

IBM Security Verify

В настоящем Описании Услуги описывается Облачная Услуга. В соответствующих документах заказа указываются цены и дополнительные сведения о заказе Клиента.

1. Облачная Услуга

Услуга IBM Cloud Identity предлагает возможности единого входа в систему (SSO), многофакторной аутентификации и управления жизненным циклом идентификационных данных для внутренних (сотрудники) и внешних пользователей.

1.1 Предложения

Клиент может выбрать из следующих доступных предложений.

1.1.1 IBM Security Verify

IBM Security Verify помогает Клиентам обеспечить высокую производительность пользователей за счёт единого входа в систему (SSO) с использованием облачных инструментов, многофакторной аутентификации, управления жизненным циклом, адаптивной аутентификации, анализа идентификационных данных и управления идентификацией, предоставляемых в рамках одного продукта. Данная Облачная Услуга также поддерживает тысячи готовых коннекторов, помогающих получить доступ к популярным приложениям облачной услуги, и готовые шаблоны для интеграции приложений собственной разработки.

- **Единый вход в систему**

В рамках данной Облачной Услуги предоставляются возможности единого входа в систему (SSO) и Open ID Connect (OIDC), Аутентификации как Услуги для авторизации в облачных API, панель запуска приложений, отчётность для администратора и информационная панель аналитики. Данная Облачная Услуга позволяет пользователям подключаться к приложениям с использованием современных стандартных протоколов аутентификации и федерации и включает сотни коннекторов для популярных приложений. Эта Облачная Услуга тесно интегрирована с установленной локально программой IBM Security Verify Access, включённой в состав Услуги как поддерживающее ПО, с целью предоставления Клиентам решения для удовлетворения производственных потребностей в управлении правами доступа для локальных и облачных приложений.

- **Многофакторная аутентификация**

Эта Облачная Услуга предоставляет возможности многофакторной аутентификации для приложений, защита которых обеспечивается с помощью Cloud Identity Connect или путём прямого вызова API, а также для других точек защиты, включая клиенты RADIUS, серверы Unix/Linux PAM и серверы Windows, для проверки их идентификационных данных при доступе к цифровой услуге. Поддерживаются такие механизмы, как доставка разовых паролей по электронной почте и в СМС-сообщениях и генерация разовых паролей на основе времени (программный токен), а также биометрическая аутентификация на мобильных устройствах с использованием push-уведомлений на основе IBM Verify. Эта Облачная Услуга интегрирована с установленной локально программой IBM Security Verify Access с целью предоставления Клиентам решения для удовлетворения производственных потребностей в управлении правами доступа для локальных и облачных приложений.

- **Адаптивный доступ**

Эта Облачная Услуга использует комбинацию аналитики угроз и искусственного интеллекта (ИИ), помогая организациям с высокой точностью отличать вредоносных пользователей от обычных пользователей при обращении пользователя к приложению, находящемуся под защитой услуги. Услуга принимает аналитическую информацию, которая охватывает пользователей, их устройства и модели поведения и позволяет в режиме реального времени определять действия, необходимые для устранения рисков: разрешить доступ, запросить идентификацию или заблокировать доступ. Услуга использует сотни точек данных и контекстную информацию, собранную в устройстве конечного пользователя, для идентификации устройства и вычисления комплексного уровня риска сеанса. Правила

доступа на основе рисков, заданные в политике управления доступом, используют уровень риска сеанса в сочетании с дополнительными параметрами для определения действия системы. Данная услуга тесно связана с отчётами для администраторов Security Verify, редактором правил политик управления доступом и услугой многофакторной аутентификации.

- Управление жизненным циклом

Эта Облачная Услуга тесно интегрирована с установленными локально программами IBM Security Identity Governance and Intelligence (IGI) и IBM Security Identity Manager (ISIM), включёнными в состав Услуги как поддерживающее ПО, с целью предоставления Клиентам решения для удовлетворения производственных потребностей в управлении идентификационными данными для локальных и облачных приложений. Данная Облачная Услуга предоставляет организациям расширенные средства управления жизненным циклом идентификационных данных в облачной среде, что включает в себя синхронизацию учётных записей, последовательность обработки запросов на получение доступа к приложениям, сертификацию доступа, предоставление ресурсов облачным и локальным приложениям. Клиенты могут включить IBM Security Verify Account Synchronization в качестве дополнительной услуги.

- Аналитика

Данная Облачная Услуга дополняет существующие решения IBM, в частности IBM Security Identity Governance and Intelligence (IGI) и IBM Security Identity Manager (ISIM), для предоставления комплексного профиля рисков для управляемых пользователей. Данная Облачная Услуга включает локальный, многоцелевой аналитический модуль, обеспечивающий обработку данных об активности и разрешениях из различных источников, что позволяет получить полное представление о рисках, связанных с доступом, с возможностью выполнения действий, исходя из результатов анализа рисков.

1.1.2 IBM Cloud Identity Connect

В рамках данной Облачной Услуги предоставляются возможности единого входа в систему (SSO) и Open ID Connect (OIDC), Аутентификации как Услуги для авторизации в облачных API, панель запуска приложений, отчётность для администратора и информационная панель аналитики. Данная Облачная Услуга позволяет пользователям подключаться к приложениям с использованием современных стандартных протоколов аутентификации и федерации и включает сотни коннекторов для популярных приложений. Эта Облачная Услуга тесно интегрирована с установленной локально программой IBM Security Access Management (ISAM), включённой в состав Услуги как поддерживающее ПО, с целью предоставления Клиентам решения для удовлетворения производственных потребностей в управлении правами доступа для локальных и облачных приложений.

1.1.3 IBM Cloud Identity Connect for ISAM

Эта Облачная Услуга тесно интегрирована с установленной локально программой IBM Security Access Management (ISAM) с целью предоставления Клиентам решения для удовлетворения производственных потребностей в управлении правами доступа для локальных и облачных приложений. Эта Облачная Услуга требует наличия у Клиента действующего разрешения на Подписку и Поддержку (S&S) для программы IBM Security Access Management (ISAM), и S&S должна оставаться в активном состоянии в течение всего периода подписки Клиента на Облачную Услугу. Разрешения Клиента для данной Облачной Услуги должны быть эквиваленты лицензионным разрешениям Клиента для локальной программы ISAM. Прекращение действия Подписки и Поддержки Клиента приведёт к прекращению действия данной Облачной Услуги. Доступ к поддерживаемому ПО, определённому в Разделе 5.2, не включён в состав Облачной Услуги.

1.1.4 IBM Cloud Identity Essentials

Эта Облачная Услуга предоставляет Клиентам функции Единого входа в систему (SSO) для различных облачных приложений IBM и общедоступных облачных приложений, используемых Клиентом. Эту Облачную Услугу можно сочетать с IBM MaaS360 для применения дополнительных уровней контроля безопасности, в частности условного доступа.

1.1.5 IBM Cloud Identity Verify

Эта Облачная Услуга предоставляет возможности многофакторной аутентификации для приложений, защита которых обеспечивается с помощью Cloud Identity Connect или путём прямого вызова API, а также для других точек защиты, включая клиенты RADIUS, серверы Unix/Linux PAM и серверы Windows, для проверки их идентификационных данных при доступе к цифровой услуге. Поддерживаются такие механизмы, как доставка разовых паролей по электронной почте и в СМС-сообщениях и генерация разовых паролей на основе времени (программный токен), а также биометрическая аутентификация на мобильных устройствах с использованием push-уведомлений на основе IBM Verify. Эта Облачная Услуга интегрирована с установленной локально программой IBM Security Access Management (ISAM) с целью предоставления Клиентам решения для удовлетворения производственных потребностей в управлении правами доступа для локальных и облачных приложений. Она доступна отдельно или в качестве дополнения к услугам Cloud Identity Connect, Cloud Identity Connect for ISAM и Cloud Identity Essentials.

1.1.6 IBM Cloud Identity Govern

Эта Облачная Услуга тесно интегрирована с установленными локально программами IBM Security Identity Governance and Intelligence (IGI) и IBM Security Identity Manager (ISIM), включёнными в состав Услуги как поддерживающее ПО, с целью предоставления Клиентам решения для удовлетворения производственных потребностей в управлении правами доступа для локальных и облачных приложений. Данная Облачная Услуга предоставляет организациям расширенные средства управления жизненным циклом идентификационных данных в облачной среде, что включает в себя последовательность обработки запросов на получение доступа к приложениям.

1.1.7 IBM Cloud Identity Connect and Verify

Эта Облачная Услуга предоставляет Клиенту функции IBM Cloud Identity Connect и IBM Cloud Identity Verify в рамках единого предложения.

1.1.8 IBM Cloud Identity Analyze

Данная Облачная Услуга дополняет существующие решения IBM, в частности IBM Security Identity Governance and Intelligence (IGI) и IBM Security Identity Manager (ISIM), для предоставления комплексного профиля рисков для управляемых пользователей. Данная Облачная Услуга включает локальный, многоцелевой аналитический модуль, обеспечивающий обработку данных об активности и разрешениях из различных источников, что позволяет получить полное представление о рисках, связанных с доступом, с возможностью выполнения действий, исходя из результатов анализа рисков.

1.1.9 IBM Cloud Identity Adaptive Access

Настоящая Облачная Услуга использует контекстную аналитическую информацию на основе искусственного интеллекта, охватывающую пользователей, их устройства и модели поведения, с помощью которой организации могут реализовать правильные политики аутентификации.

1.1.10 IBM Cloud Identity Connect Verify and Govern

Эта Облачная Услуга предоставляет Клиенту функции IBM Cloud Identity Connect, IBM Cloud Identity Verify и IBM Cloud Identity Govern в рамках единого предложения.

1.2 Дополнительные Услуги

1.2.1 IBM Security Verify Non-Production

IBM Security Verify Non-Production Environment on Cloud - это отдельный экземпляр платформы IBM Security Verify, который Клиент может использовать только для внутренней непроизводственной деятельности, включая, в частности, тестирование, настройку производительности, диагностику сбоев, внутреннее эталонное тестирование, предпроизводственный контроль качества и (или) разработку дополнений или расширений для Облачной Услуги, предназначенных для внутреннего использования, с помощью опубликованных API. Для данной Облачной Услуги предусмотрена возможность добавления соглашения об уровне обслуживания в отношении доступности услуг (SLA) в соответствии с Разделом 3 "Уровни обслуживания и Техническая поддержка". Данная Облачная Услуга предусматривает обработку 100 Событий в секунду.

1.2.2 IBM Security Verify Vanity Domain

Запоминающийся домен (один домен) позволяет Клиенту использовать домен, который принадлежит организации Клиента и является для неё более релевантным по сравнению с готовым доменом арендатора, предоставляемым платформой по умолчанию. Для этого домена IBM будет поддерживать SSL-сертификат и обеспечивать его ежегодное продление.

1.2.3 IBM Security Verify Application Gateway Hosted

Шлюз приложений предоставляет управляемое и размещаемое IBM облегчённое устройство для Клиентов, которым требуется поддержка нестандартных или устаревших механизмов аутентификации. К таким механизмам относится аутентификация на основе заголовков LTPA и HTTP. Текущий мониторинг и обслуживание находятся под управлением IBM.

1.2.4 IBM Security Verify SMS and Email One-time Password

Услуга предлагает доставку одноразовых паролей в сообщениях электронной почты и сообщениях СМС в качестве второго этапа аутентификации.

1.2.5 IBM Security Verify Account Synchronization

Синхронизация учётных записей представляет собой процесс, в ходе которого учётные записи извлекаются из целевых приложений, настроенных для предоставления ресурсов, и передаются в Security Verify. Этот процесс предусматривает проверку сведений о существующих учётных записях, а также применение стратегий адаптации и исправления с целью согласования системы с целевым приложением.

1.2.6 IBM Cloud Identity Non-Production

IBM Cloud Identity Non-Production Environment on Cloud - это отдельный экземпляр платформы IBM Cloud Identity, который Клиент может использовать только для внутренней непроизводственной деятельности, включая, в частности, тестирование, настройку производительности, диагностику сбоев, внутреннее эталонное тестирование, предпроизводственный контроль качества и (или) разработку дополнений или расширений для Облачной Услуги, предназначенных для внутреннего использования, с помощью опубликованных API. Для данной Облачной Услуги предусмотрена возможность добавления соглашения об уровне обслуживания в отношении доступности услуг (SLA) в соответствии с Разделом 3 "Уровни обслуживания и Техническая поддержка". Данная Облачная Услуга предусматривает обработку 100 Событий в секунду.

1.2.7 IBM Cloud Identity Vanity Domain

Запоминающийся домен (один домен) позволяет Клиенту использовать домен, который принадлежит организации Клиента и является для неё более релевантным по сравнению с готовым доменом арендатора, предоставляемым платформой по умолчанию. Для этого домена IBM будет поддерживать SSL-сертификат и обеспечивать его ежегодное продление.

1.2.8 IBM Cloud Identity Application Gateway Hosted

Шлюз приложений предоставляет управляемое и размещаемое IBM облегчённое устройство для Клиентов, которым требуется поддержка нестандартных или устаревших механизмов аутентификации. К таким механизмам относится аутентификация на основе заголовков LTPA и HTTP. Текущий мониторинг и обслуживание находятся под управлением IBM.

1.3 Услуги по ускорению внедрения (Acceleration Services)

1.3.1 IBM Security Verify Solution Planning

Данная услуга предоставляет профессиональные услуги продолжительностью одна (1) неделя, в течение которой IBM выполнит некоторые или все следующие задачи:

- Настройка единого входа для облачных приложений SaaS
- Настройка панели запуска для быстрого поиска приложений
- Подключение приложений с помощью готовых коннекторов
- Планирование решения, разработка архитектуры и рекомендаций
- Рекомендуемый IBM подход и методики

1.3.2 IBM Security Verify Workshop for Multi-Factor Authentication

Данная услуга включает в себя семинар под руководством специалистов IBM продолжительностью три (3) дня, нацеленный на решение проблем, связанных с многофакторной аутентификацией и защитой приложений Клиента с помощью IBM Cloud Identify Verify. Семинар охватывает некоторые или все следующие задачи:

- Встраивание привычного метода аутентификации во все цифровые и персональные взаимодействия, требующие идентификации
- Применение надёжного метода аутентификации в приложении с использованием понятного интерфейса REST API
- Предоставление рекомендаций по передовым отраслевым методам защиты идентификационных данных
- Оптимизация пользовательского интерфейса и поддержка любых платформ, включая телефоны, планшеты и ноутбуки

1.3.3 IBM Security Verify Strategy and Planning

Данная услуга включает в себя семинар под руководством специалистов IBM продолжительностью три (3) недели, нацеленный на практическое применение рекомендаций по защите облачных сред, с упором на безопасность инфраструктуры и приложений. Семинар охватывает некоторые или все следующие задачи:

- Настройка единого входа для облачных приложений SaaS
- Настройка панели запуска для быстрого поиска приложений
- Подключение приложений с помощью готовых коннекторов
- Планирование решения, разработка архитектуры и рекомендаций
- Анализ актуальных тенденций в сфере кибербезопасности
- Рекомендуемый IBM подход и методики

1.3.4 IBM Security Verify Expert On Demand

Данная услуга включает в себя двадцать (20) часов профессиональных услуг в формате семинаров продолжительностью два (2) часа, которые должны быть проведены в течение тридцати (30) дней с даты начала. Эти услуги позволят обсудить проблемы с архитектором IBM Security Verify и получить рекомендации, в частности по следующим вопросам:

- Технические навыки для расширения реализации решения в организации Клиента
- Вопросы по архитектуре и реализации решения в организации Клиента
- Рекомендации по стратегии и/или решению в организации Клиента

1.3.5 IBM Cloud Identity Connect Solution Planning

Данная услуга предоставляет профессиональные услуги продолжительностью одна (1) неделя, в течение которой IBM выполнит некоторые или все следующие задачи:

- Настройка единого входа для облачных приложений SaaS
- Настройка панели запуска для быстрого поиска приложений
- Подключение приложений с помощью готовых коннекторов
- Планирование решения, разработка архитектуры и рекомендаций
- Рекомендуемый IBM подход и методики

1.3.6 IBM Cloud Identity Verify Workshop for Multi-Factor Authentication

Данная услуга включает в себя семинар под руководством специалистов IBM продолжительностью три (3) дня, нацеленный на решение проблем, связанных с многофакторной аутентификацией и защитой приложений Клиента с помощью IBM Cloud Identify Verify. Семинар охватывает некоторые или все следующие задачи:

- Встраивание привычного метода аутентификации во все цифровые и персональные взаимодействия, требующие идентификации

- Применение надёжного метода аутентификации в приложении с использованием понятного интерфейса REST API
- Предоставление рекомендаций по передовым отраслевым методам защиты идентификационных данных
- Оптимизация пользовательского интерфейса и поддержка любых платформ, включая телефоны, планшеты и ноутбуки

1.3.7 IBM Cloud Security Strategy and Planning

Данная услуга включает в себя семинар под руководством специалистов IBM продолжительностью три (3) недели, нацеленный на практическое применение рекомендаций по защите облачных сред, с упором на безопасность инфраструктуры и приложений. Семинар охватывает некоторые или все следующие задачи:

- Настройка единого входа для облачных приложений SaaS
- Настройка панели запуска для быстрого поиска приложений
- Подключение приложений с помощью готовых коннекторов
- Планирование решения, разработка архитектуры и рекомендаций
- Анализ актуальных тенденций в сфере кибербезопасности
- Рекомендуемый IBM подход и методики

1.3.8 IBM Cloud Identity Expert On Demand

Данная услуга включает в себя двадцать (20) часов профессиональных услуг в формате семинаров продолжительностью два (2) часа, которые должны быть проведены в течение тридцати (30) дней с даты начала. Эти услуги позволят обсудить проблемы с архитектором Cloud Identity и получить рекомендации, в частности по следующим вопросам:

- Технические навыки для расширения реализации решения Cloud Identity в организации Клиента
- Вопросы по архитектуре и реализации решения Cloud Identity в организации Клиента
- Рекомендации по стратегии и/или решению Cloud Identity в организации Клиента

2. Обработка и защита Данных – Спецификации

Дополнение IBM об Обработке Данных (DPA), приведённое на веб-странице <http://ibm.com/dpa>, и Спецификации обработки и защиты данных (именуемые спецификациями или Приложениями к DPA), ссылки на которые приводятся ниже, содержат дополнительную информацию о защите данных в Облачных Услугах и её вариантах в зависимости от типа Содержимого, подлежащего обработке, применяемых операциях обработки, функциях защиты данных и особенностях сохранения и возврата Содержимого. DPA применяется к персональным данным, входящим в Содержимое, в том случае, если, и в той мере, в какой применяются i) Общеввропейский регламент о защите персональных данных (GDPR) (EU/2016/679); или ii) другие законы о защите данных, указанные на веб-странице <http://ibm.com/dpa/dpl>.

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=735E5650E26711E69CCD7F0385C6524D>

3. Уровни обслуживания и Техническая поддержка

3.1 Соглашение об уровне обслуживания

IBM предоставляет Клиенту следующее соглашение об уровне обслуживания в отношении доступности услуг (SLA). IBM будет применять наивысший применимый размер компенсации на основе совокупных показателей доступности Облачной Услуги в соответствии с нижеприведённой таблицей. Показатель доступности в процентах вычисляется как общее число минут за договорной месяц минус общее число минут Простоя Услуги за договорной месяц, делённое на общее число минут в договорном месяце; этот показатель относится к затронутому региону и учитывает количество пользователей-подписчиков в данном регионе. Определение Простоя Услуги, процесс подачи претензий и способы информирования IBM о проблемах с доступностью услуги приводятся

в обзоре IBM о поддержке SaaS, который можно найти на веб-странице по адресу: https://www.ibm.com/software/support/saas_support_overview.html.

Доступность	Кредит (% месячной платы за подписку*)
Менее 99,9%	10%

* Плата за подписку - это договорная цена за месяц, являющийся предметом претензии.

3.1.1 Другая информация, касающаяся данного SLA

В течение первых шестидесяти (60) дней периода использования Клиентом ("Начальный Период") Клиент не имеет права на получение кредитов за невозможность обеспечения минимального Процента Безотказной работы среды Облачной Услуги в 99,9% в соответствии с настоящим Соглашением. Если до начала или в течение Начального Периода IBM выявит имеющиеся у Клиента конфигурации, политики, данные или код ("Имеющиеся Компоненты"), которые планируется перенести в Облачную Услугу и которые могут препятствовать успешному достижению Процента Безотказной работы Облачной Услуги по настоящему Соглашению, IBM сохраняет за собой право уведомить Клиента о таких Имеющихся Компонентах и исключить их по собственному усмотрению из положений SLA. Если IBM уведомляет Клиента о каких-либо исключаемых Имеющихся Компонентах, IBM несёт ответственность за предоставление Клиенту плана устранения проблем, который в максимально возможной степени позволяет обеспечить Процент Безотказной работы по настоящему Соглашению для таких исключаемых компонентов. Клиент несёт единоличную ответственность за расходы по такому устранению проблем, если иное не согласовано обеими сторонами.

3.2 Техническая поддержка

Информацию о Технической поддержке для Облачной Услуги, включая контактные данные службы поддержки, уровни серьёзности, часы работы, время ответа и другие сведения о поддержке и применимых процессах, можно найти, выбрав раздел "Облачная Услуга" в руководстве IBM по поддержке, доступном на веб-странице по адресу <https://www.ibm.com/support/home/pages/support-guide/>.

4. Платежи

4.1 Системы расчёта оплаты

Системы расчёта оплаты для Облачной Услуги указываются в Документе по Транзакции.

К данной Облачной Услуге применяются следующие системы расчёта оплаты:

- Экземпляр – это каждый доступ к определённой конфигурации Облачных Услуг.
- Поручение – это профессиональные услуги или услуги по обучению, связанные с Облачными Услугами.
- Событие - это конкретное произошедшее событие, обрабатываемое или связанное с использованием Облачных Услуг.
 - Для Security Verify SMS and One-Time Password Событием считается одно сообщение электронной почты или сообщение СМС, в котором доставляется одноразовый пароль.
 - Для Cloud Identity Connect Событием считается один HTTP-запрос в рамках Облачной Услуги.
- Для Cloud Identity Verify Событием считается вызов многофакторного метода с помощью Облачной Услуги. Авторизованный Пользователь — это отдельный пользователь, которому разрешается осуществлять доступ к Облачным Услугам любым прямым или опосредованным способом (например, через программу-мультиплексор, устройство или сервер приложений) с помощью любых средств.
- Сотрудник – это отдельное лицо, которое работает на Предприятии Клиента либо иным способом получает оплату или действует от имени Предприятия Клиента, независимо от того, предоставляется ли ему доступ к Облачным Услугам.

- Соответствующий критериям Участник - это физическое или юридическое лицо, имеющее право участвовать в любой программе предоставления услуг, которой управляют или которую отслеживают Облачные Услуги.
- Единица Ресурса — это независимая единица измерения ресурса, управляемого, обрабатываемого Облачной Услугой или связанного с её использованием.

Для использования каждой из указанных возможностей необходимо указанное количество Единиц Ресурсов для подписки на данную Облачную Услугу:

Уровень (Graduated Tier)	Максимальное число активных пользователей в месяц	Функциональная возможность во взвешенных Единицах Ресурсов на Пользователя				
		Единый вход в систему	Многофакторная аутентификация	Адаптивный доступ	Управление жизненным циклом	Аналитика
1	500	0,1000	0,1000	0,1000	0,2900	0,1200
2	5000	0,0800	0,0800	0,0800	0,0750	0,1000
3	10 000	0,0600	0,0600	0,0600	0,0500	0,0750
4	100 000	0,0080	0,0080	0,0080	0,0050	0,0200
5	500 000	0,0025	0,0025	0,0025	0,0020	0,0150
6	1 000 000	0,0020	0,0020	0,0020	0,0010	0,0010
7	5 000 000	0,0015	0,0015	0,0015	0,0005	0,0005
8	10 000000	0,0015	0,0015	0,0015	0,0002	0,0002
9	50 000 000	0,0010	0,0010	0,0010	0,0001	0,0001
10	999 999 999	0,0005	0,0005	0,0005	0,0001	0,0001

Примечание: Все результаты вычислений будут округляться до следующего целого числа.

5. Дополнительные положения

К Соглашениям об Облачных Услугах (или эквивалентным базовым соглашениям об облачных инфраструктурах), заключённым до 1 января 2019 года, применяются положения, приведённые на веб-странице <https://www.ibm.com/acs>.

5.1 Ссылки на Клиента

Клиент даёт согласие на то, чтобы IBM открыто упоминала Клиента в качестве подписчика Облачных Услуг в рекламных или маркетинговых материалах.

5.2 Поддерживающее программное обеспечение

В Облачную Услугу входит следующее Поддерживающее Программное обеспечение:

- IBM Security Verify Bridge
- IBM Security Verify
- IBM Security Verify SDK (iOS)
- IBM Security Verify SDK (Android)
- IBM Security Verify SDK for JavaScript
- IBM Security Verify Bridge for Directory Sync
- IBM Application Gateway
- IBM Security Verify Hosted Application Gateway
- IBM Security Verify Gateway for Windows Login
- IBM Security Verify Gateway for PAM (на AIX)
- IBM Security Verify Gateway for PAM

- IBM Security Verify Gateway for RADIUS
- IBM Security Verify Credentials

Следующее поддерживающее программное обеспечение может использоваться только с Облачными Услугами IBM Cloud Identity Connect, IBM Cloud Identity Connect and Verify и IBM Cloud Identity Connect Verify and Govern:

- IBM Security Access Manager Virtual Enterprise Edition

Следующее поддерживающее программное обеспечение может использоваться только с Облачными Услугами IBM Security Verify, IBM Cloud Identity Govern и IBM Cloud Identity Connect Verify and Govern:

- IBM Security Identity Governance and Intelligence Enterprise Edition
- IBM Security Identity Manager