VEEAM

Победим программы-вымогатели: информирование, внедрение и ремедиация с Veeam

Рик Вановер

Старший директор по стратегии развития продуктов

Veeam Software

Содержание

Состояние угрозы **3**

3 лучшие стратегии защиты от программ-вымогателей 4

Информирование **5**

Информирование через определение направлений атаки 5

Информирование через подготовку 7

Внедрение **8**

Защита сервера и компонентов Veeam Backup & Replication 8

Сверхустойчивое хранение резервных копий и правило «3-2-1» 10

Конфигурирование нескольких методов восстановления 16

Защита компьютеров 18

Защита NAS 19

Использование Veeam для выявления программ-вымогателей 20

Инвестиции в автоматизацию 26

Ремедиация **28**

Заключение: готовьтесь сейчас, чтобы не опоздать! **29**

Об авторе **30**

О компании Veeam Software **31**

Состояние угрозы

Угрозы, представляемые программами-вымогателями, можно увидеть в широком масштабе, подобно новостным сообщениям об отключении электричества. Недавняя статья в ZDNet сообщает о том, что атаки программ-вымогателей становятся все более значительными, а дальше будет только хуже.[1] Организациям необходимо признать реальность этой угрозы и предпринять шаги для подготовки, защиты и ремедиации. Это необходимо сделать сейчас, чтобы не полагаться на незапланированные и, скорее всего, неэффективные действия, к которым придется прибегнуть в случае атаки программы-вымогателя.

Когда я выступаю на мероприятиях, то обычно прошу поднять руки тех, кто испытывал проблемы, связанные с этим вредоносным кодом. Каждый раз количество поднятых рук меня шокирует. Если у вас пока не было таких проблем, вы счастливчик. Я бы хотел поделиться информацией, которая поможет вам обезопасить данные на случай атаки программы-вымогателя.

[1] ZDNet https://www.zdnet.com/article/the-ransomware-crisis-is-going-to-get-a-lot-worse/

3 лучшие стратегии защиты от программ-вымогателей

Если вы хотите победить программы-вымогатели, предлагаю три стратегии, которые гарантированно помогут обезопасить данные: **Информирование, внедрение и ремедиация.**

Каждая из этих стратегий представляет собой отдельную дисциплину с необходимостью постоянной переоценки и корректировки для повышения уровня защиты. В каждой области есть свои собственные дисциплины и инструменты, а во многих ИТ-организациях — различные специалисты, которых тоже необходимо привлечь. Успешный подход к защите данных воплощается ИТ-подразделением при поддержке руководства компании. Данная статья посвящена этим трем стратегиям и содержит практические рекомендации по использованию технологий Veeam, а также более широких ИТ-методик, которые предоставят все нужные возможности для имплементации защиты данных сегодня и в будущем.

Многие из переживших атаку программы-вымогателя предоставили свои комментарии о том, что могло бы быть сделано для предотвращения атаки и для ускорения восстановления после нее. Эти комментарии учтены в статье и представлены в виде рекомендаций для широкого использования.

Информирование

Информирование начинается сразу после выявления рисков и угроз. Это должно уже послужить достаточной мотивацией для внедрения ИТ-практик, которые помогут избежать реактивного реагирования в случае внезапной атаки программы-вымогателя.

Информирование должно быть направлено на две основные аудитории: ИТ-персонал и пользователи. Очень важно охватить обе эти группы, так как угрозы могут исходить от любой из них. Как сообщалось, в 4-м квартале 2019 г. [2] свыше 57% атак программ-вымогателей совершались с использованием протокола RDP, более 26% — через фишинговые атаки, а более 12% использовали уязвимости ПО.

Информирование через определение направлений атаки

Информирование о том, что протокол RDP, фишинг и обновления ПО являются основными механизмами проникновения программ-вымогателей, позволяет правильно сконцентрировать усилия на защите именно этих уязвимых участков.

Большинство ИТ-администраторов используют RDP в ежедневной работе. Далее в статье, когда мы будем обсуждать конфигурацию Veeam, мы упомянем о разделении учетных записей для компонентов инфраструктуры резервного копирования. При доступе с помощью RDP это дает возможность откорректировать уровень безопасности. Трудно представить, что в современном мире ИТ существует так много RDP-серверов, напрямую подключенных к интернету. Реальность состоит в том, что практика интернет-подключения через RDP должна быть прекращена[3]. ИТ-администраторы могут использовать специальные IP-адреса, перенаправляющие RDP-порты, сложные пароли и многое другое, но данные не лгут. Факт состоит в том, что свыше половины атак программ-вымогателей происходит через RDP. Таким образом, прямое подключение по RDP через интернет не соответствует разумной стратегии борьбы с вредоносным кодом. Далее мы представим некоторые рекомендации по использованию RDP, которые помогут повысить устойчивость к атакам программ-вымогателей.

Следующим по частоте способом проникновения программ-вымогателей являются фишинговые электронные сообщения. Мы все видели эти странные сообщения, которые не имеют никакого смысла. Правильно будет такие сообщения сразу удалять, но не все пользователи делают это. Существует два популярных инструмента, которые помогают оценить риск успешной фишинговой атаки на организацию: Gophish и KnowBe4.

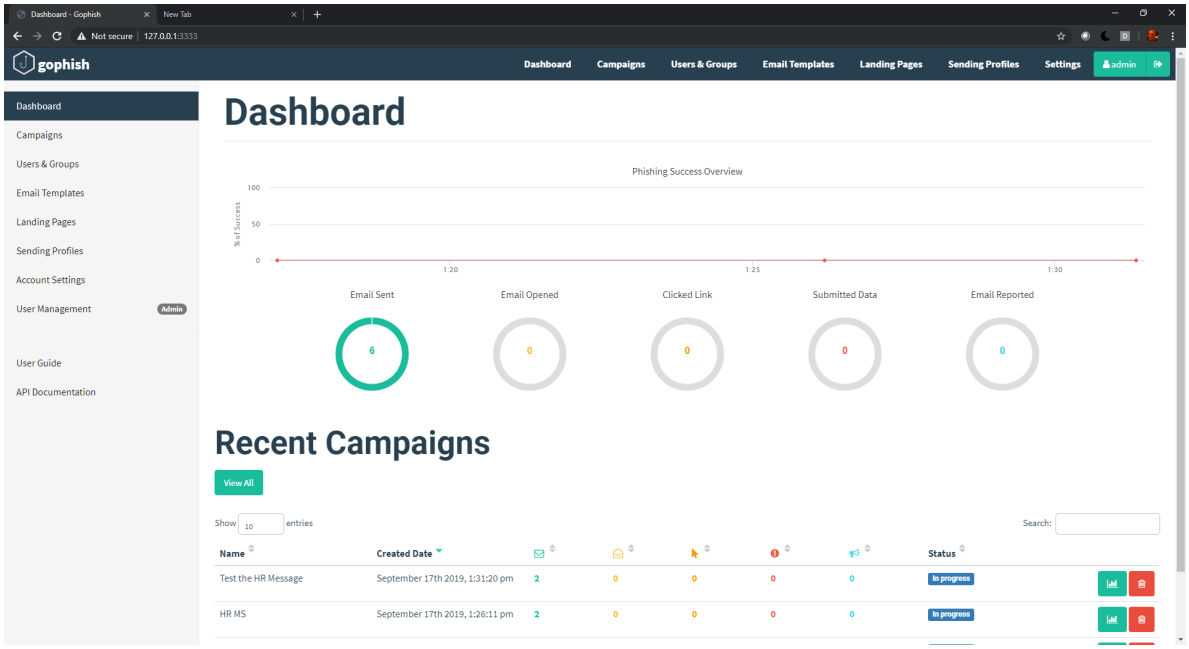
KnowBe4 (https://www.knowbe4.com) позволяет повысить уровень осознанности больше, чем простое информирование пользователей и администраторов. Этот сервис предоставляет тренинг по безопасности с эмуляцией фишинговых атак.

Помимо KnowBe4 существуют ресурсы с открытым кодом, которые также помогают бороться с фишингом. Один из них, Gophish (https://getgophish.com/), позволяет создавать панели мониторинга и рассылать электронные сообщения для проверки реакции адресатов. Тест на реакцию на фишинг можно создать всего за несколько минут.

После рассылки сообщений можно отследить, сколько сообщений было отправлено, сколько из них открыто, сколько пользователей нажало на ссылку и т.д. Это отличный способ проверить уровень подготовки пользователей в вашей организации. Панель мониторинга Gophish представлена ниже:

[2] Отчет Coveware: https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate

[3]ESET https://www.welivesecurity.com/2019/12/17/bluekeep-time-disconnect-rdp-internet/



Эти инструменты помогают эффективно измерить способность организации адекватно оценить риск, представляемый фишинговыми электронными сообщениями, вложениями и т.д.

Другим важным фактором является риск использования уязвимостей. Своевременное обновление ИТ-систем особенно важно сегодня. Конечно, это не очень увлекательное занятие, но это хорошая инвестиция, если программа-вымогатель попытается использовать известную, но уже исправленную уязвимость. Обратите внимание на необходимость своевременного обновления следующих критически важных ИТ-ресурсов: операционные системы, приложения, базы данных и встроенное ПО устройств (firmware). Некоторые программы-вымогатели использовали довольно старые уязвимости, которые уже были давно исправлены. Примеры таких программ-вымогателей: WannaCry, Petya и Sodinokibi[4]. Уязвимости могут содержать сервисы, не относящиеся к операционным системам, например njRAT[5] при использовании Adobe Flash.

Компьютеры пользователей также необходимо вовремя обновлять. С точки зрения проникновения вредоносного ПО компьютеры представляют не меньший риск, чем системы дата-центра, особенно это относится к вредоносным программам, которые занимаются сбором информации. Такие программы остаются активными в среднем в течение около трех дней[6].

[4]ZDNet https://www.zdnet.com/article/sodinokibi-ransomware-is-now-using-a-former-windows-zero-day/

[5]TrendMicro https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/lord-exploit-kit-rises-delivers-njrat-and-eris-ransomware

[6]ZDNet https://www.zdnet.com/article/most-ransomware-attacks-take-place-during-the-night-or-the-weekend/

Информирование через подготовку

Повысить уровень защиты помогут дополнительные подготовительные шаги, например, изучение возможностей инструментов, которые у вас уже есть. Например, если произойдет атака программы-вымогателя и необходимо будет восстановить данные, ИТ-специалистам поможет в этом знание различных сценариев действия. Благодаря этому ИТ-специалисты уже будут знакомы с процессом восстановления, будут в курсе необходимого для него количества времени и, что важнее всего, будут уверены в его успехе. Несколько примеров таких шагов приведены ниже.

- **Безопасное восстановление Veeam:** При безопасном восстановлении Veeam Backup & Replication™ подключает диски ВМ, которую необходимо восстановить. Далее Veeam Backup & Replication запускает антивирусную программу, которая сканирует файлы на подключенных дисках. Если при сканировании выявляется вредоносный код, Veeam Backup & Replication, в зависимости от настроек, может прервать процесс восстановления или восстановить машину или диски с ограничениями. Это только один маленький шаг в процессе восстановления, но он придает уверенности в том, что вредоносный код не проникнет в вашу среду.
- **Veeam DataLabs™:** Veeam DataLab — это задание SureBackup®, которое запускает виртуальную машину из резервной копии в виртуальной среде. Это позволяет убедиться в возможности восстановления системы, а также протестировать, например, обновления приложений и операционной системы. Задания DataLabs могут использоваться для проверки точек восстановления, чтобы убедиться, что система, которую вы будете восстанавливать, полностью функциональна. Также можно запустить одну или несколько систем в изолированной лаборатории для тестирования действий по ремедиации.

  Предварительно рекомендуется ознакомиться с возможностями технологии Veeam SureBackup. Это может помочь понять, что восстановление системы невозможно ввиду угрозы заражения программой-вымогателем или по другим причинам. При восстановлении после атаки программы-вымогателя SureBackup поможет убедиться, что система может быть корректно восстановлена, а приложения будут работать правильно. После выполнения заданий SureBackup можно оставить их работать, чтобы вручную проверить систему на наличие программы-вымогателя перед восстановлением. Подробная информация о Veeam DataLabs представлена в разделе статьи, посвященном внедрению.

- **Несколько сценариев восстановления:** В зависимости от типа инцидента, может быть рекомендовано выполнить другой тип восстановления. Например, переключение на реплику ВМ может быть самым логичным действием при атаке программы-вымогателя. Восстановление файлов может быть самым подходящим типом восстановления в этом случае. В других сценариях может лучше подойти восстановление машины целиком. Имеет смысл ознакомиться со всеми сценариями, чтобы повысить свою уверенность в успешном восстановлении после атаки программы-вымогателя.

К вопросу информирования следует подойти со всей серьезностью. Оценка риска фишинга для организации, устранение распространенных путей проникновения вредоносного кода и своевременное обновление систем и ПО — это важнейшие шаги, которыми нельзя пренебрегать. При невыполнении этих шагов риск атаки программы-вымогателя увеличивается. Чтобы оценить инвестиции в информирование, можно сравнить их с рисками, затратами и давлением, которые возникают в случае атаки программы-вымогателя, к которой вы не готовы.

Во всех ситуациях, если атака программы-вымогателя произошла, единственным способом решения проблемы является восстановление данных. Это объясняет ту серьезность, с которой мы подходим в следующих разделах статьи к внедрению и использованию продуктов Veeam для резервного копирования. Потеря данных — не вариант, как и выплата выкупа. Предпочтительный результат — надежное восстановление данных, а рекомендации, представленные далее, помогут в этом.

Внедрение

Продукты Veeam для резервного копирования известны своей простотой, гибкостью и надежностью. Они предоставляют массу новых возможностей. Внедрение решения для резервного копирования с целью защиты от программ-вымогателей напоминает прохождение аудита на соответствие требованиям законодательства. Продукт не обязательно соответствует или не соответствует стандарту. Скорее, требования стандарта диктуют, как следует внедрять продукт и проводить его аудит. Устойчивость к атакам программ-вымогателей полностью зависит от того, как настроен продукт, от поведения вредоносного кода и от способа разрешения ситуации.

Критической частью этой устойчивости является конфигурация инфраструктуры резервного копирования Veeam. Рекомендации по внедрению содержатся в следующих разделах:

- Защита сервера и компонентов Veeam Backup & Replication
- Использование Veeam для выявления программ-вымогателей
- Сверхустойчивое хранение резервных копий и правило «3-2-1»
- Конфигурирование нескольких методов восстановления
- Защита компьютеров
- Защита NAS
- Оркестрируемое восстановление из резервных копий и реплик ВМ

Защита сервера и компонентов Veeam Backup & Replication

С точки зрения защиты от программ-вымогателей сервер Veeam Backup & Replication — критическая часть решения. Для эффективной защиты важно, чтобы сервер был максимально изолирован. Предлагаем несколько важных методов, которые помогут вам в настройке:

Серверы Veeam без доступа в интернет: Изоляция сервера резервного копирования от интернета — важный метод его защиты от проникновения или распространения вредоносного кода. Если вы используете Veeam Cloud Tier или Veeam Cloud Connect, необходимо принять специальные меры для обеспечения явно заданного доступа к облачным ресурсам.

Учетные записи, используемые для установки Veeam: Учетные записи, используемые для установки Veeam, должны быть максимально обособленными. Рассмотрите подключение к прокси-серверам, репозиториям, WAN-акселераторам и другим компонентам Veeam с помощью явно заданной учетной записи с соответствующими правами доступа. Некоторые организации могут предпочесть использовать для этих компонентов набор изолированных учетных записей (не относящихся к домену). Другие организации могут создать отдельный домен Microsoft Active Directory для Veeam и соответствующих инфраструктурных инструментов, которые должны быть максимально обособлены. Конкретная рекомендация — не использовать общие учетные записи с доступом как к источникам производственных данных, так и к инфраструктуре резервного копирования. Самым худшим вариантом будет использование для всех компонентов учетной записи DOMAIN\Administrator с правами доступа к ключевым ресурсам инфраструктуры, включая Veeam, vSphere and Hyper-V. Если эта учетная запись будет скомпрометирована, и она же будет использоваться для компонентов Veeam, многие техники восстановления окажутся под угрозой.

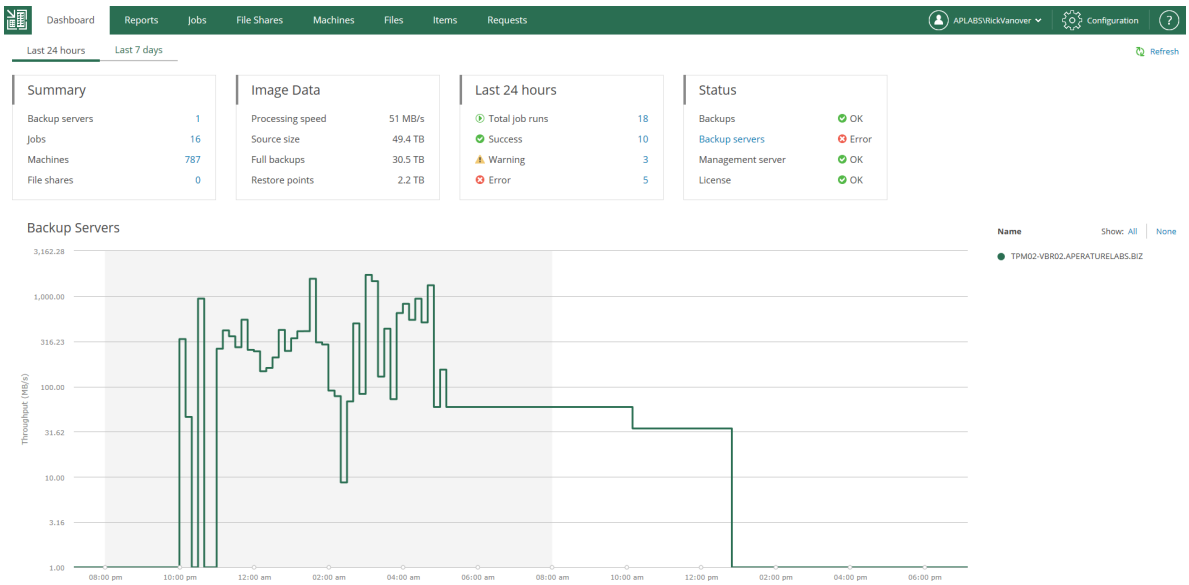
Рекомендуемые ресурсы

Необходимые права доступа для всех продуктов Veeam тщательно задокументированы (как и требования к портам для каждой роли) и представлены на https://helpcenter.veeam.com

Мы также рекомендуем Руководство Veeam по лучшим практикам защиты инфраструктуры: https://www.veeambp.com/infrastructure_hardening

Настройка явно заданного доступа к репозиторию: Репозиторий резервных копий — самый критически важный ресурс для обеспечения защиты от программ-вымогателей. Мы рекомендуем запретить доступ к этому компоненту Veeam и его просмотр в рамках всей организации (это поможет предотвратить утечку резервных копий за пределы организации). Дополнительную защиту можно обеспечить с помощью микро-сегментирования и использования брандмауера во внутренних сетях для пропуска явно разрешенного трафика к требуемым источникам и целевым устройствам.

Использование Veeam Backup Enterprise Manager: При использовании Veeam Backup Enterprise Manager (BEM) для соответствующих заданий частота доступа к центральной панели управления инфраструктуры Veeam значительно сокращается. Рутинные задачи, такие как восстановление файлов и ВМ, быстрое резервное копирование, клонирование и редактирование заданий, запрос на активное полное резервное копирование и многое другое, могут выполняться с помощью BEM. Ключевым преимуществом BEM является то, что он обеспечивает эти действия для всех серверов Veeam Backup & Replication, установленных в организации. На рисунке ниже показан главный экран BEM:



Еще одним методом снижения частоты подключений к серверу Veeam с полными правами доступа является использование встроенных ролей. Эти роли могут быть использованы как с BEM, так и с Veeam Backup & Replication. Примеры ролей — оператор восстановления, пользователь портала и администратор портала. Подробная информация о ролях представлена в Руководстве пользователя Veeam или в Справочном центре Veeam (https://helpcenter.veeam.com/docs/backup/hyperv/users_roles.html?ver=100).

Требование двухфакторной аутентификации для доступа к Veeam по RDP: Для систем, работающих в качестве консолей Veeam Backup & Replication, рекомендуется устанавливать требование двухфакторной аутентификации для подключения по протоколу RDP. RDP является одним из самых частых путей проникновения вредоносного кода (57.4% атак происходят через RDP7). Эта угроза существует даже в сетях без доступа к интернету. Популярным средством двухфакторной аутентификации является Microsoft Tools или сторонний инструмент, например, Duo.

Двухфакторная аутентификация Microsoft для RDP:
https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-plan-mfa

Мультифакторная аутентификация Duo
https://duo.com/product/multi-factor-authentication-mfa

Сверхустойчивое хранение резервных копий и правило «3-2-1»

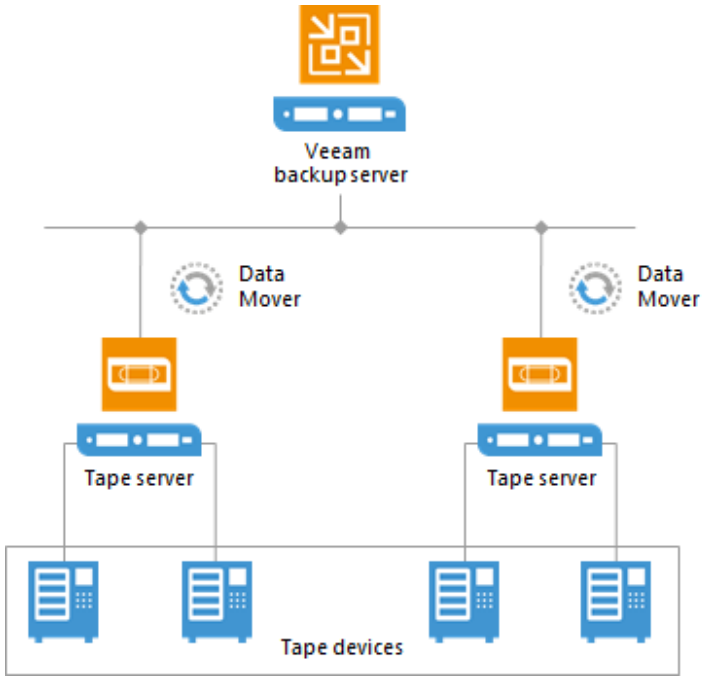
Если у этой статьи есть одна главная идея, то это необходимость обустроить сверхустойчивое хранение резервных копий. Сверхустойчивое хранение резервных копий означает, что необходимо хранить один или более экземпляров резервных копий на следующих носителях:

- Резервные копии на магнитной ленте
- Неизменяемые резервные копии в S3 или S3-совместимом объектном хранилище
- Физически изолированные и отключенные носители (например, съемные диски)
- Резервные копии в Veeam Cloud Connect с защитой от инсайдеров

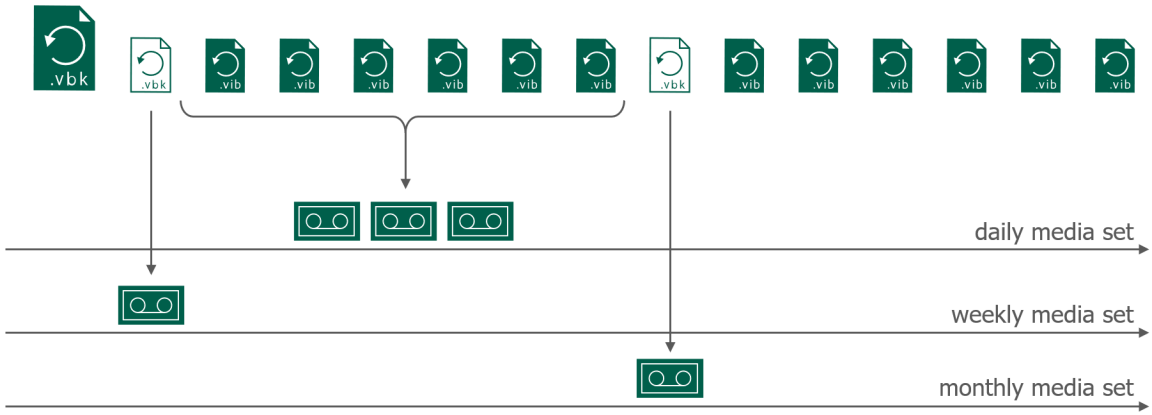
Сверхустойчивое хранение резервных копий — одна из критически важных линий обороны от атак программ-вымогателей. Каждая организация должна выбрать подход, наиболее эффективный для конкретной ситуации. Помимо программ-вымогателей, эти возможности защищают данные и от других опасностей, например случайного удаления или действий инсайдеров. Ниже приведены характеристики каждого из сверхустойчивых типов носителей:

Резервные копии на магнитной ленте: У каждой ИТ-организации есть свое мнение о магнитной ленте, но нет сомнений в том, что по цене приобретения, возможностям изолированного хранения и портативности этому носителю практически нет равных. Носитель на магнитной ленте, находящийся вне библиотеки, автоматически отключен, если с ним не производятся операции чтения или записи. Для дополнительной защиты от программ-вымогателей Veeam поддерживает носители типа WORM (однократная запись-многократное чтение). Veeam предлагает широкие возможности поддержки магнитной ленты, включая запись файлов и полное резервное копирование. Поддержка Veeam резервного копирования ВМ и физических серверов на ленту представлена в графическом виде ниже:

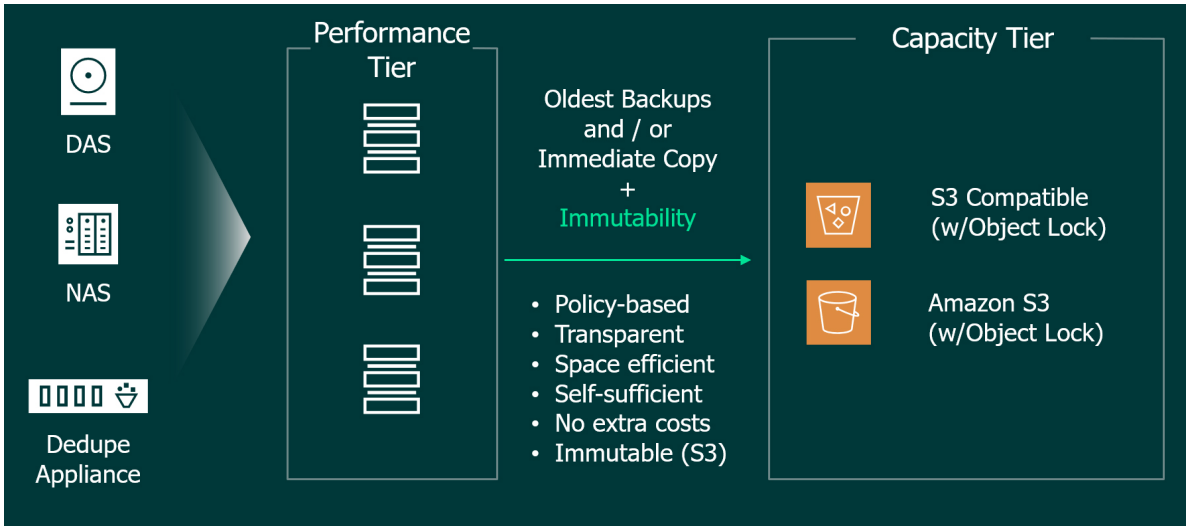
[7] https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate



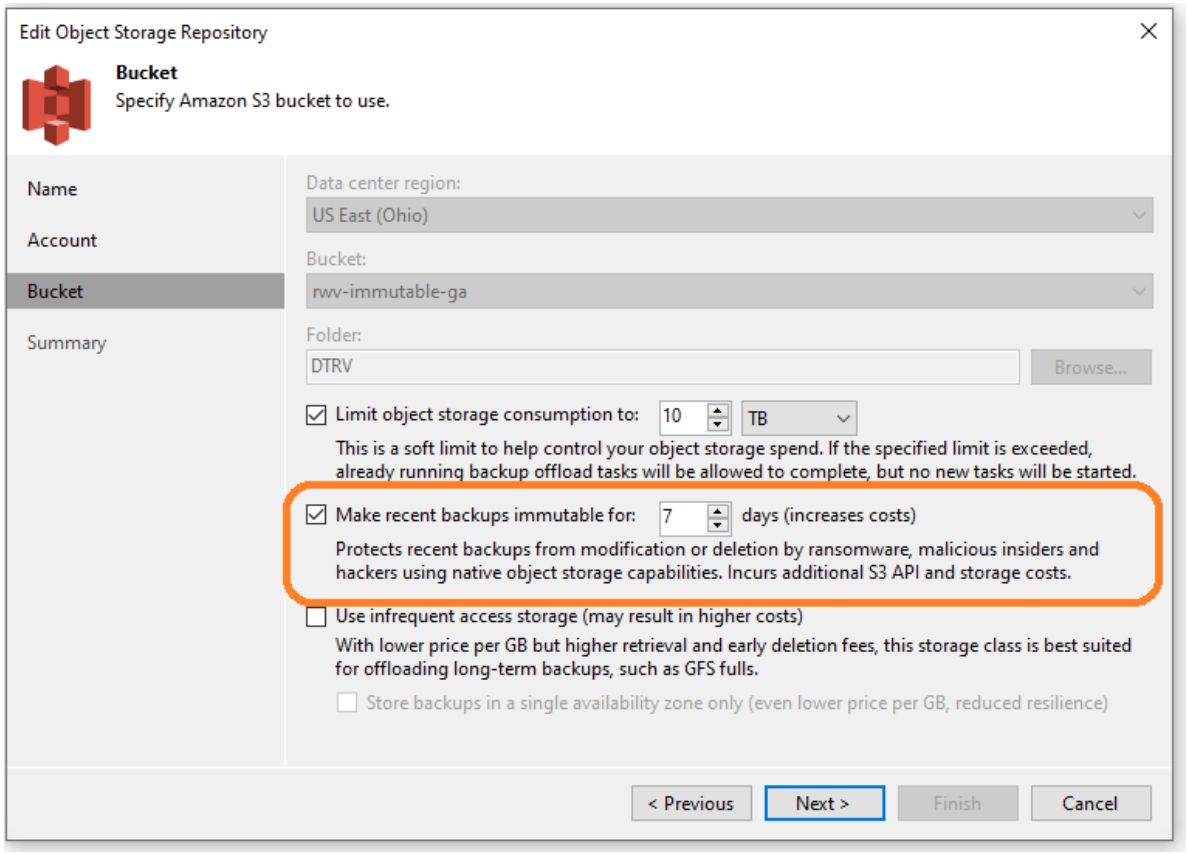
Veeam поддерживает большинство конфигураций современных ленточных накопителей и библиотек. Для повышения устойчивости к программам-вымогателям магнитную ленту можно использовать несколькими способами. Там можно размещать только ограниченный объем данных на небольшой период времени, например, на несколько недель. При словах «инфраструктура магнитной ленты» многие люди представляют себе массивные ленточные библиотеки, в которых хранятся данные за несколько лет. Однако, ленту можно использовать как сверхустойчивый тип носителя для ближайших точек восстановления. Ниже представлены ежедневный, еженедельный и ежемесячный наборы носителей Veeam:



Неизменяемые резервные копии в S3 и S3-совместимых объектных хранилищах: Veeam Cloud Tier поддерживает неизменность резервных копий в качестве эффективного метода защиты от программ-вымогателей и других угроз. Это достигается за счет использования масштабируемого репозитория Veeam (SOBR) с включенной функциональностью Capacity Tier (также известен как Cloud Tier). Capacity Tier — возможность, основанная на политиках, которая позволяет размещать данные резервных копий в объектном хранилище. Поддерживаются IBM Cloud, Azure, AWS и AWS S3-совместимые объектные хранилища, однако только публичные AWS S3 и отдельные S3-совместимые системы хранения предлагают режим блокировки объектов, который позволяет поместить резервные копии Veeam в контейнер и обеспечить их неизменность.



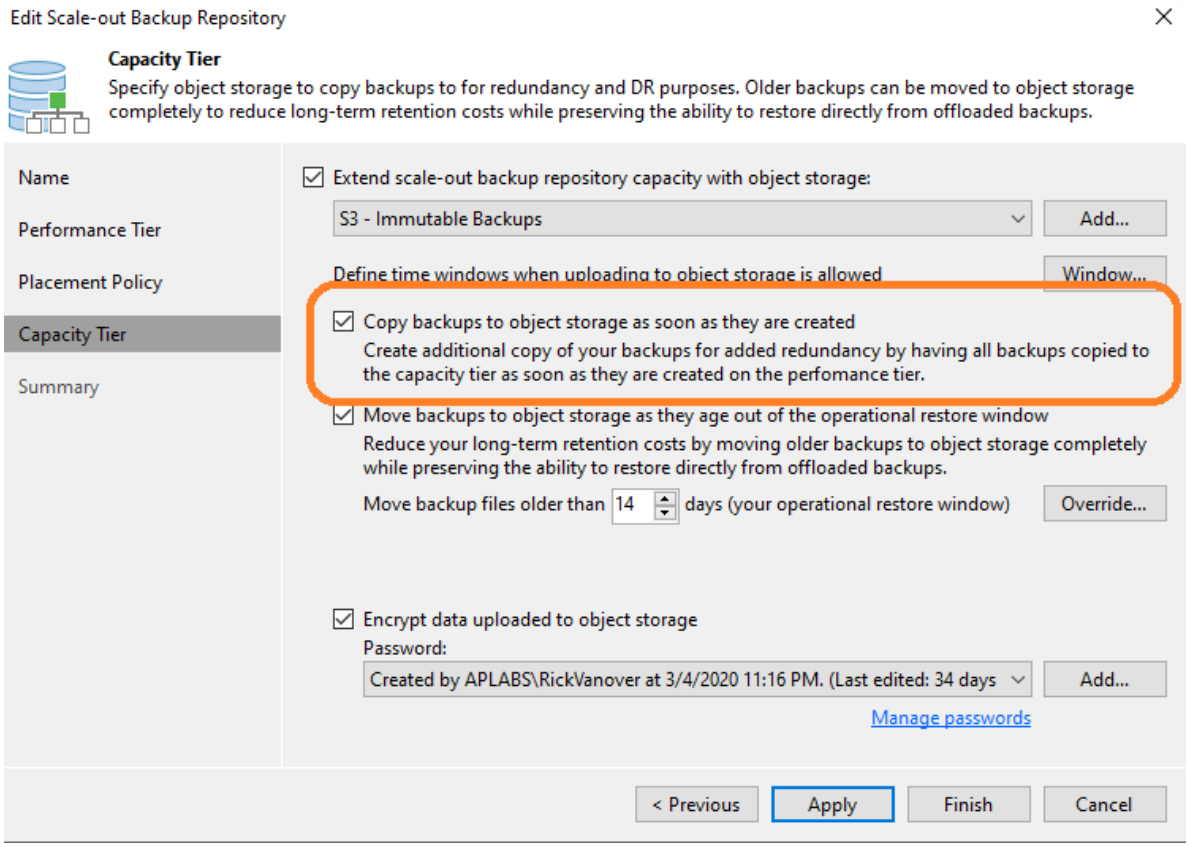
Veeam Backup & Replication позволяет максимально просто настроить неизменность резервных копий в S3. Для максимальной защиты Veeam Capacity Tier следует сконфигурировать два свойства. Во-первых, это AWS S3 или S3-совместимый контейнер, который позволит установить режим неизменности резервных копий на определенное количество дней. Это относится ко всем данным резервных копий, помещенным в контейнер в ходе распределения по уровням SOBR, которое происходит по окончании резервного копирования (режим копирования) или спустя некоторое время (режим переноса). Установка продолжительности режима неизменности для контейнера производится следующим образом:



Указанная настройка неизменности является свойством контейнера объектного хранилища. Чтобы наиболее эффективно использовать объектное хранилище для защиты от программ-вымогателей, следует применить дополнительную настройку, которая является свойством масштабируемого репозитория. Тогда в объектное хранилище Capacity Tier будут переноситься данные резервных копий, возраст которых превысил обозначенное окно оперативного восстановления (например, 14 дней). Есть также возможность копирования резервных копий в объектное хранилище сразу после их создания (с помощью режима копирования).

Режим копирования — важный дополнительный шаг в защите от программ-вымогателей, так как по окончании резервного копирования этот режим мгновенно создает копию данных в объектном хранилище. По мере старения резервных копий их данные будут переноситься из локальных хранилищ с помощью режима переноса. В промежутке времени между созданием резервной копии и окном оперативного восстановления резервные копии будут существовать как на локальной площадке, так и в объектном хранилище. Объединив это с режимом неизменности, вы получаете эффективную защиту от программ-вымогателей.

Это важно, так как во многих случаях предпочтительнее восстанавливать данные из последних точек восстановления с наименьшими показателями RPO. На рисунке показано конфигурирование режима копирования для масштабируемого репозитория:

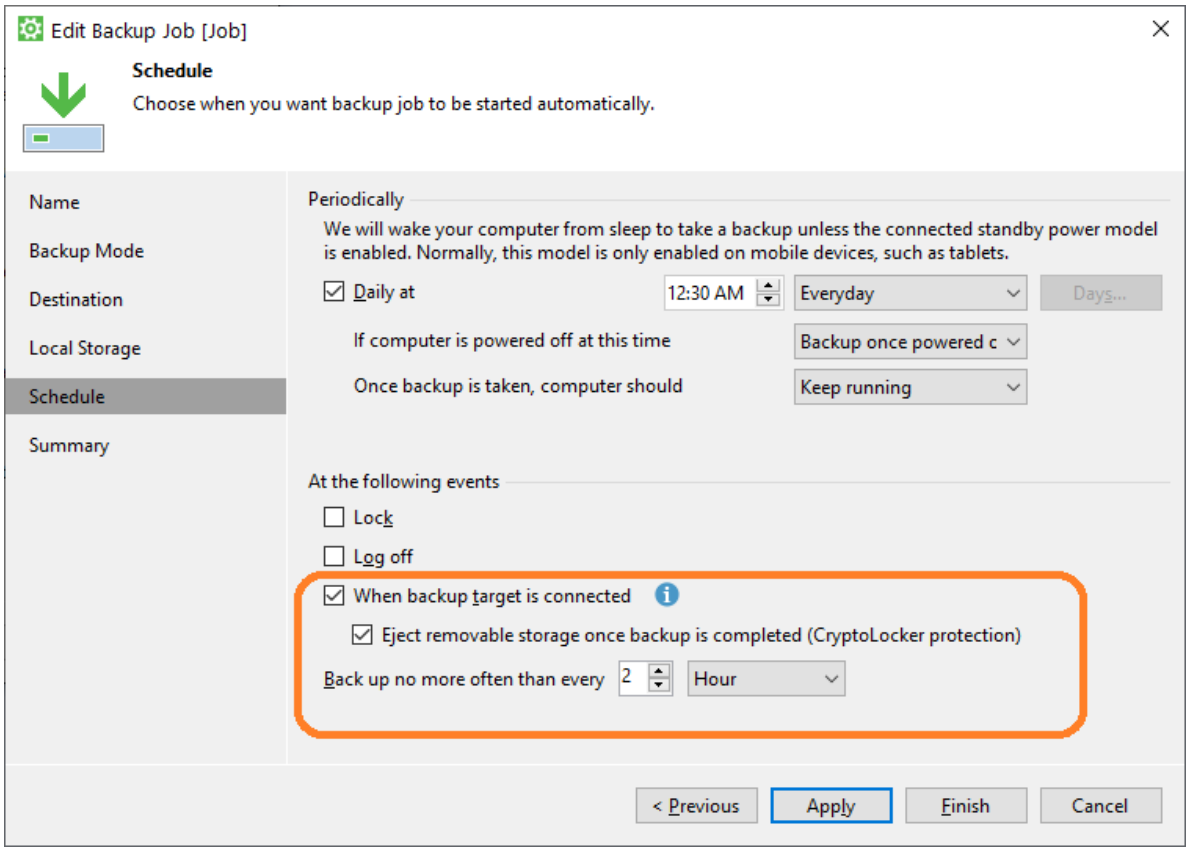


Рекомендуемые ресурсы

Подробная информации о неизменности резервных копий Veeam представлена на:http://vee.am/s3immutable

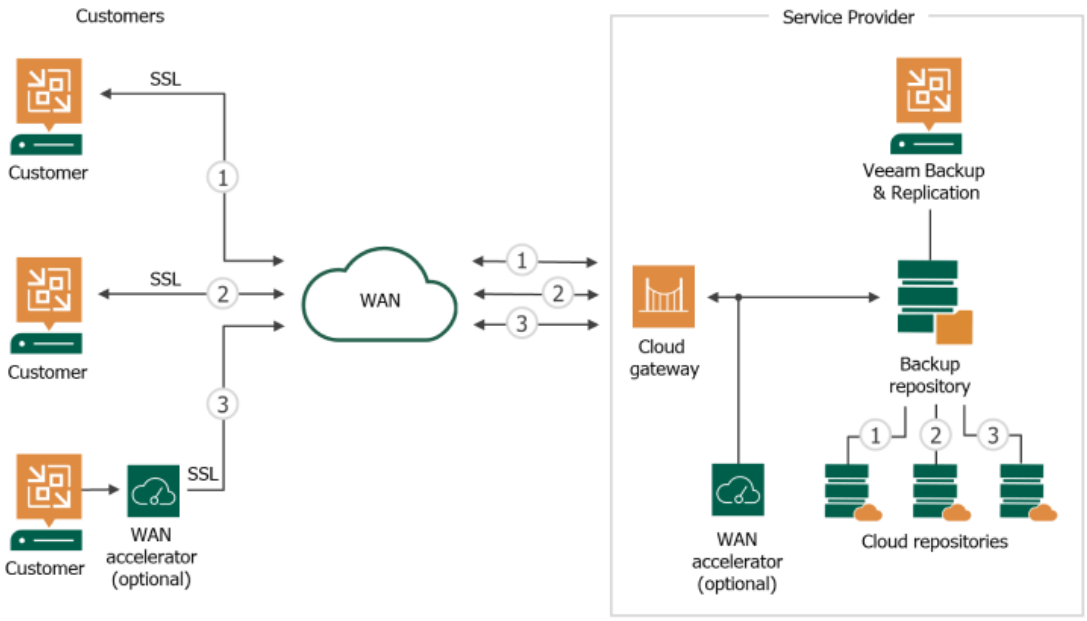
Физически изолированные и отключенные носители: Как и магнитную ленту, сменные диски тоже можно отключать. В случае больших массивов данных управление дисками может быть затруднено, так как их размер ограничен (хотя со временем размеры дисков растут). Подобный подход может применяться ситуационно, например для данных компьютеров или отдельных филиалов. Veeam Backup & Replication поддерживает репозитории со сменными носителями для взаимозаменяемых процессов.

Например, Veeam Agent *for Microsoft Windows* поддерживает целевые локации со сменными носителями. Для компьютеров существует дополнительная возможность отсоединения сменных носителей по окончании резервного копирования. Эта опция показана на рисунке:



Резервные копии в Veeam Cloud Connect с защитой от инсайдеров Veeam Cloud Connect — популярная на рынке технология, которая лежит в основе услуг по резервному копированию и послеаварийному восстановлению данных (BaaS и DRaaS) на основе решений Veeam. Veeam Cloud Connect предоставляется поставщиками услуг Veeam. Эта технология также предлагается как «Veeam Cloud Connect для крупных компаний», для использования в рамках крупных организаций.

Защита от инсайдеров Veeam Cloud Connect была разработана специально для дополнительной защиты резервных копий от программ-вымогателей, случайного удаления и злонамеренных действий администратора. В рамках этой защиты создается дополнительная резервная копия, которая хранится на площадке поставщика услуг и предоставляется по требованию, например, по звонку в службу поддержки. Благодаря этому резервная копия может быть возвращена в репозиторий Veeam Cloud Connect и использована для восстановления. Рисунок иллюстрирует Veeam Cloud Connect Backup:



Найти поставщика услуг, который предлагает Veeam Cloud Connect с защитой от инсайдеров можно здесь: http://vee.am/splookup

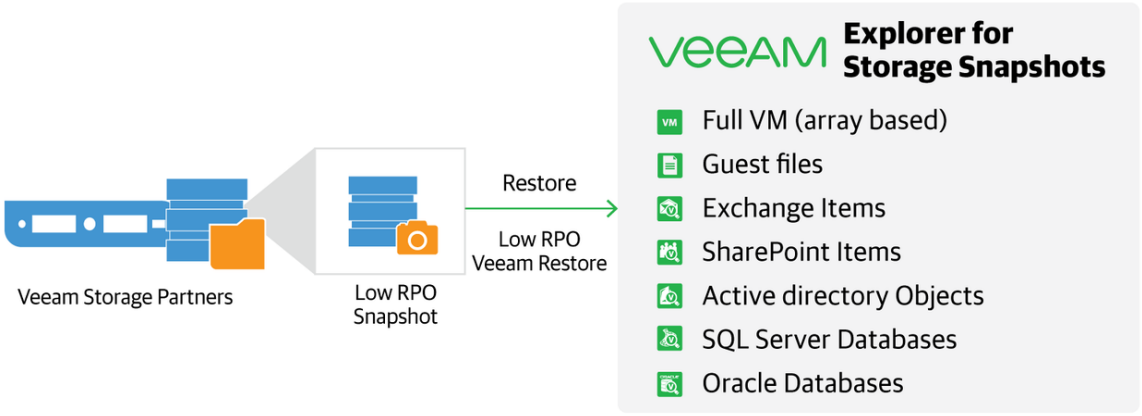
Правило «3-2-1»: Уже много лет Veeam рекомендует правило «3-2-1» в качестве базовой стратегии управления данными. Согласно этому правилу вам следует хранить по крайней мере три экземпляра важных данных на как минимум двух типах носителей. При этом хотя бы один экземпляр данных должен храниться на удаленной площадке. Правило «3-2-1» не требует использования какой-либо определенной марки оборудования и может помочь практически при любом сбое.

В связи с распространением программ-вымогателей Veeam подчеркивает, что один экземпляр данных должен храниться на сверхустойчивом носителе (т.е., изолированном, отключенном или защищенном режимом неизменности). Выполнение этой рекомендации обязательно для защиты от программ-вымогателей.

Конфигурирование нескольких методов восстановления

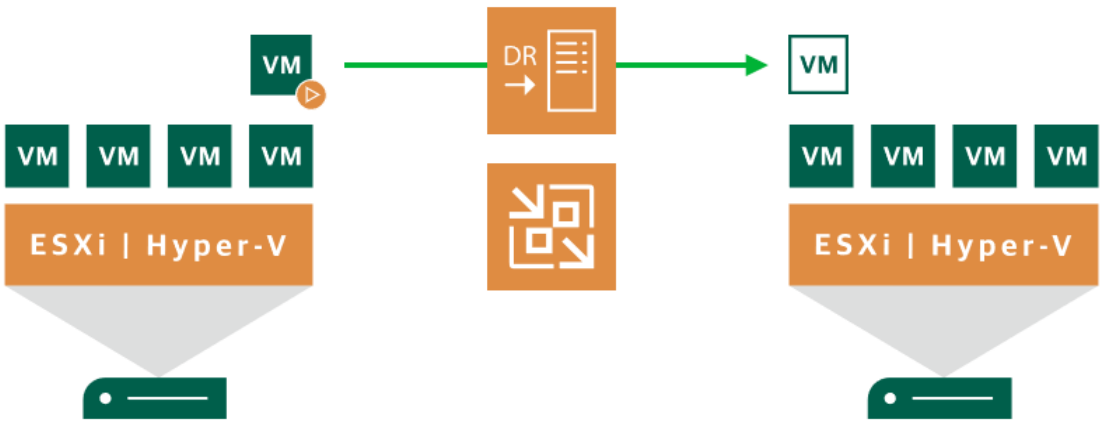
В процессе настройки Veeam Backup & Replication вы подключаетесь к различным системам. Они включают в себя виртуальные среды, такие как VMware vSphere, Microsoft Hyper-V и Nutanix AHV, физические среды, в том числе Windows, Linux, AIX и Solaris, а также системы хранения данных. В такой ситуации можно посоветовать быть готовыми использовать все опции восстановления. Самые популярные опции — это восстановление системы целиком (BM или сервера), восстановление файлов и восстановление приложений. Ниже мы приводим рекомендации относительно других типов восстановления.

Интеграция с аппаратными снимками СХД: Если основная система хранения поддерживает интеграцию аппаратных снимков с Veeam, это может предоставить разнообразные опции высокоскоростного восстановления. Veeam Explorer™ for Storage Snapshots может быстро восстанавливать ВМ из аппаратных снимков, созданных по расписанию. Veeam Explorer for Storage Snapshots представлен на рисунке:



При использовании этого метода восстановления производственные данные (например, ВМ) восстанавливаются из аппаратного снимка основной СХД. Однако, также рекомендуется создавать резервные копии данных, хранящихся на основной СХД. Veeam также поддерживает аппаратные снимки, доступные только для чтения, например, систем NetApp SnapVault и Pure Storage SafeMode.

Репликация Veeam: Многие организации используют Veeam для резервного копирования и восстановления критически важных данных, но механизм репликации ВМ также может помочь в защите от программ-вымогателей. Репликация ВМ на локальную или резервную площадку обеспечивает высокоскоростное восстановление, которое может помочь быстро избавиться от угрозы. Репликация ВМ с помощью Veeam упрощенно представлена ниже:



Обратите внимание, что при репликации в целевой локации также может присутствовать программа-вымогатель. Несколько соображений относительно репликации применительно к защите от программ-вымогателей:

- Использование различных контекстов безопасности на исходном и целевом устройстве с гипервизорами и ПО управления, как, например, vCenter или System Center.
- Точки восстановления реплик ВМ во многом похожи на механизм резервного копирования. Они представляют ВМ в момент репликации.
- Для среды VMware задания SureBackup могут быть запущены для реплик Veeam. Это поможет убедиться в возможности запуска и правильном функционировании реплики перед ее использованием для восстановления после атаки программы-вымогателя.

Другой продукт Veeam — Veeam Availability Orchestrator — предлагает простой, надежный и масштабируемый механизм оркестрации и автоматизации, специально разработанный для обеспечения непрерывности бизнес-процессов и послеаварийного восстановления (BCDR). Позволяя исключить неэффективные, длительные и подверженные ошибкам ручные процессы тестирования и восстановления, Veeam Availability Orchestrator предоставляет проверенную стратегию послеаварийного восстановления с помощью резервных копий и реплик, которая повышает надежность ИТ-операций. Veeam Availability Orchestrator автоматически проверяет резервные копии и реплики на соответствие целевым показателям RTO и RPO. Это повышает уверенность в успешности комплексной стратегии послеаварийного восстановления и доказывает возможность соблюдения требований SLA. Уверенность в стратегии DR может быть эффективным методом восстановления после атаки программы-вымогателя.

Различные опции: В зависимости от характера проблем, вызванных программой-вымогателем, не существует единого способа восстановления. Во многих случаях восстановление ВМ или системы целиком очень эффективно, но рекомендуется привлечь экспертов для выполнения других видов восстановления с целью переноса выбранных данных. Это может включать восстановление файлов, приложений или отдельных дисков, например, файлов VHDX или VMDK.

Защита компьютеров

Многие организации знают о возможностях Veeam по резервному копированию физических серверов, виртуальных машин и других систем дата-центра. Но решения Veeam Agent также предлагают резервное копирование персональных компьютеров, ноутбуков и планшетов на базе Windows. Организации могут повысить уровень защиты компьютеров на базе Linux и Windows от программ-вымогателей благодаря резервному копированию.

Резервное копирование компьютеров позволяет восстановить их в случае атаки программы-вымогателя. Использование API Veeam для интеграции данных может предоставить дополнительные преимущества. Также рекомендуется выполнить сканирование компьютера после резервного копирования, чтобы сократить время между возможным проникновением вредоносного кода и запуском эксплойта.

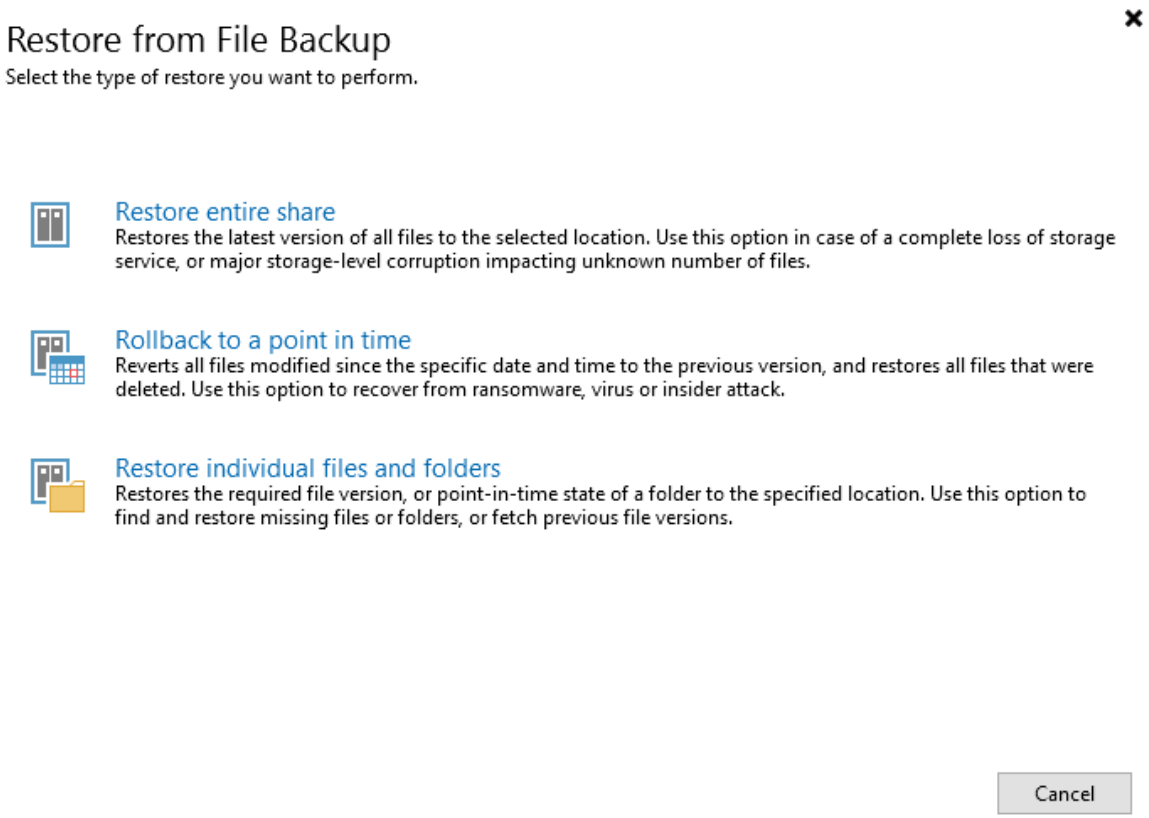
Как уже упоминалось, Veeam Agent *for Microsoft Windows* поддерживает отсоединение съемных носителей после резервного копирования. Это позволяет изолировать резервную копию с помощью двух методов защиты от программ-вымогателей. Первый метод — само создание резервной копии, а второй — хранение резервной копии на отключенном носителе. Эта возможность поддерживается для систем на базе Linux, а также ПК, ноутбуков и планшетов на базе Windows.

Защита NAS

Системы NAS часто являются объектами атак программ-вымогателей. Если учитывать угрозы случайного удаления и злонамеренных действий инсайдеров, данные файлов также подвергаются рискам. Veeam Backup & Replication предлагает поддержку резервного копирования NAS и обеспечивает хорошую возможность восстановления данных общих файловых ресурсов в случае атаки программы-вымогателя.

Механизм резервного копирования файлов Veeam предлагает три типа восстановления. Первый тип — это восстановление файлов и папок для изолированных ситуаций на базе последней резервной копии. Второй тип — откат всей сетевой папки на определенную точку восстановления. Третий сценарий — восстановление всей сетевой папки на новом устройстве при потере старого оборудования.

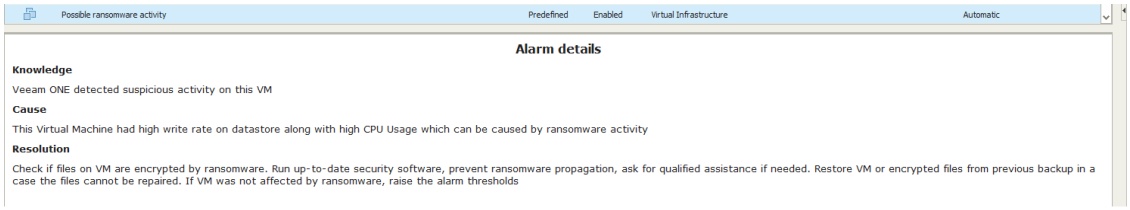
Каждый сценарий может применяться для защиты от программы-вымогателей, но именно второй сценарий предпочтителен после атаки программы-вымогателя. Если угроза была устранена, но часть ресурса NAS удалена или зашифрована, этот тип восстановления поможет вернуть данные в состояние на момент резервного копирования. Для систем NAS с миллионами файлов и глубокими путями к папкам кэш-репозиторий Veeam поможет отследить изменения файлов и папок. Это поможет выполнить восстановление системы на определенный момент времени без необходимости выяснения ущерба, нанесенного данным. Опции восстановления NAS представлены ниже:



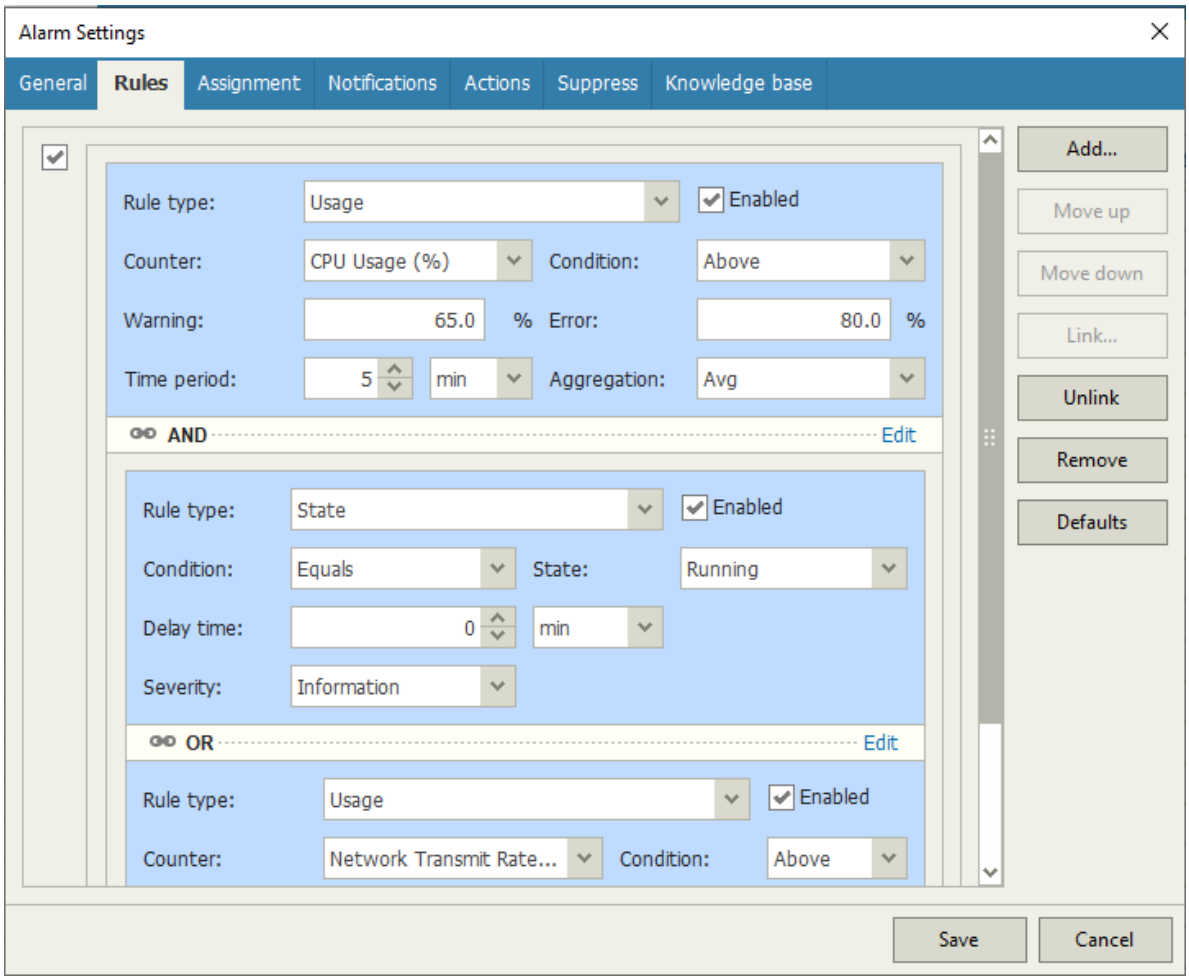
Использование Veeam для выявления программ-вымогателей

Невозможно переоценить важность как можно более раннего обнаружения активности программы-вымогателя, так как именно это дает ИТ-организации неоспоримые преимущества. Veeam использует две техники обнаружения программ-вымогателей:

Оповещение о возможной активности программы-вымогателя: Оповещение Veeam ONE™ обнаруживает сочетание высокой активности ЦП и постоянных запросов к диску на запись. Оповещение представлено ниже:

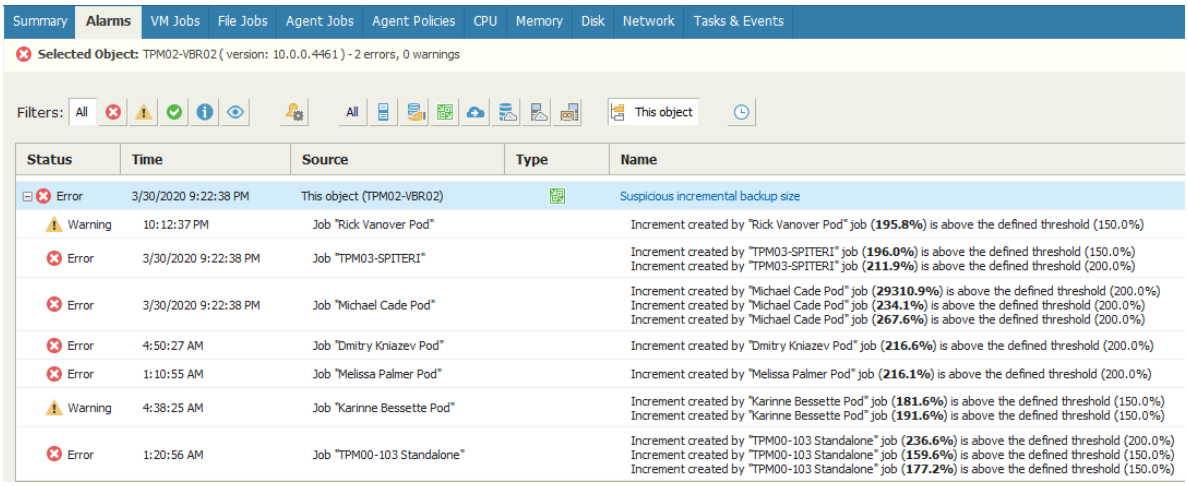


Настройки оповещения можно изменять. Настройки по умолчанию — хорошее начало для обнаружения подозрительной активности, но их можно изменить в сторону более консервативных значений. Опции для изменения настроек показаны ниже:



Следующая рекомендация будет особенно важна для организаций, использующих Veeam ONE. Она касается того, что произойдет после срабатывания оповещения. Я рекомендую использовать некоторые конкретные действия, которые встроены в оповещение и помогают более агрессивно привлечь внимание к проблеме. Это включает в себя отправление SMS-сообщений, оповещение специалистов по безопасности и даже такие экстремальные шаги, как отключение BM от питания и отсоединение сетевого интерфейса через шаг «Actions» в оповещении Veeam ONE. Если вы используете VMware и Hyper-V, сделайте эти действия обязательными для каждой среды.

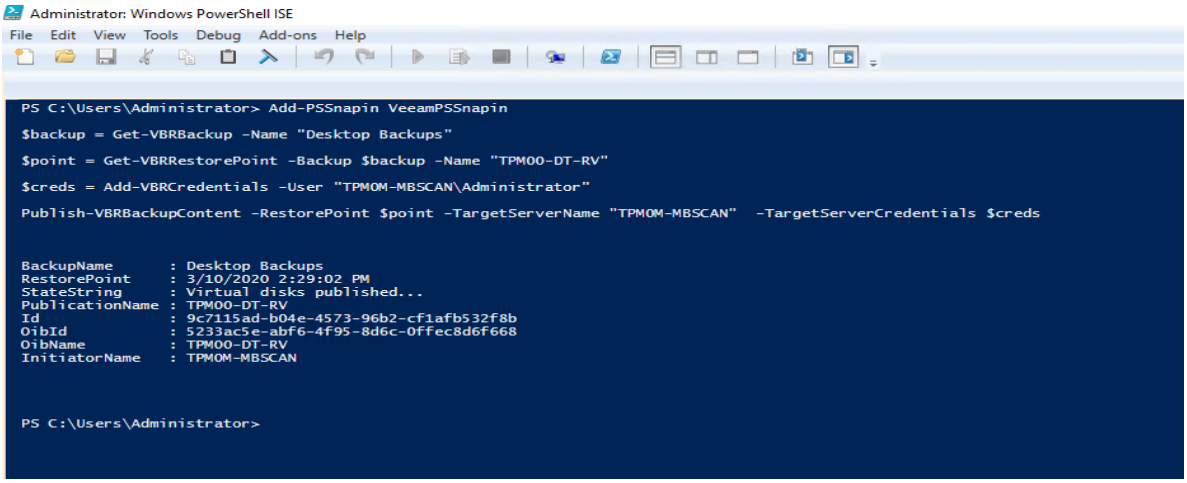
Оповещение о подозрительном размере инкрементальной копии: Это оповещение относится к Veeam ONE, когда он выполняет мониторинг Veeam Backup & Replication в представлении Data Protection. Это оповещение сообщает о подозрительно большом размере инкрементальной резервной копии. Логика основана на нормальном уровне изменения данных и на вероятности того, что исходные данные зашифрованы, что исключает применение опций сокращения их объема. Как и в большинстве оповещений Veeam ONE, настраиваемые правила позволяют задать глубину анализа. По умолчанию выполняется анализ трех точек восстановления. При уровне изменений 150% выдается предупреждение, а при уровне 200% — сообщение об ошибке. Оповещение показано ниже.



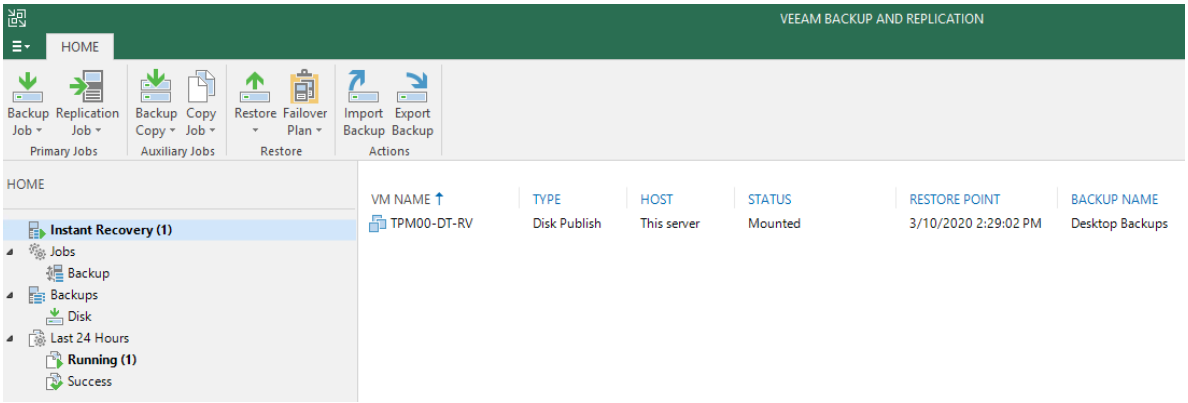
API для интеграции данных: API Veeam для интеграции данных, который входит в Veeam Backup & Replication v10, лучше всего использовать с помощью PowerShell. Эта возможность позволяет представить данные резервной копии Veeam Backup & Replication в виде подключенной папки Windows и обеспечивает доступ к этим данным. Это отличный новых метод защиты от программ-вымогателей, который позволяет дополнительно сканировать данные, сохраненные в резервных копиях, на предмет угроз.

Такое сканирование данных резервных копий может выполняться с применением дополнительных, более инвазивных инструментов, которые не могут быть использованы на производственных данных. Дополнительно, если резервные копии компьютеров находятся в репозиториях Veeam, это предоставляет широкие возможности для анализа на предмет проникновения потенциальных угроз.

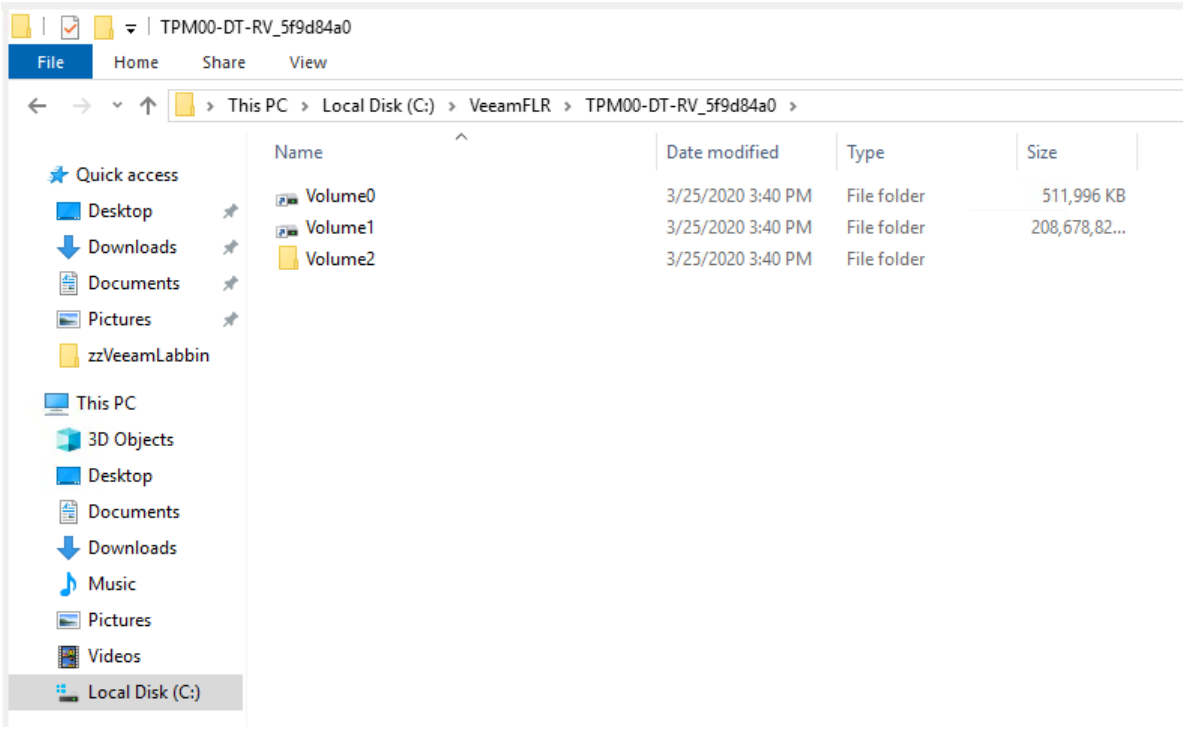
Использование API для интеграции данных начинается с резервных копий, размещенных в репозитории Veeam. Скрипт PowerShell, приведенный в качестве примера, запускает подключение резервной копии системы (TPM00-DT-RV) с помощью командлета Publish-VBRBackupContent. Это продемонстрировано на иллюстрации:



Это пример скрипта PowerShell для подключения одной резервной копии, но командлет также позволяет подключать несколько резервных копий. Здесь происходит выполнение задания мгновенной публикации диска в Backup & Replication. Это действие похоже на мгновенное восстановление виртуальной машины, но, вместо публикации резервной копии ВМ или агента в среде VMware или Hyper-V, публикация выполняется на сервере Veeam Backup & Replication. Процесс происходит прозрачно через iSCSI с помощью командлета. Сервер Veeam Backup & Replication представляет резервную копию в виде публикации диска, как показано ниже:

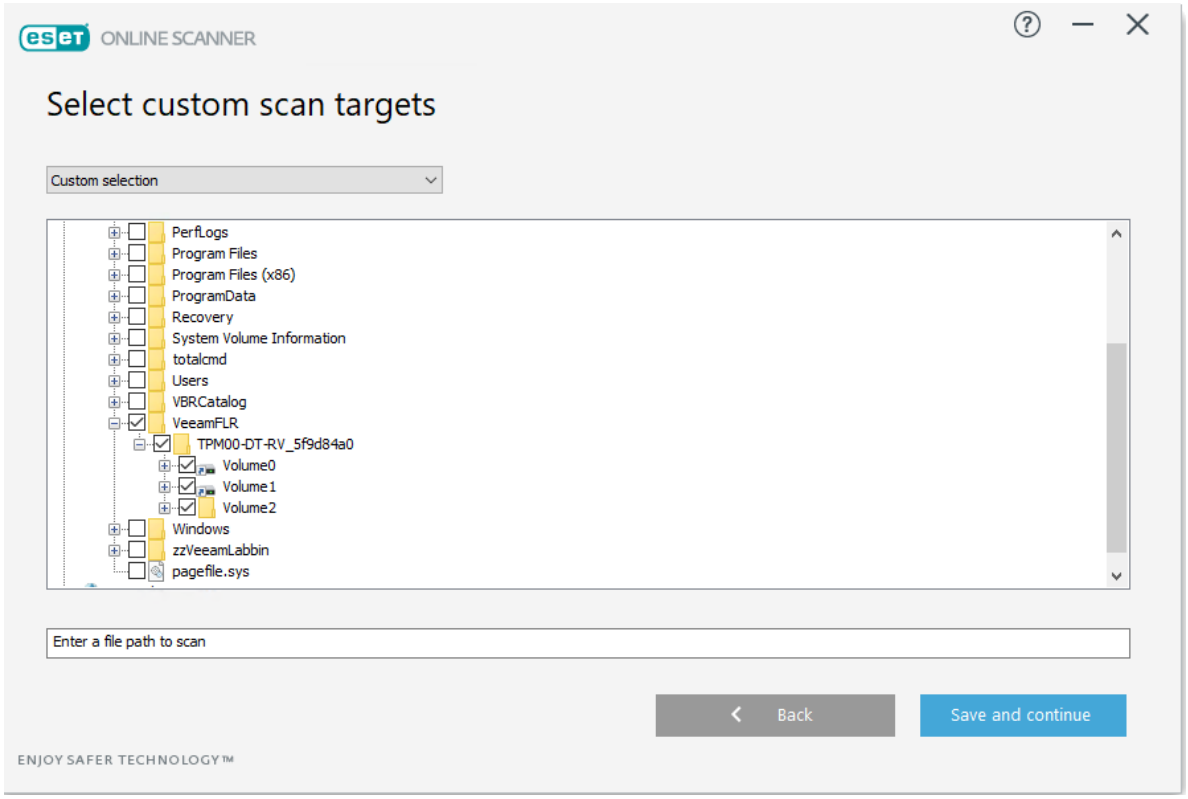


Содержимое резервных копий дисков представлено локально в виде папок на сервере Veeam Backup & Replication:

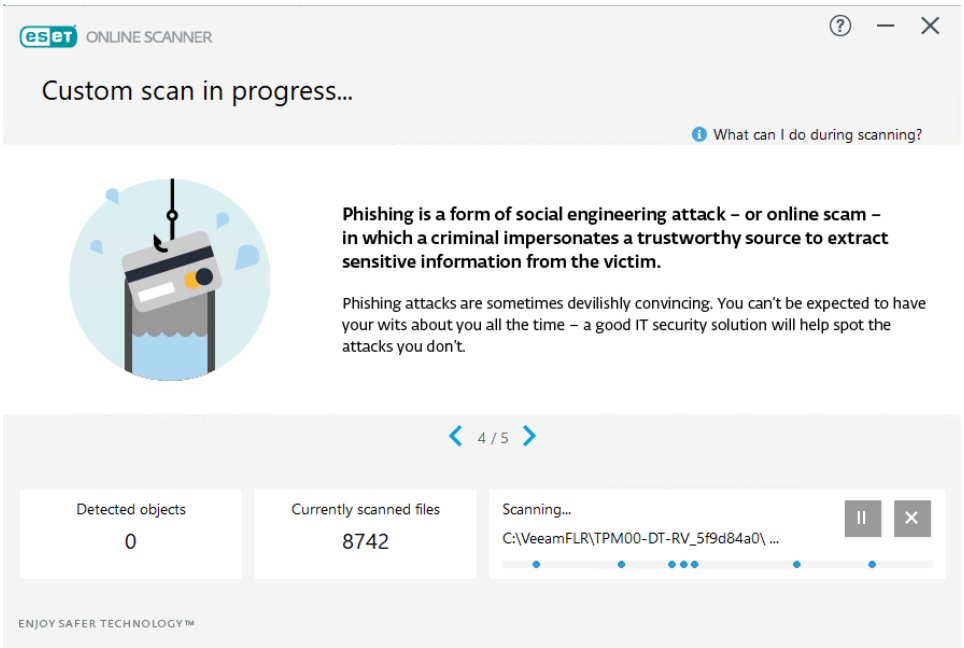


Благодаря этой функциональности вы можете использовать инфраструктуру резервного копирования наиболее эффективно. Можно выполнять расширенное сканирование систем, резервные копии которых были созданы с помощью Veeam. Два конкретных примера выявления угроз используют ESET и Total Commander.

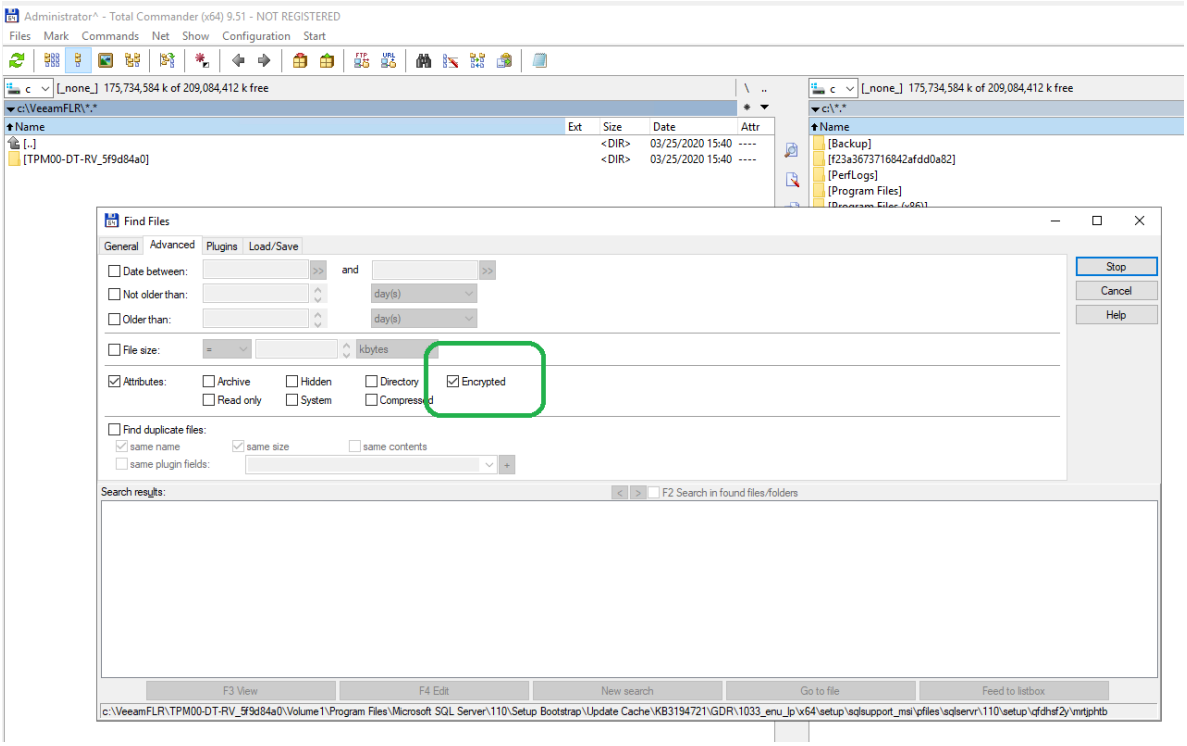
В первом примере ESET может использоваться для сканирования только пути VeeamFLR, который содержит опубликованные резервные копии.



После выбора пути VeeamFLR с помощью ESET можно выполнить сканирование. Перед сканом ESET скачивает последние сигнатуры угроз, чтобы обладать полнотой информации. Прогресс сканирования показан ниже:



Другой инструмент, который я хочу привести в пример как технику выявления угроз — это Total Commander. Многие ИТ-администраторы используют этот инструмент для расширения функций хранения. Интересная особенность Total Commander состоит в том, что поиск может просматривать путь VeeamFLR на предмет нахождения зашифрованных файлов, как показано ниже:



Ввиду фрагментации угроз не исключено, что поиск зашифрованных файлов не сможет показать файлы, зашифрованные программами-вымогателями. Возможности API Veeam для интеграции данных, в сочетании с другими инструментами, позволяют выявить угрозы до того, как они станут заметны в более широком масштабе. API Veeam для интеграции данных также предоставляет невероятные возможности для крупных сценариев автоматизации. Рассмотрим внедрение рабочих процессов, которые осуществляют резервное копирование, выполняют задания SureBackup и затем автоматически используют API для интеграции с данными. Это нужно, чтобы выполнить более интенсивное сканирование, чем то, которое допустимо на производственных данных. Возможность позволяет сократить время от внедрения угрозы до запуска эксплойта.

Глубокий анализ с помощью API Veeam для интеграции данных

Подробная информация об API Veeam для интеграции данных и соответствующих командлетах представлена здесь: http://vee.am/vdapi

Veeam DataLabs: Veeam DataLabs может использоваться для выявления угроз, а также для ремедиации. Задание SureBackup запускает Veeam DataLab для выполнения различных задач:

- Проверка возможности восстановления из резервных копий
- Тестирование системы, в том числе ее обновлений, изменений в приложениях и т.д.
- Поэтапный и безопасный методы восстановления

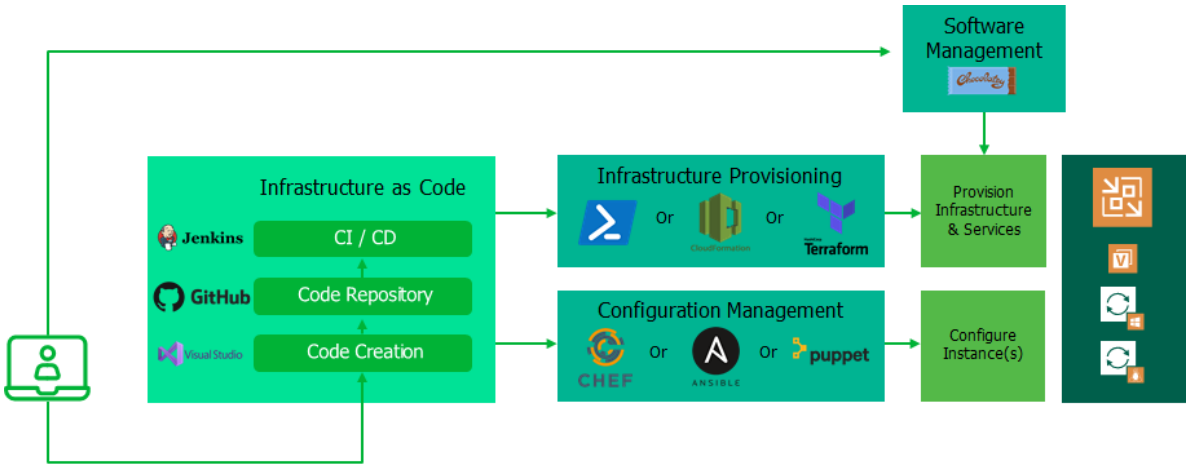
Если при запуске системы обнаруживается угроза, задание SureBackup определит, что система или приложения не запускаются, как обычно. Задания SureBackup помогают убедиться, что приложения запускаются из резервных копий (или реплик ВМ в среде VMware), а в отчете будет указано, что точка восстановления обеспечивает восстановление данных.

Задание SureBackup может продолжить работу после завершения всех проверок. По умолчанию задание SureBackup выполняет сконфигурированные тесты. Если задание продолжит работу, могут быть выполнены дополнительные проверки системы из точки восстановления резервной копии. Это может быть ручная проверка на предмет наличия угрозы, проверка наличия и зашифрованности конкретных файлов, а также извлечение отдельных данных.

Инвестиции в автоматизацию

Автоматизация также помогает повысить уровень защиты от программ-вымогателей. Если исходная инфраструктура не вызывает доверия, автоматизация может помочь в ситуациях ремедиации. Технологии Veeam, Microsoft, VMware и другие предлагают множество техник Infrastructure-as-Code.

Различные инструменты могут предоставить инфраструктуру, конфигурацию и ключевые сервисы.



Возможность создания полностью новой платформы для автоматического восстановления — привлекательная часть потенциального сценария использования. Платформа, в которой вам понадобится новая «среда» для восстановления, но с хорошими данными резервных копий Veeam. Рассмотрите некоторые из этих инструментов, которые можно быстро установить, если потребуется полное восстановление. Предлагаем дополнительную информацию об этих технологиях:

Сессия Veeam VMworld 2018:
https://videos.vmworld.com/global/2018/videoplayer/26243

Установка Veeam в Chef (Часть 1):
https://vzilla.co.uk/vzilla-blog/cooking-up-some-veeam-deployment-with-chef-automation-part-1

Установка Veeam в Chef (Часть 2):
https://vzilla.co.uk/vzilla-blog/cooking-up-some-veeam-deployment-with-chef-automation-part-2

Примеры инструментов Infrastructure-as-Code:
https://vzilla.co.uk/vzilla-blog/summerproject-infrastructure-as-code-example-tools

Операции Windows и использование Chocolatey для управления пакетами Windows с помощью Veeam Agents: https://vzilla.co.uk/vzilla-blog/windowsoperationsusingchocolateyforveeamdeployment

Ремедиация

Несмотря на все техники информирования и внедрения, используемые для защиты от программ-вымогателей, в случае проникновения угрозы следует быть готовыми к устранению последствий. В Veeam принят следующий подход к ремедиации после атаки программы-вымогателя:

- Не платить выкуп
- Единственный выход — восстановление данных

С учетом рекомендаций, приведенных выше в этом документе, у организаций должно быть несколько слоев защиты от атаки программы-вымогателя. О чем организации могли не подумать — это о том, что делать в случае обнаружения угрозы.

Предлагаем несколько рекомендаций по ремедиации, которые вы сможете применить в случае реальной атаки программы-вымогателя:

Техподдержка Veeam: В службе поддержки Veeam есть специальное подразделение, которое помогает заказчикам восстановить данные после атаки программы-вымогателя. Вы не хотите рисковать своими резервными копиями; они критически важны для возможности восстановления.

Коммуникация решает все: При любом бедствии правильная коммуникация становится важнейшей задачей. Составьте план эффективной коммуникации с нужными специалистами. План должен включать групповые списки, телефонные номера или другие способы коммуникации, обычно используемые по требованию, но расширенные на все группы ИТ-операций.

Эксперты: Составьте список экспертов по безопасности, ответам на инциденты, управлению идентификаторами и т.д, которые будут готовы оказать помощь в случае необходимости. Это могут быть как внутренние, так и внешние эксперты. Если вы сотрудничаете с поставщиком услуг Veeam, они могут предлагать дополнительные сервисы (например, защиту от инсайдеров через Veeam Cloud Connect).

Цепочка решений: Одним из труднейших аспектов восстановления после аварии может стать распределение ответственности за принятие решений. Кто дает указания восстанавливать данные, переключаться на реплики ВМ и др.? Это необходимо обсудить заранее.

Готовность к восстановлению: Когда условия благоприятствуют восстановлению, перед подключением систем к сети следует провести дополнительные проверки безопасности. Часть рекомендаций уже обсуждались в этом документе, но дополнительные шаги могут включать восстановление с отключенным доступом к сети для финальной проверки.

Возможности восстановления: В зависимости от ситуации полное восстановление ВМ может быть более предпочтительным. Восстановление файлов также имеет смысл. Знание доступных опций восстановления очень вам поможет.

Безопасное восстановление: Как мы уже упоминали, безопасное восстановление Veeam запускает антивирусное сканирование данных в процессе восстановления. Используйте последние сигнатуры вредоносного кода и, возможно, дополнительный инструмент для защиты от случайного повторного заражения.

Принудительная смена пароля: Пользователи не любят этого, но необходимо ввести принудительную смену пароля. Это сократит потенциальное поле распространения угрозы.

Заключение: готовьтесь сейчас, чтобы не опоздать!

Угроза реальна, а подготовка — полностью наша ответственность. Какие шаги необходимы для защиты от программ-вымогателей? В статье содержится несколько рекомендаций относительно информирования, внедрения и ремедиации. С правильной подготовкой шаги, представленные в статье, помогут улучшить защиту от программ-вымогателей и избежать потерь данных, а также финансовых, репутационных и многих других проблем.

Подробная информация о возможностях Veeam по защите от программ-вымогателей представлена здесь: http://vee.am/ransomwareseriespapers

Об авторе

Рик Вановер (Cisco Champion, vExpert) — старший директор Veeam Software по стратегии развития продуктов. Опыт Рика в ИТ-индустрии включает системное администрирование и управление ИТ, с акцентом на виртуализацию. Следите за публикациями Рика в Твиттере @RickVanover или @Veeam.

О компании Veeam Software

Veeam — лидер в области резервного копирования для управления данными в облаке. Veeam предлагает единую платформу для модернизации резервного копирования, ускорения перехода на технологии гибридного облака и защиты данных. У Veeam более 375 000 заказчиков по всему миру, в том числе 82% компаний из списка «Fortune 500» и 67% компаний из рейтинга «Global 2000». Показатели уровня удовлетворенности и коэффициента лояльности наших заказчиков — самые высокие в отрасли, в 3,5 раза выше среднего уровня. Экосистема глобальных партнеров Veeam включает в себя HPE, NetApp, Cisco и Lenovo и других эксклюзивных реселлеров. Офисы Veeam открыты более чем в 30 странах. Подробную информацию о компании можно найти на сайте https://www.veeam.com/ru. Подписывайтесь на Veeam в Твиттере https://twitter.com/Veeam.

VEEAM

Cloud Data

Backup for what's next

5 Stages of Cloud Data Management — start your journey today!

Learn more: veeam.com