Рішення Dell Technologies

для захисту даних в середовищах хмарних провайдерів

Компанія Dell пропонує комплекс рішень, які забезпечують не лише створення резервних копій, але і захист їх від кіберзагроз.

Dell має у своєму портфелі повний спектр рішень для резервного копіювання – як на землі, так і у хмарах. Компанія співпрацює з основними постачальниками хмарних рішень (AWS, Microsoft Azure, Google Cloud тощо), а також забезпечує інтеграцію з продуктами VMware, які працюють на цих платформах. Сценарії використання рішень Dell різноманітні: резервне копіювання в хмару і всередині хмари, використання хмари як майданчика для аварійного відновлення, для довготривалого зберігання даних, для захисту cloud-native навантажень на кшталт контейнерів, а також для побудови ізольованого середовища для захисту від кіберзагроз.

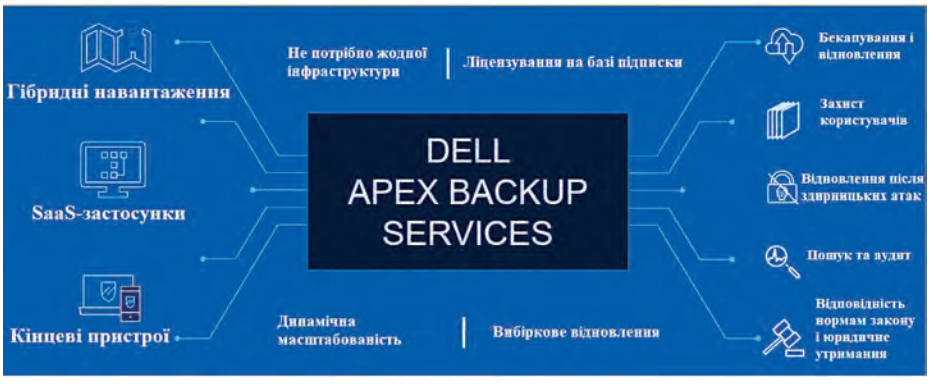

Рис. 1. Сервіс APEX Backup Services та його можливості

Зберігаймо ощадливо

APEX Protection Storage – це пристрій для зберігання резервних копій, який можна розгорнути як в наземному датацентрі, так і в хмарі. Він доступний у маркетплейсах усіх основних хмарних провайдерів, має розмір від 1 до 256 ТБ корисного простору для даних до дедублікації. Пристрій ліцензується за схемою BYOL (Bring Your Own License), тобто можна в хмарі активувати існуючу ліцензію для «наземного» пристрою. В маркетплейсах же доступна тимчасова ліцензія на 90 діб. До речі, саме ця можливість дуже допомогла на початку війни тим українським компаніям, які шукали швидкий і дешевий варіант евакуації своїх даних за кордон.

Важливо, що розміщення системи APEX Protection Storage в публічній хмарі дозволяє суттєво заощадити простір під резервні копії завдяки дедублікації. Звісно, сам віртуальний пристрій використовує деякі обчислювальні ресурси, але зате ємність сховища можна скоротити в декілька разів або навіть десятки разів, а вартість зберігання в обрахунку на 1 ГБ скорочується в середньому на 30%. Водночас зменшуються витрати на трафік під час повернення резервної копії зі сховища.

Як доповнення до APEX Protection Storage Dell пропонує PowerProtect Data Manager – програмне забезпечення, за допомогою якого можна створювати на платформах хмарних провайдерів резервні копії віртуальних машин, баз даних, застосунків тощо. Це ПЗ ліцензується за тією самою схемою, що й APEX Protection Storage, і разом обидва продукти утворюють готову систему резервного копіювання в хмарі, яка пропонується на маркетплейсах як один шаблон. Разом з Data Manager замовник автоматично отримує можливість користування SaaS-сервісом Cloud Snapshot Manager, який призначений для захисту «cloud-native» навантажень.

Також Dell пропонує послугу APEX Backup Services – повноцінну систему резервного копіювання, яка надається як сервіс на базі ресурсів AWS (**рис. 1**). Її беззаперечною перевагою є те, що створені даним сервісом резервні копії передаються безпосередньо в хмару, без використання будь-яких проміжних сховищ для розміщення резервних даних. Розміщені у хмарі резервні копії захищені за допомогою подвійного шифрування, ключ до якого має тільки замовник.

APEX Backup Services включає три послуги: захист SaaS-застосунків (Microsoft Office 365, Google Workspace, Salesforce), кінцевих пристроїв і гібридних навантажень (віртуалізовані середовища, бази даних, файлові сервери, мережеві сховища). Єдина веб-консоль забезпечує повну видимість резервних копій і управління ними. Замовник обирає підписку лише на ті послуги, які йому потрібні, і платить фіксовану суму, у яку вже включено вхідний і вихідний трафік.

Цифровий бункер від Dell

На жаль, наявність резервних копій у хмарі ще не гарантує безпеки даних, оскільки резервні копії необхідно додатково захистити від кіберзагроз. Зокрема чи не найбільш руйнівними є інсайдерські атаки, адже, по-перше, виявити

On-premises, Cloud, Hybrid, — яке б не було середовище, де працюють робочі навантаження організації, завжди необхідно потурбуватися про їх належний захист, убезпечити цифрові активи від логічних помилок, навмисних чи випадкових деструктивних операцій, від дій кіберзлочинців, від фізичної втрати середовища унаслідок стихійного лиха чи воєнних дій. Це все дуже важливо, але це зовсім не означає що це має бути складно або дорого: навпаки, такі рішення як APEX Protection Storage, APEX Backup Services, PowerProtect Data Manager допоможуть вирішити ці завдання, разом з тим забезпечуючи простоту розгортання, керування та економічну доцільність використання.

Володимир ЛЮДВІНОВСЬКИЙ,
технічний пресейл-консультант компанії Dell Technologies

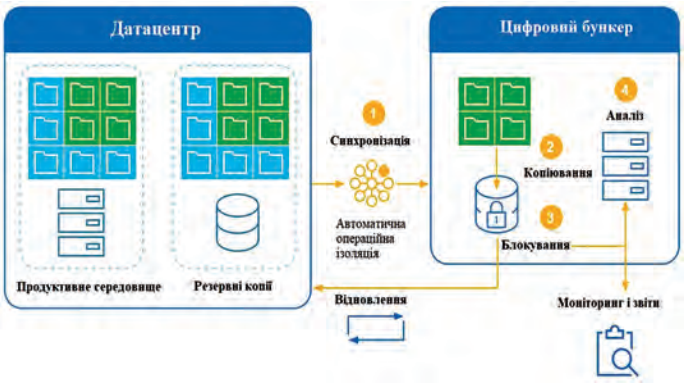

Рис. 2. PowerProtect Cyber Recovery

Рис. 3. Аналіз резервних копій за допомогою CyberSense

їх практично неможливо, а по-друге, внутрішні зловмисники прагнуть знищити не лише дані, а й їхні копії.

Стратегія захисту резервних копій повинна включати три основні елементи, якими є: 1) ізоляція, тобто фізичне або логічне відокремлення сховища резервних даних протягом усього часу, окрім періодів оновлення даних; 2) незмінюваність (Immutability) – заборона внесення будь-яких змін протягом визначеного часу, зокрема і користувачем з правами адміністратора; 3) контроль – відстеження та аналіз даних, які зберігаються, на предмет маніпуляцій з ними.

У цій царині Dell пропонує, як наступний після резервного копіювання рівень захисту даних, рішення PowerProtect Cyber Recovery (**рис. 2**). Воно доступне як у «наземному» виконанні, так і на базі публічних хмар. Важливо, що Cyber Recovery може працювати з системами резервного копіювання від інших виробників. Таким чином вирішується проблема захисту середовищ, де використовується декілька систем резервного копіювання, а також зникає необхідність змінювати методи захисту від кіберзагроз при заміні ПЗ резервного копіювання.

PowerProtect Cyber Recovery створює ізольоване середовище, від'єднане від корпоративного датацентру і недоступне нікому, окрім тих, хто має на це відповідні дозволи та має право відвідувати цифровий бункер фізично. Інакше кажучи, щоб мати можливість керувати ізольованим середовищем та отримати доступ до даних, які воно зберігає, вам потрібно знаходитися в цьому середовищі. У «наземному» виконанні цифровий бункер може бути фізично окремим приміщенням, тоді як у хмарі забезпечується логічна ізоляція. Сполучення між ЦОД і бункером відкривається лише у визначений час для синхронізації даних, і цей процес керується з боку бункера, а не з продуктивного середовища, а всередину ізольованого середовища в односторонньому порядку пропускається лише трафік, який пов'язаний з реплікацією тих даних, які ми хочемо захистити.

Всередині бункера забезпечується захист даних від видалення або змінення протягом визначеного періоду часу навіть для адміністратора з повними правами. Додатково включено протидію атакам на внутрішній годинник з метою передчасного зняття блокування. Також є можливість самостійного конфігурування періоду блокування.

Надважливою особливістю цього рішення є те, що всередині цифрового бункера відбувається аналіз даних, які там зберігаються, задля додаткового гарантування їх цілісності і забезпечення швидкого відновлення. Аналіз допомагає визначити, чи дані є взагалі придатними для відновлення, чи їх було якимось чином зіпсовано. Для цього використовується аналітичний механізм CyberSense, який здійснює повну індексацію контенту і за допомогою моделі машинного навчання визначає ознаки псування, які свідчать про атаку шифрувальника (**рис. 3**). CyberSense помічає псування даних з достовірністю у 99,5%, що допомагає ідентифікувати загрози і діагностувати вектори атак, захищаючи критично важливий контент в межах бункера.

CyberSense розпочинає сканування даних щойно їх репліковано до бункера Cyber Recovery і поставлено блокування. Система створює цільові точки спостереження, за допомогою яких відстежує зміни у файлах. Сканування відбувається на резервній копії без потреби звертання до ПЗ, яке здійснювало бекапування. Аналіз дає змогу зафіксувати шифрування чи псування файлів і баз даних, відомі зловмисні програми, масове знищення або створення файлів. У разі виявлення атаки надсилається сповіщення на консоль Cyber Recovery. Для швидкої діагностики та відновлення після атаки CyberSense генерує звіт про розслідування.

На відміну від інших подібних рішень, CyberSens аналізує не лише метадані файлів, але й їхній вміст, зокрема помічає псування структури файлів і часткове шифрування, що можливо лише при відстеженні змін у цих файлах з плином часу.

Відновлення даних можливе у різних варіантах: зворотна реплікація резервної копії з бункера в датацентр (на APEX Protection Storage), безпосередньо у продуктивне середовище, з запуском віртуальних машин в самому бункері або, навпаки, з попередньою перевіркою відновлених даних у відокремленій «чистій кімнаті».

Наразі технологією PowerProtect Cyber Recovery користуються у світі понад 1800 замовників, і починаючи від 2015 року, коли це рішення з'явилося на ринку, не було зафіксовано жодного випадку знищення або компрометації захищених нею даних. В Україні технологія використовується з 2019 року.

Дізнатися більше про рішення **Dell Technologies** *для захисту даних у хмарах можна у платинового партнера — компанії* **АМ-БІТС**.

Маючи досвід реалізованих успішних проєктів, АМ-БІТС пропонує послуги з переміщення IT-інфраструктури, критичних сервісів та резервних копій даних на ресурси хмарних інфраструктур, використовуючи рішення від Dell Technologies та інших провідних вендорів.

бул. Лесі Українки, 23А,
01133, Київ, Україна
Телефон: +38 044 225 66 52
https://am-bits.com/

У зв'язку з війною в Україні наразі актуально для бізнесу мати резервні копії корпоративних даних на серверах, розташованих за межами країни. Рішення від Dell може стати важливим кроком для забезпечення надійного та безпечного зберігання цих даних і створити стабільний IT-фундамент для подальшої роботи. Наша команда спеціалістів допоможе з проєктуванням та реалізацією.

Вячеслав РОМАНЧЕНКО,
керівник відділу системної інтеграції АМ-БІТС