Безопасность в Smartsheet

Подробный обзор функций и средств обеспечения безопасности Smartsheet

Введение

SaaS-платформы корпоративного уровня, такие как Smartsheet, должны иметь несколько уровней защиты и множество средств, обеспечивающих контроль над конфиденциальными данными компании и их безопасность. Кроме того, важно, чтобы эти решения были гибкими и интегрировались с существующими системами и процессами обеспечения безопасности.

Цель этого документа — описать функции и методы управления и обеспечения безопасности, а также средства защиты, предлагаемые Smartsheet. Основное внимание будет уделено возможностям, которыми могут воспользоваться наши клиенты. Smartsheet рекомендует использовать эти функции для создания безопасной и хорошо управляемой рабочей среды, соответствующей нормативным требованиям. Обратите внимание: в данный технический документ не включены функции обеспечения безопасности, которые ещё не являются общедоступными.

Обзор

Чтобы обеспечить максимальную безопасность вашей организации, мы рекомендуем внедрить средства контроля в трёх основных областях: управление идентификацией и доступом пользователей, управление данными и глобальная конфигурация учётной записи. Помимо их описания, данный документ содержит общую информацию о методах обеспечения безопасности, защиты конфиденциальности и соблюдения нормативных требований компанией Smartsheet.

- **Управление идентификацией и доступом** — это технологии, контролирующие то, как пользователи получают доступ к Smartsheet. При этом обеспечивается соответствие роли и идентификационных данных каждого пользователя вашей организационной структуре и существующим политикам. Кроме того, мы расскажем, как обеспечить безопасность при сотрудничестве с внешними пользователями с учётом ваших потребностей.

- **Управление данными** должно обеспечиваться как на уровне пользователей, так и на уровне организации в целом. В Smartsheet пользователи по умолчанию получают только необходимый минимум полномочий. При этом вы можете использовать дополнительные элементы управления для дальнейшего ограничения доступа к данным и контроля их видимости, чтобы пользователи имели доступ только к тому, что им нужно, и тогда, когда им это нужно. Что касается организационного уровня, мы рассмотрим как простые механизмы, такие как безопасный совместный доступ и отчёты по пользователям, так и дополнительные возможности, такие как политики вывода данных.

- **Глобальная конфигурация учётной записи** позволяет настроить внешний вид Smartsheet в соответствии с фирменным стилем организации. Обеспечению безопасности способствуют даже такие сравнительно простые вещи, как обозначения, указывающие, что пользователи находятся в защищённой среде организации. Вы можете обеспечить единообразие, установив параметры фирменного стиля и индивидуальные настройки, чтобы им соответствовал каждый созданный ресурс.

- **Практики в области обеспечения безопасности, конфиденциальности и соблюдения нормативных требований** — это методы и инструменты, которые компания Smartsheet применяет за пределами своей платформы, чтобы поддерживать высокий уровень защиты клиентских данных. Грамотное распоряжение кадровыми ресурсами, технологиями и процессами позволяет Smartsheet внедрять лучшие в отрасли стратегии, обеспечивающие конфиденциальность, целостность и доступность сред и активов.

Оглавление

Управление идентификацией

Управление идентификацией пользователя в Smartsheet и, таким образом, его доступом к системе так же важно, как и управление данными в пределах платформы.

На раннем этапе внедрения Smartsheet вы сможете решить, какой метод аутентификации использовать. Smartsheet предлагает различные варианты: адрес электронной почты и пароль, а также службы единого входа (SSO) Google, Microsoft, поставщиков SAML 2.0 и Apple.

Вы можете выбрать один или несколько методов для своей организации, однако мы рекомендуем использовать для всех пользователей единый метод аутентификации SSO, а другие методы отключить. Мы также рекомендуем добавить ещё один уровень безопасности, активировав многофакторную аутентификацию (MFA) при настройке единого входа.

У Smartsheet есть надёжный набор REST API. API Smartsheet использует OAuth 2.0 для аутентификации и авторизации. Для аутентификации каждого запроса требуется HTTP-заголовок, содержащий маркер доступа. В целях дополнительной безопасности рекомендуется использовать протокол OAuth 2.0 для любых интеграций.

Управление доступом

Управление пользователями и их доступом — это ключевая функция администрирования, которая может повлиять как на безопасность вашей организации, так и на успех внедрения Smartsheet. Необходимо найти баланс: с одной стороны, поддерживать эффективность совместной работы, а с другой стороны, предотвращать возникновение рисков, связанных с тем, что данные всё чаще хранятся распределённым образом, а сотрудники находятся в разных местах. Учитывая это, Smartsheet предлагает три различные модели управления, соответствующие основным способам работы с приложением, которые используют наши клиенты.

Модели управления Smartsheet

Первый подход — это наша децентрализованная (федеративная) модель, в рамках которой отдельные бизнес-подразделения напрямую контролируют оплату подписки и планы. При этом ИТ-отдел обычно не участвует в администрировании, и каждое подразделение самостоятельно производит оплату счетов, а также управляет данными и параметрами пользователей. Эта модель обычно применяется в компаниях, которые уже начали пользоваться Smartsheet.

Второй подход — это централизованная (консолидированная) модель, в рамках которой все планы Smartsheet объединены в одну подписку, управляемую ИТ-отделом. Это обеспечивает прямой контроль над расходами, управлением пользователями и инструментами безопасности. Эта модель лучше всего подходит для ИТ-команд, которые хотят тщательно контролировать каждый аспект работы со Smartsheet.

Наконец, гибридная модель — это компромиссный подход, при котором ИТ-отдел контролирует настройки организации в целом с помощью диспетчера планов "Корпоративный", а управление лицензиями и пользователями осуществляется непосредственно системными администраторами бизнес-подразделений. Выставление счетов может производиться для каждого плана в отдельности (каждое подразделение получает счета самостоятельно), т. е. по модели, в рамках которой расходы на Smartsheet включаются в бюджеты подразделений, а не выставляются централизованно ИТ-отделу.

Чтобы обеспечить высокий уровень безопасности, Smartsheet рекомендует использовать гибридную или централизованную модель. Они позволяют ИТ-отделу непосредственно управлять параметрами планов.

Администрирование пользователей

Если различные отделы и группы сотрудников вашей компании используют Smartsheet независимо друг от друга, можно создать несколько отдельных планов. Ситуация, в которой используется несколько планов одновременно, также может возникнуть в результате слияний и поглощений.

Чтобы управлять параметрами пользователей в этих планах, используя децентрализованную модель, мы рекомендуем включить обнаружение учётных записей для каждого из планов. Благодаря этому новые пользователи, приступающие к работе со Smartsheet, или другие пользователи из домена вашей организации могут просматривать список планов Smartsheet, имеющихся у вашей компании, и централизованно подавать запросы на присоединение к одному из этих планов вместо того, чтобы создавать новый. Такие запросы автоматически перенаправляются вашим системным администраторам (через Центр администрирования Smartsheet) на рассмотрение и утверждение.

Если у вас есть несколько отдельных планов и вы хотите управлять параметрами пользователей с помощью централизованной модели, возможно, вам придётся выполнить консолидацию учётных записей. Примечание. В ходе консолидации клиентам, использующим возможности Advance, такие как Dynamic View, соединители и Control Center, потребуется обратиться в службу поддержки Smartsheet.

Если вы используете гибридную модель и диспетчер планов "Корпоративный", рекомендуется создавать планы для отдельных подразделений, команд или центров затрат. Это позволит вам определить политику автоматического назначения пользователей соответствующим планам на основе их принадлежности к одному из этих объектов.

Управление пользователями

Мы понимаем, что добавление пользователей по одному становится неэффективным, если их количество исчисляется десятками, сотнями или тысячами. Поэтому при внедрении Smartsheet рекомендуется использовать функцию массового импорта пользователей в Центре администрирования. Она позволяет добавлять до 1000 пользователей одновременно. Вы также можете использовать пакетное обновление, чтобы изменять роли существующих пользователей.

Слияния и поглощения часто приводят к ребрендингу, в процессе которого пользователи получают новые адреса электронной почты. Объединение пользователей позволяет производить пакетное обновление основных адресов электронной почты и удалять дубликаты учётных записей.

В консолидированном плане Smartsheet можно использовать две дополнительные возможности для дальнейшей оптимизации и автоматизации управления пользователями.

- Автоматическая подготовка пользователей (UAP) автоматизирует процесс добавления пользователей в корпоративную учётную запись. Когда пользователи регистрируются или входят в Smartsheet, используя корпоративный адрес электронной почты, они автоматически добавляются в вашу учётную запись. Кроме того, вы можете выбрать, следует ли предоставлять пользователям лицензии или они будут автоматически присоединяться к учётной записи в качестве нелицензированных (бесплатных) соавторов.

    - Если вы выбрали нашу консолидированную модель, мы рекомендуем включить автоматическую подготовку пользователей, чтобы сотрудники автоматически присоединялись к центральной учётной записи, контролируемой ИТ-отделом.

    - Если вы используете гибридную модель (и если в организации задокументировано, к какому отделу или центру затрат относятся те или иные пользователи), мы рекомендуем включить UAP. Вы сможете импортировать сведения о пользователях и соответствующих отделах, чтобы при запросе лицензии они автоматически добавлялись к нужному плану. UAP также можно использовать для автоматического перемещения нелицензированных пользователей между планами.

- Интеграция со службой каталогов позволяет напрямую синхронизировать пользователей Microsoft Azure Active Directory (AD) со Smartsheet. Подключите Smartsheet к существующей системе автоматизации в Azure AD, чтобы полностью автоматизировать регистрацию пользователей в системе и выход из неё, сводя к минимуму риск того, что пользователи продолжат использовать учётные записи Smartsheet, даже покинув вашу организацию. Дополнительным преимуществом будет то, что атрибуты AD на уровне пользователя, такие как отдел/центр затрат/подразделение, включаются в отчёт Smartsheet о возвратных платежах, который доступен в Центре администрирования и может использоваться для упрощения внутреннего возврата платежей. Рекомендуется синхронизировать всех пользователей каталога с учётной записью Smartsheet вашей организации. Благодаря этому пользователи не смогут создавать дополнительные, "теневые" учётные записи Smartsheet при первом входе в систему. В качестве второго уровня защиты вы также можете оставить автоматическую подготовку пользователей включённой для всех пользователей, которые, возможно, ещё не были синхронизированы с использованием службы каталогов.

Когда кто-то покидает компанию, необходимо отозвать его доступ к Smartsheet. Это можно сделать двумя способами. При удалении пользователя он и принадлежащие ему ресурсы удаляются из учётной записи Smartsheet, но при этом могут быть затронуты ещё используемые элементы, необходимые другим сотрудникам. Вместо этого рекомендуется производить деактивацию пользователей. Это по-прежнему полностью лишает их доступа к Smartsheet, но не влияет на доступность их контента и стабильность зависящих от него объектов, а также не создаёт затруднений при назначении новых владельцев.

Роли и типы пользователей Smartsheet

Независимо от метода подготовки учётных записей пользователей вам будет необходимо определить роли Smartsheet для сотрудников организации.

Обратите внимание, что назначение роли не даёт сотруднику доступ к ресурсам Smartsheet вашей организации. Необходимо непосредственно предоставить пользователю доступ к конкретным ресурсам. Таким образом, то, какие элементы Smartsheet могут просматривать и изменять пользователи, определяется как ролями, так и настройками доступа к ресурсам. Smartsheet поддерживает следующие основные роли.

- Лицензированный пользователь. Использует функции, доступные обладателям лицензии, такие как создание таблиц.

- Администратор группы. Может создавать группы Smartsheet и управлять ими. *

  * Администраторы группы должны быть лицензированными пользователями.

- Системный администратор. Управляет параметрами пользователей, настройками учётной записи и элементами контроля безопасности.

Мы настоятельно рекомендуем добавить в учётную запись Smartsheet как минимум двух активных системных администраторов, чтобы хотя бы один системный администратор был доступен в любой момент времени.

Администраторы групп могут создавать группы Smartsheet, чтобы можно было предоставлять доступ к контенту нескольким пользователям одновременно, а не повторять эту операцию для каждого сотрудника в отдельности. Администраторы групп могут управлять только группами, которыми они владеют. При необходимости, чтобы ограничить внешнее соавторство, разрешите включать в группы только сотрудников своей организации.

Если вы не назначите пользователю ни одну из вышеперечисленных ролей, он сможет работать только с теми ресурсами Smartsheet (таблицами, отчётами, панелями мониторинга или приложениями WorkApps), к которым ему будет предоставлен доступ. Создавать ресурсы Smartsheet могут только лицензированные пользователи. Запросить лицензию можно напрямую через приложение Smartsheet. Системные администраторы могут отслеживать запросы и отвечать на них по одному или в пакетном режиме, используя раздел "Управление запросами лицензий" Центра администрирования. Если в вашей компании уже налажен процесс работы с запросами на лицензию, советуем настроить экран повышения уровня, чтобы пользователи могли отправлять запросы на лицензии через эти внутренние процессы.

Внешние соавторы

Внешним соавтором считается любой пользователь за пределами вашего домена, которому предоставляется доступ к вашим ресурсам Smartsheet. Используя Smartsheet, вы можете организовать совместную работу с любыми внешними партнёрами без дополнительных затрат для них. Чтобы обеспечить безопасность, мы рекомендуем использовать три элемента централизованного административного управления.

Безопасный совместный доступ позволяет указать доверенные домены или адреса электронной почты, для которых будет разрешено внешнее соавторство.

Отчёты о доступе к таблицам предоставляют список внешних соавторов, которые имеют доступ к элементам Smartsheet вашей организации.

Централизованный запрет доступа к элементам в Центре администрирования лишает внешних соавторов возможности работать с контентом, доступ к которому вы хотите отозвать.

Управление данными

Эффективное управление данными необходимо компаниям, чтобы создание, использование, защита информации и обмен ей происходили в соответствии с действующими законами, нормативами, политиками компании и передовыми отраслевыми практиками.

Эти меры контроля применяются не только для соблюдения нормативных требований, но и для обеспечения эффективной и непрерывной работы компании, а также для защиты данных.

На уровне пользователя организация должна иметь эффективные инструменты для ограничения видимости, чтобы пользователи получали доступ только к той информации, которая нужна именно им и именно сейчас.

На уровне организации предприятие должно располагать средствами для эффективного создания и внедрения политик.

Управление данными на уровне пользователя

Большинство пользователей знакомы с уровнями разрешений в Smartsheet (наблюдатель, редактор, администратор и владелец). В модулях Dynamic View и WorkApps имеются дополнительные, более гибкие средства управления, которые помогают эффективно управлять данными на уровне пользователя. Предоставление доступа только к самому необходимому контенту не только делает работу эффективнее (пользователи не отвлекаются на работу с посторонними элементами), но и повышает уровень безопасности за счёт точечного применения принципа минимальных полномочий.

Dynamic View

Не все бизнес-процессы гарантируют полную прозрачность. Многие процессы — управление заказами, сотрудничество с поставщиками, проекты с участием внешних партнёров — требуют жёсткого контроля над тем, к каким данным пользователи получают доступ.

Модуль Dynamic View позволяет наладить совместную работу без ущерба для конфиденциальности. Используя Dynamic View, владельцы таблиц могут выборочно делиться соответствующими строками и полями с конкретными соавторами, не предоставляя общий доступ к исходным таблицам. Это даёт несколько сценариев использования, в которых отдельные корпоративные пользователи могут выборочно делиться элементами с поставщиками, командами, состоящими как из внутренних, так и из внештатных сотрудников, или другими организациями, приглашая к совместной работе только с определённым подмножеством данных. Таким образом каждый пользователь будет иметь доступ к необходимой ему информации — и только к той информации, которая ему действительно нужна.

WorkApps

Модуль WorkApps позволяет оптимизировать процессы и упростить совместную работу с помощью удобных в навигации приложений, созданных на основе ваших таблиц, форм, панелей мониторинга, отчётов и других элементов. Настройки доступа к данным могут отличаться для различных ролей, однако все ваши сотрудники будут работать с одним и тем же массивом информации. Приложения WorkApps масштабируются с помощью многоуровневой системы безопасности — той же самой, которая используется в работе Smartsheet.

Они устраняют необходимость предоставлять доступ к исходным ресурсам, на основе которых создаётся приложение WorkApps. Вы можете создать приложение WorkApps с отфильтрованным представлением выбранных таблиц и отчётов, но пользователю приложения не понадобится доступ к этим таблицам и отчётам. Он сможет просматривать их в соответствии с настройками приложения WorkApps.

Средства работы с политикой управления данными на уровне организации

Smartsheet даёт администраторам возможность сделать так, чтобы возможности платформы использовались в рамках корпоративной политики управления данными. Администраторы могут ограничивать работу с данными таким образом, чтобы взаимодействие с ними проходило согласно установленным правилам, а доступ к ним получали только те пользователи, которым это разрешено.

Администраторы могут выбирать, как пользователи будут взаимодействовать с конкретными функциями. Должны ли владельцы таблиц иметь возможность публиковать таблицы и создавать новые автоматизации? Из каких источников можно прикреплять вложения? Могут ли внешние соавторы скачивать контент, к которому им был предоставлен доступ? Это примеры вопросов, на которые администраторы должны ответить, чтобы подобрать средства контроля, применимые в масштабах всей организации.

Ограничения политики также распространяются на безопасный совместный доступ. Этот инструмент подойдёт вам, если вы хотите ограничить предоставление доступа к данным и ресурсам определёнными доменами или адресами электронной почты. Как упоминалось ранее, безопасный совместный доступ также определяет, могут ли сотрудники вашей организации предоставлять доступ к элементам Smartsheet другим организациям, например поставщикам и партнёрам.

Управление виджетами веб-контента

Панели мониторинга поддерживают возможность встраивания интерактивного контента (видео, диаграмм, документов и т. д.). Администраторы имеют возможность включать или отключать эту функцию и определять утверждённый список поддерживаемых доменов для виджета веб-контента. Рекомендуем ограничить его внутренними доменами компании.

Разрешения для автоматизации

Выбирайте, кто может получать данные, содержащиеся в таблицах, с помощью автоматизации. Уровень "Строгий" предусматривает наиболее жёсткие ограничения (автоматизация работает только для пользователей, имеющих доступ к таблице), а наименее жёсткие предусматривает уровень "Нестрогий" (автоматизация применима для любых адресов электронной почты и сторонних интеграций, например Slack). Рекомендуем изучить эти настройки и проверить, соответствуют ли они потребностям вашей организации.

Элементы управления вложениями

Определите, как участники плана могут загружать файлы: со своих компьютеров, в виде ссылок на сайты (URL-адресов) или из сторонних облачных хранилищ, включая Google Диск, OneDrive, Box, Dropbox, Evernote и Egnyte. Чтобы предотвратить получение данных из неутверждённых источников, включите только тех поставщиков вложений, использование которых разрешено внутренними политиками организации.

Настройка параметров публикации

При публикации таблицы, отчёта или панели мониторинга создаётся уникальный URL-адрес. Используя его, любой пользователь, даже не имея доступа к Smartsheet, сможет просмотреть вашу публикацию. Кроме того, генерируется код iframe, с помощью которого можно встроить таблицу или отчёт на внешний веб-сайт.

Вы можете запретить публикацию таблиц, отчётов, панелей мониторинга и календарей iCal. При этом при просмотре ресурса в Smartsheet перестанет отображаться кнопка "Опубликовать". Вы также можете ограничить доступ к опубликованным элементам, чтобы их могли просматривать только пользователи из вашей организации. Согласно нашим наблюдениям клиенты, отдающие приоритет безопасности, обычно разрешают публикацию, но открывают доступ к опубликованным элементам только пользователям своей учётной записи.

Безопасный совместный доступ

Эта функция позволяет предоставлять доступ к объектам только определённым адресам электронной почты или адресам в пределах домена организации, например для того, чтобы доступ к таблицам получали только пользователи с корпоративным адресом электронной почты. Настоятельно рекомендуем использовать её, чтобы контролировать, какие из внешних соавторов могут работать с элементами вашей учётной записи (и могут ли вообще). Кроме того, чтобы упростить обновление и обслуживание списка безопасного совместного доступа, мы рекомендуем вам собирать запросы на обновление с помощью веб-формы Smartsheet.

Элементы управления отправкой офлайн-форм

Мобильное приложение Smartsheet автоматически разрешает отправку форм в автономном режиме. Это необходимо пользователям, работающим в условиях нестабильного подключения к Интернету (например, на строительной площадке). Этот элемент управления предоставляет администраторам возможность отключать (и снова включать) отправку форм в автономном режиме, чтобы контролировать, может ли пользователь запустить мобильное приложение без подключения к Интернету для отправки форм.

Управление интеграцией с мессенджерами

Smartsheet поддерживает следующие приложения для обмена сообщениями: Google Chat, Microsoft Teams, Slack и Cisco Webex. Администраторы учётной записи могут включить один или несколько сервисов по вашему усмотрению.

Журналы и отчёты

Вы можете скачивать отчёты, охватывающие различные аспекты работы со Smartsheet в вашей организации, чтобы получать актуальные сведения об использовании Smartsheet, пользователях, контенте, выставлении счётов и доступе.

Отчёт о доступе к таблице

Создаёт файл Excel с названиями всех таблиц, отчётов и панелей мониторинга, принадлежащих лицензированным пользователям учётной записи, названием рабочего пространства, в котором сохраняются эти элементы (если применимо), соавторами, имеющими доступ к каждой таблице, и указанием времени последнего изменения. Рекомендуем периодически просматривать этот отчёт, чтобы проверять список внешних соавторов, которые имеют доступ к ресурсам, принадлежащим пользователям в вашей организации.

Отчёт об опубликованных элементах

Создаёт файл Excel со списком всех опубликованных элементов. Может применяться для обеспечения безопасности данных или получения сведений о том, кто из пользователей опубликовал те или иные элементы. Используйте этот отчёт, чтобы настроить средство управления публикацией.

Отчёт "Список пользователей"

Создаёт файл Excel со списком всех членов учётной записи (как приглашённых, так и активных), временем их добавления в учётную запись, их уровнем доступа (системный администратор, администратор группы и т. д.), количеством принадлежащих им таблиц и временем их последнего входа в Smartsheet.

Отчёт об истории входов

Системные администраторы многопользовательских учётных записей могут использовать Центр администрирования для получения по электронной почте файла Excel с историей входов.

Отчёт о возвратных платежах

Клиенты, использующие интеграцию со службой каталогов, могут использовать отчёты о возвратных платежах, доступные в Центре администрирования, для упрощения внутреннего возврата платежей. Эта функция добавляет столбцы для подразделения, отдела и центра затрат в существующий отчёт, который генерируется, когда вы скачиваете список пользователей организации. Таким образом добавляются данные, необходимые для создания внутренних отчётов о возвратных платежах.

Для более детального отслеживания действий пользователей на уровне таблицы, панели мониторинга или ячейки вы можете использовать журнал действий, историю ячейки и системные столбцы.

- **Журнал действий** представляет собой журнал аудита изменений, внесённых в документ, а также информацию о том, кто их внёс и когда они были внесены. Сюда входит информация о внесённых изменениях: какие строки были удалены, что в них содержалось, кто просматривал какие элементы и как изменялись разрешения на доступ.

- **История ячейки** представляет собой журнал изменений, внесённых на уровне ячейки, с подробным описанием того, кто внёс изменения, какие они были и когда они были сделаны. Пользователи могут копировать данные из истории ячейки, чтобы восстановить данные, которые были удалены или изменены по ошибке.

- **Системные столбцы** содержат время последнего изменения каждой строки и сведения о пользователе, внёсшем это изменение.

Дополнительные средства управления данными

В Smartsheet имеется ряд дополнительных возможностей, которые помогают осуществлять управление данными клиентам с особенно строгими требованиями к уровню безопасности. Эти средства включены в пакеты Smartsheet Advance Platinum и Smartsheet Safeguard.

Ключи шифрования под управлением клиента

Smartsheet использует шифрование, чтобы защитить ваши данные и помочь вам сохранить контроль над ними. Ключи шифрования под управлением клиента (CMEK) предназначены для организаций, имеющих конфиденциальные данные или соблюдающих требования, в соответствии с которыми необходимо иметь собственный ключ шифрования. Система CMEK позволяет организациям использовать облачные приложения типа SaaS, в то же время обеспечивая уровень контроля, сравнимый с использованием локальных сервисов, и добавляет управляемый клиентом уровень шифрования к хранилищу данных Smartsheet. Таким образом клиенты могут внедрять сложные политики обеспечения безопасности и управления данными.

Примечание. Чтобы использовать CMEK, клиенты должны иметь доступ к службе управления ключами Amazon Web Services (AWS KMS), поскольку ключи клиентов настраиваются и управляются непосредственно в AWS.

Smartsheet использует CMEK для шифрования данных вашей организации, чтобы они всегда оставались под вашим контролем. В частности, Smartsheet не хранит и не контролирует такие ключи шифрования. Мы запрашиваем и получаем ключи из службы управления ключами AWS (KMS) клиента всякий раз, когда Smartsheet требуется доступ к его данным.

Поскольку ваша организация контролирует CMEK, хранящийся в системе управления ключами AWS, вы можете в любое время отозвать доступ Smartsheet к CMEK и, следовательно, к вашим данным. Уничтожив ключи доступа в системе управления ключами AWS, организация сможет удалить свои данные из систем Smartsheet. Даже имея копию базы данных Smartsheet, исходный код и ключи облачного шифрования, злоумышленники всё равно не смогут прочитать данные, зашифрованные с помощью CMEK.

Политики вывода данных

Передача данных всегда сопряжена с определённым уровнем риска, но при работе с особо важными документами необходимо, чтобы данные компании оставались только в вашей учётной записи и под вашим контролем.

Системные администраторы могут использовать политики вывода данных для защиты конфиденциальной информации посредством детального контроля над экспортом данных как внутри вашей организации, так и за её пределами.

Политики вывода данных позволяют запретить внутренним и внешним соавторам выполнять следующие действия с таблицами, отчётами и панелями мониторинга:

- сохранить как новую;
- сохранить как шаблон;
- отправить как вложение;
- опубликовать;
- распечатать;
- экспортировать.

Пользователи, которые попытаются выполнить запрещённое действие, получат уведомление о том, что оно недоступно в соответствии с политикой вывода данных, применяемой в вашей организации.

Эти ограничения позволяют предотвратить сохранение или передачу конфиденциальной информации соавторами в злонамеренных целях.

Отчёты о событиях

Чтобы обеспечить информационную безопасность, многим предприятиям требуется постоянно получать сведения о том, как именно используются бизнес-приложения, например Smartsheet. Целесообразно иметь наглядное представление о следующем:

- кто создаёт таблицы;
- кто создаёт рабочие пространства;
- кто удаляет объекты;
- кто и кому предоставляет доступ к таблицам.

Отчёты о событиях обеспечивают детальное представление о поведении и активности пользователей в учётной записи Smartsheet. Эта функция позволяет отслеживать потерю данных и выявлять отклонения от сложившихся тенденций использования платформы. Это поможет более строго обеспечивать соблюдение политик безопасности и соответствие нормативным требованиям.

Отчёты о событиях представляют собой поток данных в формате JSON о действиях, выполняемых в Smartsheet ("События") в рамках плана (организации), доступ к которому осуществляется через API. Сервис сообщает о более чем 120 типах событий в Smartsheet и хранит данные за шесть месяцев, начиная с даты включения потока.

Чтобы использовать этот инструмент наиболее эффективно, данные отчётов о событиях обычно интегрируют с другими системами безопасности, которые обеспечивают мониторинг событий и оповещение о них, создание и применение политик, а также предотвращение потери данных (DLP). Эти приложения предлагаются сторонними организациями. Обычно это брокеры безопасного доступа в облако (CASB), системы управления информацией о безопасности и событиями (SIEM) или комбинация CASB и SIEM, работающих вместе. Иногда предприятия разрабатывают собственные системы мониторинга и реагирования вместо того, чтобы полагаться на системы, предоставляемые третьими сторонами.

Основные сферы применения отчётов о событиях:

- предотвращение потери данных;
- обработка данных, позволяющих установить личность (PII);
- управление данными;
- аналитика совместной работы.

Управление сохранением данных

Чем больше информации организация хранит в SaaS-приложениях, тем большему риску она себя подвергает.

Средства управления сохранением данных Smartsheet дают организациям возможность создавать политики, определяющие, когда информация должна быть удалена, на основе необходимых критериев.

Эти политики могут основываться на дате создания таблицы или времени последнего её изменения, обеспечивая сохранение только активного или недавнего содержимого в вашем экземпляре Smartsheet и снижая уровень риска.

Глобальная конфигурация учётной записи

Безопасность учётной записи не ограничивается такими техническими функциями, как шифрование данных, классификация или аутентификация. Даже размещение логотипа вашей организации на каждом принадлежащим ей элементе уже может сыграть роль в обеспечении безопасности.

Средства управления глобальной конфигурацией учётной записи позволяют применять визуальный брендинг (а также разные ограничения), чтобы пользователи знали, что им предоставлен доступ именно к требующейся информации.

Системные администраторы могут добавлять логотипы на глобальном уровне, чтобы внедрение Smartsheet происходило в соответствии с требованиями к фирменному стилю. Используйте блокировку фирменного стиля, чтобы все новые ресурсы имели одинаковый стиль.

Средства настройки и работы с учётной записью Smartsheet также позволяют создавать настраиваемые персонализированные экраны приветствия. Вы можете создавать экраны справки с учётом ваших собственных требований с описанием того, как начать работу, экраны запроса лицензии, которые помогут пользователям связаться с вами, или настраиваемые экраны приветствия с фирменной символикой, которые появляются при входе пользователя в систему. На такой экран можно вывести требование согласиться с условиями обслуживания, прежде чем получить доступ к дальнейшей информации.

Единообразие фирменного стиля и настраиваемый стартовый экран направляют пользователя к искомой информации и предназначенным для него инструментам, что тоже способствует защите данных.

Практики Smartsheet в области обеспечения безопасности, конфиденциальности и соблюдения нормативных требований

В Smartsheet применяется комплексный подход к обеспечению кибербезопасности, конфиденциальности и защиты данных. Всё начинается с разработки стратегических политик информационной безопасности. Этим занимается Руководящий комитет по обеспечению информационной безопасности Smartsheet (ISSC) и представители руководящего состава. Политики разрабатываются так, чтобы соответствовать практикам стратегического управления рисками, способствовать упреждающему управлению рисками в области безопасности, повышать уровень безопасности за счёт зрелости процессов и эффективной системной архитектуры. Наконец, наши политики помогают пользователям принимать взвешенные решения касательно рисков в области безопасности посредством обучения и повышения осведомлённости.

Безопасность данных

Наши функции защиты и обеспечения безопасности призваны гарантировать сохранность ваших данных. Smartsheet сотрудничает с третьими сторонами для проведения аудита наших методов обеспечения безопасности, включая оценку и аттестацию SOC2 Type II, а также сторонние технические оценки безопасности при участии компаний, занимающихся тестированием на проникновение. Кроме того, программа управления уязвимостями Smartsheet автоматизирует выявление и устранение уязвимостей сетей и систем в корпоративной и производственной среде Smartsheet. Smartsheet использует шифрование, чтобы защитить ваши данные и помочь вам сохранить контроль над ними. Вы можете быть уверены в том, что в Smartsheet все данные надёжно защищены с помощью шифров, одобренных Национальным институтом стандартов и технологий (NIST), протокола TLS, стандарта шифрования неактивных данных AES 256 и сервиса Amazon S3 для хранения и обслуживания загруженных файлов.

Конфиденциальность

Компания Smartsheet ценит вашу конфиденциальность и серьёзно относится к вашему праву знать, каким образом собирается и используется информация о вас. В нашем уведомлении о конфиденциальности приведены сведения о том, как Smartsheet собирает, использует и раскрывает персональные данные и другие сведения, которые попадают к нам через наши веб-сайты, мобильные приложения и платформу Smartsheet для совместной работы.

- Мы признаем права наших потенциальных и настоящих клиентов и партнёров на конфиденциальность и соблюдаем международные правовые нормы в области конфиденциальности, включая Общий регламент ЕС по защите данных (GDPR).

- Клиенты, которым требуются особые условия для обработки контента, включающего личную информацию, могут запросить соглашение об обработке данных (DPA). Если вы определили, что вам требуется Соглашение DPA со Smartsheet, вы можете отправить форму согласия с условиями DPA на странице smartsheet.com/legal/DPA .

Операционное управление

Мы внедряем политики и процедуры, которые позволяют обеспечить сохранность и резервное копирование данных в нескольких физических местах. Наши специалисты постоянно анализируют новые угрозы в области безопасности и внедряют новые меры противодействия с целью защитить данные от несанкционированного доступа и исключить незапланированные перебои в доступности платформы. Доступ к производственным системам и данным Smartsheet имеют только авторизованные сотрудники группы технического обслуживания Smartsheet; они получают его на основе принципа минимальных полномочий и служебной необходимости. Smartsheet публикует информацию о статусе системы на странице сведений о состоянии Smartsheet. Как правило, Smartsheet уведомляет клиентов о серьёзных системных инцидентах по электронной почте и/или текстовым сообщением, если они подписались на автоматические обновления на странице сведений о состоянии Smartsheet.

Резервирование, обеспечение безопасности и непрерывной работы центров обработки данных

Smartsheet работает с признанными в отрасли хостинг-провайдерами, чтобы гарантировать клиентам бесперебойное функционирование сервисов. Мы используем резервирование данных на нескольких площадках, хостинг на объектах AWS, а наши собственные объекты проверены и сертифицированы на соответствие стандартам SOC 1, SOC 2, ISO 27001 и FISMA. Мониторинг включает протоколы биометрического сканирования, непрерывное наблюдение и круглосуточное управление производственной средой. Smartsheet использует внутренние процессы и планы, обеспечивающие непрерывность деятельности в случае сбоев и аварийное восстановление. Эти планы ежегодно пересматриваются, тестируются и распространяются среди соответствующего персонала по всей организации. Наши центры обработки данных географически изолированы (на расстоянии около 965 км) друг от друга, чтобы предотвратить одновременное воздействие на центры обработки данных в случае крупномасштабного стихийного бедствия.

Аудит и сертификация

Основные службы приложений Smartsheet проходят следующие аудиты и сертификации в области безопасности и конфиденциальности.

- SOC 2/SOC 3. Smartsheet проходит ежегодную проверку и тестирование в рамках процесса аудита SOC. Итоговые отчёты внешнего аудита подтверждают структуру и эффективность внутреннего контроля в нашей компании, включая обеспечение безопасности, доступности и конфиденциальности.

- Сертификация программы по защите конфиденциальности Privacy Shield ЕС — США и Швейцарии — США. Данные клиента, передаваемые в рамках Покрываемых услуг, подпадают под действие ежегодной сертификации в соответствии с Рамочной программой защиты конфиденциальности между ЕС и США и Рамочной программой защиты конфиденциальности между Швейцарией и США, администрируемой Министерством торговли США. Сведения о текущей сертификации можно получить на сайте Privacyshield.gov/list, если набрать в строке поиска "Smartsheet".

- FedRAMP (moderate). Платформа Smartsheet была выбрана для участия в программе FedRAMP Connect Объединённым советом по авторизации (JAB), который отдал приоритет Smartsheet Gov для сертификации на основании спроса со стороны федеральных правительственных учреждений. Smartsheet Gov — это отдельная среда Smartsheet, одобренная FedRAMP и специально разработанная для использования в правительстве США. Она соответствует высоким требованиям безопасности и нормативно-правового соответствия.

- Закон Сарбейнса — Оксли 2002 г. Smartsheet является публичной компанией, которая обязана соответствовать требованиям Закона Сарбейнса — Оксли (SOX). Соблюдение требований SOX улучшает взаимодействие между сотрудниками и помогает поддерживать эффективную коммуникацию при проведении аудита.

Как указано на нашей веб-странице, посвящённой юридическим вопросам, Smartsheet использует инфраструктуру, предоставляемую Amazon Web Services, Inc. (AWS), для размещения данных клиентов. Информацию об аудитах и сертификациях, связанных с безопасностью и конфиденциальностью, полученных AWS, включая сертификацию ISO 27001 и отчёты SOC, можно найти на веб-сайте AWS Security и веб-сайте AWS Compliance. Полный список сертификаций, а также дополнительные официальные документы и технические характеристики можно найти на странице "Соответствие юридическим требованиям" на портале Trust Center.

Заключение и дополнительные ресурсы

Для эффективной работы необходима современная платформа управления, удобная и безопасная. Это утверждение справедливо сегодня и не потеряет своей актуальности завтра. Создавая Smartsheet, мы с самого начала предъявляли строгие требования к конфиденциальности данных и средствам обеспечения безопасности. В дополнение к тому, что уже доступно сегодня, у нас имеется ряд дополнительных функций обеспечения безопасности, которые в настоящее время находятся в стадии разработки. Чтобы получить более подробную информацию о возможностях, программах и средствах защиты Smartsheet, посетите сайт smartsheet.com/trust и воспользуйтесь дополнительными ресурсами ниже.

Интернет-справка для системного администратора Smartsheet
Функции Smartsheet по планам
Интеграции Smartsheet
Документация по API Smartsheet

sales@smartsheet.com
+44 (20) 39001410
smartsheet.com
/smartsheet
/company/smartsheet-com
@smartsheetplatform
/@smartsheet
/smartsheet
/smartsheet