27 мая 2026

Zero Trust и Data Governance: как управление данными превращает дата-каталог в ядро контура безопасности

Многие компании воспринимают каталог данных как «игрушку для аналитиков», позволяющую осуществлять быстрый поиск терминов, их описаний и связей с таблицами и полями. Каталогизация данных в этих компаниях строится безотносительно систем информационной безопасности, хотя на практике это может и должно быть единым окном для бизнес-подразделений и отделов информационной безопасности, так как именно через каталог фиксируются владельцы данных, их критичность, классы чувствительности и регуляторные/внутренние требования.

Периметр корпоративной сети уже давно перестал быть надежным рубежом обороны и контролируемой на сто процентов зоной, а облачные сервисы, удалённый доступ, распределенные команды — превратили классическую модель «доверяй внутреннему, блокируй внешнее» в опасную иллюзию. Частичным решением проблем информационной безопасности стала концепция Zero Trust, которая вылилась в подход, при котором ни один пользователь, устройство или сервис не получают доступ к ресурсам без непрерывной верификации.

Но за достаточно короткий промежуток времени стало понятно, что Zero Trust-подход сам по себе не решает задачу и без практик и инструментов Data Governance, «Нулевое доверие» остается односторонним процессом и требует постоянного «ручного» пересмотра правил доступа. В данной статье я рассмотрю, как симбиоз двух подходов может помочь компаниям выстроить

целостную систему защиты информационных активов.

Что стоит за «абсолютным недоверием» пользователям

В 2020 году NIST (US National Institute of Standards and Technology) формализовал концепцию Zero Trust в стандарт SP 800-207. Коротко всю суть подхода можно выразить двумя блоками:

1. Три основных базовых принципа:

- Непрерывная верификация каждого запроса на доступ,
- Предоставление минимально необходимых привилегий
- Допущение о том, что инфраструктура уже скомпрометирована.

2. Три ключевых архитектурных компонента:

- механизм принятия решений на базе текущих политик — Policy Engine,
- перевод принятых решений в действия — Policy Administrator,
- применение обновленных политик на точке доступа — Policy Enforcement Point

Где пересекаются Zero Trust и Data Governance

На первый взгляд, Zero Trust — это про сетевую безопасность, а Data Governance — про управление данными и их качество. Однако именно на

стыке этих дисциплин формируется по-настоящему зрелая система защиты.

В 2024 году NIST обновил свой Cybersecurity Framework (CSF) до версии 2.0, дополнив базовые принципы еще одним — Govern, который обязывает формировать контекст, т.е. совокупность бизнес и технических характеристик данных, позволяющую четко идентифицировать данные и уйти от абстрактных «есть таблица в БД», а также стратегию и политики управления рисками при работе с данными.

В результате, сложились следующие ключевые области Zero Trust:

- корпоративное управление данными и метаданными;
- маркировка/тегирование;
- мониторинг;
- шифрование;
- контроль доступа;
- предотвращение утечек.

Фундаментом этого «столпа» выступает Каталог данных, так как невозможно защитить актив, о существовании которого организация не знает. Каталог описывает, какие данные есть, где они хранятся, кто ими владеет, содержат ли они персональные(чувствительные) данные и прочие метаданные цифровых активов компании. Бизнес-глоссарий дополняет картину, формируя единый язык описания данных.

Практическая связка выглядит так: инструменты Data Governance проактивно классифицируют данные (к примеру: «персональные данные клиентов» и/или «коммерческая тайна»), присваивая, в том числе автоматически через функции внутреннего анализа, встроенные в каталог данных, теги чувствительности, а Zero Trust-инфраструктура на основе этих тегов применяет политики RBAC и ABAC — вплоть до динамической маскировки столбцов при нетипичных запросах.

Если данные классифицированы как «данные с ограниченным доступом» в каталоге, система управления безопасностью использует эту информацию для автоматического применения соответствующих правил доступа, шифрования, маскировки или обезличивания. Результат — не просто закрытый периметр, а контекстно-зависимый контроль, который адаптируется к уровню риска каждого запроса.

Корпоративные кейсы

Крупные банковские организации, внедряющие Zero Trust, сообщают о снижении инцидентов несанкционированного доступа к клиентским данным на 30% в первый год после объединения практик Zero Trust и Data Governance.

Микросегментация в сочетании с каталогизацией данных позволяет изолировать транзакционные системы от систем управления персоналом — даже если злоумышленник скомпрометирует одну учётную запись, горизонтальное перемещение по сети сильно ограничено или невозможно вовсе.

Очень показателен опыт Airbus, применившего Zero Trust подход в период роста эпидемии COVID-19 даже для корпоративной электронной почты, средств совместной работы и внутренних приложений компании, сохранив баланс между безопасностью и производительностью.

Что из инструментов объединяет два подхода

Реализация связки Zero Trust и Data Governance требует интеграции нескольких классов решений:

- Каталог данных и бизнес-глоссарии — обеспечивают инвентаризацию активов, классификацию, ведение data lineage и единого словаря терминов.
- IAM (Identity and Access Management) системы аутентификации — реализуют многофакторную аутентификацию, ролевой и атрибутный контроль доступа.
- DLP (Data Loss Prevention — предотвращение потери данных) и системы классификации — автоматически обнаруживают и тегируют чувствительные данные.
- SIEM-платформы (Security Information and Event Management — управление информацией и событиями безопасности) — собирают и коррелируют события безопасности, обеспечивая непрерывный мониторинг.
- API Gateway и средства микросегментации — контролируют межсервисное взаимодействие с применением токенов ограниченного срока действия.

Ключевой принцип

Инструменты не работают изолированно. Классификация из каталога данных транслируется в политики IAM и DLP, а аудит доступа из SIEM возвращается в каталог, формируя полный цикл обратной связи.

Data Governance формирует основу: каталог данных инвентаризирует активы и присваивает теги чувствительности, бизнес-глоссарий обеспечивает консистентность терминологии, а data lineage отслеживает происхождение

данных.

Инфраструктура Zero Trust использует эти теги для принятия решений в реальном времени: Policy Engine оценивает контекст запроса (кто, откуда, с какого устройства, к каким данным) и принимает решение на основе текущих политик, Policy Administrator переводит принятое решение в действие, а Policy Enforcement Point применяет его — вплоть до динамической маскировки отдельных столбцов. Контур мониторинга замыкает цикл: SIEM и DLP фиксируют все действия с данными и возвращают обратную связь в каталог, что позволяет автоматически корректировать уровни чувствительности и политики доступа.

Для более полного понимания, разберем цикл еще раз по шагам:

1. **Фиксация действий.** Каждый раз, когда пользователь или сервис обращается к данным через Policy Enforcement Point, генерируется событие безопасности — кто запросил доступ, к каким данным, с какого устройства, в какое время, какое решение принято (разрешение, отказ, маскировка). Эти события потоком уходят из IAM в SIEM, который коррелирует их с другими сигналами: сетевой активностью, авторизациями, геолокацией.
2. **Проактивный контроль.** Параллельно с фиксацией действий пользователей, DLP-система сканирует данные «в движении» и «в покое», автоматически обнаруживая чувствительный контент — номера паспортов, финансовые записи, интеллектуальную собственность — и генерирует собственные инциденты при попытках несанкционированной передачи.
3. **Обратная связь в каталог.** Ключевой момент — результаты работы SIEM и DLP не остаются изолированными. Они передаются обратно в каталог данных, обогащая метаданные конкретных активов и обновляя классификаторы.

Пример конкретных сценариев

Повышение чувствительности. DLP обнаружила, что в таблице, классифицированной как «внутренняя», появились номера кредитных карт. Система (связка из DLP и каталога данных) автоматически повышает тег чувствительности до «конфиденциально», и Zero Trust-инфраструктура сразу ужесточает политику доступа — например, требует MFA и запрещает экспорт.

Обнаружение аномалий доступа. SIEM выявляет, что к определенному датасету за сутки обратилось в 10 раз больше пользователей, чем обычно. Эта метрика записывается в каталог как маркер повышенного риска. Policy Engine начинает запрашивать дополнительную верификацию для этого актива.

Переклассификация «тихих» данных. Данные, к которым давно никто не обращался, могут быть автоматически помечены как кандидаты на архивирование или деклассификацию — что снижает нагрузку на систему контроля.

«Назначили и забыли» или почему это важно

Без обратной связи система работает в режиме «Назначили и забыли».

- бизнес-роль назначили … и забыли
- классификатор присвоили … и больше не обновляют
- интеграционный контракт подписали … и положили на полку

Как роли, так и информация о данных, устаревают по мере изменения данных. Замкнутый цикл делает систему адаптивной — политики доступа эволюционируют вместе с реальным поведением пользователей и систем, а изменение содержимого данных влияет на политики доступа. Именно это превращает связку из Zero Trust инструментов Data Governance (Каталога данных) из статичной конфигурации в живой механизм непрерывной защиты.

Роль интегратора: от стратегии к реализации

Внедрение Zero Trust в связке с Data Governance — это не покупка одного продукта, а выстраивание архитектуры из множества компонентов. Компании-интеграторы играют здесь критическую роль: они проводят аудит текущего ландшафта, проектируют целевую архитектуру с учетом отраслевой специфики и нормативных требований, подбирают и интегрируют решения, а затем сопровождают внедрение поэтапно — от пилотного сегмента до масштабирования на всю организацию.

Именно интегратор помогает преодолеть типичные барьеры: сложность интеграции с legacy-системами, сопротивление со стороны бизнес-подразделений и необходимость поэтапного перехода без прерывания бизнес-процессов.

К чему стремиться

К концу текущего десятилетия, организации, которые хотят выжить, будут вынуждены забыть про старые подходы к построению контролируемой зоны и перейти к более совершенным, отвечающим современным реалиям, в том числе из-за рисков, связанных с развитием технологий искусственного интеллекта, принципам защиты своих данных. А те компании, которые уже сегодня выстраивают связку Zero Trust и Data Governance, получат

стратегическое преимущество, а также прозрачный контроль доступа, аудируемые процессы и способность адаптировать защиту к новым угрозам без перестройки архитектуры с нуля.