Dell PowerProtect Data Domain: фундамент кіберстійкості

Юрій Степовик, співвласник та директор з розвитку бізнесу компанії INTRASYSTEMS, проводить екскурсію по сучасній платформі Dell, яка не тільки зберігає резервні копії, але й надає кіберзахист та можливість відновлення даних.

У сучасному цифровому ландшафті, де дані є одночасно і найціннішим активом, і головною мішенню для атак, традиційні підходи до їх захисту стрімко втрачають актуальність. Для керівників IT-департаментів у критично важливих секторах, таких як банківська справа та телекомунікації, вже стоїть питання не «чи станеться атака?», а «коли вона станеться і чи зможемо ми відновитися?».

Експоненціальне зростання обсягів даних у поєднанні з дедалі більш витонченими програмами-вимагачами та іншими загрозами вимагає переходу від простого резервного копіювання до створення комплексної стратегії кіберстійкості. У цій статті ми розглянемо, як платформа Dell PowerProtect Data Domain відповідає на ці виклики як стратегічна основа для збереження та відновлення даних.

Нова парадигма захисту даних

Сучасні організації стикаються не лише з технічними збоями чи випадковою втратою даних, а й із цілеспрямованими кібератаками, коли зловмисники намагаються знищити як первинні дані, так і їх резервні копії. Традиційні механізми резервного копіювання допомагають відновити інформацію, проте сучасні кіберзагрози вимагають ширшого підходу — такого, що забезпечує захист даних, їхню доступність і можливість відновлення навіть у випадку складних та навмисних атак.

Для банків, де безперервність операцій та довіра клієнтів є основою бізнесу, або для телеком-операторів, що забезпечують роботу критичної інфраструктури зв'язку, ціна невдалого відновлення є катастрофічною. Тому оцінювати рішення для захисту даних виключно за традиційними показниками, такими як швидкість резервного копіювання або коефіцієнт дедуплікації, вже недостатньо. Платформа повинна оцінюватися за її здатністю відновлюватися після навмисної, зловмисної атаки (**рис. 1**).

Архітектурний фундамент: технології, що забезпечують надійність та ефективність

В основі платформи PowerProtect Data Domain лежать дві унікальні архітектури:

- Stream-Informed Segment Layout (SISL), що забезпечує високоефективну дедуплікацію;
- Data Invulnerability Architecture (DIA), яка підтримує цілісність та відновлюваність даних.

Разом вони створюють фундамент, на якому будуються всі інші можливості системи.

Наразі рішення PowerProtect Data Domain вже довело свою ефективність (швидкість резервного копіювання та стиснення даних) за рахунок великої кількості інсталяцій та позитивних відгуків замовників з різних сфер ринку.

Відновлення за допомогою архітектури невразливості даних (DIA)

DIA — це не окрема функція, а комплексна філософія, розроблена з припущенням, що Data Domain є «сховищем останньої надії». Її мета — цілісність та відновлюваність даних. Це свідомий проєктний вибір, який фундаментально відрізняє Data Domain від конкурентів, котрі адаптують системи зберігання загального призначення для резервного копіювання.

«Невидаляємість» даних та архітектура Zero Trust

Функція Retention Lock надає можливість зберігати дані без змін протягом визначеного періоду, запобігаючи їх модифікації або видалення. Режим Compliance Mode розроблений для відповідності суворим регуляторним вимогам, таким як SEC Rule 17a-4(f) у США,

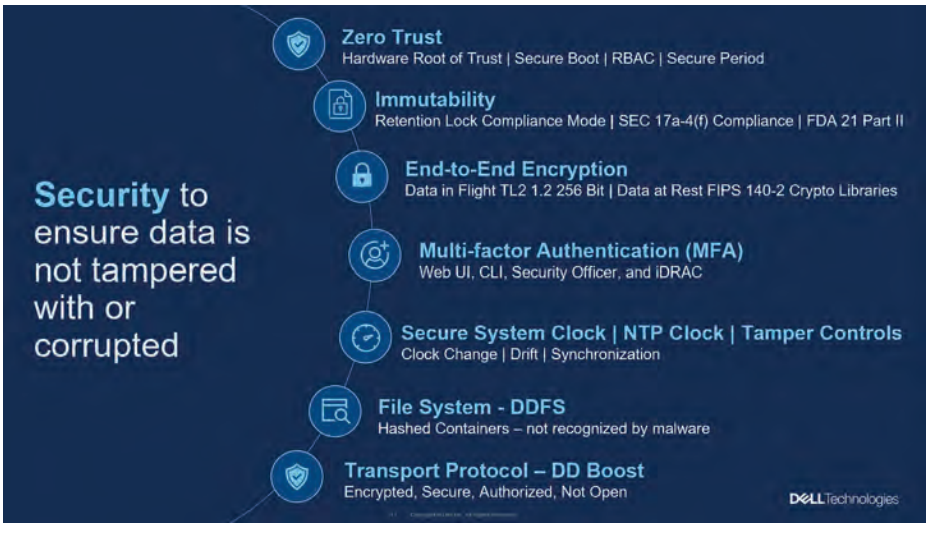

Рис. 1. Dell PowerProtect Data Domain не лише зберігає дані, а й захищає їх від зловмисників

і включає захист від маніпуляцій з системним часом. Атестація цієї функції третьою стороною перетворює її з простої характеристики продукту на рішення для забезпечення відповідності, що є критично важливим для фінансового сектору.

Кіберстійкість як стандарт: захист від програм-вимагачів

У сучасному ландшафті загроз захист резервних копій є таким же важливим, як і захист первинних даних. Платформа PowerProtect Data Domain пропонує багаторівневий підхід до кіберстійкості.

Ізольоване сховище Cyber Recovery Vault: остання лінія оборони

Рішення PowerProtect Cyber Recovery створює фізично або логічно ізольоване середовище, відоме як «air-gapped vault» (сховище з повітряним зазором). Воно відокремлює критично важливі резервні копії від основної мережі (**рис. 2**). Доступ до цього сховища суворо контролюється і вимагає окремих облікових даних та багатофакторної автентифікації (MFA). Дані періодично синхронізуються у сховище, після чого мережевий зв'язок розривається. Зазор робить дані у сховищі недоступними для зловмисників, які могли проникнути в основну мережу, тим самим ефективно захищаючи резервні копії від шифрування або видалення.

Інтелектуальна аналітика CyberSense: виявлення прихованих загроз

Простий повітряний зазор захищає від видалення репозиторію резервних копій. А якщо сама резервна копія, переміщена у сховище, вже містила зашифровані файли? Резервна копія буде цілою, але марною. Саме тут вступає в дію CyberSense — аналітичний інструмент на основі штучного інтелекту та машинного навчання (AI/ML), інтегрований у Cyber Recovery Vault.

На відміну від рішень, що сканують лише метадані, CyberSense проводить аналіз усього вмісту (full-content analytics), шукаючи ознаки шифрування, характерні для атак програм-вимагачів, з точністю виявлення 99.99%. У разі виявлення атаки CyberSense допомагає швидко ідентифікувати останню «чисту» копію даних, що значно прискорює процес відновлення. Згідно з дослідженням Forrester Consulting, це рішення може скоротити час простою бізнесу після кібератаки на 75%.

Готовність до DORA: новий стандарт стійкості ЄС

З 17 січня 2025 року для фінансового сектору стає обов'язковим дотримання Регламенту

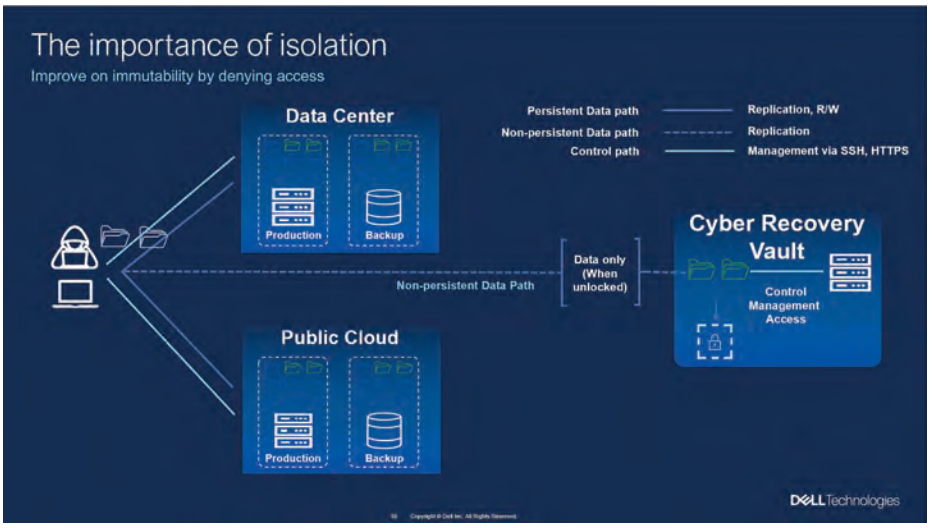

Рис. 2. Cyber Recovery Vault — ізольоване сховище даних

про цифрову операційну стійкість (Digital Operational Resilience Act — DORA, Regulation (EU) 2022/2554). Цей документ докорінно змінює підхід регуляторів: від вимог до капіталу акцент зміщується на здатність банків та фінансових установ витримувати ІКТ-інциденти, реагувати на них та відновлюватися. Платформа Dell PowerProtect Data Domain підтримує зусилля організацій із досягнення операційної стійкості відповідно до підходів, закладених у статті 12 регламенту DORA, завдяки рішенню PowerProtect Cyber Recovery, технології Retention Lock та можливості проводити автоматизоване тестування відновлюваності даних всередині ізольованого сховища без впливу на виробничі процеси.

Таким чином, впровадження рішень Dell дозволить вітчизняним фінансовим установам у майбутньому (при вступі України у ЄС) не просто формально відповідати новим європейським нормам, а побудувати реально діючу систему цифрової стійкості.

Ефективність та гнучкість розгортання

Для мобільних операторів, що генерують величезні обсяги даних, ефективна дедуплікація Data Domain дозволяє мінімізувати витрати на сховища. Мережево-ефективна реплікація, при якій через WAN-канали передаються тільки унікальні, стиснуті дані, значно зменшує навантаження на інфраструктуру, що критично важливо для географічно розподілених мереж. Платформа доступна не тільки у вигляді фізичних пристроїв, але й у вигляді віртуальної версії — PowerProtect DD Virtual Edition (DDVE), яку можна розгорнути на периферії мережі (edge) або в публічних хмарах (AWS, Azure, Google Cloud). Це дозволяє будувати єдину архітектуру захисту даних, що охоплює всю інфраструктуру — від ядра до периферії та хмари.

Висновки

Платформа Dell PowerProtect Data Domain виходить далеко за межі традиційного сховища для резервних копій. Її унікальні архітектурні рішення, такі як DDBoost та DIA, забезпечують фундамент для високої продуктивності та, що найважливіше, відновлюваності даних. Передові можливості кіберзахисту, зокрема ізольоване сховище Cyber Recovery Vault та інтелектуальна аналітика CyberSense, надають організаціям потужні інструменти для протидії найсучаснішим загрозам.

В умовах, коли вартість простою та втрати даних через кібератаку може бути катастрофічною, інвестиція в надійну платформу захисту даних, таку як Data Domain, є не просто витратою на IT, а інвестицією в стійкість, репутацію та майбутнє компанії. Вона дає впевненість у тому, що дані можна буде відновити — завжди. Вона допомагає значно підвищити ймовірність успішного відновлення даних навіть у разі складних кібератак.