В.І. Слюсар к.т.н., професор, ГНС;
І.П. Гусаковський, ад’юнкт (штатний) НОВ.
Центральний науково-дослідний інститут озброєння та військової техніки
Збройних Сил України

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ СУЧАСНИХ ПЛАТФОРМ ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ В УМОВАХ ЕВОЛЮЦІЇ КІБЕРНЕТИЧНИХ ЗАГРОЗ

В умовах перманентної еволюції кібернетичних загроз, що характеризуються зростанням складності, використанням багатоетапних векторів атак та застосуванням елементів штучного інтелекту, класичні методи захисту кінцевих пристроїв, що базуються переважно на сигнатурному аналізі, демонструють недостатню ефективність. Сучасна парадигма безпеки вимагає переходу до комплексних, багаторівневих платформ захисту (Endpoint Protection Platforms, EPP), які інтегрують превентивні, аналітичні та проактивні технології. Дослідження проведено для порівняльного аналізу десяти провідних програмних рішень у цій галузі з метою об'єктивної оцінки їхньої ефективності, функціональної повноти та операційної надійності. Метою є визначення оптимальних стратегій захисту корпоративного середовища на основі емпіричних даних з незалежних тестувань.

Ефективність сучасного антивірусного програмного забезпечення (далі – АВПЗ) залежить від того, наскільки добре поєднуються декілька ключових технологій, які захищають систему на всіх етапах атаки, від її початку до завершення. До основних компонентів такої комплексної системи захисту належать:

1. Антивірус нового покоління (Next-Generation Antivirus, NGAV), який, на відміну від традиційних антивірусів, використовує безсигнатурні методи детектування. До них належать поведінковий аналіз (моніторинг активності процесів у реальному часі), евристичні алгоритми та моделі машинного навчання (Machine Learning, ML), що дозволяє превентивно блокувати не лише відомі, але й раніше невідомі загрози на основі їхньої аномальної поведінки.

2. Виявлення та реагування на кінцевих точках (Endpoint Detection and Response, EDR) – це системи, що функціонують за принципом “припущення про злам”, забезпечуючи глибоку видимість процесів у системі. Вони безперервно збирають та аналізують великі обсяги телеметричних даних (запуски процесів, мережеві з'єднання, зміни в системі) для виявлення складних загроз, що оминули превентивний захист. EDR надає фахівцям з безпеки інструментарій для розслідування інцидентів, полювання на загрози та оперативного реагування (ізоляція хоста, завершення процесів).

3. Управління вразливостями та оновленнями (Vulnerability and Patch Management, VM) – це проактивний компонент, спрямований на зменшення “поверхні атаки” шляхом ідентифікації, пріоритезації та усунення програмних вразливостей в ОС та сторонніх додатках. Функція VM працює на випередження, нейтралізуючи потенційні вектори атак ще до того, як вони можуть бути проексплуатовані зловмисниками.

4. Системи запобігання витоку даних (Data Loss Prevention, DLP) – це клас технологічних рішень, основною метою яких є ідентифікація, моніторинг та захист чутливої інформації від несанкціонованого розповсюдження. На відміну від АВПЗ, що фокусується на протидії шкідливому коду, DLP-системи зосереджені на аналізі вмісту (контенту) самих даних та контексті їх використання. Вони контролюють дані у трьох основних станах: під час передачі (мережевий трафік, пошта), у стані зберігання (файлові сховища) та під час їхньої обробки (операції на кінцевих пристроях, копіювання на USB-накопичувач). Таким чином, DLP є компонентом, що доповнює антивірусний захист, контролюючи не загрози для цілісності системи, а безпосередньо загрози для конфіденційності даних.

Методологія оцінювання базується на систематизації та узагальненні даних з авторитетних незалежних джерел, що дозволяє отримати комплексну та об'єктивну оцінку кожного продукту.

Оцінка технічної ефективності ґрунтується на результатах провідних лабораторій. До них належить Virus Bulletin (VB100), що оцінює базову надійність; AV-TEST Institute, який проводить комплексне тестування за критеріями захисту, продуктивності та точності роботи; SE Labs, що імітує реальні багатоетапні атаки для оцінки EDR-можливостей; та AV-

Comparatives, який проводить тести ефективності у корпоративному середовищі.

Для повноти картини, ринкове позиціонування та стратегічне бачення вендорів аналізуються за допомогою звітів Gartner Magic Quadrant. Водночас реальний досвід експлуатації продуктів оцінюється на основі верифікованих відгуків з платформи Gartner Peer Insights.

На основі сукупності даних, аналізовані продукти класифікуються за їхніми технологічними перевагами та стабільністю результатів. Чітко виокремлюється група лідерів, до якої належать як рішення зі збалансованою ефективністю, так і технологічні платформи нового покоління. Продукти ESET Endpoint Security та Bitdefender GravityZone Elite демонструють найвищий рівень стабільності в усіх типах технічних тестів, поєднуючи потужний локальний захист із хмарною аналітикою. Водночас CrowdStrike Falcon Endpoint Protection та SentinelOne Control Platform підтверджують свій статус провідних EDR-платформ, оптимальних для організацій з високими вимогами до виявлення та реагування на цілеспрямовані атаки, що підтверджується їх лідерськими позиціями в аналітичних звітах Gartner.

До другої групи входять надійні корпоративні рішення від Symantec (Broadcom), Trellix (McAfee), Trend Micro та Avast, які демонструють стабільно високі результати в більшості тестів, підтверджуючи свій статус перевірених часом продуктів. Окремо слід відзначити продукти Panda Adaptive Defense 360 та Zillya! Антивірус для Бізнесу, об'єктивне порівняння яких ускладнене через брак актуальних даних у провідних корпоративних тестах.

Окрім антивірусного захисту та EDR-можливостей, важливим аспектом є наявність функціоналу запобігання витоку даних (DLP). Більшість провідних платформ, зокрема від Bitdefender, Symantec, Trellix, ESET, CrowdStrike та SentinelOne, пропонують інтегровані DLP-модулі. Проте, слід зазначити, що ця функція, як правило, є опціональною та вимагає окремого ліцензування або придбання розширених пакетів, не входячи до стандартної конфігурації.

Вибір оптимальної платформи захисту кінцевих пристроїв є комплексним завданням, що вимагає врахування профілю ризиків, операційних сценаріїв та рівня зрілості служби кібербезпеки установи.

Для установ, що потребують максимальної надійності та збалансованого захисту для гібридних умов роботи (з тимчасовим підключенням до мережі), пріоритетними є рішення від ESET та Bitdefender.

Для установ, яким критично важливим є захист від цілеспрямованих атак та наявність потужного EDR-функціоналу, слід звернути увагу на платформи CrowdStrike та SentinelOne.

Важливо зазначити, що ключові технології, такі як EDR (для глибокого аналізу, розслідування та реагування на складні інциденти); VM (для проактивного пошуку та усунення вразливостей) та DLP (для контролю та запобігання витоку конфіденційної інформації), у більшості випадків є опціональними компонентами, що вимагають окремого ліцензування або придбання розширених пакетів.

Разом з тим, проведений аналіз свідчить , що завдання антивірусного захисту може бути покладене на мультиагентну систему штучного інтелекту. Відповідні агенти мають охоплювати зазначені напрями, що раніше охоплювалися альтернативними варіантами програмного забезпечення.

Комплексний підхід до вибору, що враховує результати різних типів тестувань, дозволяє побудувати найбільш ефективну та ешелоновану стратегію захисту корпоративної інфраструктури.