

Платформа, обеспечивающая централизованный контроль и безопасный доступ к структурированным данным в современных дата-платформах — включая базы данных, корпоративные DWH и озёра данных (data lakes).

Решение также поддерживает безопасное использование данных в AI-сценариях, работу с большими языковыми моделями (LLM), такими как ChatGPT, обеспечивая контроль доступа и защиту чувствительной информации при их использовании.

Ключевая область Satori –

управление доступом к данным на уровне запросов и пользователей без необходимости изменений в самих источниках, включая:

- централизованные политики доступа (RBAC/ABAC)
- динамическое маскирование и фильтрацию данных на уровне SQL запросов
- контроль в реальном времени и динамические (just-in-time) разрешения
- аудит и мониторинг использования данных на уровне каждой отдельной строки в СУБД

Satori обеспечивает безопасный доступ к данным для AI-систем, предлагая:

- контроль данных, используемых AI-приложениями
- защиту чувствительной информации (PII, финансовые данные) при обращении к LLM
- применение политик доступа к данным, используемым в RAG (Retrieval-Augmented Generation) сценариях
- аудит запросов и ответов AI для соблюдения требований безопасности и комплаенса.

Satori не просто отслеживает действия с данными, а в реальном времени принудительно применяет политики доступа, мгновенно блокируя любые неразрешённые или подозрительные запросы. За счёт этого бизнес получает не «журнал для расследования», а действующую защиту: доступ к данным разрешается только в строгом соответствии с правилами.

Основные функции:

Data Discovery & Classification

Автоматизированный поиск и классификация чувствительных данных в базах, DWH и data lake/lakehouse платформах => данные помечаются пользовательскими тегами для лучшей видимости конфиденциальных данных

Data Access Visibility & Monitoring

Полная видимость всех обращений к данным (SQL и др.) в реальном времени: кто, когда и к каким данным получает доступ => фиксируется активность и обеспечивается применение политик доступа и защита данных непосредственно в момент запроса

Dynamic Data Masking & Protection

Динамическое маскирование и защита чувствительных данных «на лету» без изменений в источниках данных => безопасно предоставляет доступ к данным пользователям и приложениям, минимизируя риск утечки конфиденциальной информации

Data Access Governance

Управление доступом к данным на основе ролей и атрибутов (RBAC/ABAC), включая контроль и оптимизацию прав доступа => обеспечивает принцип минимальных привилегий и снижает риски несанкционированного доступа к чувствительной информации

Centralized Data Access Control

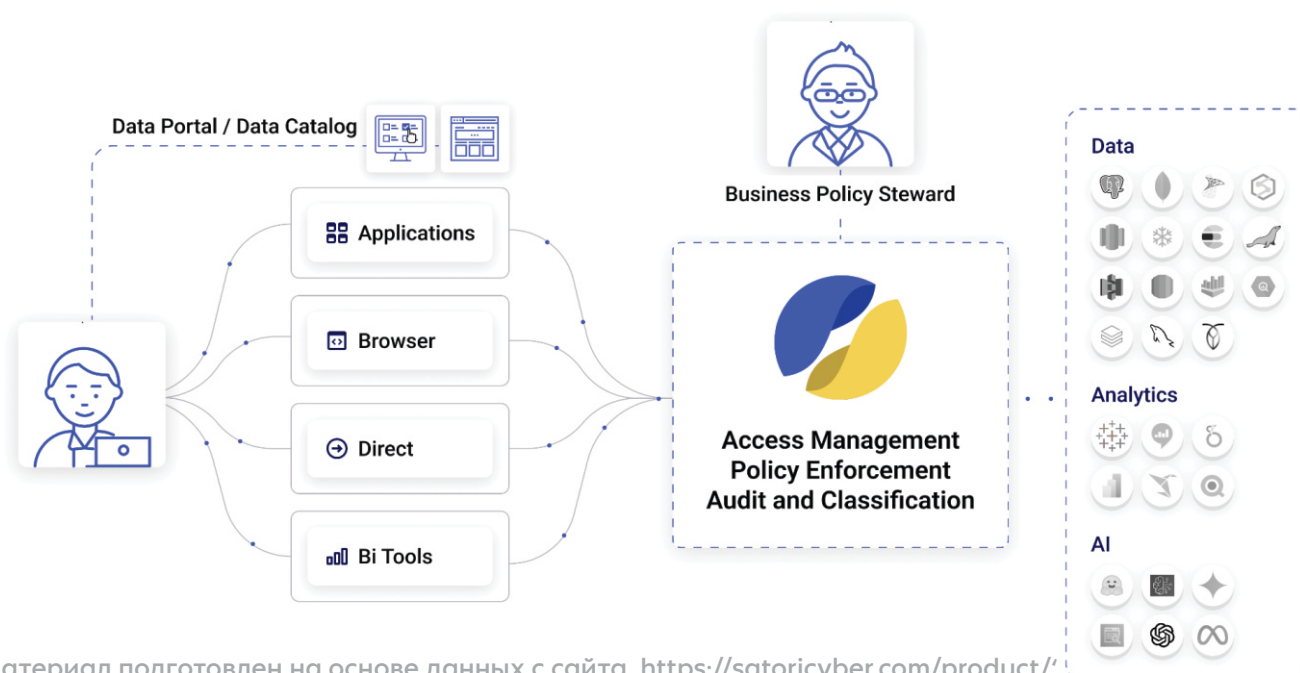
Централизованное управление доступом на уровне данных (таблицы, строки, столбцы) из единой точки без изменений приложений и инфраструктуры => упрощает администрирование и гарантирует согласованность политик доступа во всех источниках данных

Security, Privacy & Compliance (DSPM)

Поддержка требований безопасности и конфиденциальности (GDPR и др.), включая аудит доступа, защиту чувствительных данных и элементы Data Security Posture Management (DSPM) => больше не нужно беспокоиться о комплаенсе

Secure Data Access for AI & LLM

Контроль использования данных в AI-сценариях, включая большие языковые модели (например, ChatGPT) => предотвращение утечек чувствительной информации и применение политик доступа при работе AI с данными



© Материал подготовлен на основе данных с сайта <https://satoricyber.com/product/>