Synology®

Защита организации от программ-вымогателей

Согласно прогнозам, атаки программ-вымогателей будут стоить организациям триллионов в 2023 году[1]. Планы защиты данных с возможностью быстрого восстановления являются критически важными для снижения влияния программ-вымогателей и других форм киберпреступности.

Date 13 окт. 2023 г.

Резервное копирование: последняя линия защиты в непредвиденной ситуации

Если данные теряются после злонамеренного удаления или изменения, резервные копии позволяют восстанавливать критически важные данные и избегать дорогостоящих простоев. Используйте решения Synology для защиты данных в разработке стратегии резервного копирования для всей ИТ-инфраструктуры.

Полная защита

Защита конечных точек и основных резервных копий для создания нескольких уровней защиты ваших данных.

Быстрое восстановление

Сокращение простоев до минимума при возникновении непредвиденных ситуаций благодаря возможностям мгновенного восстановления.

Неизменяемое хранилище

Предотвратите несанкционированные изменения данных и снимков.

Резервное копирование без лицензий

Резервное копирование любого объема данных, доступного в вашей системе хранения, без ограничений и скрытых платежей.

Централизованная защита от программ-вымогателей

Консолидация резервных копий из парка рабочих станций, серверов, виртуальных машин и облачных приложений. Оптимизация потребления ресурсов хранения и устранение узких мест полосы пропускания с помощью технологий дедупликации данных и инкрементного резервного копирования. https://www.synology.com/dsm/solution/infrastructure

Физические рабочие нагрузки

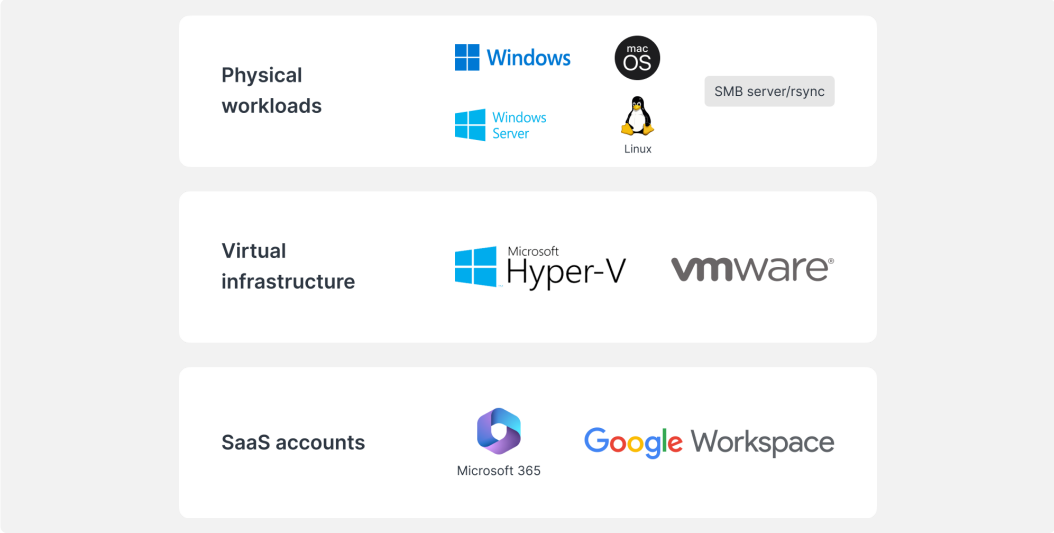
Защитите конечные точки в случае вредоносных атак с помощью комплексного резервного копирования "bare-metal" и гибкого восстановления на уровне файлов.

Виртуальная инфраструктура

Резервное копирование виртуальных машин и LUN VMware® vSphere™ и Microsoft® Hyper-V® с помощью мощных технологий сокращения объемов данных.

Учетные записи SaaS

Обеспечение непрерывной защиты данных, хранящихся в облаке, с автоматическим обнаружением новых учетных записей.



Эффективное восстановление

Минимизация простоев критически важных производственных систем за счет быстрого восстановления резервных копий из локальной или удаленной системы Synology.

Целевое время восстановления близкое к нулю

Подключите образы резервных копий в VMware®, Hyper-V® или Synology Virtual Machine Manager, чтобы возобновить работу как можно быстрее. Восстановление виртуальных машин на альтернативном гипервизоре во избежание прерывания обслуживания.

Минимальная целевая точка восстановления

Настройте частоту резервного копирования в соответствии с вашими потребностями, сведя к минимуму объем данных, которые могут быть затронуты во время атаки. Быстрая защита систем благодаря технологиям инкрементного резервного копирования и дедупликации.

Интуитивно понятное управление

Позвольте сотрудникам находить и просматривать электронные письма, контакты и файлы с удобного портала перед их восстановлением, обеспечивая удобство работы и снижая нагрузку на ИТ-отделы.

Дополнительный уровень защиты

Придерживайтесь стратегии резервного копирования «3-2-1», сохраняя третий набор данных в удаленной системе или в облаке, чтобы защитить ваши данные от пожара, стихийных бедствий или кражи.

Удаленные серверы

Храните резервные копии на сервере Synology в дополнительном расположении для защиты от физических аварий и выполняйте репликацию неизменяемых снимков для дополнительной защиты от программ-вымогателей.

В облаке

Выполняйте резервное копирование данных в облачное хранилище любого из крупных поставщиков для защиты от несанкционированного доступа с помощью шифрования AES-256 на стороне клиента. https://c2.synology.com/ru-ru/storage/nas

Надежность доказана в различных отраслях

«Synology [...] позволила нам сократить расходы на серверное оборудование [...] упростив при этом резервное копирование инфраструктуры и рабочих станций, ведение системных журналов и управление файлами».
https://www.synology.com/company/case_study/Investortools

«Благодаря Active Backup for Business обеспечивается централизованное хранение и круглосуточная доступность всех резервных копий, что помогает нам минимизировать время простоя и обеспечить соответствие нормативам FERPA».
https://www.synology.com/company/case_study/University_of_Washington

«[...] Active Backup for Business выполняет резервное копирование с невероятно высокой скоростью, а также эффективно удаляет дублирующиеся данные, используя всего 28 ТБ из 58 ТБ на сервере. [...]»
https://www.synology.com/company/case_study/SHISEIDO_Taiwan_ABB

«[...] Active Backup for Business [...] решение для централизации всех задач резервного копирования и управления ими с единой консоли. А быстрое и надежное восстановление обеспечивает непрерывность бизнеса».
https://www.synology.com/company/case_study/UNESCO

Часто задаваемые вопросы

Что такое программы-вымогатели?

Программы-вымогатели — это вредоносное ПО, шифрующее файлы жертв. После этого злоумышленники требуют выкуп для восстановления доступа к данным, часто угрожая окончательно удалить файлы, если выкуп не будет выплачен. Атаки программ-вымогателей бывают очень разрушительными и могут привести к значительным финансовым убыткам для отдельных лиц и организаций. Важно защитить себя и свои устройства от программ-вымогателей, например, регулярно обновляя программное обеспечение и выполняя резервное копирование файлов.

Какие типы программ-вымогателей существуют?

Существует множество различных типов программ-вымогателей, и постоянно разрабатываются новые «штаммы». К наиболее распространенным типам программ-вымогателей относятся:

- **Шифрующие программы-вымогатели** — наиболее распространенный тип программ-вымогателей, шифруют файлы жертвы таким образом, что к ним нельзя получить доступ без ключа дешифрования. Злоумышленники затем требуют выкуп в обмен на ключ
- **Блокирующие программы-вымогатели** — этот тип программ-вымогателей, которые блокируют доступ жертвы к компьютеру, изменяя учетные данные для входа или отображая сообщение. Затем злоумышленники требуют выкуп, чтобы разблокировать компьютер
- **Программа-вымогатель как услуга (RaaS)** — бизнес-модель, в которой злоумышленники предлагают программы-вымогатели другим лицам или группам, которые хотят совершать атаки. Как правило, первая компания предоставляет программы-вымогатели и обрабатывает платежи, а вторая получает процент от суммы выкупов
- **Программы для запугивания** — программы-вымогатели, разработанные для того, чтобы вынудить жертву заплатить выкуп путем запугивания. Обычно в таких программах используется отображение поддельных предупреждений или сообщений, которые заявляют о заражении компьютера жертвы вирусом. После этого злоумышленник требует выкуп, чтобы удалить предполагаемое заражение

Как распространяются программы-вымогатели?

Программы-вымогатели обычно распространяются через фишинговые электронные письма или посредством использования уязвимостей в компьютерной системе. При фишинговой атаке злоумышленник отправляет электронное письмо от безопасного источника, например банка или известной компании. Электронное письмо часто содержит ссылку или вложение, которые при нажатии на них установят программу-вымогатель на компьютере жертвы. Использование уязвимостей в системе происходит аналогичным образом, за исключением того, что злоумышленник будет использовать уязвимость в системе безопасности для установки программ-вымогателей без ведома жертвы. В любом случае после установки программы-вымогателя она может быстро распространиться на другие компьютеры в той же сети.

Каков типичный процесс атаки программ-вымогателей?

Процесс атаки программ-вымогателей обычно следующий:

1. Злоумышленник получает доступ к компьютеру жертвы либо путем отправки фишингового электронного письма, либо путем использования уязвимости в системе
2. После того, как злоумышленник получит доступ к компьютеру жертвы, он устанавливает в системе программу-вымогатель
3. Затем программа-вымогатель шифрует файлы жертвы, делая их недоступными для пользователя
4. После этого злоумышленник отправляет жертве требование выкупа, как правило, в виде цифровой валюты, например Bitcoin, в обмен на ключ дешифрования, который разблокирует зашифрованные файлы
5. Если жертва выплачивает выкуп, злоумышленник предоставляет ключ дешифрования, и жертва снова получает доступ к своим файлам. Тем не менее, злоумышленник не гарантирует, что он предоставит ключ, и даже если он сделает это, файлы жертвы могут быть повреждены в результате процесса шифрования

Важно отметить, что существует множество вариаций этого процесса, и не все атаки программ-вымогателей будут точно следовать описанным этапам. Некоторые атаки могут не включать шифрование файлов или включать другие формы вымогательства или шантажа.

Как программа-вымогатель может попасть на компьютер?

Существует несколько способов загрузки программы-вымогателя. Одним из наиболее распространенных является переход по вредоносной ссылке или открытие вложения в фишинговом электронном письме. Этот тип электронных писем предназначен для того, чтобы выглядеть безопасным, зачастую подражающим сообщению от хорошо известной компании или организации. При нажатии на ссылку или вложение программа-вымогатель устанавливается на компьютер. Другим способом получения программ-вымогателей является посещение скомпрометированного веб-сайта. Злоумышленники взломали эти веб-сайты и внедрили код, автоматически устанавливающий программу-вымогатель на ваш компьютер при посещении сайта. Вы также можете получить программы-вымогатели, скачав зараженные файлы из Интернета. Это может произойти, если вы скачиваете файл с подозрительного веб-сайта или файл, к которому вам предоставил доступ незнакомый человек. Если коротко, важно соблюдать осторожность при просмотре веб-страниц и избегать перехода по ссылкам или скачивания файлов из незнакомых источников. Это поможет вам защититься от программ-вымогателей и других вредоносных программ.

Кто является целью программ-вымогателей?

Атаки программ-вымогателей могут быть нацелены на любого пользователя компьютера или другого устройства, подключенного к Интернету. Тем не менее, некоторые группы с большей вероятностью становятся целью, чем другие. Например, атаки программ-вымогателей часто нацелены на компании, поскольку они зачастую владеют более ценными данными и более охотно заплатят выкуп, чтобы их вернуть. Больницы, школы и другие организации, предоставляющие критически важные услуги, также довольно часто становятся целями, поскольку атаки программ-вымогателей могут нарушить их работу и подвергнуть жизни людей риску. Отдельные пользователи также могут стать целью атак программ-вымогателей. В этих случаях злоумышленники могут попытаться получить деньги от жертвы, угрожая удалением личных файлов или публикацией конфиденциальной информации, если выкуп не будет выплачен. Цели атак программ-вымогателей часто выбираются на основе ценности их данных и их готовности заплатить вымогателю, чтобы вернуть их.

Какие риски связаны с оплатой программ-вымогателей?

Выплата выкупа злоумышленнику может показаться самым простым способом вернуть ваши файлы, но это может быть очень рискованным решением. Существует несколько рисков, связанных с выплатой выкупа, в том числе:

- Нет никакой гарантии, что злоумышленник предоставит ключ дешифрования. Во многих случаях жертвы, заплатившие выкуп, так и не получают ключ и не могут получить доступ к своим файлам
- Выплата выкупа может побудить злоумышленников продолжить свою кампанию атак. Если злоумышленники знают, что жертвы готовы заплатить выкуп, они с большей вероятностью продолжат совершать атаки в будущем
- Выплата выкупа может сделать вас объектом для будущих атак. Если злоумышленник знает, что вы готовы заплатить выкуп, то вы станете более вероятной целью атак в будущем
- Выплата выкупа может быть нарушением закона. В некоторых случаях выплата выкупа преступной организации может считаться формой финансирования терроризма или другой незаконной деятельности

Несмотря на то, что выплата выкупа может показаться самым простым способом возврата файлов, это очень рискованное решение. Перед принятием такого решения важно тщательно рассмотреть риски.

Какую сумму требуют программы-вымогатели?

Сумма выкупа программ-вымогателей может значительно различаться в зависимости от ряда факторов, таких как тип используемой программы-вымогателя, количество зашифрованных файлов и эффективность атаки. В некоторых случаях сумма выкупа программ-вымогателей может быть относительно низкой, например злоумышленники требуют несколько сотен долларов. В других случаях затраты могут быть значительно выше, а злоумышленники требуют тысячи долларов или даже больше для восстановления доступа к файлам жертвы. Помимо прямых расходов, связанных с выкупом, атаки программ-вымогателей также могут нести за собой значительные косвенные расходы. Например, атака программы-вымогателя может привести к простою и потере производительности, что, в свою очередь, может привести к потере выручки и доходов. Кроме того, это может нанести ущерб репутации компании и доверию клиентов, что может отрицательно повлиять на бизнес в долгосрочной перспективе. Эти косвенные расходы часто намного выше, чем сумма выкупа.

Каковы симптомы программ-вымогателей?

Симптомы атак программ-вымогателей могут различаться в зависимости от типа используемой программы-вымогателя. Однако некоторые распространенные симптомы включают:

- Ваши файлы зашифрованы, и вы не можете получить к ним доступ
- Вы получили сообщение от злоумышленника с требованием выкупа в обмен на ключ дешифрования
- Вы видите незнакомые программы или процессы, запущенные на вашем компьютере
- Компьютер работает медленно или не отвечает
- Компьютер отображает необычные сообщения об ошибках или всплывающие окна

Если вы подозреваете, что компьютер заражен программой-вымогателем, важно действовать быстро. Отключите компьютер от Интернета, чтобы предотвратить распространение программы-вымогателя.

Как предотвратить атаку программ-вымогателей?

Есть несколько шагов, которые можно предпринять для предотвращения атак программ-вымогателей:

- Используйте зарекомендовавшее себя антивирусное программное обеспечение или программное обеспечение для обеспечения безопасности и регулярно обновляйте его. Это поможет защитить компьютер от программ-вымогателей и других вредоносных программ
- Будьте осторожны при открытии вложений или ссылок в электронных письмах. Программы-вымогатели часто доставляются через фишинговые электронные письма, поэтому важно тщательно следить за тем, что вы нажимаете
- Регулярно обновляйте операционную систему и другое программное обеспечение. Обновления программного обеспечения часто включают в себя исправления системы безопасности, которые помогают защитить компьютер от программ-вымогателей и других угроз
- Регулярно выполняйте резервное копирование файлов. Это поможет защитить ваши данные в случае заражения компьютера программами-вымогателями. Обязательно придерживайтесь одной из рекомендованных стратегий резервного копирования, таких как стратегия резервного копирования «3-2-1»
- Помните о рисках программ-вымогателей и расскажите другим сотрудникам организации об этих угрозах. Это поможет предотвратить атаки программ-вымогателей и облегчить их обнаружение и реагирование на них в случае их возникновения

Лучший способ предотвратить атаки программ-вымогателей — сохранять бдительность и принимать меры по защите компьютера и данных. Это поможет снизить риск атаки программ-вымогателей и упростить восстановление после такой атаки.

Как Synology защищает меня от программ-вымогателей?

Для защиты от программ-вымогателей необходимо принять превентивные меры. Используйте эти решения Synology в дополнение к антивирусному программному обеспечению на ваш выбор.

- **Предотвращение доступа** — для снижения распространения программ-вымогателей установите права доступа к файлам и приложениям и настройте учетные данные для безопасного входа с помощью Secure SignIn и C2 Password
- **Защита устройств** — устаревшие системы подвержены большему риску. Обновите все NAS с помощью Synology CMS и защитите другие устройств с помощью групповых политик в Synology Directory Server и решения C2 Identity
- **Избегайте подозрительных файлов** — спам и фишинговые электронные письма, содержащие подозрительные файлы, являются распространенными методами внедрения программ-вымогателей. Synology MailPlus обеспечивает надежную защиту от вредоносных программ и спама
- **Проверяйте наличие уязвимостей** — используйте Synology Security Advisor для регулярного отслеживания вредоносных программ, уязвимостей и необычных попыток входа в систему. Внедряйте рекомендованные изменения для повышения безопасности NAS. https://www.synology.com/dsm/overview/security

Дополнительные способы защиты данных

Управление парком систем

Используйте расширенные функции для централизованного управления разрешениями на доступ к данным, состоянием программного обеспечения, состоянием системы и т. д.
https://www.synology.com/dsm/overview/administration

Мониторинг всех систем

Выявляйте подозрительные попытки входа, управляйте обновлениями и осуществляйте мониторинг состояния устройств независимо от их местоположения.
https://www.synology.com/dsm/feature/active-insight

Защита ваших данных

Следуйте правилу резервного копирования «3-2-1», чтобы защитить данные от случайного или злонамеренного изменения или удаления.
https://www.synology.com/dsm/solution/data_backup

Защита со всех сторон

Получите наш чек-лист по кибербезопасности и определите свои слабые места на случай хакерской атаки.
https://global.download.synology.com/download/Document/Software/Brochure/Firmware/DSM/7.0/rus/Se

Начало работы

Контакты

Обратитесь в региональный отдел продаж для получения дополнительных сведений
https://www.synology.com/form/inquiry/sales

Где купить

Найти партнера Synology в вашем регионе
https://www.synology.com/wheretobuy

Примечания:

1. eSentire, Официальный отчет о киберпреступлениях 2022
   https://www.esentire.com/resources/library/2022-official-cybercrime-report

Защита организации от программ-вымогателей

https://www.synology.com/ru-ru/dsm/solution/ransomware

Веб-сайт Synology

https://www.synology.com/

Контакты

https://www.synology.com/company/contact_us