гибридных мультиоблачных средах.

3 Поддерживает ли платформа соединения и интеграции с внешними инструментами?

Современные организации применяют широкий спектр инструментов обеспечения безопасности от множества поставщиков. Отдельные платформы безопасности допускают интеграцию инструментов только конкретного поставщика и это может ограничивать ваши возможности. Если вы используете инструменты обеспечения безопасности от разных поставщиков, попытайтесь найти платформу с поддержкой открытых соединений с широким спектром инструментов обеспечения безопасности и ИТ-инструментов. Выберите тот вариант, который включает:

- Обширную экосистему партнеров
- Комплект для разработки приложений с открытым исходным кодом (SDK)
- Услуги поддержки для добавления нестандартных соединений

Такой подход поможет определить, будет ли платформа работать с вашими инструментами, и избежать полной замены инструментов.

4 Способна ли платформа адаптироваться к изменениям программы безопасности?

При выборе платформы стоит обратить внимание на тот вариант, который сможет обеспечить достаточную гибкость и открытость для поддержки изменений программы безопасности. Проверьте, предлагает ли она:

- Открытые стандарты
- Технологию с открытым исходным кодом
- Открытые соединения

Открытая платформа может подключаться к внешним инструментам, а также поддерживает нестандартные соединения и разработку специализированных решений. Такой подход помогает избежать привязки к одному поставщику и улучшить совместимость с разными инструментами.

5 Предлагает ли она базовые средства координации, автоматизации и реагирования?

Решения для согласования мер безопасности, автоматизации защиты и реагирования на угрозы (SOAR) часто позиционируются как самостоятельные платформы. Однако функции SOAR могут принести больше пользы в составе комплексной платформы безопасности. Вам нужна платформа безопасности со встроенными функциями SOAR для повышения эффективности работы специалистов по безопасности с рядом рабочих процессов и сценариев использования.

6 Каким образом она поддерживает интеграцию анализа угроз?

Аналитики по вопросам безопасности часто используют множество каналов информации об угрозах и разные продукты для исследования угроз и обоснования принимаемых решений. Проверьте, предоставляет ли платформа отчеты об анализе угроз и способы интеграции аналитики с другими функциями. Интеграция анализа угроз в платформу безопасности помогает снизить нагрузку на аналитиков по вопросам безопасности и быстрее принимать обоснованные решения.

7 Предлагает ли поставщик услуги в дополнение к программному обеспечению?

Платформа безопасности без сомнения является мощным инструментом, но вашей организации или программе безопасности также могут потребоваться дополнительные услуги. Вы можете выбрать среди множества услуг в области безопасности, но если поставщик платформы также предоставляет дополнительные услуги в области безопасности, то процесс добавления и интеграции таких услуг в платформу будет значительно более простым.

Изучите ваши потребности и желания относительно платформы безопасности

Подходы на основе платформы помогают обеспечить взаимосвязь между данными, инструментами и специалистами по безопасности. При выборе оптимальной платформы безопасности для вашей организации из множества вариантов важно найти ответы на следующие ключевые вопросы:

- Можете ли вы оставить данные там, где они находятся?
- Нужна ли вам поддержка гибридных, мультиоблачных архитектур?
- Требуется ли вам открытые интеграции и соединения с другими инструментами обеспечения безопасности и ИТ-инструментами.
- Можете ли вы оперативно адаптироваться и подстраиваться под изменения программы безопасности?
- Принесут ли вам пользу средства координации, автоматизации и реагирования?
- Каким образом обеспечивается интеграция анализа угроз?
- Предлагает ли ваш поставщик услуги в области безопасности в дополнение к программному обеспечению?

IBM Cloud Pak for Security: связанная безопасность для гибридного, мультиоблачного мира

IBM Cloud Pak for Security – это открытая, интегрированная платформа безопасности, предлагающая глубокий анализ угроз в различных средах – сейчас и в будущем. Вы сможете искать угрозы, координировать действия и автоматизировать ответные меры, не перемещая данные с места на место.

Благодаря открытым стандартам и инновациям IBM, IBM Cloud Pak for Security позволяет организовать поиск признаков угроз в облачных и локальных средах с помощью инструментов IBM и других поставщиков. IBM принимала участие в разработке технологии с открытым исходным кодом, которая применяется в IBM Cloud Pak for Security, и установила взаимоотношения с десятками компаний в рамках OASIS Open Cybersecurity Alliance для продвижения открытой совместимости и уменьшения привязки к отдельным поставщикам.

В состав IBM Cloud Pak for Security входит контейнеризованное программное обеспечение, предварительно интегрированное с платформой приложений корпоративного класса Red Hat OpenShift. Благодаря такой информации он может работать как в локальных средах, так и в частных и общедоступных облаках. Средства SOAR, встроенные в IBM Cloud Pak for Security, позволяют координировать и автоматизировать действия, выполняемые в ответ на угрозы безопасности.

Подробнее об IBM Cloud Pak for Security

[Посетите веб-страницу IBM Cloud Pak for Security](#) и узнайте, как вы можете выявлять скрытые угрозы и принимать обоснованные решения с учетом рисков для оптимального планирования времени своего коллектива.

Если вам нужны дополнительные специалисты и навыки, [воспользуйтесь услугами IBM Security](#) для создания надежной стратегии и преобразования вашей программы защиты.



IBM Восточная Европа/Азия
123112 Москва
Пресненская наб., 10

Веб-сайт IBM:
ibm.com

IBM, логотип IBM, ibm.com и IBM Cloud Pak – товарные знаки International Business Machines Corp., зарегистрированные во многих странах. Названия других продуктов и услуг могут быть товарными знаками IBM или других компаний. Актуальный список товарных знаков IBM можно найти на веб-странице “Copyright and trademark information” (Информация об авторских правах и товарных знаках) по адресу: ibm.com/legal/copytrade.shtml.

Red Hat и OpenShift – зарегистрированные товарные знаки Red Hat, Inc. или ее дочерних компаний в США и других странах.

Настоящий документ актуален по состоянию на момент публикации и может быть изменен IBM в любое время. Не все предложения могут быть доступны во всех странах, в которых IBM ведет свою деятельность.

Пользователь несет ответственность за оценку и проверку взаимодействия любых других продуктов и программ с продуктами и программами IBM. ИНФОРМАЦИЯ В НАСТОЯЩЕМ ДОКУМЕНТЕ ПРЕДОСТАВЛЯЕТСЯ “КАК ЕСТЬ”, БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ ЛЮБЫЕ ГАРАНТИИ ТОВАРОПРИГОДНОСТИ, СООТВЕТСТВИЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ И ЛЮБЫЕ ГАРАНТИИ ИЛИ УСЛОВИЯ НЕНАРУШЕНИЯ ПРАВ. В отношении продуктов IBM действуют гарантии на основании положений и условий соглашений, в соответствии с которыми эти продукты предоставляются.

Заявление о добросовестной политике безопасности: в процесс обеспечения безопасности ИТ-систем входит защита систем и информации путем предотвращения, обнаружения и блокирования несанкционированного доступа к ним изнутри и снаружи организации. Несанкционированный доступ может привести к подмене, уничтожению, краже или неправомерному использованию информации, повреждению систем или их использованию в корыстных целях, в том числе для осуществления атак на других пользователей. Ни одну ИТ-систему или продукт нельзя считать абсолютно безопасными, равно как ни один продукт, услуга или мера безопасности не может обеспечить абсолютную эффективность в предотвращении несанкционированного доступа или неправомерного использования. Системы, продукты и услуги IBM предназначены для работы в комплексе законных мер по обеспечению безопасности, в который для максимальной эффективности обязательно будут входить другие процедуры и, возможно, будут задействованы другие системы, продукты и услуги. IBM НЕ ГАРАНТИРУЕТ, ЧТО СИСТЕМЫ, ПРОДУКТЫ И УСЛУГИ ПОЛНОСТЬЮ ЗАЩИЩЕНЫ ОТ ЗЛОНАМЕРНЫХ ИЛИ ПРОТИВОЗАКОННЫХ ДЕЙСТВИЙ ЛЮБОЙ ИЗ СТОРОН ИЛИ ЗАЩИТЯТ ВАШЕ ПРЕДПРИЯТИЕ ОТ ПОДОБНЫХ ЗЛОНАМЕРНЫХ ИЛИ ПРОТИВОЗАКОННЫХ ДЕЙСТВИЙ.

© Copyright IBM Corporation 2020