

HPE Zerto:

Hewlett Packard Enterprise
operated by Sophela

захист бізнесу від програм-вимагачів та гнучка міграція даних

Рішення від HPE забезпечує не лише захист даних і програм від кібератак і непередбачуваних ситуацій, а й дозволяє легко переносити дані між різними середовищами.

Кожні 14 секунд одна компанія у світі стає жертвою атаки програм-вимагачів. Зараження цим шкідливим ПЗ може мати руйнівні наслідки як для великих корпорацій, так і для малого бізнесу. Якщо хакери отримують контроль над серверами компанії, вони зможуть обмежити доступ до важливих даних, зашифрувати або вкрасти особисту інформацію. Тенденція останніх десятиліть у світі така: у багатьох компаній, від середніх до великих, з'являється більше грошей, які вони можуть витратити, що спонукає зловмисників здійснювати спроби масштабніших здіриств. За

оцінками експертів з кібербезпеки, до 2025 року витрати на запобігання атакам програм-здіричків перевищать \$40 млрд, це щороку буде приносити кіберзлочинцям понад мільярд доларів прибутку.

Виникає питання: яких заходів ви можете вжити, щоб знизити кіберризик та захистити свої цінні бізнес-активи?

Розв'язання проблеми — HPE Zerto

Рішення HPE Zerto пропонує безперервний захист даних для багатьох

застосунків від загроз у різних віртуалізованих і хмарних середовищах, незалежно від того, чи потрібно IT-відділам захистити віртуальні машини локально за допомогою VMware (для усіх версій HPE Zerto) та Hyper-V (для усіх версій HPE Zerto, але не вище версії 9.7), чи в якомусь з варіантів загальнодоступних або приватних хмар. HPE Zerto фокусує увагу на трьох основних варіантах використання. Ці варіанти допоможуть IT-відділам відновлюватися після аварій, які можуть вивести з ладу основний майданчик (ЦОД). Також це рішення здатне захистити критично важливі дані завдяки

ПОСТІЙНИЙ ЗАХИСТ

Будь-який додаток, будь-яка хмара, будь-яка загроза



Відновлення від програм-вимагачів

Відновлення від хвилин до секунд перед атакою



Аварійне відновлення

Надійне відновлення з найшвидшим RTO та RPO



Мультихмарна Мобільність

Свобода інновацій у хмарах

Безперервний захист даних

Microsoft Azure

Google Cloud

aws

IBM Cloud

ORACLE
CLOUD

Hewlett Packard
Enterprise

vmware

Azure
Kubernetes
Service
(AKS)

Google Kubernetes Engine

AmazonEKS

Microsoft
Hyper-V

RED HAT
OPENSIFT

Рис. 1. HPE Zerto захищає дані та забезпечує їх вільне перенесення

дуже малим значенням RTO і RPO. HPE Zerto робить бізнес-застосунки та дані стійкими до програм-вимагачів, даючи змогу швидко відновлювати дані до стану за секунди або хвилини «до атаки». Та найголовніше — HPE Zerto виходить за рамки захисту даних, адже забезпечує їх мобільність/міграцію даних, надаючи IT-фахівцям свободу для інновацій у декількох сферах (рис. 1).

Основні варіанти використання HPE Zerto

Можна виділити три основні сценарії використання HPE Zerto (рис. 2).

Перші два допомагають IT-фахівцям мінімізувати незаплановані збої у доступності даних і роботі застосунків, які цими даними користуються. HPE Zerto допомагає компаніям відновлюватися, наприклад, після стихійних лих та катастроф, а також захищатися від непередбачуваних ситуацій. До «катастроф» також можна віднести будь-які збої інфраструктури, які заважають правильній роботі сервісів на основному майданчику. Людський фактор теж може призводити до помилок, які завдають шкоди повсякденним операціям з даними.

HPE Zerto робить компанії більш стійкими до програм-вимагачів — ще однієї «катастрофи», яка може уразити дані. Діями програм-вимагачів керує зловмисний інтелект — програмне забезпечення. Саме це ускладнює захист від подібних загроз. HPE Zerto не тільки допомагає IT-відділам відновлювати дані до стану за лічені секунди або хвилини «до атаки», але також може допомогти в аналізі подій (професійній експертизі) та посиленні захисту після атаки.

Також в HPE Zerto реалізовано технологію безперервного захисту даних (CDP), яка може допомогти з підтриманням запланованої діяльності компанії. Замість того, щоб реплікувати дані на інший майданчик для подальшого відновлення, IT-адміністратори, відповідальні за резервне копіювання, можуть з легкістю перенести їх деінде в рамках ширшої стратегії цифрової трансформації. У сучасному вже установленому гібридному і багатохмарному світі у компанії може бути безліч причин переміщувати застосунки та дані. Вони можуть захотіти перенести дані з однієї хмари в іншу, яка пропонує вигідніші фінансові умови або кращу придатність/збереження для нових варіантів використання. Або повернути застосунки та дані з хмари назад у локальне середовище (ЦОД), щоб зменшити затримку чи краще контролювати суверенітет даних. Якою б не була причина, IT-відділам буде простіше виконувати міграцію за допомогою HPE Zerto.

Додаткові варіанти використання HPE Zerto

Хоча більшість компаній купують рішення HPE Zerto для вищевказаних сценаріїв використання, слід розуміти кілька додаткових варіантів, які можуть забезпечити додаткову цінність цього продукту.

IT-відділи можуть використовувати HPE Zerto при створенні та експлуатації середовища тестування або розробки. HPE Zerto може безперервно реплікувати туди дані з виробничого середовища, гарантуючи їх точне узгодження. Чим краща узгодженість, тим надійніші результати розробки або тестування. Аналогічним чином HPE Zerto може допомогти відповідальним

адміністраторам створити середовище тестування виправлень/патчів, яке точніше відповідає виробничому середовищу. Завдяки цій більш точній відповідності розробники застосунків можуть з впевненістю розгортати виправлення у виробничому середовищі.

Оркестрація, автоматизація та аналітика

Які ще вигоди використання цього рішення можна виділити? Це простота у масштабуванні — основний принцип платформи, який реалізується завдяки можливостям оркестрації, автоматизації та аналітики від HPE. Впровадження та розгортання локально або у хмарі відбувається швидко завдяки інтеграції зі стеком технологій, які вже розгорнуті в компаніях. Це спрощує поточне управління і дає змогу легко масштабувати захист до 1000 віртуальних машин і петабайтів даних для дотримання критично важливих угод про рівень обслуговування (SLA).

Завдяки вбудованій оркестрації автоматизуються ручні процеси, забезпечується просте тестування відновлення і міграції без переривання роботи та можливість проводити ці дії, наприклад, у робочий час. Згідно з опитуванням, проведеним серед компаній, які вже експлуатують це рішення, HPE Zerto дає повну впевненість у відновленні працездатності у разі збою.

Ще один компонент рішення HPE Zerto — Zerto Analytics — гарантує повну прозорість і звітність щодо об'єктів IT-середовищ, а також повну відповідність нормативним вимогам, як-от GDPR, PCI, ISO, SOX, HIPAA та ін., і уможливорює інтелектуальне прогнозне планування інфраструктури.

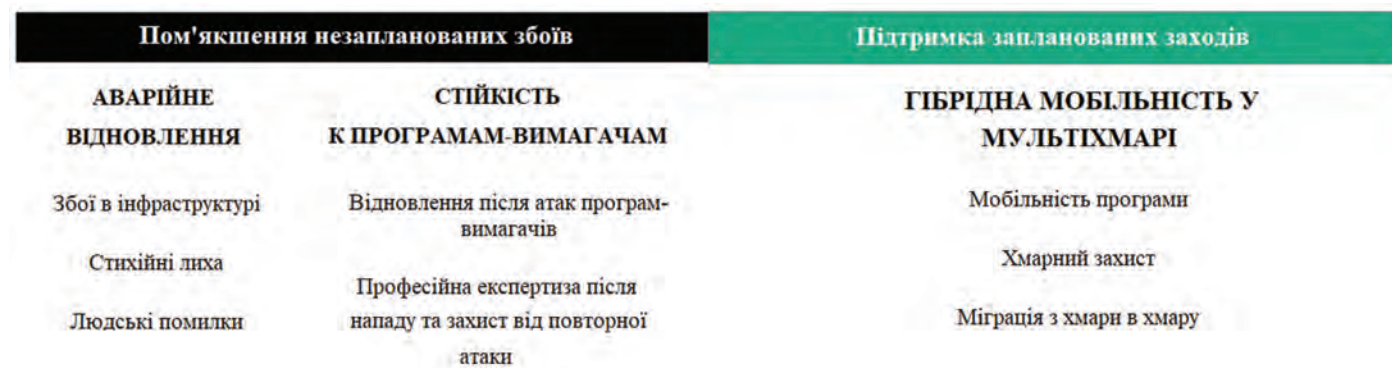


Рис. 2. Три основні сценарії використання HPE Zerto



Рис. 3. HPE Zerto — рішення для компаній всіх типів і розмірів

Хто може використовувати HPE Zerto?

Якщо уважно подивитись на список клієнтів (рис. 3), можна побачити компанії з багатьох галузей і різного розміру, від великих до малих підприємств, з різними інфраструктурами та потребами. Їх об'єднує необхідність вести безперебійний бізнес незалежно від того, як розвиваються технології або які нові загрози виникають. В Україні вже є кінцеві замовники, які мають досвід тестування, впровадження та експлуатації цього продукту. Головне, щоб середовище було віртуальним, мінімальна кількість віртуальних машин — 5. Так само підтримується велика кількість відомих хмарних провайдерів.

Висновки

Розглядаючи рішення HPE Zerto детальніше, слід пам'ятати, що його основою є безперервний захист даних (CDP). Постійне використання HPE Zerto усуває необхідність планування, створення знімків і нагляду за резервними копіями. HPE Zerto об'єднує функції аварійного відновлення, безперервного резервного копіювання та довгострокового зберігання. Крім того, механізм реплікації HPE Zerto є найкращим у своєму класі для забезпечення мобільності та міграції даних: на «землі», між «землею» і хмарою та між хмарами. Ця технологія відкриває різноманітні можливості, серед яких — повторне використання даних і створення «пісочниць» для розроблення та тестування на вимогу, які відстають лише на кілька секунд від виробничого середовища. Така деталізація також корисна для боротьби з програмами-здириками, аналізу стану безпеки та інших випадків використання, пов'язаних із кіберзахистом.

Невіддільна частина рішення — це оркестрація та автоматизація, вбудовані у платформу. Таким чином під час

експлуатації виключаються ручні процеси та підвищується ефективність, що спрощує захист даних.

Платформа містить аналітику включно з готовими інформаційними панелями та звітами, які забезпечують повну видимість у багатосайтових і багатохмарних середовищах і дають змогу легко та автоматично складати звіти про відповідність нормативним вимогам. Це не просто видимість — це інструменти для інтелектуального прогнозного планування інфраструктури, які розширюють можливості діяти на випередження.

Аналітичну підсистему цього рішення розроблено з використанням методології API First. Це означає: все, що ви бачите в призначеному для користувача інтерфейсі аналітики, доступно в API. Ці API постачаються з відкритим вихідним кодом Swagger, який допоможе вам розробляти та тестувати інтеграцію REST з використанням стандартизованих прикладів і готових шаблонів.

Усе перелічене доступне на найрізноманітніших платформах і хмарах незалежно від того, чи хоче компанія локальне розгортання або ж загальнодоступну, гібридну чи власну хмару. А глибока інтеграція з рішеннями стратегічних технологічних партнерів забезпечує простоту взаємодії між платформою HPE і стеком технологій вашої компанії.



Михайло ФЕДОСЕЄВ,
архітектор
інфраструктурних рішень Lantec
+38 044 360-56-27,
office@lantec.ua, <https://lantec.ua>

LANTEC
25 років партнерства

