Почему важны проверенные и безопасные операции с медиаданными

Семь парадоксов, формирующих следующую эру медиапроизводства

Часть 3

Ронни ван Гил, директор Grass Valley по маркетингу продукции

В этой серии статей рассматриваются технологии, архитектуры и эксплуатационные реалии, формирующие современную работу с медиаданными. От статьи к статье анализируется, как эти отдельные компоненты влияют на более масштабную эксплуатационную картину и определенно помогают организациям выстраивать унифицированную работу.

В предыдущей статье внимание уделялось тому, почему совместимости самой по себе уже недостаточно. По мере того как процессы работы с медиаданными, опирающиеся на программное обеспечение, становятся все более распределенными и динамичными, сохранение смысла и контекста с помощью Media eXchange Layer (MXL) дает нечто все более ценное – свободу.

Но со свободой приходит и новая проблема. В то время как организации все больше полагаются на людей, опыт и партнеров, находящихся вне их традиционных границ, встает вопрос: как им выстраивать доверие в эксплуатационной модели, в основе которой лежат открытость и постоянные изменения?

Третий парадокс: чем мы более открыты, тем больше защиты требуется

Безопасность всегда была частью того, как медиаорганизации выстраивают доверие. В каждой медиаорганизации понимают, что создаваемая ею стоимость зависит от активов, которые должны быть защищены. Контент, операционные системы и доверие аудитории всегда были основой успеха этого бизнеса.

Но в среде, все более определяемой искусственным интеллектом, технологической зависимостью от программного обеспечения и быстро меняющимися угрозами, защита не может рассматриваться как разовая мера. Безопасность нужно оценивать, поддерживать и совершенствовать по мере изменения операционной среды.

Изменение ландшафта рисков становится еще более существенным с изменением самих операционных моделей. Переход на динамические медиакомплексы не избавляет от ответственности по защите, но усиливает необходимость постоянно обеспечивать ее в условиях более подвижной распределенной инфраструктуры. Меняется также скорость возникновения рисков. Поскольку программные средства, инфраструктура и сервисы эволюционируют быстрее и чаще, поддержание доверия требует способности сохранять неизменную осведомленность об уязвимостях и реагировать на них прежде, чем они перерастут в эксплуатационные проблемы.

Такой сдвиг обусловлен меняющейся бизнес-реальностью. У зрителей есть как никогда широкий выбор. Лояльность сложнее заслужить и проще потерять. Обладатели контента должны увеличить объемы его производства, увеличивать аудиторию и быстрее реагировать на меняющиеся возможности, по-прежнему поддерживая качество и узнаваемость того, что делает их уникальными.

Чтобы соответствовать этим требованиям, медиаорганизации все чаще полагаются на дистанционно работающих сотрудников, региональные центры, экосистемы партнеров и программно-определяемые рабочие процессы. Эксперты могут подключаться к работе из любой точки мира. Динамические медиакомплексы позволяют задействовать ресурсы там, где они наиболее эффективны, а не там, где они находятся. И не потому, что это позволяет технология, а потому, что таковы бизнес-потребности.

Десятилетиями операции с медиаданными строились обычно на основе инфраструктуры, которая всегда находилась под непосредственным контролем. Сигнальные тракты, аппаратно-студийные комплексы, оборудование и операционные границы – все это было под тщательным управлением, потому что формировало основу, на которой строится доверие.

Сегодня многие возможности, создающие стоимость, больше не находятся в этих границах. Как раз здесь и возникает парадокс – чем больше людей, рабочих процессов и возможностей задействовано в работе, тем меньше доверие может опираться на традиционные рамки.

Настоящая проблема не в том, чтобы полностью все закрыть

Традиционная операционная модель формировала простую и понятную модель доверия. Доступ зачастую был связан с присутствием. Нахождение внутри операционного периметра подразумевало определенный уровень доверия, поскольку сам этот периметр жестко контролировался.

Эта модель все еще сохраняет ценность во многих смыслах. Специализированная инфраструктура, частные сети и управляемые комплексы продолжают играть важные роли в масштабах отрасли. Суть не в том, что одна модель приходит на смену другой, а в том, что программно-определяемые и распределенные рабочие процессы формируют другую модель доверия. Когда коллективы работают в разных местах, когда приложения запускаются на вычислительных средствах общего доступа, когда сбор данных происходит по менее управляемым сетям и когда партнеры становятся частью операционной цепочки, старые допущения больше не действуют. Доступ больше не может пользоваться доверием просто потому, что он инициируется изнутри привычного периметра. Идентичность больше не может быть признана только потому, что кто-то находится внутри комплекса.

И задача уже заключается не только в том, кому разрешить доступ. Она в том, чтобы понимать, кто находится внутри системы, что ему разрешено делать и остается ли этот уровень доступа актуальным по мере эволюции операционной среды.

В традиционных операционных моделях ответить на эти вопросы достаточно просто. Если системы, люди или рабочие процессы остаются в четко определенных рамках, доверие в значительной степени может происходить из самой инфраструктуры.

Программно-определяемые операции меняют ситуацию. Доверие необходимо целенаправленно выстраивать, регулировать и поддерживать. Оно все более становится самостоятельной операционной компетенцией. Именно это изменение парадигмы является основой современной безопасности медиакомпании.

Организации хотят работать с лучшими творческими специалистами вне зависимости от места их нахождения. Они желают создавать больше контента, не перемещая каждого человека и каждый ресурс на тот или иной объект. Им хочется сочетать внутренние возможности с партнерскими сервисами и программно-определяемыми рабочими процессами. Все эти намерения требуют участия. Вопрос в том, как сделать это участие безопасным настолько, чтобы обеспечить доверие.

Доверяй, но проверяй

Концепция нулевого доверия (Zero Trust) порой обсуждается так, как если бы она была инструментом защиты или технической архитектурой. В действительности, Zero Trust означает, что системы, пользователи и устройства не обладают доверием по определению. Доступ требует аутентификации и авторизации, он ограничен только тем, что необходимо. Разрешения должны соответствовать ролям и уровням ответственности. Необходима возможность отслеживать активность. Допущения нужно заменить проверками.

Этот же принцип нужно распространить не только на доступ. Программное обеспечение, сервисы и компоненты, формирующие рабочую среду, не должны восприниматься защищенными только потому, что они были защищены при первоначальном развертывании. Именно здесь начинает рушиться традиционный компромисс между открытостью и защитой. Защита часто воспринимается как препятствие, нечто, что замедляет работу персонала, ограничивает творчество и усложняет внедрение новых операционных моделей.

Плохо продуманная защита определенно может быть такой. Но хорошо организованная защита работает диаметрально противоположно – она создает условия, в которых открытость становится практичной. Защита – это не цена, которую приходится платить за открытость. Защита – это то, что делает открытость возможной.

Отраслевая перспектива

Важность этой перспективы четко отражена в дискуссиях, проходящих в масштабах всей отрасли. Через GVx Council мы попросили руководителей медиакомпаний поделиться их мыслями об эксплуатационных реалиях, формирующих переход в направлении более динамических и программно-определяемых производственных сред. Одно соображение стало более чем очевидным – защиту нельзя добавлять в самом конце.

Как отметила Эмили Планас (Emili Planas): «Защита разрабатывается с самого начала. Управление, администрирование идентификации и целостность бизнеса – все это должно быть частью обсуждения».

Это утверждение важно, поскольку оно очерчивает защиту не как отдельный уровень, инструмент или функцию. Оно обозначает доверие как свойство системы. Безопасность, управление, идентичность и целостность взаимосвязаны, поскольку все они отвечают на разные аспекты одного и того же вопроса: можно ли положиться на эту систему, когда это действительно имеет значение?

Вот почему доверие в программно-определяемых рабочих процессах должно выходить за пределы кибербезопасности как таковой. Доверие зависит от управления, распределения ответственности, подотчетности и непрерывности работы не в меньшей степени, чем от технических средств обеспечения безопасности. Организациям требуется знать не только о том, что системы защищены, но и о том, кто несет ответственность, как принимаются решения и можно ли полагаться на систему при изменении обстоятельств.

Такой более общий взгляд на доверие все больше формирует как отраслевые практики, так и правовые ожидания. Такие нормативные рамки, как Cyber Resilience Act, отражают растущее понимание того, что устойчивость, подотчетность и безопасность должны закладываться непосредственно в саму операционную деятельность, а не добавляться на более поздних этапах. Они также усиливают все более важное требование: организации должны быть способны постоянно выявлять уязвимости, управлять изменениями и устранять выявленные проблемы, вместо того чтобы полагаться на редкие циклы проверки.

Глава отдела безопасности, руководитель службы эксплуатации или технический директор оценивает не просто технологии. Он защищает то, что для него действительно важно. Медиапроизводство всегда привлекало людей, которые умеют смотреть вперед. Они ищут слабые места, потому что хотят, чтобы система работала успешно.

Они ставят под сомнение устоявшиеся предположения, потому что понимают важность надежности. Они задают сложные вопросы, потому что осознают ценность

того, что помогают создавать и защищать. Это не вопросы, продиктованные страхом. Это вопросы, продиктованные профессиональной гордостью, ответственностью за результат и чувством личной ответственности.

Переход уже идет

Движение в сторону доверенных и защищенных операций с медиаданными уже заметны в масштабах отрасли. Эталонная архитектура динамического медиакомплекса (Dynamic Media Facility Reference Architecture) определяет защиту, мониторинг, управление и администрирование как общие для всей работы аспекты, а не как отдельные второстепенные меры, о которых можно подумать позже. Это важно, поскольку подтверждает более широкое отраслевое признание – динамические операции требуют доверия, интегрированного в каждый уровень жизненного цикла рабочей нагрузки.

Такой жизненный цикл не заканчивается, как только система внедрена. В мире постоянно эволюционирующего программного обеспечения и разработок с применением искусственного интеллекта возможность отслеживания вновь выявленных общих уязвимостей и угроз – (CVE Common Vulnerabilities and Exposures) и быстрого реагирования, где это нужно, стала частью эксплуатационной ответственности. И это может быть причиной, усложняющей работу.

Как отметил Гейр Бёрдален (Geir Børdalen): *«Мы строим IP-инфраструктуру на основе концепции Zero Trust. Процесс очень длительный и постоянно заставляет сдвигать сроки».* Столь честное признание отражает реальность, с которой сталкиваются многие организации. Интеграция доверия в современную эксплуатационную модель требует большего, чем применение технологии. Она требует от организаций переосмысления допущений, процессов и уровней ответственности, которые часто существовали десятилетиями.

Она также требует развития системы управления изменениями. Обновления системы безопасности не всегда могут ждать небольшого количества заранее запланированных окон релиза. Организациям необходимы четко выстроенные процессы, позволяющие быстро оценивать, проверять, согласовывать и внедрять важные меры по устранению уязвимостей, сохраняя при этом контроль над операционной деятельностью.

Да, эти усилия могут быть значительными, но значительны и связанные с ними риски и возможности. Те же основы, которые укрепляют безопасность, позволяют внедрять более открытые, гибкие и совместные подходы к работе.

Для Grass Valley этот переход определил развитие AMPP OS с самого начала. Цель заключалась не просто в том, чтобы сделать медиапроцессы более связанными. Задача состояла в том, чтобы обеспечить возможность такой взаимосвязи без утраты доверия, на котором эти процессы основаны.

Эта философия влияет на все – от администрирования идентификации и доступа до управления, возможности аудита и подотчетности. Вместо того чтобы рассматривать безопасность как отдельный уровень, добавляемый поверх платформы, эти возможности интегрированы непосредственно в саму операционную модель.

AMPP OS основана на простом принципе: участие должно быть простым, но доверие никогда не следует принимать как данность. Для Grass Valley безопасность не рассматривается как отдельный этап жизненного цикла устройства или решения. Это принцип, заложенный в проектирование и эксплуатацию системы, что означает постоянный контроль состояния всего портфеля решений, включая регулярное сканирование на наличие CVE – еженедельно, а при необходимости и ежедневно.

Обнаружение уязвимости – лишь часть ответственности. Настоящая проверка заключается в том, располагает ли организация культурой, процессами и возможностями для оперативного реагирования. Наш подход призван обеспечивать своевременный выпуск обновлений там, где они необходимы, чтобы устранение уязвимостей, соответствие требованиям и уверенность в стабильности работы оставались согласованными по мере изменения условий.

Это особенно важно в эпоху AI. По мере ускорения разработки программного обеспечения и одновременного изменения ландшафта угроз доверие зависит от способности адаптироваться, не ставя под угрозу стабильность и контроль, необходимые для медиапроцессов.

Этот подход также отражен в соответствии AMPP требованиям SOC 2, которое обеспечивает важное независимое подтверждение. Однако соответствие требованиям – не конечная цель. Это лишь одно из проявлений более широкого стремления постоянно выявлять, оценивать и устранять риски, которые имеют наибольшее значение для клиентов и их операционной деятельности.

По мере того как медиапроцессы становятся все более распределенными, динамичными и совместными, доверие должно оставаться неизменным независимо от того, где находятся люди, выполняются рабочие процессы или работают сервисы.

Организации редко сомневаются в новом операционном подходе из-за отсутствия необходимых возможностей. Они сомневаются, когда еще не уверены, что могут на него положиться. Именно доверие позволяет преодолеть этот разрыв.

В конце концов, все сводится к людям

Зрители редко задумываются о модели доверия, лежащей в основе производства. Они лишь понимают, работает ли все так, как должно – приходит ли контент вовремя, с ожидаемым качеством, целостностью и надежностью.

Люди, отвечающие за то, чтобы это происходило, понимают, что даже самая надежная архитектура в конечном итоге зависит от поведения людей. Пароли необходимо защищать. Учетные данные нужно надлежащим образом контролировать. Права доступа должны соответствовать реальным потребностям. Разрешения, которые больше не нужны, необходимо своевременно отзывать.

Это далеко не самые захватывающие аспекты медиапроизводства, но зачастую одни из самых важных. Та же дисциплина необходима и при реагировании организаций на изменения. Уязвимости требуется выявлять и понимать. Обновления должны иметь соответствующий приоритет.

В соответствующих случаях решения нужно принимать оперативно, но никогда – без подотчетности. Специалисты медиаиндустрии серьезно относятся к

этой ответственности. Они ставят под сомнение устоявшиеся предположения, потому что этого требует их ответственность. Они ищут слабые места, потому что от этого зависит непрерывность работы. Они понимают, что доверие не возникает само по себе благодаря системе. Его поддерживает сама организация – посредством дисциплины, ответственности и внимания к деталям. Это не страх. Это профессионализм.

Что становится возможным благодаря доверию

На протяжении всей этой статьи речь шла о безопасности, управлении, идентификации, правах доступа и подотчетности. Можно было бы сделать вывод, что надежная операционная деятельность в конечном счете сводится к защите. Но это не так.

Доверие всегда имело значение. Изменилось лишь то, что сегодня ценность доверия определяется не только тем, что оно защищает. Оно ценно еще и тем, что благодаря ему становится возможным.

Цель доверия никогда не заключалась в том, чтобы просто ограничивать людей. Она заключалась в том, чтобы понимать, кто может безопасно получить доступ. Это различие меняет все.

Доверие позволяет организациям расширять круг участников, не жертвуя подотчетностью. Оно позволяет наращивать гибкость, не теряя контроля. Оно создает среду, в которой люди, рабочие процессы и возможности могут объединяться с уверенностью.

На протяжении десятилетий медиакомпании выстраивали доверие, ограничивая участие. Сегодня они все чаще создают стоимость, расширяя его.

Заключение

Очевидно, переход к более открытым медиапроцессам обусловлен не только развитием технологий. Он продиктован необходимостью создавать более актуальный контент, эффективнее использовать профессиональные кадры, организовывать сотрудничество между различными площадками и реагировать на растущие ожидания аудитории.

Доверие, необходимое для такого перехода, зависит не только от защиты, обеспечиваемой в конкретный момент времени. Оно основывается на идентификации, управлении, подотчетности и принципах безопасности, которые закладываются в операционную модель с самого начала и затем постоянно поддерживаются по мере ее развития.

Когда эти основы сформированы, организации могут подключать больше людей, рабочих процессов и возможностей, не теряя контроля. И тогда логично возникает следующий вопрос: если операционной системе можно доверять, как поддерживать ее работу, развивать и совершенствовать ее, не нарушая стоимость, которую она уже создает каждый день.

Ответу именно на этот вопрос будет посвящена следующая статья.

Продолжение следует

НОВОСТИ

Аксессуары Wooden Camera для Sony FX5

Компания Wooden Camera выпустила новую линейку клеток и аксессуаров для цифровой кинокамеры Sony FX5. Эти приспособления предназначены для адаптации оборудования к различным сценариям съемки — от ручной работы до профессиональных киносъемочных платформ и различных стабилизаторов.

В основу системы положена модульная клетка с низким профилем и быстросъемным креплением типа «ласточкин хвост» (dovetail). Она позволяет без инструментов переставлять камеру со штатива на стабилизатор и обратно, сохраняя компактность съемочной системы камеры. Для работы с ручными электронными стабилизаторами DJI RS предусмотрена быстросъемная площадка ARCA с креплением на болтах.

Линейка также содержит адаптеры-переходники с байонета Sony E на PL и LPL для установки соответствующих кинообъективов, дополнительные опоры для тяжелой оптики, а также регулируемые крепления аккумуляторов Gold Mount и V-Mount. Это позволяет увеличить время автономной работы и гибко размещать батареи с учетом конфигурации оптики, мониторов и беспроводных систем.

Модульная конструкция поддерживает варианты комплектов от облегченной полуклетки до полноценного кинообвеса на базе Elite Cage System. Дополнительные точки крепления предназначены для мониторов, радиосистем, шарнирных кронштейнов и моторов управления объективом.

По словам Wooden Camera, аксессуары изготовлены из авиационного алюминия 6061 с анодированием Type III, рассчитанным на интенсивную профессиональную эксплуатацию. Новая система призвана сохранить мобильность Sony FX5, предоставляя операторам больше возможностей для настройки камеры под конкретные производственные задачи.