Траектория развития рынка резервного копирования

Екатерина ЮДИНА,
контент-инженер, облачный провайдер «ИТ-ГРАД» (входит в группу МТС)

Потеря ценных данных – всегда катастрофа. Причин, по которым повреждается информация, немало: начиная с человеческого фактора, физического взлома и заканчивая кражей с использованием вредоносного ПО. Минимизировать негативные последствия помогают системы резервного копирования, благодаря которым можно создавать копии данных с учетом заданного плана, а также восстанавливать информацию в случае потери.

Создать резервную копию несложно. Можно самостоятельно подключить внешний накопитель к компьютеру и скопировать содержимое жесткого диска. Но это примитивный вариант. Больше возможностей дают специализированные решения, которыми сегодня пользуются различные компании. Корпоративному сегменту не обойтись без серьезных инструментов, поскольку последствия от потери данных могут быть разными – вплоть до банкротства. Красноречивы цифры, которые показывают, что при отсутствии доступа к данным на протяжении десяти дней 93% компаний в течение года становились банкротами. Поэтому системы резервного копирования должны решать важнейшую задачу – предотвращать потерю данных.

Безусловно, каждая компания ищет решение «для себя». Выбор во многом зависит от сложности инфраструктуры, критичности бизнес-процессов, объема и типа резервируемых данных. К счастью, за последние десять лет BaaS-системы значительно трансформировались, и сегодня есть из чего выбирать.

Рассмотрим динамику развития рынка корпоративных систем резервного копирования и восстановления, новинки вендоров и перспективные тенденции на ближайшие годы.

Правило защиты «3-2-1»

Отдельные компании по-прежнему считают, что для реализации BaaS-стратегии достаточно использовать одну полную резервную копию и дополнять ее инкрементальными бэкапами. Но современные тенденции говорят об обратном. В частности, не стоит забывать о золотом правиле «3-2-1», которое впервые описал Питер Крог в книге «Управление цифровыми активами для фотографов». Как профессионал он понимал, что потеря личного фотоархива – катастрофа. Неудивительно, что BaaS-вендоры всех мастей рекомендуют придерживаться этого правила. Вот к чему оно призывает (рис. 1):

- создайте три резервные копии – основную и две дополнительные;
- храните резервные копии на двух типах носителей, например на локальном диске, сетевом ресурсе или NAS, ленточном накопителе и т. п.;
- храните одну копию за пределами локальной площадки, например в облаке.

Рис. 1.

Помимо создания бэкапов следует ответственно подойти к составлению плана резервного копирования. Резервные копии необходимо делать настолько часто, насколько вы не готовы потерять данные. Очень важен параметр Recovery Point Objective (RPO) – время, за которое можно потерять данные из-за инцидента. Его точная оценка и исполнение позволят не допустить серьезных последствий.

Резервное копирование в облако

Облачные сервисы переживают бум популярности. Все больше компаний выносят собственную инфраструктуру в облако провайдера – это удобно, быстро, экономически эффективно. Защищать от потери данных приходится не только локальные ресурсы, но и сложную, порой разрозненную инфраструктуру, в том числе виртуальную. Для таких задач лидеры «Магического квадранта» решений для резервного копирования и восстановления данных создают многофункциональные платформы, способные делать копии физических серверов, рабочих станций, виртуальных машин, файлов или отдельно взятых информационных систем как в on-premise, так и в облачных средах.

Облако часто рассматривается как ресурс для размещения резервных копий (рис. 2). Во-первых, при cloud-подходе ответственность за обслуживание аппаратной платформы перекладывается на облачного провайдера, во-вторых, хранение копий на альтернативной площадке – большой шаг в сторону защиты данных. Исследование Commvault, проведенное среди клиентов, показало, что свыше половины респондентов планируют в ближайшие 12 месяцев использовать облако в качестве резервной площадки, так как считают облачное хранилище важным технологическим достижением.

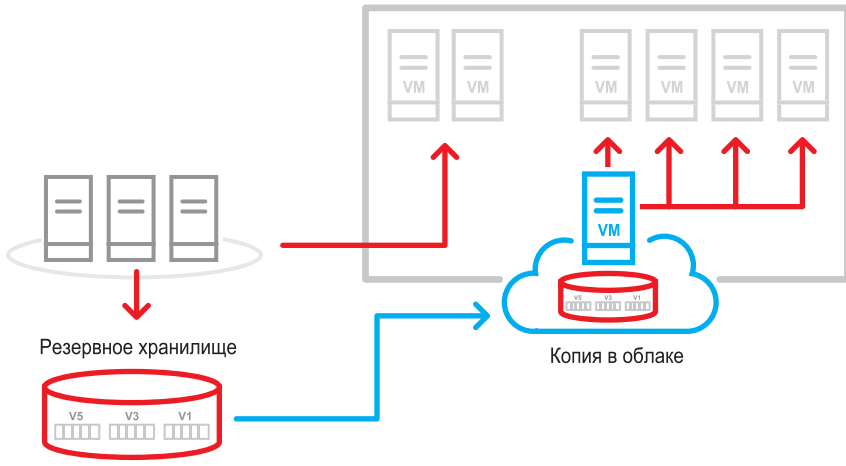

Рис. 2.

Поскольку услуга защиты корпоративных данных востребована среди заказчиков, облачные провайдеры предлагают клиентам сервис резервного копирования (BaaS). Используемый набор инструментов в составе услуги может различаться. В целом такие решения обеспечивают регулярное резервное копирование файлов, приложений, баз данных, серверов, рабочих станций, виртуальных машин или ИТ-инфраструктуры целиком. Как правило, клиент получает удобную панель управления и самостоятельно настраивает задачи резервного копирования ресурсов – локальных и облачных.

> Вымогатели – один из неприятных типов вредоносного ПО.

Защита от программ-вымогателей

Вымогатели – один из неприятных типов вредоносного ПО. Они блокируют доступ к данным до момента, пока компания не заплатит злоумышленникам. Причем нет гарантий, что после оплаты файлы будут разблокированы.

По словам бывшего сотрудника ФБР подразделения по борьбе с терроризмом и контрразведке Эрика О'Нила, убытки компаний от действий вымогателей составляют ежегодно 2 млрд долл. Атаки совершают не только профессиональные хакеры, но и пользователи сети Интернет с низким социальным статусом, желающие разбогатеть легким способом.

Поскольку атаки вымогателей направлены на данные, разработчики систем резервного копирования и восстановления стали оснащать собственные продукты функциями защиты. Например, специально созданное антивирусное программное обеспечение выполняет поиск вредоносного ПО исходя из базы сигнатур. Платформы резервного копирования используют технологии ИИ и машинного обучения для поиска аномалий с данными и успевают блокировать объекты, подвергающиеся атаке, до момента их заражения. Если инцидент все-таки произошел, данные можно мгновенно восстановить из резервной копии и быстро решить проблему с блокировкой. Поэтому производители систем резервного копирования и восстановления Acronis, Veeam, Commvault и другие уделяют так много внимания защите от вымогателей.

Аутсорсинг резервного копирования

Понятие аутсорсинга не ново для большинства компаний. Если можно поручить решение какой-либо задачи третьему лицу и это экономически выгодно, стоит обратить внимание на такое решение. Сегодня на аутсорсинг выносят многие ИТ-процессы, в том числе задачи резервного копирования и восстановления.

Облачные провайдеры предлагают BaaS-услуги. Кроме того, клиенты могут взять в аренду хранилища для резервных копий. Важная деталь: для адекватного использования сервиса требуется высокая скорость соединения (для восстановления) и поддержка платформы резервного копирования. В рамках стандартного решения клиенту предоставляется доступ к консоли, где он самостоятельно выбирает локальные или виртуальные серверы, физическое оборудование или рабочие станции. Дополнительно можно настроить планы резервного копирования, а при необходимости запустить процесс восстановления отдельных файлов, фрагментов данных, серверов или инфраструктуры целиком.

BaaS-вендоры постоянно совершенствуют и оптимизируют системы для работы в облаке. Так, комплекс Veeam Backup & Replication, интегрированный в виртуальную инфраструктуру облачного провайдера, предоставляет клиенту веб-интерфейс с возможностью управления всеми функциями сервиса (доступен из консоли vCloud Director). С помощью Veeam Cloud Connect Replication можно выполнять репликацию корпоративной инфраструктуры в облако, обеспечивая в случае аварии быстрое аварийное переключение как отдельных виртуальных машин, так и площадки целиком.

Мгновенное восстановление

В современных условиях не каждая компания может позволить себе тратить слишком много времени на восстановление данных. Зачастую даже кратковременный простой сервиса приводит к потере денег и снижению конкурентоспособности. Если, например, у онлайн-магазина повреждается база данных, у пользователей пропадает возможность заказа товаров через сайт, они уходят к конкуренту. Следовательно, компания терпит убытки и теряет клиентов. Запрос на мгновенное восстановление данных сформулировал задачу для разработчиков систем резервного копирования.

BaaS-вендоры понимают, что клиентам необходимо восстанавливать данные из копии как можно быстрее. Решения Veeam позволяют восстанавливать данные не только отдельно взятых файлов, но и с нескольких виртуальных машин одновременно.

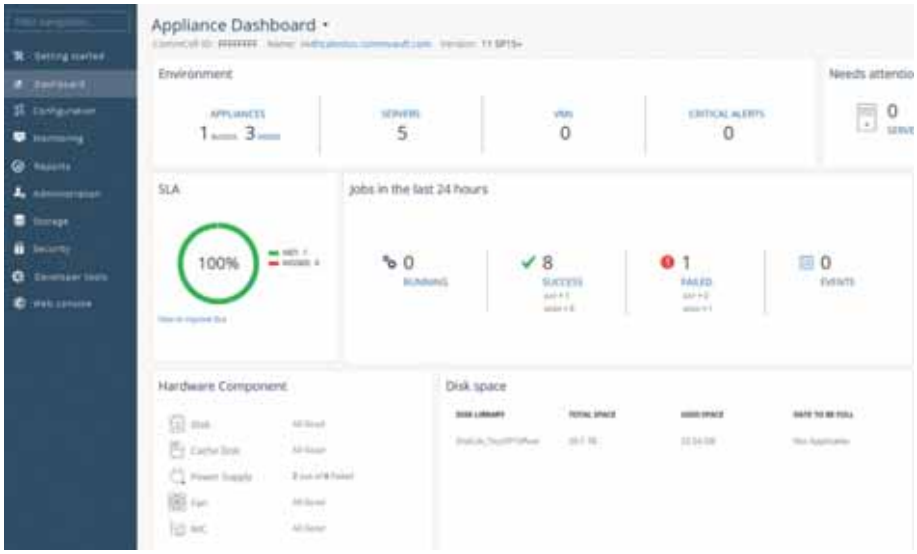

Рис. 3.

UI и UX

Лет пять-семь назад системы резервного копирования были настолько сложными в освоении, что для настройки требовалось проходить специальные курсы. Благодаря современному дизайну пользовательского интерфейса (UI) и проработке пользовательского опыта (UX) теперь освоить решение можно за несколько дней (рис. 3).

Несмотря на обилие BaaS-сервисов, клиенты по-прежнему ищут удобные инструменты управления, способные повысить скорость решения задач. Например, компания Commvault добавила в панель Commvault Command Center упрощенную, интуитивно понятную консоль. Основные ее преимущества: инновационный механизм индексации объектов и глобальный поиск, а также быстрое выполнение популярных задач с помощью команд (/GOTO, /HELP, /ADD и других команд для отдельных сущностей).

Заключение

Постоянно увеличивающиеся объемы данных диктуют новые требования к системам резервного копирования. С учетом этого вендоры предлагают рынку функционально гибкие инструменты. Помимо стандартных возможностей – создавать резервные копии и восстанавливать данные – решения помогают оптимизировать процессы, в том числе обеспечивая защиту информации от программ вымогателей. Сегодня практически все BaaS-сервисы оснащены удобным интерфейсом управления и поддерживают облачный подход. Поэтому клиенту остается лишь выбрать подходящее решение и использовать его, следуя лучшим практикам и рекомендациям. ■