protegrity

ПЛАТФОРМА БЕЗОПАСНОСТИ ДАННЫХ

Contents

1. Обзор Решения

Для большинства организаций данные —новая валюта. Всё больше данных собирается и анализируется с беспрецедентной скоростью. Большая часть из них касается физических лиц - потребителей, их демографической информации, моделей поведения, местожительства, привычек и т. д. Очевидно, что чем лучше вы знаете ваших клиентов, тем лучше вы можете продавать им свои продукты и услуги. Компании, которые не в полной мере используют потенциал доступной им информации, неизбежно отстают.

Данные на вес золота. В то же время, внутренние корпоративные политики, регулирующие организации и законы требуют ответственного подхода к защите всех типов конфиденциальных данных, в том числе финансовой информации, данных частных лиц и сотрудников, интеллектуальной собственности, операционных и внутренних данных бизнеса. Для удовлетворения всех мандатов и защиты ценных активов, конфиденциальные данные должны находиться под надёжной защитой, которая в то же время должна быть максимально незаметной для авторизированных пользователей и процессов.

Неудивительно, что крупным организациям требуется единая унифицированная платформа безопасности данных, легко интегрирующаяся с обширным парком корпоративных решений и поддерживающая широкий спектр платформ, безустанно работающих с чувствительной информацией предприятия.

Решения Protegrity позволяют максимизировать безопасность с минимальным влиянием на повседневную работу и бизнес-операции, эффективно сбалансировать бизнес-потребности и требования политик безопасности. Наша корпоративная платформа защиты данных поддерживает гетерогенные ИТ-экосистемы, включая сценарии интеграции с уже существующими продуктами и разработки новых решений, и приближает Вас к настоящей платформо-независимости. Она показывает высокую производительность и масштабируемость на всех узлах и обеспечивает беспрецедентную безопасность данных сегодня и легкое восстановление из архивов завтра. Платформа безопасности данных Protegrity поддерживает ваши усилия по созданию упреждающей, учитывающей риски стратегии безопасности начиная с момента приобретения данных до момента их удаления. Она создана, чтобы упростить управление безопасностью данных и значительно облегчить приведение инфраструктуры в соответствие с нормативными требованиями; облегчает достижение намеченных целей, предоставляя инструменты централизованного администрирования для создания и управления политиками и ключами безопасности; включает возможности оповещения, отчетов и аудита безопасности на уровне предприятия. Платформа предоставляет различные методы защиты данных, включая токенизацию, шифрование, различные уровни маскирования и мониторинга.

Protegrity – проверенный новатор и лидер в отрасли безопасности данных. Мы слушаем наших клиентов и партнёров, растём вместе с ними и быстро внедряем поддержку новых технологий. С нашими крупнейшими заказчиками мы работаем уже много лет, мы прислушиваемся к их потребностям, запросам и вызовам. Мы постоянно развиваем и модифицируем платформу безопасности данных в соответствии с современными требованиями, чтобы удовлетворить любые запросы организаций и предприятий любого уровня сегодня и в будущем.

Усовершенствованные методы защита данных Protegrity обеспечивают гибкую, ответственную обработку и извлечение ценной информации из чувствительных данных, обеспечивая конфиденциальность и безопасность при сохранении удобства пользования. Платформа безопасности данных Protegrity может использоваться для приведения инфраструктуры в соответствие с нормативными и юридическими нормами и предназначена выходить за рамки обычного «реактивного» соответствия нормативным требованиям и упреждающе защищать бизнес от реальных и активно распространяющихся угроз, с которыми компании сталкиваются сегодня.

2. Платформа безопасности данных Protegrity

Сложность бизнес-процессов и технологий, их поддерживающих, обуславливают множество проблем защиты данных. Обеспечение широкой совместимости с различными базами данных, операционными системами и платформами имеет одно из важнейших значение для успешного решения критических и сложные задачи защиты корпоративных данных.

Платформа безопасности данных Protegrity многие годы совершенствовалась и эволюционировала для эффективного решения задач защиты данных в средах крупных предприятий. Она состоит из **сервера ESA (Enterprise Security Administrator)** – центрального инструмента управления политиками безопасности, ключами, аудитом и отчетностью – и различных **модулей защиты данных**, которые предваряют в жизнь политики безопасности на каждой отдельной системе.

Платформа безопасности данных Protegrity обеспечивает жизненно важную гибкость во многих областях, включая:

- Широкий охват платформ и исчерпывающая совместимость с большим набором приложений, баз данных, операционных систем и платформы, в том числе облачных и больших данных (Hadoop).
- Гибкость: полный арсенал методов (шифрование, токенизация и маскирование) для защиты данных, де-идентификации и анонимизации на уровне томов, файлов, столбцов и полей.
- Межплатформенная согласованность: данные, защищённые в одной системе (например, Oracle), могут быть с лёгкостью перенаправлены на системы другого поставщика (например, Teradata) и дешифрованы/детокенизированы для авторизированных пользователей и процессов.

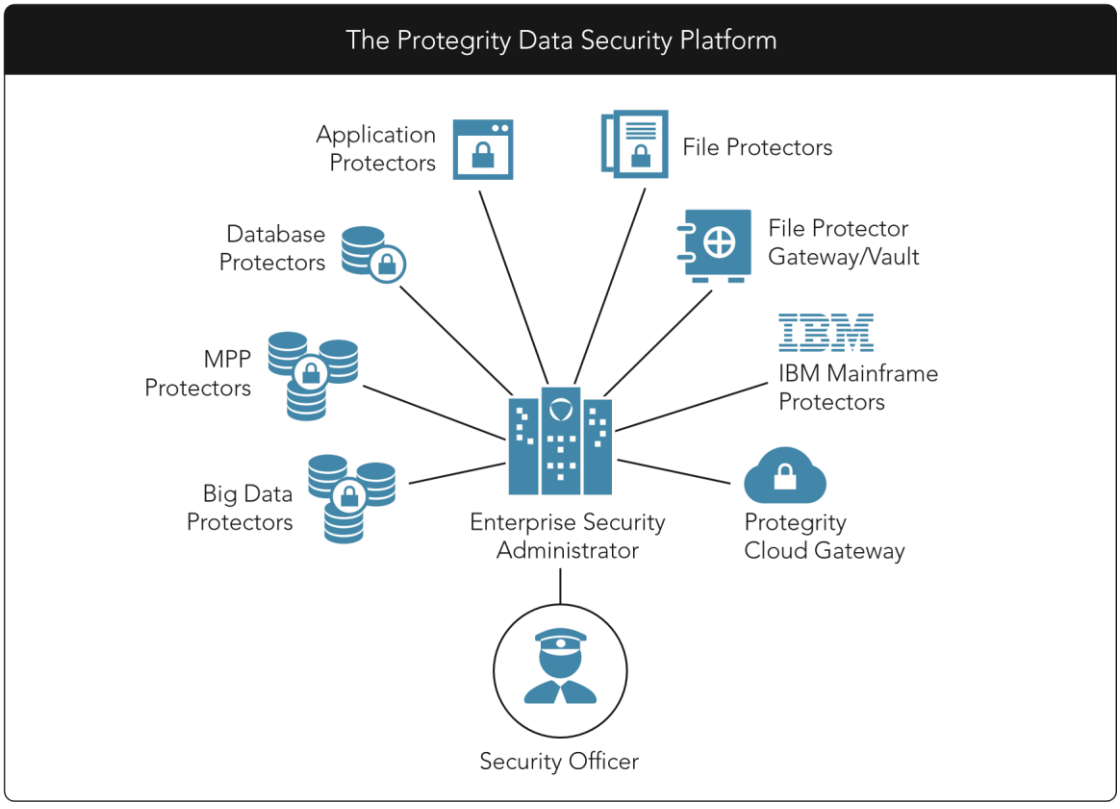

Рис. 1: Высокоуровневая архитектура платформы защиты данных Protegrity.

3. Сервер ESA (Enterprise Security Administrator)

Сервер ESA является центральным командным центром управления корпоративными политиками безопасности данных, ключами шифрования и токенизации, мониторинга, аудита и отчетности во всех системах с установленным программным обеспечением Protegrity. ESA позволяет авторизованным администраторам задавать и конфигурировать корпоративные политики безопасности и развёртывать их в модулях защиты данных Протегрити, установленных в различных системах предприятия, в местах хранения и использования конфиденциальных данных. Модули защиты данных предваряют сконфигурированные политики безопасности в жизнь, а также ведут и отправляют журналы аудита всех операций над конфиденциальными данными обратно в ESA для отчетности.

3.1. Общая архитектура

ESA общается со всеми модулями защиты данных в соответствии с алгоритмом, проиллюстрированном на рисунке 2.

1. ESA создаёт и сопровождает политики безопасности в течении их жизненного цикла, а также ведёт контроль за их исполнением; берёт на себя функции управления и ротации ключей, используемых Протегрити.
2. Политики безопасности конфигурируются на ESA и посылаются модулям защиты данных. Они включают в себя правила авторизации, в которых сотрудник службы безопасности проинструктировал модули защиты данных как защищать и снимать защиту с конфиденциальных данные в зависимости от роли, пользователя, процесса, времени, места и других факторов.
3. После выполнения операций над данными модули защиты данных отправляют журнал всех операций и попыток доступа обратно в ESA. Журналы содержат полный список всех авторизованных и несанкционированных попыток доступа к конфиденциальным данным, а также попытки изменить или удалить их.
4. Все операции с данными выполняются модулями защиты данных. ESA сервер в работе с данными не участвует и не является слабым звеном или центральным узлом отказа.

Перемещение политик безопасности и журналов аудита между ESA и модулями защиты данных осуществляется по безопасному каналу. В случаях, когда соединение с ESA было прервано или отсутствует, модули защиты данных будут продолжать работать в соответствии с политикой безопасности, полученной ранее; журналы аудита будут временно кэшированы локально в шифрованном виде до момента, когда соединение с ESA сервером снова будет установлено.

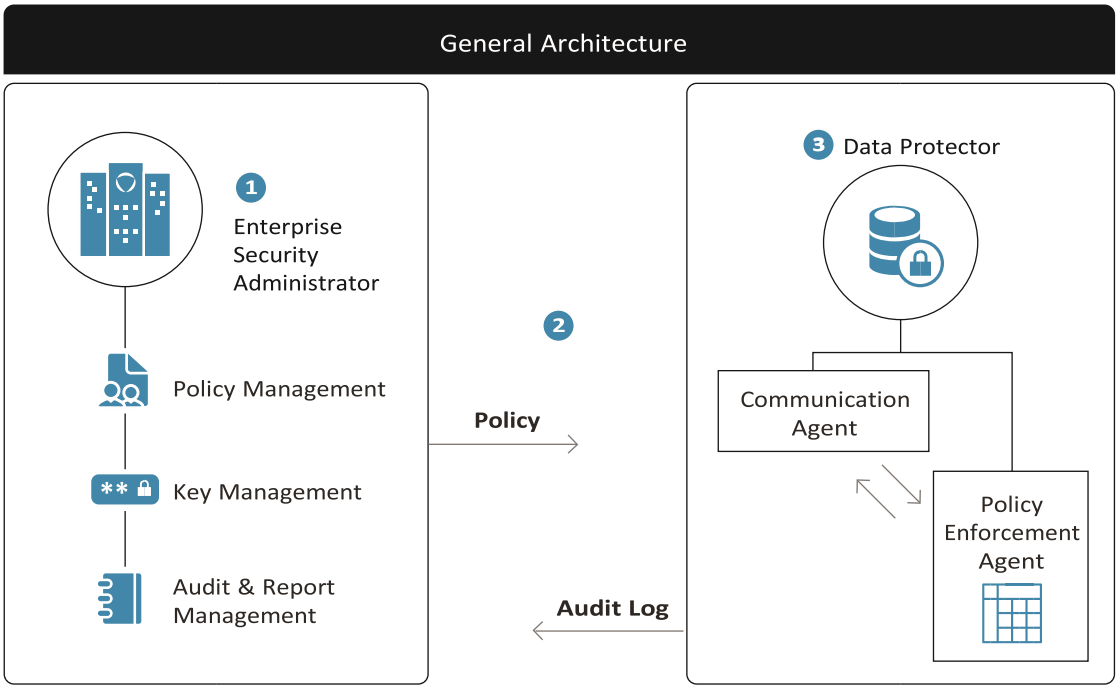

Рис. 2: Общая архитектура ESA и модулей защиты данных.

4. Модули Защиты Данных

Защита конфиденциальных данных крупного гетерогенного предприятия специализированными точечными решениями невероятно сложна. Платформа безопасности данных Протегрити значительно упрощает эту задачу благодаря совместной распределённой работе модулей защиты данных, устанавливаемых на конечные сервера заказчика. Множество поддерживаемых платформ поволяет реализовать сквозную защиту: данные защищены с момента их появления до архивирования и удаления.

Модули защиты данных, каждый на своей системе, предваряют в жизнь политики безопасности, сконфигурированные на ESA, ведут журналы аудита операций с данными на подотчётных системах и отправляют их ESA для ведения централизованной отчётности.

4.1. Архитектура

Модули защиты данных имеют два основных компонента: Агент Связи (также известный как "PEP сервер") и Агент Исполнения Политик Безопасности (PEA).

- Агент PEP является коммутатором между ESA и операциями защиты данных, выполняемых PEA. Он скачивает политики безопасности, кэширует их локально и подготавливает их для использования PEA. Также он отправляет ESA журналы аудита.
- Агент PEA, предваряет в жизнь политики безопасности на системе, где он установлен. Он защищает данные и снимает защиту, в соответствии с ролями, пользователями, процессами, временем, местом и другими факторами, определёнными ESA в политиках безопасности.

4.2. Исполнение Политик Безопасности

На рисунке 4 проиллюстрированы шаги, выполняемые Агентом PEA в процессе защиты конфиденциальных данных от злоумышленников и несанкционированного доступа, а также вывода данных в незащищённом виде для авторизованных пользователей.

1. Пользователь делает запрос на просмотр конфиденциальных данных (например, через приложение или консоль).
2. Пользователь желает увидеть поля "Имя" и "Адрес" в чистом виде. Оба этих поля защищены в покое внутри хранилища данных (например, в файле, таблице базы данных, Hadoop и т.д.).

3. Агенты PEA и PEP работают в связке, как основные компоненты модуля защиты данных. Все запросы на просмотр конфиденциальных данных инициируют в агенте PEA создание журналов аудита и их ретранслирование агенту PEP для передачи ESA.
4. В ответ на запрос агент PEA выясняет, кто является пользователем, и проверяет в локальных политиках безопасности, имеет ли запрашивающая сторона доступ к защищенным полям.
5. Если в какой-либо из политик безопасности указано, что роль, к которой принадлежит запрашивающая сторона, имеет право видеть "Имя" и "Адрес" в чистом виде, то агент PEA возьмет данные из хранилища, снимет с них защиту, используя CPU ресурсы сервера, где он установлен, и вернёт пользователю. (Данные в хранилище останутся в защищённом виде.) Политика безопасности также может содержать сведения, указывающие, что только определённая часть конфиденциальных данных может быть показана пользователю.

   Если запрашивающая сторона не авторизована и не имеет доступа к защищенным данным, то агент PEA отклонит запрос и проинформирует агент PEP о попытке несанкционированного доступа, который в свою очередь проинформирует ESA.

   Политики безопасности также могут быть настроены на возврат различных видов ответов на попытки несанкционированного доступа, включая возврат молчаливый возврат данных в неизменённом виде, возврат строки "нет доступа", значения NULL или исключения.
6. "Имя" и "Адрес" возвращаются пользователю как часть набора результатов. Параллельно создаётся запись журнала аудита, которая направляется агенту PEP и далее в ESA.

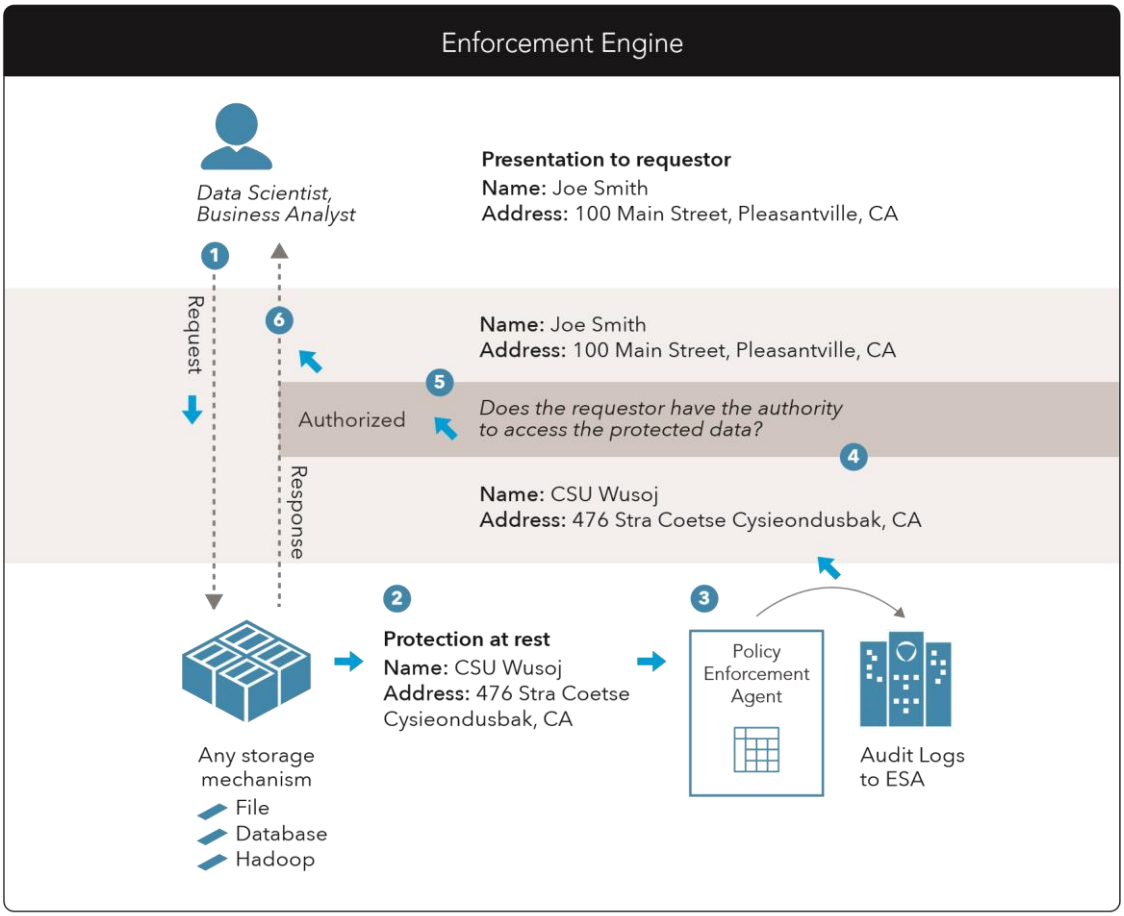

Figure 4: Operation of the Policy Enforcement Agent

protegrity

Corporate Headquarters
Protegrity USA, Inc.
5 High Ridge Park, 2nd Floor
Stamford, CT 06905
Phone: **203.326.7200**

United Kingdom
3 Regius Court
Church Road
Penn
Buckinghamshire
HP10 8RL
Phone: **+44 1494 857762**

www.protegrity.com