Hewlett Packard Enterprise | Veeam

**Краткий обзор решения**

# Защитите свои данные от угроз со стороны вредоносных программ-вымогателей

Рекомендации по обеспечению доступности данных помогут компаниям могли предотвратить потенциальные потери данных и простой из-за атак программ-вымогателей или эффективно подготовиться к этим атакам. Следуя отраслевым рекомендациям, ИТ-руководители смогут избежать финансовых потерь и обеспечить доступность данных используя программное обеспечение HPE и Veeam®.

«Нет единого способа или средства, которые полностью защитят вас и вашу организацию от атак программ-вымогателей. Но подготовка к непредвиденным ситуациям и планирование восстановительных операций играют важную роль в восстановлении и непрерывности работы компании — и эти планы должны проверяться регулярно».

– Бывший помощник директора киберподразделения ФБР, Джеймс Трейнор (James Trainor).

Эта цитата помогает пользователям понять, что программа-вымогатель является только частью всей картины угроз и в конечном итоге какая-нибудь из них все равно попадет в вашу сеть. Наилучшим решением является защита того, за чем охотятся злоумышленники, — ваших данных. **fbi.gov/news/stories/incidents-of-ransomware-on-the-rise**

## Рост числа атак программ-вымогателей

Атаки программ-вымогателей охватывают все большее число отраслей, используя уязвимости, связанные с соответствием нормативным и законодательным требованиям, слабой защитой сетей и неэффективными методиками резервного копирования. По мере роста числа угроз все больше отраслей и компаний разного рода становятся мишенью атак с использованием уязвимостей. И даже надежные решения кибербезопасности и передовые практики не всегда могут предотвратить атаки. Согласно данным Института технологий ключевой инфраструктуры, в 2016 и 2017 гг. программы-вымогатели нанесут компаниям серьезный ущерб. Атаки в целях вымогательства находятся на подъеме — им подверглись «почти 40 % предприятий»[1].

## Риски атак программ-вымогателей для компаний и ИТ

Атаки программ-вымогателей связаны не только с риском безопасности. Компании, которые стали жертвами программ-вымогателей, столкнулись с финансовыми и техническими проблемами, а также с потерей репутации, которую никогда не восстановить.

## Финансовые потери

Расходы на выкуп, потеря драгоценного времени ИТ-сотрудников и потенциальный простой критически важных приложений могут нанести непоправимый ущерб бизнесу.

## Утрата контроля над ИТ-инфраструктурой

Хакеры могут контролировать сеть сеть атакованной компании и получать к ней доступ для организации будущих атак с целью получения выкупа. ИТ-руководители сталкиваются с регулярно возникающими угрозами и выделяют больше ресурсов на предотвращение атак программ-вымогателей. Этих ресурсов не хватает ИТ-задачам, которые играют важную роль для бизнеса.

## Потеря репутации компании

Многие компании не сообщают об атаках программ-вымогателей, чтобы не навредить своей репутации, не потерять клиентов и свою долю на рынке. Но и те компании, которые заплатили выкуп или не создали резервные копии своих данных, в конечном счете становятся жертвами более сложных атак, что приводит к серьезным имиджевым потерям на рынке.

[1] «**Атаки в целях вымогательства находятся на подъеме — им подверглись "почти 40 % предприятий"**». The Guardian, август 2016 г.

**Обзор решений Veeam и HPE**
Ведущие отраслевые решения Veeam и HPE обладают всем необходимым для компаний любого размера, чтобы бороться с вредоносными атаками и защищать данные компаний.

- **Хранение и быстрое восстановление данных**
  Моментальные снимки систем хранения данных HPE позволяют использовать быструю виртуальную машину и выполнять поэлементное восстановление зашифрованных программами-вымогателями баз данных, приложений, файлов и операционных систем. Быстрое восстановление и предотвращение простоя приложений с помощью зарекомендовавшей себя интеграции с HPE 3PAR StoreServ, Store Virtual, StoreOnce и StoreOnce Catalyst.
- **Блокировка инфраструктуры**
  Программы-вымогатели не смогут заразить то, что не они не могут видеть. Это стало возможным благодаря интеграции с решением HPE StoreOnce Catalyst, которое делает образы резервных копий невидимыми для программ-вымогателей, обеспечивая тем самым возможность восстановления. Дополнительная защита обеспечивается благодаря наличию пленочных копий вне рабочего места и асинхронной удаленной репликации.
- **Проверка среды**
  Быстрая проверка и удаление вредоносных элементов перед восстановлением с помощью виртуальных машин и решений Veeam On-Demand Sandbox™ и Veeam SureBackup.
- **Простота использования по умолчанию**
  Использование встроенной оценки резервной копии для обеспечения защиты критически важных виртуальных машин с помощью средства мониторинга, создания отчетов и планирования ресурсов Veeam ONE™.

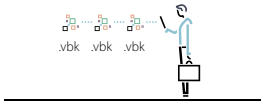
Эти возможности доступны по умолчанию при совместной интеграции Veeam Availability Suite™ и системы хранения данных HPE. Для этого решения не требуются специальные сценарии, и в нем используются стандартные продукты HPE и Veeam.

**Подпишитесь и будьте в курсе последних новостей**

## Возможности обеспечения доступности Veeam

Мгновенное восстановление с помощью ВМ/песочница по запросу/репликация для любых источников и мест назначения/проверка резервных копий/комплексный мониторинг

**3 различные копии данных**




Уменьшение бизнес-рисков; гарантия наличия хорошего образа для восстановления

- В одной копии используются мгновенные снимки HPE для мгновенного перезапуска и восстановления — лучший показатель ЦВВ.
- Одна копия в безопасном репозитории резервных копий в StoreOnce с применением Catalyst — базовый образ.
- Одна копия на автономном носителе (ленточном накопителе HPE StoreEver) — исключение рисков.

**2 различных носителя**

Устранение зависимости от одного типа носителей

- Одна копия в безопасном репозитории резервных копий в StoreOnce с применением Catalyst — образ на защищенных дисках.
- Одна копия на автономном носителе (ленточном накопителе HPE StoreEver) — долгосрочный образ на автономной пленке.

**1 из которых вне рабочего места**

Перемещение данных с рабочего места

- Ограничение долгосрочного сбоя в работе — дополнительная защита с помощью удаленного аварийного восстановления.

## Пример внедрения: успешная защита от программ-вымогателей с помощью Veeam

Жертвой атаки программы-вымогателя стала школа Бедфорд в Англии. Вирус Cryptolocker атаковал компьютер сотрудника факультета и зашифровал все файлы. У школы не было ресурсов, чтобы заплатить солидный выкуп, и она больше не могла ждать, когда снова заработает ее сеть.

ИТ-отдел школы Бедфорда следовал правилу резервного копирования 3-2-1, что помогло не платить выкуп и восстановить работоспособность сети. Компания Veeam помогла быстро восстановить все зашифрованные файлы.

## Решение HPE и Veeam для защиты от программ-вымогателей

Это решение для обеспечения доступности данных от компаний Veeam и HPE разработано для борьбы с атаками программ-вымогателей злоумышленников. Следуя рекомендациям о резервном копировании 3-2-1 компании Veeam, компании могут обеспечить целостность и доступность своих данных. На диаграмме выше изображено правило 3-2-1 вместе с передовыми рекомендациями.

## Использование правила резервного копирования 3-2-1

Целью правила 3-2-1 является предоставление клиентам решения для защиты данных, которое максимально увеличивает время бесперебойной работы приложений и доступность данных. Правильно применяя рекомендации резервного копирования 3-2-1, ИТ-руководители могут защитить свои данные. Указания к правилу 3-2-1 см. ниже.

- **Храните три (3) копии своих данных (первичные данные и две копии), чтобы избежать потери данных из-за неисправной резервной копии.**
- **Храните резервные копии на двух (2) разных типах носителей, таких как ленточный накопитель, дисковый накопитель, вспомогательный накопитель или облако.**
- **Храните одну (1) копию вне рабочего места — на ленточном накопителе или в облаке — на случай локальных опасных факторов или заражений программами-вымогателями внутренней сети.**

## Заключение

Решение для обеспечения доступности данных — это полностью интегрированное решение на основе существующих технологий. Оно не только позволяет организациям быстро восстановиться после атаки программ-вымогателей, но и предоставляет решение для обеспечения доступности данных корпоративного уровня для повседневных операций. Это решение основано на передовом опыте, оно достаточно гибкое и недорогое и может быть быстро развернуто сертифицированным партнером Veeam.

**Подробнее** о том, как следовать правилу 3-2-1 с помощью Veeam Backup & Replication™.

© Hewlett Packard Enterprise Development LP, 2017 г. Информация в настоящем документе может быть изменена без предварительного уведомления. Гарантийные обязательства для продуктов и услуг Hewlett Packard Enterprise приведены только в условиях явной гарантии, прилагаемой к каждому продукту и услуге. Никакие содержащиеся здесь сведения не должны трактоваться как дополнительные гарантийные обязательства. Hewlett Packard Enterprise не несет ответственности за технические или редакторские ошибки или пропуски, имеющиеся в этом документе.

a00000445rue, январь 2017 г.