

Обзор от ESG Lab

Расширенные возможности защиты с Acronis Backup 12.5

Автор: Винни Коински, ведущий аналитик ESG Lab

Аннотация

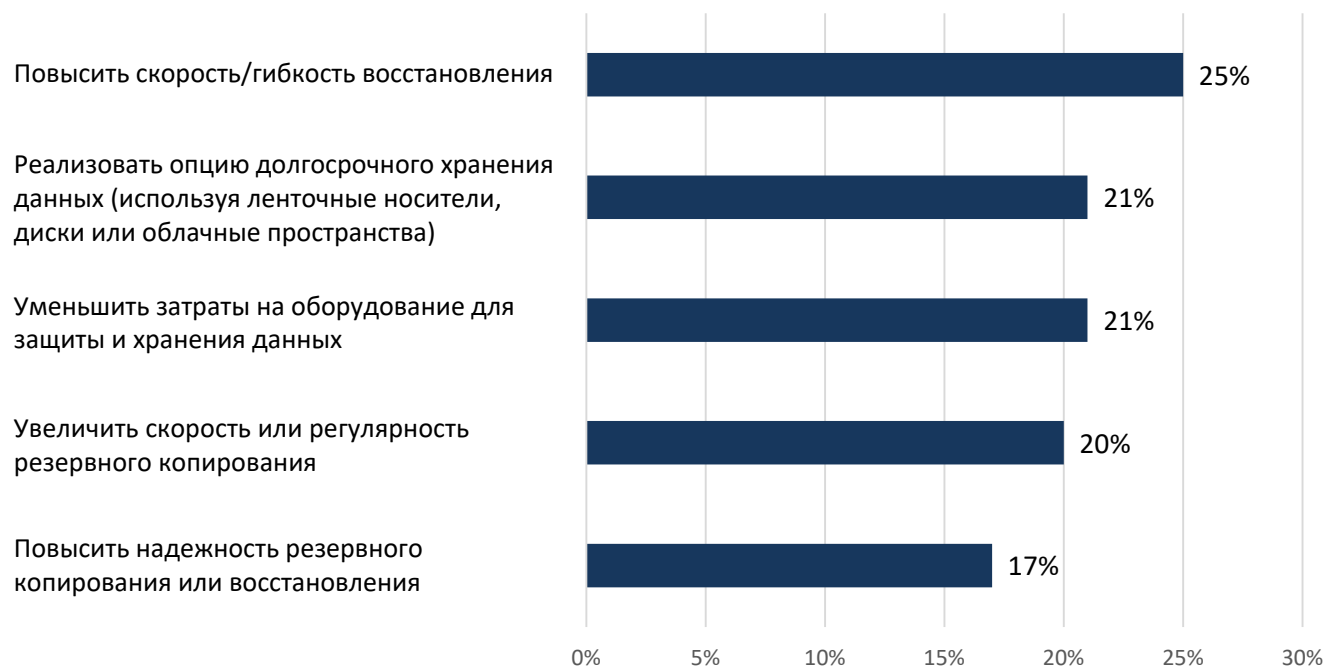
В настоящем докладе представлено практическое тестирование Acronis Backup 12.5 – решения для защиты данных. Результаты демонстрируют, как надежная система резервного копирования, восстановления и расширенной защиты помогает клиентам просто и эффективно защищать и восстанавливать критически важные системы и данные.

Задачи

Бизнес не может работать без своих данных, независимо от того, где они хранятся, а гибридные облачные ИТ-среды требуют от решений для защиты данных все больше и больше возможностей. Зачастую от современных решений ожидают не только функции резервного копирования и восстановления данных, но также аварийного восстановления и возможности использования на физических, виртуальных, удаленных и облачных системах. В недавнем опросе в рамках исследования ESG 25% респондентов отметили высокую скорость/гибкость процесса восстановления как одну из самых важных требований ИТ-менеджмента, выведя его в топ ответов (см. Рис. 1). В дополнение, это же исследование показало серьезное стремление ИТ-менеджмента повысить надежность как систем резервного копирования, так и восстановления.

Рис. 1. Топ-5 требований ИТ-менеджмента к защите данных

Какие наиболее важные требования к защите данных выдвигает ИТ-менеджмент Вашей компании?
(% респондентов, N=387, возможно дать 3 ответа; на графике показаны 10 наиболее частотных ответов)



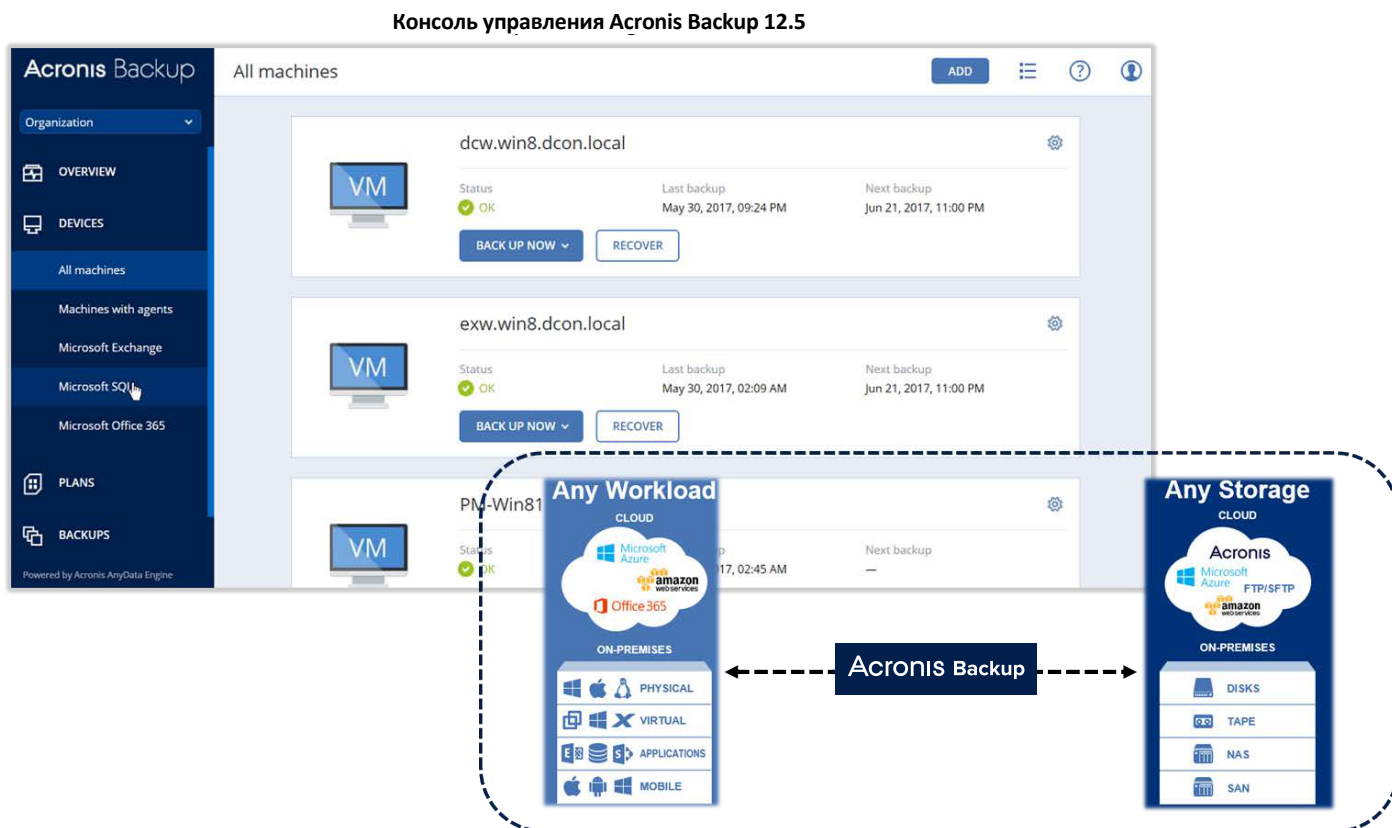
Источник: Enterprise Strategy Group, 2017

¹ Источник: Доклад об исследовании ESG: Тренды модернизации систем защиты данных.

Решение: Acronis Backup 12.5

Acronis Backup 12.5 объединяет защиту облачных и локальных данных в единое решение, созданное для быстрого и надежного восстановления критически важных приложений. ПО управляется при помощи понятной и удобной веб-консоли. Как показано на Рис. 2, оно защищает весь бизнес целиком, включая физические и виртуальные серверы и рабочие станции, открытые/частные облачные инфраструктуры, а также мобильные приложения и устройства. СРК поддерживает хранение резервных копий как в локальных, так и в облачных хранилищах, позволяя вам полностью контролировать расположение ваших данных, систем и резервных копий.

Рис. 2. Обзор решения



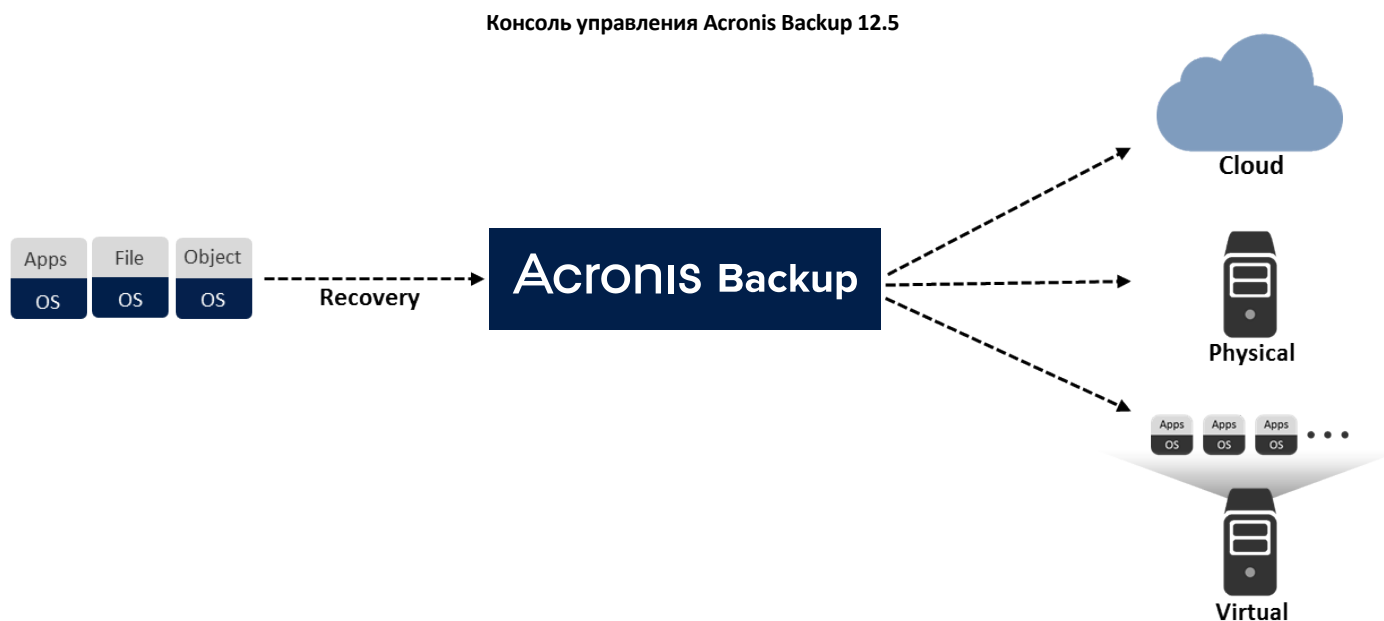
Источник: Enterprise Strategy Group, 2017

Ключевые функции решения включают в себя:

- Резервное копирование полных образов физических, виртуальных и облачных систем.
- Резервное копирование виртуальных машин VMware vSphere и Microsoft Hyper-V в режиме «с агентами» или «без агентов».
- Масштабирование до 2000 устройств за одну установку.
- Резервное копирование для конечных пользовательских устройств, таких как ПК, ноутбуки и мобильные устройства.
- Оптимизированное использование глобальной компьютерной сети (WAN). Репликация, аварийное переключение и восстановление после отказа виртуальных машин VMware.
- Простая в использовании веб-консоль для управления всеми физическими системами, виртуальными машинами и облачными пространствами, резервными копиями приложений и конечных систем.
- Acronis Active Protection – защита от программ-вымогателей, предупреждающая их атаки.
- Acronis Notary, использующий технологию блокчейн для аутентификации и проверки подлинности данных резервных копий.
- Снапшоты сетей хранения данных (SAN), уменьшающие нагрузку на гипервизоры, используя аппаратные снапшоты для резервного копирования.
- Резервное копирование в режиме «off-host», которое уменьшает нагрузку на систему, делегируя задачи копирования на отдельный агент.

Acronis Backup 12.5 позволяет малому и среднему бизнесу копировать свои данные на непосредственно подключенный носитель, в сетевое хранилище NAS, SAN или в облачные хранилища Acronis Cloud Storage или Microsoft Azure. Такая гибкость системы обеспечивает расширенные возможности оперативного восстановления. С Acronis Backup 12.5 клиенты могут восстанавливать свои данные, где бы они не находились, в любой момент времени. Как видно на Рис. 3, приложение, файл, или любой другой объект данных может быть легко восстановлен на облачные, физические или виртуальные системы.

Рис. 3. Обзор процесса восстановления



Источник: Enterprise Strategy Group, 2017

Ключевые функции восстановления включают в себя:

- Acronis Startup Recovery Manager для быстрого восстановления систем Windows.
- Восстановление машин Windows или Linux на то же самое или отличающееся оборудование, включая виртуальные и облачные среды.
- Резервное копирование и восстановление систем Mac с устройства на устройство.
- Acronis Instant Restore, предлагающий гибкий выбор опций восстановления за считанные минуты.
- Отслеживание изменений блоков данных (СВТ) для оптимизации процесса восстановления данных, обновленных с момента последнего резервного копирования.
- Восстановление файлов, папок, баз данных, почтовых ящиков, электронных писем и др.
- Гранулярное восстановление из резервных копий Exchange и SharePoint.
- Автоматизированное восстановление «на голое железо» с настраиваемыми установочными файлами.
- Возможность восстановления «на голое железо» удаленных офисов посредством WAN для сокращения времени простоя.
- Репликация резервных копий в различные хранилища для уменьшения риска возникновения ситуаций, когда восстановление невозможно.
- Аутентификация данных Acronis Notary для обеспечения целостности восстановленных данных.

Проверено ESG Lab

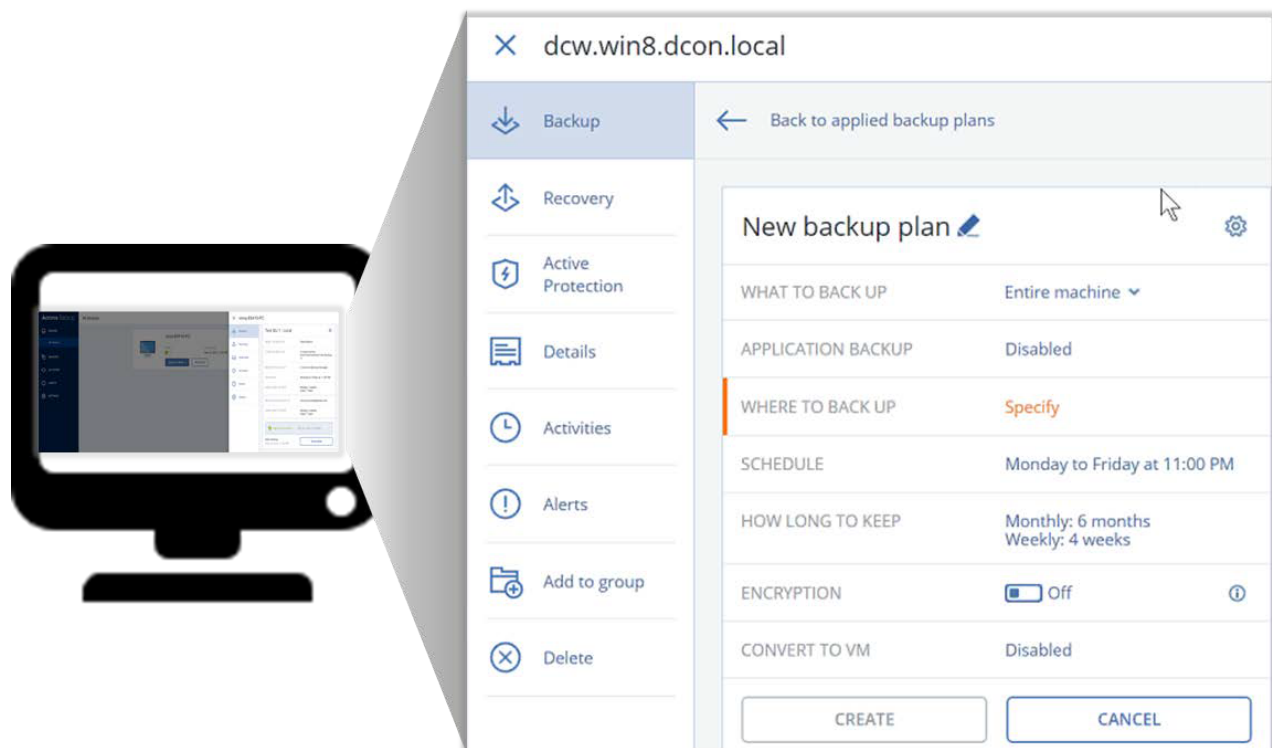
ESG Lab провел удаленный практический анализ Acronis Backup 12.5, используя демо-среду Acronis Cloud и пробную версию Acronis, в корпоративном офисе в г. Милфорд, США. Результаты анализа демонстрируют, как надежная система резервного копирования, восстановления и расширенной защиты помогает клиентам просто и эффективно защищать, и восстанавливать критически важные системы и данные.

Простота использования

В этой части доклада описывается опыт использования интерфейса администратора Acronis Backup 12.5 для настройки и выполнения различных сценариев процессов резервного копирования и восстановления, таких как, например, простое восстановление и резервное копирование файлов, восстановление писем MS-Exchange, восстановление виртуальных машин при помощи Acronis Instant Restore. В процессе тестирования ESG Lab использовал демо-среду Acronis Cloud, а также локальное приложение на небольшом сервере Windows с дисковым хранилищем USB. Демо-среда Acronis Cloud позволила нам протестировать более сложные сценарии, в то время как локальное приложение позволило нам детально разобрать возможности графического интерфейса.

Как показано на рис. 4, ESG Lab использовал демо-среду Acronis Cloud для конфигурации плана резервного копирования для сервера Microsoft Exchange с именем dcw.win8.dcon.local в тестовой среде. Интерфейс делает процесс настройки простым, позволяя с легкостью выбрать, что копировать, куда копировать, настроить расписание копирования, а также определить время хранения копии. Для того чтобы перейти к расширенным настройкам, необходимо нажать на пиктограмму «шестерёнка», которая находится справа от поля редактирования плана резервного копирования.

Рис. 4. Настройка плана резервного копирования

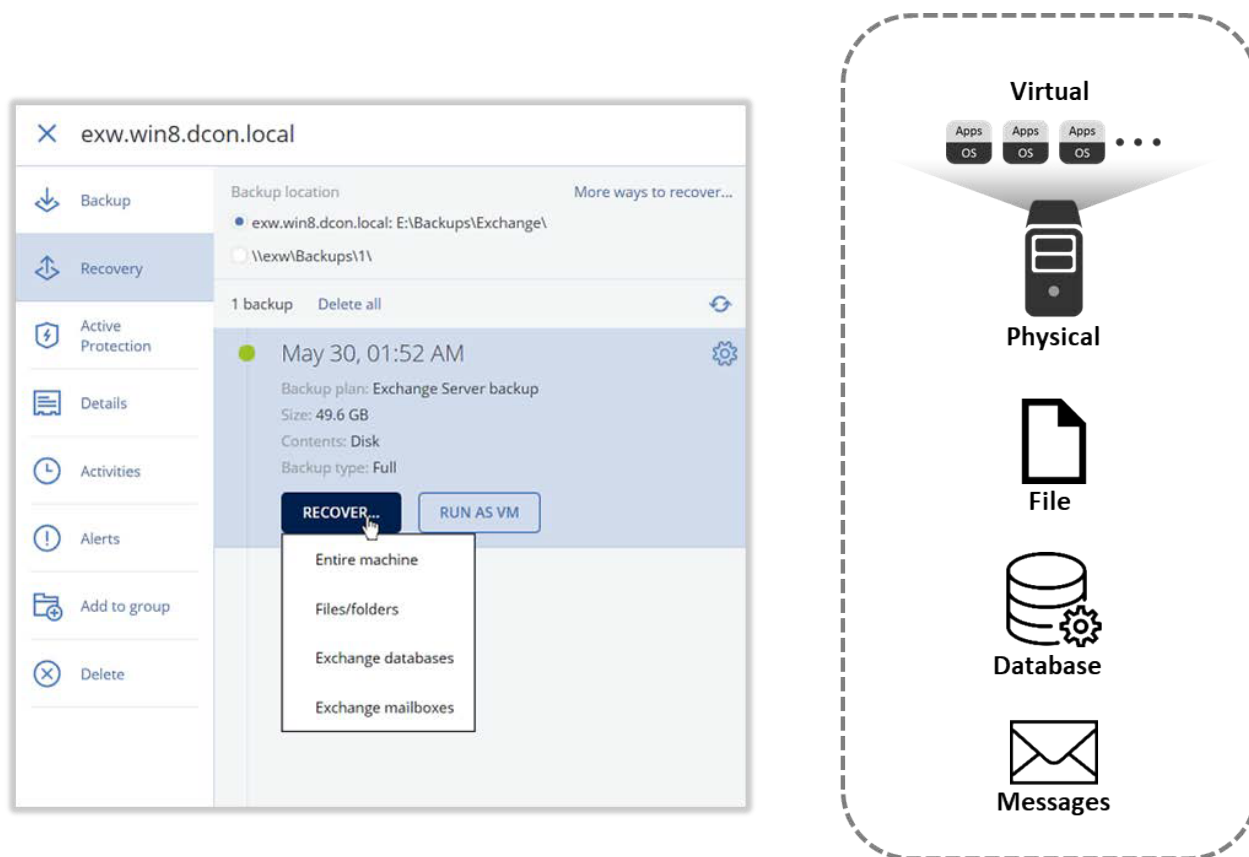


Источник: Enterprise Strategy Group, 2017

Мы также использовали 30-дневную пробную версию для использования 1 Тб из Acronis Cloud Storage в качестве локальной тестовой среды. В качестве локального хранилища резервных копий был использован SSD-накопитель емкостью 250 Гб. Локальным хранилищем резервных копий была обычная папка под названием «Acronis Backup Storage», созданная на внешнем SSD-накопителе. Локальное и облачное хранилища были использованы в разных сценариях. ESG Lab успешно провел резервное копирование и восстановление файлов, папок и состояний систем, используя локальное хранилище и Acronis Cloud.

Далее, как показано на Рис. 5, ESG проверил способность Acronis Backup 12.5 восстанавливать отдельные сообщения MS-Exchange. Для этих целей была использована демо-среда Acronis, в которой был запущен сервер Exchange. Мы удалили два сообщения из тестового аккаунта Outlook и использовали интерфейс Acronis Backup 12.5, чтобы восстановить сообщения обратно в почтовый ящик. Интерфейс позволяет с легкостью найти резервные копии удаленных сообщений и даже предлагает предварительно просмотреть текст сообщения и прикрепленные файлы перед восстановлением.

Рис. 5. Настройка стратегий резервного копирования



Источник: Enterprise Strategy Group, 2017

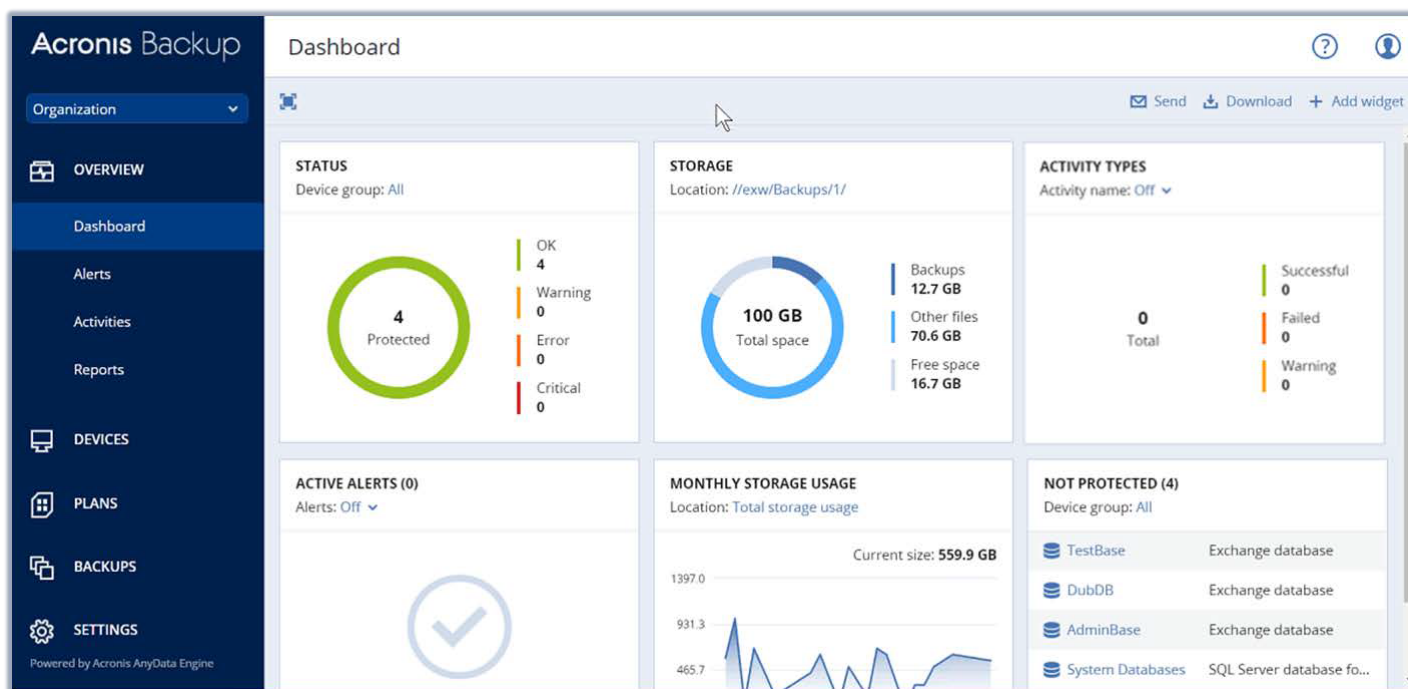
Мы использовали ту же самую демо-среду для выполнения мгновенного восстановления виртуальной машины из образа в резервной копии. Мы выбрали машину Windows Hyper-V с резервной копией всей системы. Далее мы выбрали опцию запуска в качестве виртуальной машины. С сервера Windows Hyper-V мы наблюдали за процессом и удостоверились в том, что виртуальная машина появилась и начался процесс загрузки. Это заняло примерно 12 секунд. Еще через несколько секунд виртуальная машина полностью инициализировалась, и мы смогли получить доступ к ее консоли.

Затем ESG Lab использовал локальную тестовую среду для дальнейшего изучения графического интерфейса, протестировав расширенные опции настройки резервного копирования. Стоит заметить, что для каждого устройства, добавленного в среду, Acronis создает настройки резервного копирования по умолчанию, чтобы было проще начать пользоваться программой. Эти настройки, включая название плана резервного копирования, тип резервного копирования (напр., файл, приложение или вся система в целом), объект резервного копирования, расположение хранилища, расписание, срок хранения и репликация, могут быть легко подстроены конкретно под ваши требования. Функция репликации позволяет устанавливать различные сроки хранения для реплицированных данных. Интерфейс позволяет очень детально настроить резервное копирование. А настройки по умолчанию позволяют быстро запустить систему сразу после установки.

Наконец, как показано на Рис. 6, мы изучили новые функции визуализации, доступные в версии 12.5. Эти функции находятся в разделе Обзор в меню слева. Функции отображаются на новой панели мониторинга, предоставляющей

настраиваемое представление инфраструктуры системы резервного копирования. Можно легко добавить различную информацию в виде таблиц, диаграмм, графиков или виджетов, как, например, виджеты Статус, Хранилище и Тип Активности в верхнем ряду на Рис. 6. Виджеты можно перемещать и удалять. Уведомления и последние действия в виде детализированных списков отображаются на отдельных страницах для тщательного мониторинга и быстрого устранения неполадок. Эту информацию можно экспортировать в виде настраиваемого отчета PDF или MSExcel, которые могут, согласно графику, рассылаться соответствующим получателям, например, администраторам департаментов или удаленных офисов. Кроме этого, стоит уделить внимание вкладке Организация вверху раздела Обзор. Именно здесь можно настроить управление системой сразу несколькими офисами или департаментами. Во вкладке Организация можно создать роли администраторов для разных отделов, филиалов и удаленных офисов. Администратор имеет доступ к конкретным устройствам, которыми он управляет. Администраторы организации имеют доступ ко всей среде.

Рис. 6. Наглядность решения



Источник: Enterprise Strategy Group, 2017

Почему это важно

Простота использования – важный элемент в работе малого и среднего бизнеса, где ИТ-отделу зачастую приходится выполнять много функций одновременно, но это лишь одна сторона юзабилити в целом. Не менее важен тот факт, что решение для защиты данных поддерживает всю среду и отличается особой гибкостью, чтобы отвечать всем требованиям компании к защите данных.

ESG Lab считает, что решение является не только простым в управлении, но также очень функциональным. Оно включает в себя все атрибуты, необходимые для защиты данных компании, а легкие в использовании опции делают его идеальным выбором для малого и среднего бизнеса. В процессе тестирования мы смогли легко настроить параметры (напр., местоположение хранилища, частота резервного копирования, срок хранения копий) на очень гранулярном уровне. Мы также использовали новую панель отображения данных мониторинга, уведомления, историю действий и отчеты для простого и интуитивного контроля за защитой всей среды.

Эффективность использования ресурсов

В этой части доклада ESG изучает две новые возможности Acronis Backup 12.5, которые влияют на общую эффективность использования ресурсов: снимки сетей хранения данных (SAN) и резервное копирование в режиме «off-host». Эти элементы улучшают масштабируемость решения и показатели RPO благодаря переносу нагрузки с критических систем. В первую очередь был изучен процесс создания снимков SAN для защиты виртуальных сред. Для этой конфигурации Acronis Backup 12.5 использовал API для настройки взаимодействия как гипервизора виртуальных машин, так и системы SAN. Как показано на Рис. 7, для данной среды в качестве хранилища SAN, содержащего базу данных виртуальных машин, была использована система NetApp по протоколу NFS, подключенная к платформе виртуализации.

Чтобы выполнить резервное копирование снимка SAN, приложение Acronis Backup сперва через API сделало вызов к хосту гипервизора, который создал снимок на уровне виртуальных машин. Далее, приложение через API сделало вызов к системе хранения данных, чтобы мгновенно сделать снимок тома, который содержит базу данных виртуальных машин. Как только снимок хранилища был создан, снимок на уровне виртуальных машин был снят. Далее, снимок тома был отправлен на сервер, на котором запущен агент Acronis. Данные резервной копии были переданы агентом Acronis в хранилище. Передача данных резервной копии никак не повлияла на производительность виртуальных машин, а снимок на уровне виртуальных машин был доступен только на короткое время для приведения базы данных в неизменяемое состояние. Для контроля над ветвлением снимков, снимок хранилища был удален сразу после окончания процесса резервного копирования. Необходимо отметить, что весь процесс управлялся при помощи интуитивно понятного меню настроек Acronis. Нам были необходимы лишь имя и учетные данные системы хранения NetApp для завершения настройки. Машины, которые имели доступ к хранилищу NFS и на которых был установлен агент Acronis, были заранее настроены на доступ к NFS и отображались в списке опций в меню. Доступ к API был также предварительно настроен для различных сценариев. Нам понадобилось лишь выбрать конфигурацию, включающую снимок ESXi.

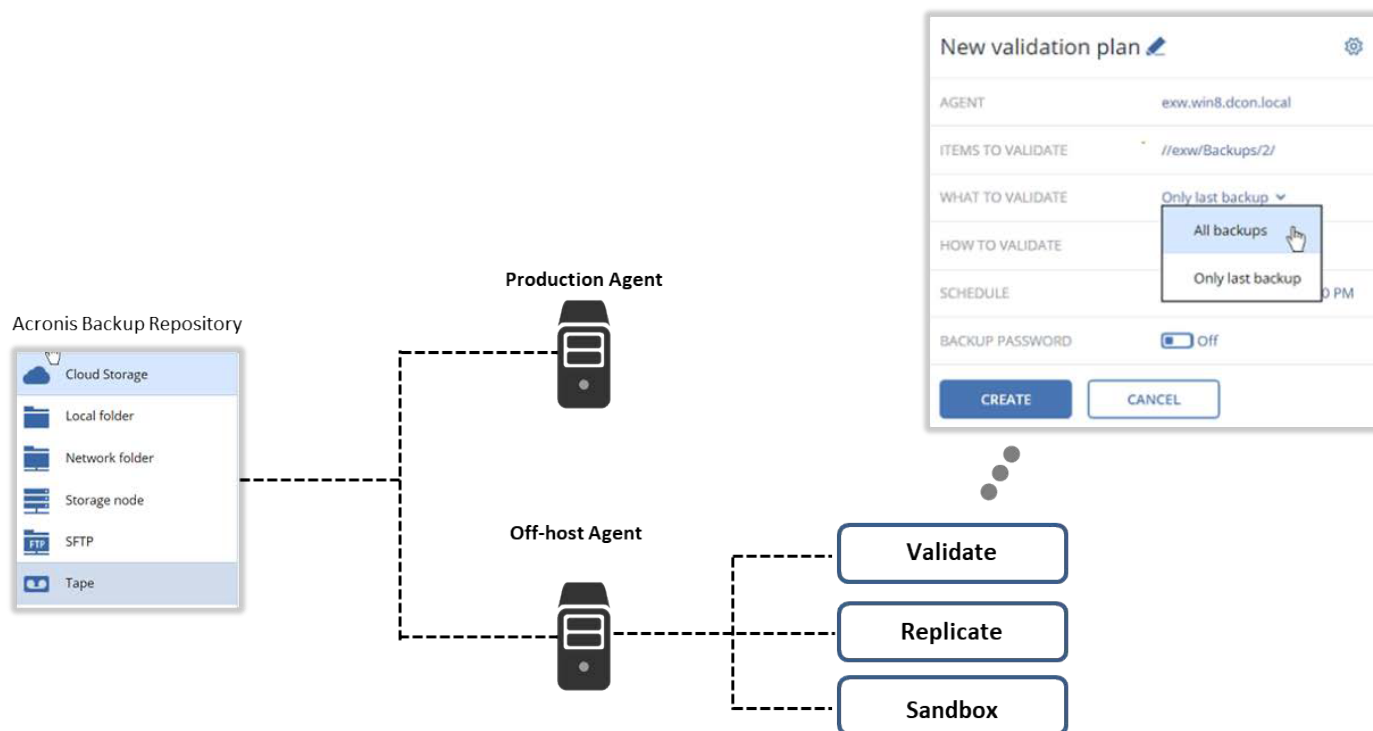
Рис. 7. Снимок сети хранения данных (SAN)



Источник: Enterprise Strategy Group, 2017

Более того, мы изучили возможность делегирования задач по управлению защитой данных, таких как валидация, репликация, дедупликация и даже создание песочниц, на другой хост. Эта возможность повышает доступность системных ресурсов для рабочих приложений благодаря сокращению количества ресурсов, необходимых для операций по защите данных. Как показано на Рис. 8, выполнение таких задач (например, валидация) в режиме «off-host» может быть легко настроена при помощи меню в пользовательском интерфейсе Acronis Backup. ESG использовал меню New для настройки верификации контрольных сумм для рабочего сервера, находящегося под защитой Acronis Backup 12.5. Чтобы запустить процесс сверки контрольных сумм, агенту «off-host» понадобился лишь доступ к образам резервных копий на рабочем сервере, хранящимся в хранилище резервных копий. Этот же процесс может использоваться для репликации, дедупликации, реализации стратегии D2D2C или даже для переноса виртуальных машин в песочницу для валидации или тестовых операций, если инфраструктура поддерживает этот процесс.

Рис. 8. Резервное копирование в режиме «off-host»



Источник: Enterprise Strategy Group, 2017

i Почему это важно

Мы зачастую забываем, какую большую роль гибкость и оперативность могут играть в общей производительности решения для защиты данных. Дело не только в том, насколько быстро какая-нибудь порция данных может быть перемещена из точки А в точку В. Маловероятно, что компания готова выделять все свои аппаратные ресурсы, для того чтобы добиться максимальной производительности во время резервного копирования. Более важно иметь возможность применить правильные ресурсы там, где необходимо удалить копию приложения по защите данных с рабочего хоста как можно быстрее.

ESG Lab убедился в том, что благодаря снапшотам SAN и резервному копированию в режиме «off-host» пользователи Acronis Backup 12.5 могут эффективно применять защиту данных там, где необходимо, с минимальным использованием системных ресурсов, необходимых для рабочих приложений. Мы считаем, что сочетание этих функций значительно повышает общую эффективность защиты данных Acronis Backup 12.5.

Расширенная защита

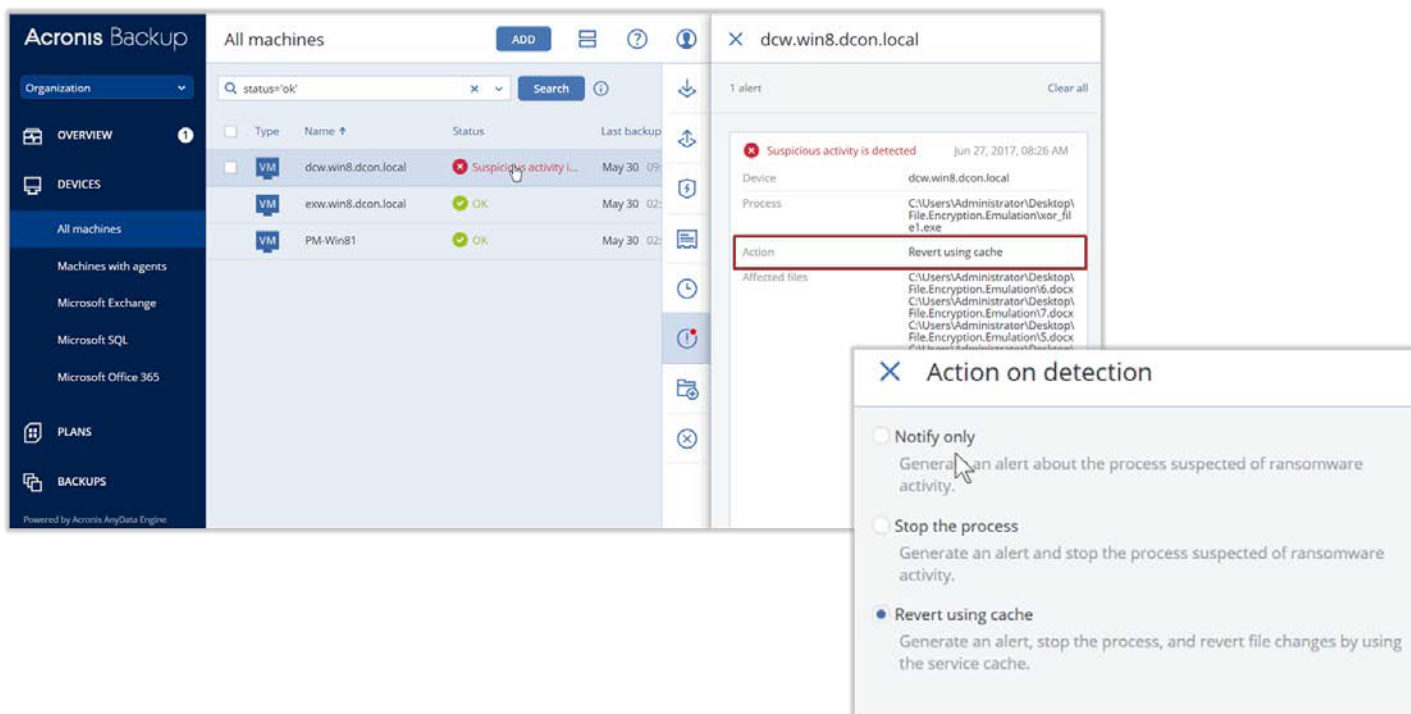
В этой части доклада рассматриваются новые функции Acronis Backup 12.5: Acronis Active Protection и Acronis Notary, которые выходят за рамки традиционной концепции функциональных возможностей решения для резервного копирования и восстановления данных. Первая функция - Acronis Active Protection, дополняет существующие решения для защиты, помогая компаниям обнаруживать, прекращать и мгновенно восстанавливать данные после вредоносных действий, которые могут сделать корпоративные данные недоступными. Вторая функция - Acronis Notary, помогает обеспечивать подлинность корпоративных данных, что обычно является задачей отдела внутреннего контроля компании.

Тестирование функций расширенной защиты ESG начал с изучения возможностей Acronis Active Protection. Эта функция включена в приложение Acronis Backup 12.5 и может быть запущена на любом устройстве инфраструктуры. После запуска приложение в реальном времени следит за вредоносными действиями на устройстве, которые зачастую выявляются только тогда, когда большой объем данных уже зашифрован, или изменены их расширения. Если подозрительная активность обнаружена, приложение предпринимает меры согласно конфигурации. Во время тестирования мы использовали скрипт, симулирующий вредоносное шифрование тестовых файлов и папок.

После того как скрипт был запущен, как показано на Рис. 9, мы кликнули на уведомление об обнаружении подозрительных действий, чтобы увидеть детальное описание события. Описание включает в себя имя пораженного устройства, название и адрес файла, спровоцировавшего уведомление, действие, которое было предпринято, а также файлы, которые были изменены. Для этого тестового сценария мы использовали кэшированные данные Acronis Active Protection для возвращения к изначальному состоянию файлов.

Меню настройки Acronis Backup в правой нижней части на Рис. 9 показывает список доступных мер, которые могут быть предприняты при обнаружении вредоносной активности. Эти меры включают в себя просто уведомление, остановку процесса и остановку процесса и возвращения к изначальному состоянию файлов.

Рис. 9. Acronis Active Protection

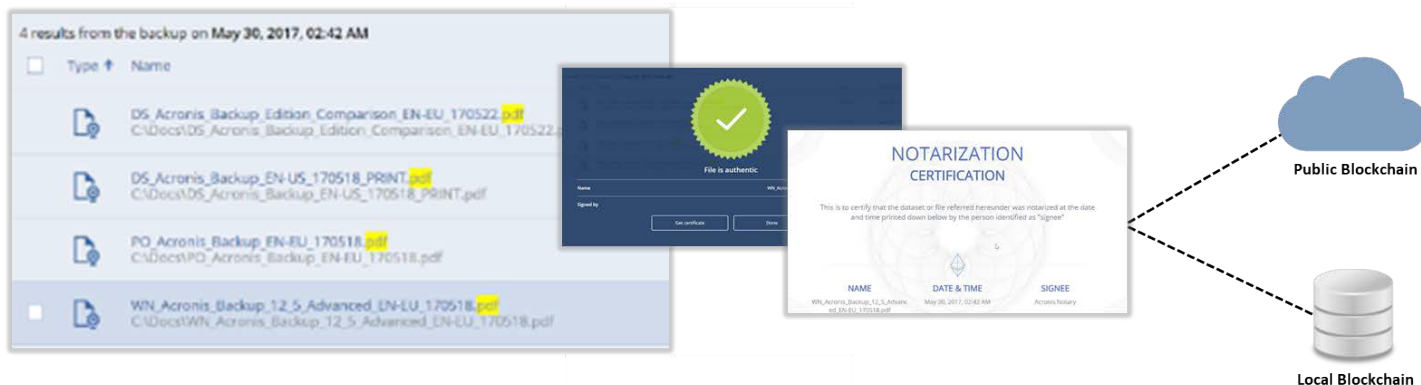


Источник: Enterprise Strategy Group, 2017

Наконец, ESG Lab изучил функцию Acronis Notary, теперь доступную в Acronis Backup 12.5, которая использует технологию распределенного реестра для обеспечения неизменности и подлинности данных и транзакций, называемую блокчейн. Технология блокчейн была впервые использована в финансовой сфере для регистрации и подтверждения транзакций. Она быстро стала стандартом в самых разных индустриях, таких как финансы, банкинг, логистика, производство, и стала использоваться для подтверждения и аудита данных. Acronis Notary использует блокчейн для обеспечения достоверности данных при помощи временных меток и ссылок на предыдущие блоки в цепочке.

Как показано на Рис. 10, мы включили Acronis Notary в план резервного копирования, чтобы подтвердить подлинность нескольких файлов во время процесса резервного копирования. Для этого Acronis Notary в фоновом режиме выполнил сложные задачи по созданию уникальных хэш-значений (SHA-2) и организации информации в виде особой структуры данных (Merkle Patricia tree). Он также зафиксировал транзакцию в публичном блокчейне Ethereum, чтобы подтвердить, что файл действительно находился в резервной копии во время его заверения. Эта схема проверки подлинности данных также предоставляет гибкий выбор того, как и где долгосрочные архивные данные обрабатываются и хранятся.

Рис. 10. Acronis Notary



Источник: Enterprise Strategy Group, 2017



Почему это важно

В области современных бизнес-сред, которые должны быть доступны всегда и везде, технологии не стоят на месте, особенно если речь идет о безопасности и защите информации. Границы между защитой данных, безопасностью и контролем соответствия нормативным требованиям стираются. После серии крупных атак на данные за последние несколько лет, улучшение безопасности и управление рисками стали одной из главных статей инвестиций для любой ИТ-компании.

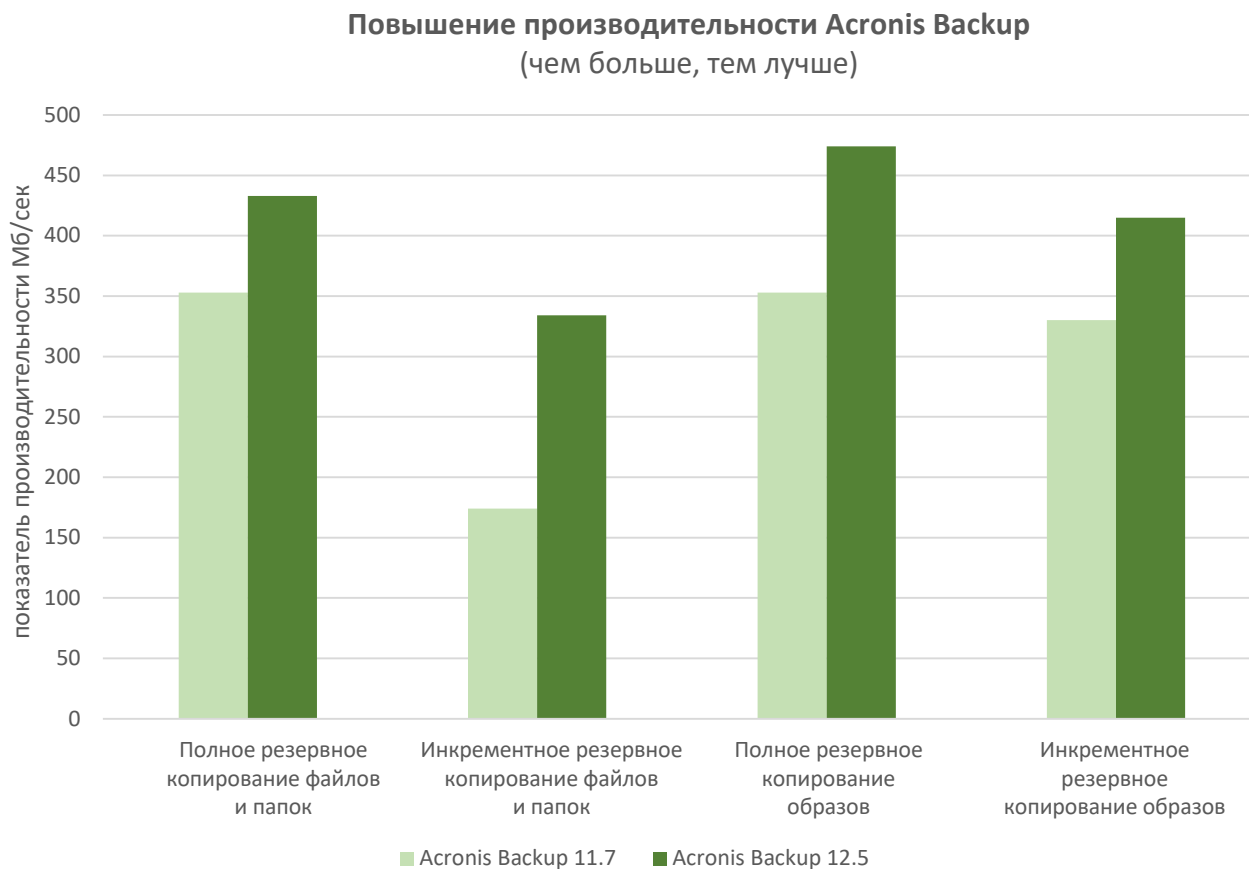
ESG подтверждает, что вместе с Acronis Active Protection и Acronis Notary, Acronis Backup 12.5 ушел далеко за рамки традиционных ожиданий от решений для резервного копирования и восстановления. ESG подтверждает, что Acronis Active Protection повышает степень защиты, предоставляемой решением, и не вызывает конфликтов с другими программами-антивирусами. А возможность подтверждения подлинности и целостности данных при помощи Acronis Notary необходима для соблюдения нормативных требований и создания стратегий по долгосрочному хранению данных.

Повышение производительности

Производительность является важным компонентом в любом решении для резервного копирования, и последняя версия Acronis Backup предлагает пользователям значительное ее повышение. С целью ее тестирования ESG изучил тестовую среду разработки Acronis и проверил результаты трех разных тестов на производительность. Тесты включают в себя сравнение производительности с другой версией Acronis, сравнение с производительностью конкурентного продукта для резервного копирования и восстановления файлов и папок, а также сравнение с производительностью конкурентного продукта для резервного копирования и восстановления образов.

Как показано на Рис. 11, ESG начал изучение производительности с сравнения результатов Acronis Backup 12.5 с Acronis 11.7. На Рис. 11 показаны результаты полного и инкрементного резервного копирования файлов и папок и полного и инкрементного резервного копирования образов двух версий. Тестовые данные включают в себя реальные пользовательские данные из рабочей среды.

Рис. 11. Повышение производительности



Источник: Enterprise Strategy Group, 2017

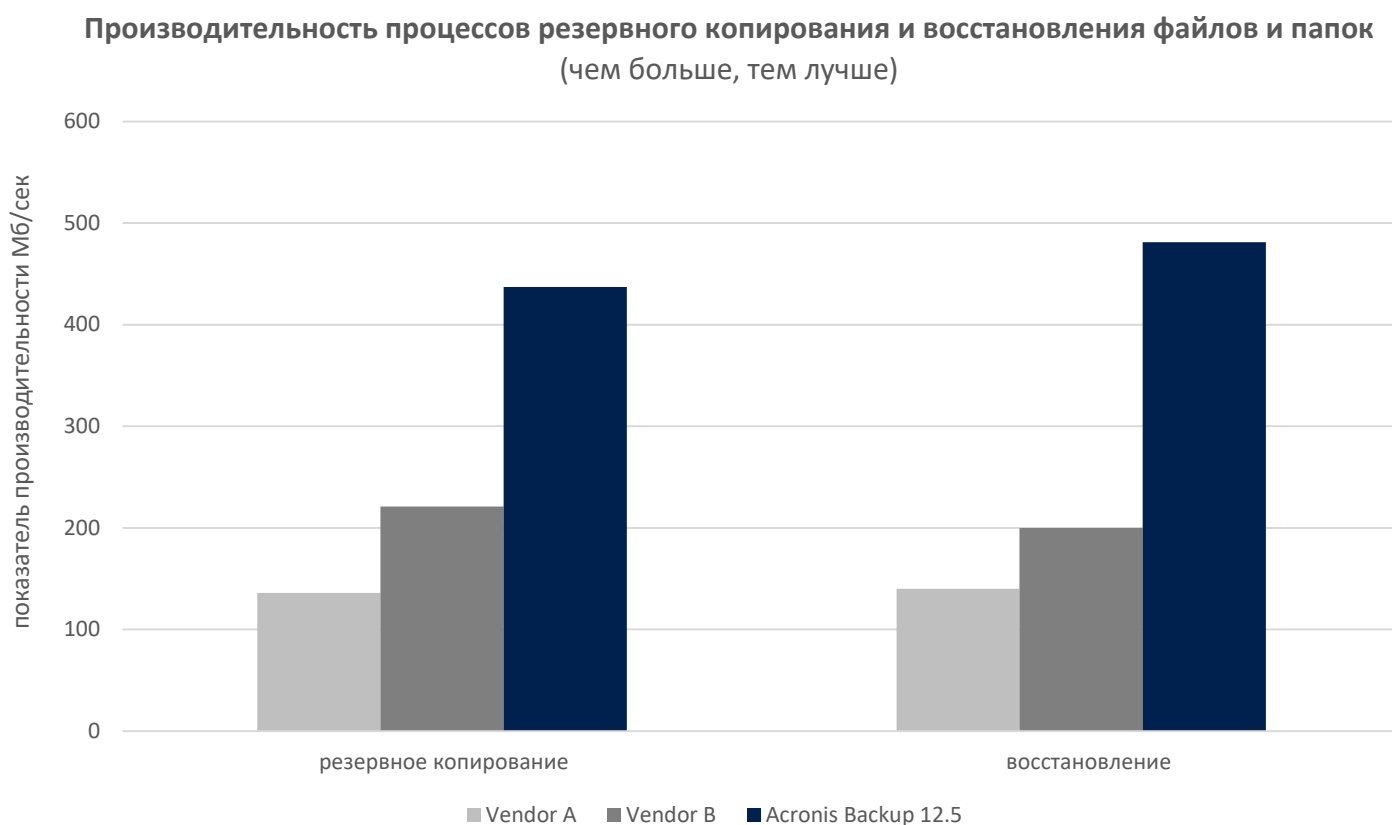
Что означают эти цифры

- Производительность Acronis Backup 12.5 при полном резервном копировании файлов и папок на 18% выше производительности версии 11.7.
- При инкрементном резервном копировании файлов и папок производительность версии 12.5 на 48% выше производительности версии 11.7.
- Производительность Acronis 12.5 при полном резервном копировании образов на 20% выше производительности версии 11.7.
- Производительность версии 12.5 при инкрементном резервном копировании образов на 20% выше производительности версии 11.7

Далее, как показано на Рис. 12, ESG сравнил производительность процессов резервного копирования и восстановления с Acronis Backup 12.5 и двумя другими известными продуктами. На Рис. 12 показаны результаты резервного копирования и восстановления файлов и папок с агентом. В качестве тестовых данных были использованы те же самые данные, что и в предыдущем сценарии. В качестве оборудования был использован сервер Supermicro с процессором Xeon E5-2640 и 128 ГБ RAM для хостинга каждого приложения во время теста. Объектом резервного копирования был дисковый массив RAID-0 объемом 7.2 Тб со значением stripe-size 256 Кб, сделанном из четырех дисковых устройств с 7200 об./мин.

На Рис. 12 Производитель А – это традиционное agent-based-решение для среднего бизнеса, которое изначально предназначалось только для защиты данных на физических устройствах. Сегодня оно поддерживает как физические, так и виртуальные среды. Производитель Б начинал как решение для резервного копирования только виртуальных сред, а теперь оно поддерживает и физические системы с агентами на Windows и Linux.

Рис. 12. Резервное копирование и восстановление файлов и папок



Источник: Enterprise Strategy Group, 2017

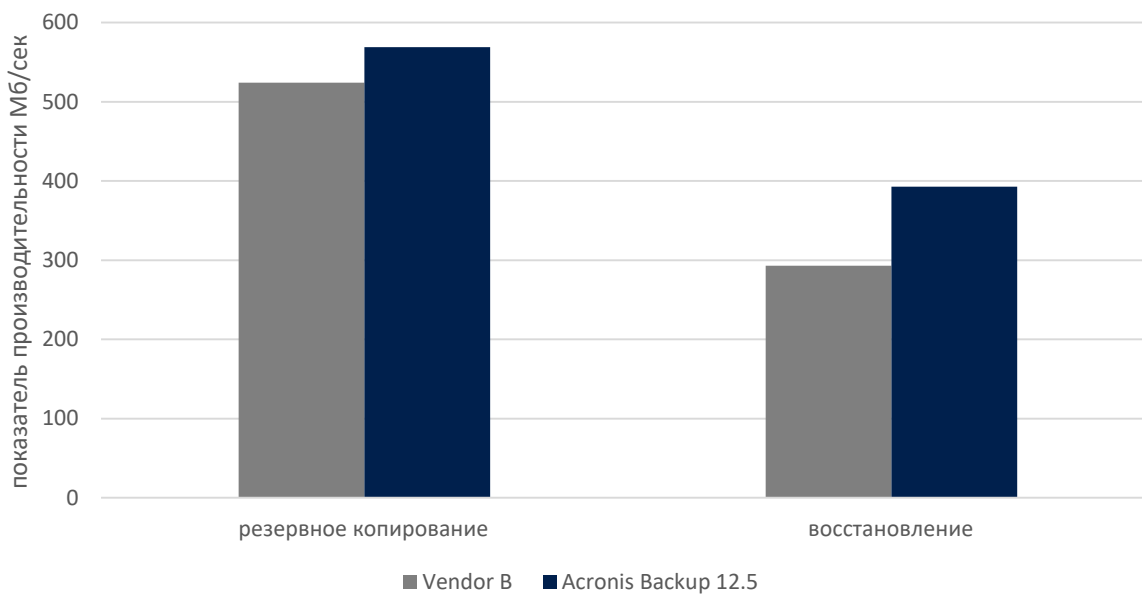
Что означают эти цифры

- При резервном копировании файлов и папок производительность Acronis выше вендора А на 69%.
- При восстановлении файлов и папок производительность Acronis выше вендора А на 71%.
- При резервном копировании файлов и папок производительность Acronis Backup 12.5 выше вендора Б на 49%.
- При восстановлении файлов и папок производительность Acronis Backup 12.5 выше вендора Б на 58%.

Наконец, на Рис. 13 показаны результаты производительности резервного копирования и восстановления образов виртуальных машин в сравнении с возможностями защиты данных виртуальных сред Производителя Б.

Рис. 13. Резервное копирование и восстановление образов

Производительность процессов резервного копирования и восстановления образов виртуальных машин (чем больше, тем лучше)



Источник: Enterprise Strategy Group, 2017

Что означают эти цифры

- Производительность резервного копирования образов при помощи Acronis Backup 12.5 на 8% больше вендора Б.
- Acronis Backup 12.5 показывает на 25% больше производительности при восстановлении образов, чем вендора Б



Почему это важно

Согласно исследованию ESG, три проблемы: защита данных, стоимость оборудования и быстрый рост объемов данных – с 2015 г. остаются самыми приоритетными в области хранения данных. В то время как в 2017 г. защита данных заняла первое место в списке этих задач, всеобщая проблема хранилищ данных остается неизменной – рост данных ускоряется, а хранение и защита данных становится все более сложной и дорогой задачей. Для решения этих проблем, производителям продуктов для защиты данных необходимо постоянно стремиться к повышению производительности.

ESG подтверждает, что, с каждым новым релизом, Acronis предпринимает значительное количество усилий для улучшения производительности и эффективности Acronis Backup, а также значительные усилия для того, чтобы соответствовать современным вызовам индустрии и своевременно отвечать на них.

²Источник: ESG brief, 2017 Storage Trends: Challenges and Spending, август 2017.

Заклучение

Современные ИТ-среды постоянно меняются: сегодня можно с трудом встретить среду без виртуализации и без облачных технологий. Зачастую именно эти окружения используются для запуска критических приложений на физических серверах или как локальное хранилище, потому что некоторым приложениям лучше всего подходит именно такие среды.

Устаревшие приложения, которые нельзя перенести на другую систему в ближайшем будущем, и приложения, которые требуют особую локальную инфраструктуру для запуска критических бизнес-процессов, делают задачу внедрения простого в управлении и использовании решения для защиты данных все более трудной. Кроме того, ИТ-отделу может быть сложно поддерживать и физические, и виртуальные, и облачные среды, а также различные процессы, такие как защита, аварийное восстановление, репликация и миграция.

ESG подтверждает, что Acronis Backup 12.5 – это больше, чем просто решение для резервного копирования данных. Оно также предоставляет возможность полного восстановления системы, от мгновенного восстановления виртуальных и физических машин до восстановления «на голое железо», возможность миграции систем, аварийного восстановления облака, репликации, резервного копирования в режиме «off-host», снапшоты SAN, а также высокую практичность.

ESG с удовольствием открыл для себя новые функции визуализации в версии 12.5, включая панель мониторинга, уведомления и отображение действий вместе с системой отчетности, которая позволяет легко отслеживать защищенность окружения. Мы были также приятно удивлены новыми дополнениями Acronis Active Protection и Acronis Notary – функциями, которые выходят за рамки традиционного понимания возможностей систем резервного копирования и восстановления.

Если вам поручили оценить работу вашего текущего решения для защиты данных, и если вы желаете перейти на более быстрое, гибкое, современное решение, ESG считает, что Acronis Backup 12.5 заслуживает вашего внимания. Это решение для малого и среднего бизнеса имеет множество инструментов для защиты данных, зачастую предлагаемых в решениях для предприятий. И, потратив немного времени и системных ресурсов, вы сможете легко протестировать его сами.

Все товарные знаки являются собственностью соответствующих компаний. Информация, содержащаяся в данной публикации, полученная The Enterprise Strategy Group (ESG), является надежной, но не покрывается гарантией ESG. Публикация может содержать мнения ESG, которые могут меняться. Эта публикация защищена авторским правом The Enterprise Strategy Group, Inc. Любое воспроизведение или распространение, частично или целиком, в распечатанном виде, в электронном виде или любым другим способом в пользу лиц, неуполномоченных ее получать, без явно выраженного согласия со стороны The Enterprise Strategy Group, Inc., является нарушением закона США об авторском праве и подлежит подаче гражданского иска, и, если применимо, уголовному преследованию. Если у вас возникли какие-либо вопросы, пожалуйста, свяжитесь с отделом по работе с клиентами ESG по тел. 508.482.0188.

Целью докладов ESG Lab является распространение информации среди ИТ-специалистов о продуктах для обработки данных для компаний всех типов и размеров. Доклады ESG Lab не могут заменить процесс оценивания, который должен проводиться до принятия решения о покупке, но являются средством ознакомления с новыми технологиями. Наша цель – осветить наиболее выдающиеся функции/возможности решения, показать, как они могут быть использованы для решения реальных проблем, а также указать возможные улучшения. Сторонняя точка зрения ESG Lab основана на собственных тестированиях, а также на интервью с клиентами, которые используют эти продукты в своих рабочих средах.