ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТАЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захисту кінцевих точок організації на прикладі рішення Trellix»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Марія РУДОМЬОТОВА
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-63
РУДОМЬОТОВА Марія
(прізвище, ім'я)

Керівник д.т.н., професор ГАЙДУР Галина
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ABSTRACT

Text part of the qualification work: 61 pages, 13 figures, 1 tables, 11 sources.

Object of research – protection of the organization's endpoints.

Subject of research – the organization's endpoint protection technology using the Trellix Endpoint Security solution as an example.

The aim of research – there is the development of a version of the organization's endpoint protection technology using the Trellix Endpoint Security solution as an example and the development of a recommendation for its application

Research methods – the studying the literature on this topic, analysing operational documentation, international standards and comparing them.

The paper analyzes the problem of using the endpoints of the organization from the point of view of cyber security. As a result of the analysis, the need to protect the endpoints of the organization from attacks that could lead to information leakage and unauthorized access to the organization's resources through users was revealed. The methods and tools of the Trellix Endpoint Protection Platform were studied. The Trellix Endpoint Security technology is proposed and a workflow is provided for the necessary technology modules for automatic endpoint protection that meets organizational priority needs in the field of cybersecurity.

Field of application – cybersecurity of enterprise information systems.

INFORMATION SYSTEM, CYBER SECURITY, REMOTE USERS, END POINTS, METHODS AND TOOLS, TECHNOLOGY.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПК – Персональний комп’ютер

EPP – Endpoint Protection Platforms

EDR – Endpoint detection and response

XDR – extended detection and response

VPN – virtual private network

MFA – multi-factor authentication

Threat Prevention – запобігання загрозам

ВСТУП

Актуальність захисту кінцевих точок в організації сьогодні є надзвичайно високою, оскільки зростає кількість кіберзагроз, які можуть вплинути на безпеку даних і систем.

Зростання кількості кіберзагроз на кінцеві точки є серйозною проблемою для організацій по всьому світу. Це пов’язано з багатьма факторами, серед яких технологічний прогрес, зміни в методах роботи, а також підвищення кількості користувачів, які працюють з чутливими даними. Однією з розповсюджених атак на кінцеві точки можна виділити фішинг, який є розповсюдженою тактикою, яка використовується для атак на кінцеві точки. Кіберзлочинці надсилають електронні листи або повідомлення, які виглядають як законні запити, з метою отримання конфіденційної інформації.

Звертати увагу також необхідно на шкідливе програмне забезпечення (Malware), таке як віруси, трояни та руткіти, здатне заражати кінцеві точки, викрадаючи дані або намагаючись отримати контроль над системами організації. Таке програмне забезпечення може призвести до зупинки роботи багатьох сервісів компанії, оскільки зловмисники можуть зашифрували дані, вимагаючи викуп.

Захист кінцевих точок організацій вимагає постійного застосування методів пошуку вразливості програмного забезпечення. Такі методи дозволяють захистити від несанкціонованого доступу до систем організацій. Кінцеві точки, які не отримують регулярних оновлень безпеки, стають легкими мішенями для атак.

Мобільні пристрої, які використовуються працівниками, також є потенційними мішенями для атак. Вразливості в додатках або операційних системах можуть бути використані для доступу до чутливих даних.

Отже зростання кіберзагроз на кінцеві точки є результатом як технологічного прогресу, так і підвищення кількості віддалених працівників. Організації повинні вживати активних заходів для захисту своїх кінцевих точок, включаючи навчання співробітників, регулярні оновлення програмного забезпечення та використання

антивірусних рішень, щоб зменшити ризики та загрози. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

Об'єкт дослідження – захист кінцевих точок організації.

Предмет дослідження – технологія захисту кінцевих точок організації на прикладі рішення Trellix Endpoint Security.

Метою роботи – є розробка варіанту технології захисту кінцевих точок організації на прикладі рішення Trellix Endpoint Security та розробка рекомендації щодо її застосування.

Наукові завдання:

дослідити сутність проблеми захисту кінцевих точок організації;

проаналізувати підходи до вирішення проблеми захисту кінцевих точок організації;

проаналізувати існуючі технології захисту кінцевих точок організації;

проаналізувати методи та засоби захисту кінцевих точок організації на прикладі Tellix Endpoint Protection Platform.

розкрити порядок реалізації технології кінцевих точок організації на прикладі рішення Trellix Endpoint Security.

Методи дослідження: опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, практичне використання засобів захисту віддалених користувачів.

Практичне значення одержаних результатів: запропоновано варіант застосування технології захисту кінцевих точок організації на прикладі рішення Trellix, а також розроблено рекомендації фахівцям з кібербезпеки щодо застосування даної технології.

Апробація результатів роботи. Результати роботи доповідались на всеукраїнській конференції «Актуальні проблеми кібербезпеки» 25 жовтня 2024 року на тему: «ТЕХНОЛОГІЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ».

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ

1.1. Роль і місце кінцевих точок в інформаційній системі організацій

Пристрій підключений до мережі вважається кінцевою точкою. Із зростанням популярності BYOD (принесіть свій власний пристрій) та IoT (Інтернет речей) кількість окремих пристроїв, підключених до мережі організації, може швидко досягати десятків (і сотень) тисяч.

Кінцеві точки можуть варіюватися від пристроїв, які зазвичай вважаються такими як:

планшети;

мобільні пристрої;

розумні годинники;

принтери;

сервери;

банкомати;

медичні прилади.

Крім того, кінцеві точки можна розділити на дві категорії залежно від використання:

Кінцеві точки користувача — це інтерфейс між людьми та іншими пристроями в мережі.

Кінцева точка хост-пристрою взаємодіє з іншими кінцевими точками, але не використовується безпосередньо людиною. Ці кінцеві точки включають веб-сервери, сервери електронної пошти та бази даних.

Кінцеві точки забезпечують потік інформації та даних через мережу, локальну чи всесвітню, але вони не є частиною мережевої інфраструктури.

Таким чином, ці пристрої не є кінцевими точками:

Мережні шлюзи

Маршрутизатори

Рис. 1.1. Види кінцевих точкок

Перемикачі

Брандмауери

Чому кінцеві точки такі важливі?

Кінцеві точки дозволяють людям бути продуктивними та створювати роботу, яка сприяє досягненню цілей організації, для якої вони працюють. Кінцеві точки також є найбільш вразливими точками входу для кіберзлочинців, тому безпека кінцевих точок є важливою. Оскільки організації все частіше застосовують віддалені та гібридні моделі робочих місць користувачів, які підключаються до мереж із зовнішніх кінцевих пристроїв, які роблять їх захист дедалі важливішим для запобігання кібератакам.

Організації з розробленою стратегією керування кінцевими точками використовують інструменти, які допомагають їм обліковувати всі свої пристрої,

оновлювати та виправляти програмне забезпечення кінцевих точок, стежити за спробами кібератак і безпечно та надійно утилізувати їх після виходу з експлуатації з дійсної служби. Комплексне керування кінцевими точками включає, але не обмежується:

Конфігурація та розгортання пристрою

Безпека кінцевої точки

Управління IT активами

Віддалене керування кінцевою точкою

Керування виправленнями

Розпорядження IT-активами

У міру того, як робоча сила розвивається, і все більше співробітників працюють віддалено або в гібридних системах, необхідно запровадити програму ретельного керування кінцевими точками, щоб підтримувати функціональність і безпеку пристроїв у мережі та поза нею . Це включає програми керування мобільними пристроями (MDM) і політики BYOD (Візьміть свій власний пристрій).

Оскільки вони є точками входу для загроз і зловмисного програмного забезпечення, кінцеві точки (особливо мобільні та віддалені пристрої) є улюбленою мішенню зловмисників. Мобільні кінцеві пристрої стали набагато більшим, ніж просто пристрої Android та iPhone. Прикладом кінцевих точок є годинники, розумні пристрої, цифрові помічники з голосовим керуванням та інші розумні пристрої з підтримкою Інтернету речей. Тепер ми маємо підключені до мережі датчики в наших автомобілях, літаках, лікарнях і навіть на бурових нафтових вишках. Оскільки різні типи кінцевих точок розвивалися та розширювалися, рішення безпеки, які їх захищали, також мали адаптуватися.

Безпека кінцевих точок є життєво важливою, оскільки кінцеві точки є звичайними цілями для кібератак. Захист кінцевих точок допомагає захистити конфіденційні дані, запобігає несанкціонованому доступу та забезпечує цілісність і доступність мережевих ресурсів. Ефективна безпека кінцевої точки може

пом’якшити ризики, пов’язані зі зловмисним програмним забезпеченням, програмами-вимагачами, фішингом та іншими кіберзагрозами, таким чином підтримуючи загальну безпеку мережі та відповідність нормам. Кінцеві точки часто служать точками входу для зловмисників, щоб отримати доступ до ширших ресурсів мережі.

1.2. Аналіз проблеми захисту кінцевих точок організації

Безпека кінцевих точок — це практика захисту кінцевих точок або точок входу пристроїв кінцевих користувачів, таких як настільні ПК, ноутбуки та мобільні пристрої, від використання зловмисниками та кампаніями. Системи безпеки кінцевих точок захищають ці кінцеві точки в мережі або в хмарі від загроз кібербезпеці. Безпека кінцевих точок еволюціонувала від традиційного антивірусного програмного забезпечення до комплексного захисту від складного шкідливого програмного забезпечення та нових загроз нульового дня.

Організації будь-якого розміру піддаються ризику з боку національних держав, хактивістів, організованої злочинності, а також зловмисних і випадкових внутрішніх загроз. Безпека кінцевих точок часто розглядається як головна лінія кібербезпеки, і це одне з перших місць, де організації прагнуть захистити свої корпоративні мережі.

Оскільки обсяг і складність загроз кібербезпеці неухильно зростають, зростає потреба в більш досконалих рішеннях безпеки кінцевих точок. Сучасні системи захисту кінцевих точок розроблені для швидкого виявлення, аналізу, блокування та стримування поточних атак. Для цього їм потрібно співпрацювати один з одним та з іншими технологіями безпеки, щоб надати адміністраторам бачення передових загроз, щоб пришвидшити час виявлення та реагування на їх виправлення.

Безпека кінцевої точки дуже важлива для захисту інформаційної системи організації, тому використання платформи захисту кінцевої точки є важливою частиною кібербезпеки підприємства. Перш за все, у сучасному діловому світі дані є найціннішим активом компанії, і втрата цих даних або доступу до них може

поставити весь бізнес під загрозу банкрутства. Підприємствам також доводиться стикатися не лише зі зростанням кількості кінцевих точок, але й із збільшенням кількості типів кінцевих точок. Ці фактори самі по собі ускладнюють безпеку кінцевої точки підприємства, але вони ускладняються політиками віддаленої роботи та BYOD, які роблять захист периметра дедалі недостатніми і створюють уразливості. Ландшафт загроз також ускладнюється, тому що хакери завжди винаходять нові способи отримати доступ, викрасти інформацію або змусити співробітників надати конфіденційну інформацію.

Розглянемо як працює захист кінцевої точки. Безпека кінцевої точки — це практика захисту даних і робочих процесів, пов’язаних з окремими пристроями, які підключаються до інформаційної системи організації. Платформи захисту кінцевих точок (EPP) перевіряють файли, коли вони надходять у мережу. Сучасні EPP використовують потужність хмари для зберігання постійно зростаючої бази даних інформації про загрози, звільняючи кінцеві точки від роздування, пов’язаного зі збереженням усієї цієї інформації локально та обслуговуванням, необхідним для підтримки актуальності цих баз даних. Доступ до цих даних у хмарі також забезпечує більшу швидкість і масштабованість.

EPP надає системним адміністраторам централізовану консоль, яка встановлюється на мережевий шлюз або сервер і дозволяє фахівцям з кібербезпеки дистанційно контролювати безпеку кожного пристрою. Потім клієнтське програмне забезпечення призначається кожній кінцевій точці — воно може поставлятися як SaaS і керуватися віддалено, або його можна встановити безпосередньо на пристрої. Після налаштування кінцевої точки клієнтське програмне забезпечення може надсилати оновлення на кінцеві точки, коли це необхідно, автентифікувати спроби входу з кожного пристрою та адмініструвати корпоративні політики з одного місця. EPP захищають кінцеві точки за допомогою контролю програм, який блокує використання небезпечних або неавторизованих програм, а також за допомогою шифрування, що допомагає запобігти втраті даних.

Коли EPP правильно налаштовано, воно може швидко виявляти зловмисне програмне забезпечення та інші загрози. Деякі рішення також включають

компонент виявлення та реагування кінцевої точки (EDR). Можливості EDR дозволяють виявляти більш складні загрози, такі як поліморфні атаки, безфайлове шкідливе програмне забезпечення та атаки нульового дня. Використовуючи безперервний моніторинг, рішення EDR може запропонувати кращу видимість і різноманітність варіантів реагування.

Рішення EPP доступні в локальних або хмарних моделях. Хоча хмарні продукти є більш масштабованими та легше інтегруються у вашу поточну архітектуру, певні нормативні/відповідні правила можуть вимагати локальної безпеки.

Розглянемо компоненти безпеки кінцевої точки. Як правило, програмне забезпечення безпеки кінцевої точки включає в себе такі ключові компоненти:

Класифікація машинного навчання для виявлення загроз нульового дня майже в реальному часі.

Розширений захист від зловмисного програмного забезпечення та антивірусний захист для захисту, виявлення та виправлення зловмисного програмного забезпечення на кількох кінцевих пристроях і операційних системах.

Проактивна веб-безпека для безпечного перегляду веб-сторінок.

Класифікація даних і запобігання втраті даних для запобігання втраті та ексфільтрації даних.

Інтегрований брандмауер для блокування ворожих мережевих атак.

Шлюз електронної пошти для блокування спроб фішингу та соціальної інженерії, націлених на ваших співробітників.

Криміналістична експертиза загроз, що дозволяє адміністраторам швидко ізолювати інфекції.

Захист від внутрішніх загроз для захисту від ненавмисних і зловмисних дій.

Централізована платформа керування кінцевими точками для покращення видимості та спрощення операцій.

Шифрування кінцевої точки, електронної пошти та диска для запобігання викраденню даних.

Десятиліттями організації здебільшого покладалися на антивірус як засіб захисту кінцевих точок. Однак традиційний антивірус більше не може захистити від сучасних складних загроз.

Сучасні рішення безпеки кінцевих точок менш орієнтовані на сигнатури, а набагато більше на поведінку, включаючи ширший набір можливостей, таких як антивірус, захист від експлойтів, виявлення та реагування на кінцеві точки (EDR), аналітику та контроль пристроїв. Стратегії безпеки корпоративних кінцевих точок поєднують платформи захисту кінцевих точок (EPP) і рішення EDR із інструментами хмарної та мережевої безпеки, такими як аналіз мережевого трафіку (NTA), щоб отримати видимість зростаючої частки підключених до мережі пристроїв, які є «некерованими» (тобто вони не мають або не можуть мати встановлених агентів кінцевих точок), наприклад багато пристроїв IoT.

Найпотужніші та комплексні рішення безпеки кінцевих точок (часто включені в категорію рішень XDR) можуть централізовано збирати та співвідносити всі ці дані на додаток до виконання локального аналізу на окремих кінцевих точках.

Розширене рішення безпеки кінцевої точки повинно запобігати відомим і невідомим зловмисним програмам і експлойтам; включити автоматизацію для полегшення робочого навантаження групи безпеки; а також захищати та надавати можливість користувачам, не впливаючи на продуктивність системи.

Згідно зі звітом, Data Breaches Investigations 20231 [5], опублікований американським багатонаціональним телекомунікаційним конгломератом Verizon2, інциденти, які призводять до витоку даних, класифікуються за 7 (за винятком підкатегорії «все інше») підкатегорій: вторгнення в систему, соціальна інженерія, базові атаки веб-додатків, різноманітні помилки, відмова в обслуговуванні, втрачені та вкрадені активи та зловживання привілеями.

Рис.1.2. Класифікація інцидентів [6]

Найпоширенішими трійкою чинників у порядку є відмова в обслуговуванні, вторгнення в систему та втрачені або викрадені активи, причому вторгнення в систему має найвищу ймовірність призвести до витоку даних (2 з 5 вторгнень у дані належать до підкатегорії вторгнення в систему). Вторгнення в систему – це загальна назва таких інцидентів, як зловмисне програмне забезпечення та програми-вимагачі, які використовують конфіденційну інформацію для досягнення своїх цілей.

Найкращі методи безпеки кінцевих точок допомагають компаніям подолати ризики безпеки кінцевих точок, які стали частими за останні кілька років.

Рішення для захисту кінцевих точок, які також називають програмним забезпеченням для захисту кінцевих точок, посилюють вимірювання безпеки від кіберзагроз, які є результатом кібератак, людських помилок і недоліків керування кінцевими точками. Навіть якщо жодна вразливість у безпеці не призводить до витоку даних, компанії зобов’язані за законом гарантувати безпеку своїх конфіденційних даних і виправляти вразливості. Тому надалі проведомо аналіз рішень щодо захисту кінцевих точок.

1.3. Аналіз технологій захисту кінцевих точок

При виборі рішення необхідно щоб були визначені основні критерії для вибору постачальника рішень [4].

Деякі організації вибирають вендорів винятково з урахуванням рекомендацій аналітиків чи порівняльних тестів. Але важливо розуміти, що кожен бізнес є унікальним, і вибір постачальників повинен ґрунтуватися конкретно на конкретних запитах організації, а не на глобальному аналізі або результатах випробувань. Якщо аналітики високо оцінює рішення в хмарі та середовищах, розрахованих на багато користувачів, але за фактом його продукти не закривають вимоги конкретної організації, очевидно, що ця компанія не купуватиме таких рішень. Вкрай важливо розібратися в нюансах та результатах сторонніх тестів, щоб зрозуміти, чи актуальні ці рішення для конкретної організації [4].

Щоб знизити ризики, краще надавати перевагу рішенню, яке спеціалізується на EDR-рішеннях і протягом тривалого часу веде активну діяльність на ринку. Наявність керованої сервісної екосистеми, яку в наші дні шукають багато компаній, також має бути частиною оцінки, якщо це застосовується для вашого бізнесу [4].

У вибраного для організації рішення має бути сильний дослідницький відділ. Таким чином, дослідницька група матиме достатні можливості для раннього виявлення атак і вразливостей, щоб потім врахувати їх у своїх розробках. Співпраця дослідницької групи відповідного рішення з правоохоронними органами та розвідувальними організаціями є ключем до надання дієвої інформації для усунення кіберзлочинців.

Чекліст гарної платформи безпеки кінцевих точок може складатися з модульних рішень. Тому, щоб побудувати надійний захист безпеки кінцевих точок, рекомендовано використовувати модульний підхід, який на високому рівні містить:

● Датчики запобігання, які можуть усунути відомі шкідливі файли в режимі реального часу за допомогою сигнатур, політик захисту доступу, вмісту запобігання експлойтів, захисту пам'яті, репутації файлів та інших методів, що діють оперативно.

● Датчики розширеного запобігання, які можуть виконувати розширену перевірку — з використанням штучного інтелекту, інтеграції з пісочницею, аналізу сценаріїв тощо — і згодом покращувати своє навчання. Деякі з них можуть відбуватися не в режимі реального часу, особливо якщо загроза перебуває в середовищі вперше. Однак датчики додають захист без втручання користувача, як тільки механізм розуміє, що зіткнувся зі шкідливим програмним забезпеченням — зазвичай це відбувається протягом декількох секунд. Будь-які дані також передаються датчикам, що дозволяє блокувати загрозу в режимі реального часу, коли вона наступного разу з'явиться в навколишньому середовищі.

● Датчики розширеного виявлення, які команди SOC використовують, щоб зосередитися на стратегічному захисті, а також зібрати, узагальнити та візуалізувати докази за запитом або графіком. Оскільки дані тут мають значно більший масштаб, під час їхньої реалізації широко використовуються ШІ та хмара. Підсумовуючи, можна сказати, що ці датчики можуть бути надзвичайно корисними, коли атака перебуває в активній стадії.

● Датчик зі збору форензики, який використовується групою IR (реагування на інциденти) для збору необхідних аналітичних даних та маркерів компрометації для постійного аналізу оперативної пам'яті, тактики, методів та процедур поведінки у разі атаки в поєднанні із запланованими та автоматизованими методами. Ці датчики дуже ефективні під час збирання доказів і аналізу після інцидентів.

Всі названі датчики також мають бути підкріплені потужною аналітикою, щоб випереджати ландшафт загроз, який динамічно змінюється, виявляти та скорочувати можливості для атак. Якщо ваш бізнес об'єднує фізичне, віртуальне та хмарне обладнання, дуже важливо, щоб обраний вендор надав гібридну архітектуру розгортання та управління. Постачальники систем безпеки не повинні змушувати вас змінювати вашу бізнес-модель, а адаптуватися до наявної.

У кожного з названих датчиків є своє призначення, але вони використовуються як взаємозамінні, що призводить до плутанини на ринку рішень. Важливо, що всі рішення повинні мати можливість обмінюватися інформацією одне з одним, оскільки ізольована робота зводить нанівець всю мету.

Тож розглянемо рішення різних вендорів для вибору кращого рішення за квадрантом гартнера по розподілу гравців на ринку захисту кінцевих точок.

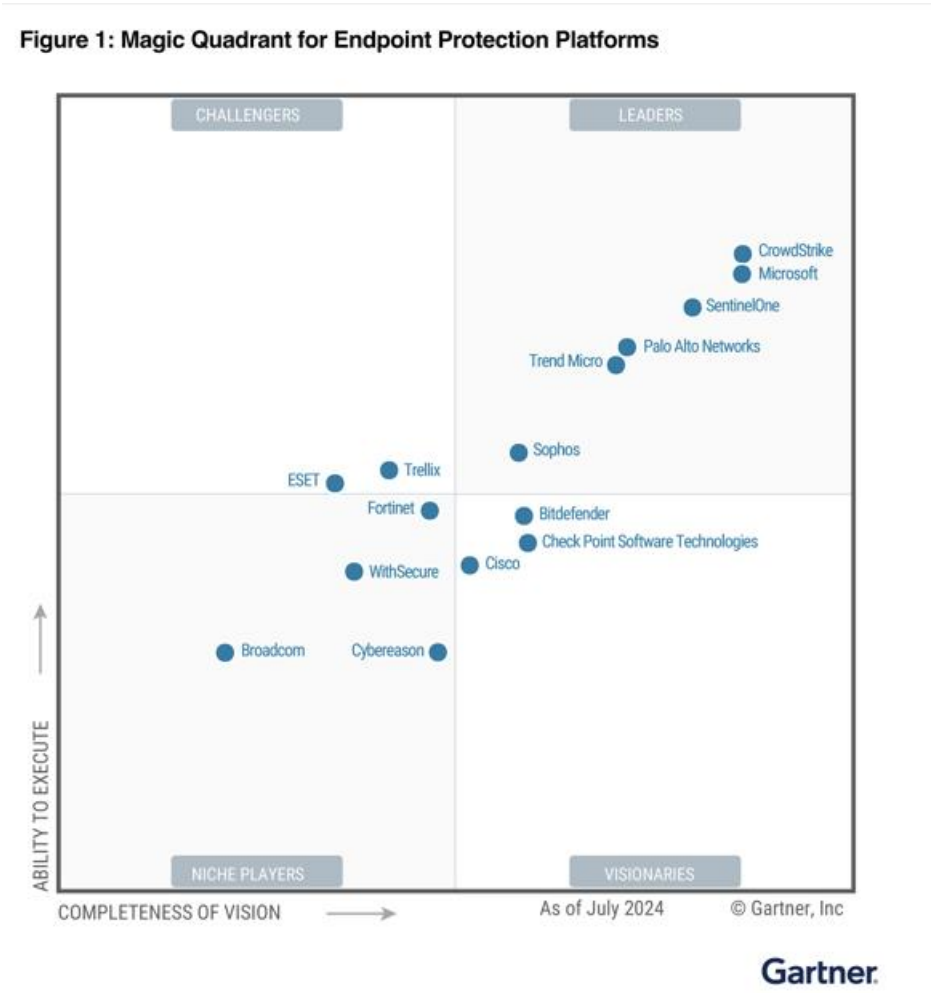

Рис.1.3. Гравці захисту кінцевих точок на ринку

Керування кінцевими точками NinjaOne

NinjaOne , раніше NinjaRMM, надає інструменти для IT-команд і MSP, зокрема: автоматизоване керування виправленнями , віддалений моніторинг і керування , керування кінцевими точками та керування мобільними пристроями (MDM) [6, 7].

плюси

Управління активами та простота використання: користувачі стверджують, що ним легко користуватися, а функції керування активами вважають ефективними.

Керування політикою: рецензенти хвалять інструмент і додають, що його можна настроювати та легко використовувати.

мінуси

Інтерфейс користувача: рецензенти визнають, що хоча єдина платформа забезпечує легкість, графічний інтерфейс можна покращити.

Сторонні інтеграції: деяких користувачів не влаштовують доступні сторонні інтеграції, такі як Splashtop і TeamViewer.

Microsoft Intune

Intune — це рішення Microsoft для керування кінцевими точками, яке має переваги глибокої інтеграції в екосистему Microsoft (тобто операційні системи Windows і програмне забезпечення, як-от Microsoft 365).

плюси

Просте використання: Рецензент високо оцінив можливості віддаленого моніторингу та керування продуктом.

Інтеграція. Стверджується, що продукт повністю інтегрований в екосистему Microsoft.

мінуси

Керування додатком: рецензент визнав інструмент керування додатком проблематичним. Інструмент займає багато часу, оскільки вимагає непотрібних завдань.

Функції сумісності з операційною системою: продукт виявився менш ефективним у macOS, ніж у Windows.

Щоб отримати інформацію про рішення Microsoft у суміжній категорії, перегляньте розділ Microsoft Purview DLP та його альтернативи.

Omnissa раніше VMware Workspace One

VMware — це хмарна компанія, яка виробляє інструменти керування додатками, а також хмарні рішення для безпеки та мережевого програмного забезпечення. VMware була придбана компанією Broadcom Inc у 2023 році, а її обчислювальні продукти для кінцевих користувачів були виділені під брендом Omnissa.

плюси

MDM: За словами багатьох рецензентів, функція Airwatch робить керування мобільним пристроєм практичним.

мінуси

Крива навчання: Користувачі стверджують, що продукт вимагає крутої кривої навчання.

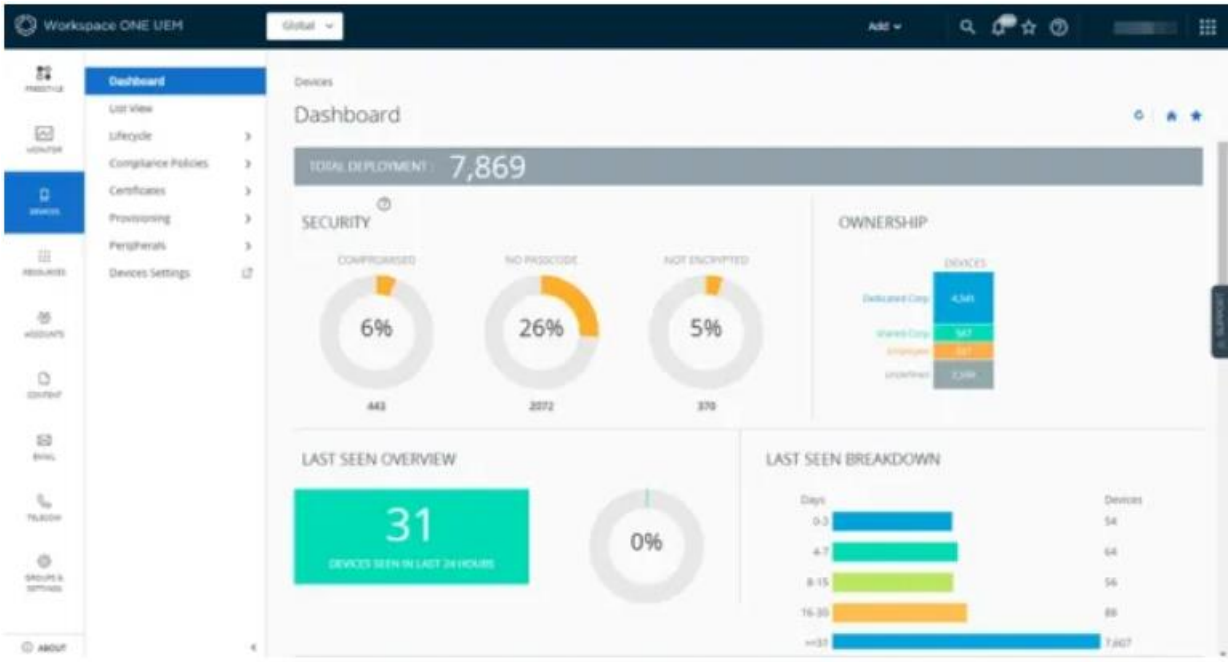

Рис. 1.4. Інформаційна панель Workspace One UEM [6]

Системний менеджер Cisco Meraki

Cisco розробляє та продає широкий спектр технологій, включаючи мережеве обладнання, телекомунікаційне обладнання та високотехнологічні послуги та продукти.

плюси

Конфігурація пристрою: Конфігурація пристроїв вважається практичною.

мінуси

Вартість: За словами кількох користувачів, загальна вартість видається високою.

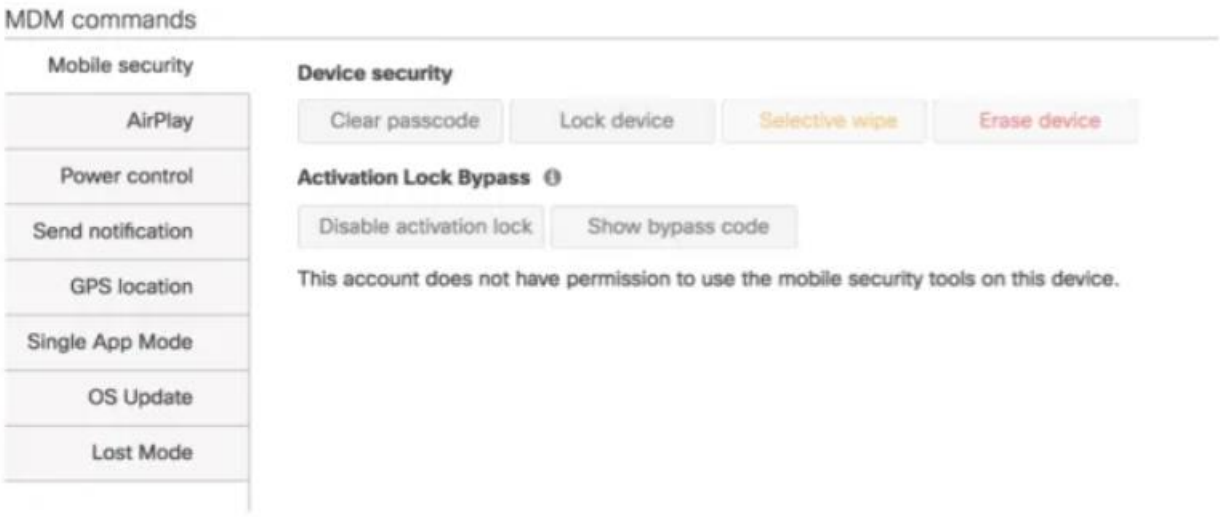

Рис.1.5. сторінку Meraki MDM [7]

Управління кінцевими точками Citrix

Citrix надає IT-рішення, орієнтовані на параметри гібридної/віддаленої роботи, такі як аналітика ефективності роботи співробітників, служби віддаленого підключення, рішення для доступу до мережі та керування кінцевими точками.

плюси

Мобільний доступ: Користувач стверджує, що задоволений мобільним доступом до продукту.

Просте використання: більшість користувачів задоволені простим налаштуванням продукту.

мінуси

Оновлення: виявлено, що оновлення продукту працюють повільно.

Продуктивність системи: деякі користувачі описують розгортання як дороге за часом через безліч функцій, які пропонує продукт.

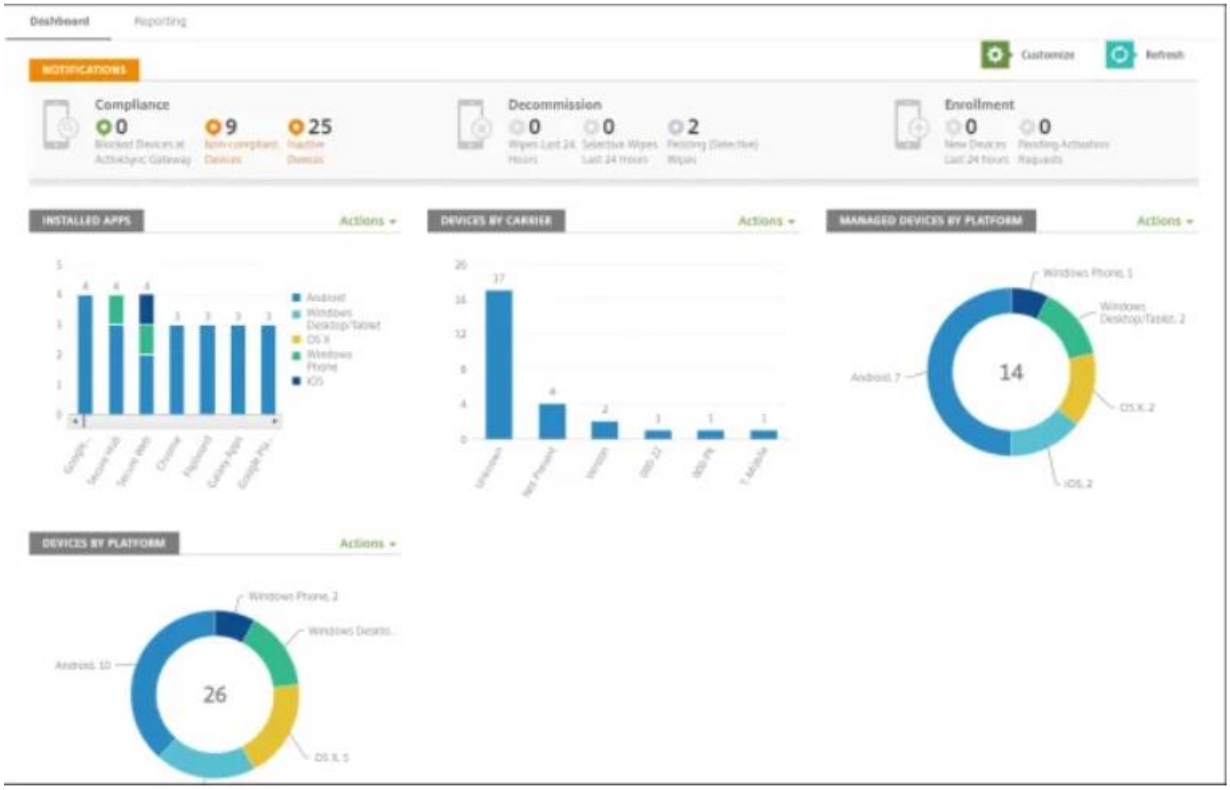

Рис. 1.6. Інформаційна панель Citrix Endpoint Management [7].

В даній роботі пропонується ознайомитися з підходом Trellix до захисту кінцевих точок. Платформа Trellix XDR дозволяє бути на крок попереду актуальних загроз завдяки постійному розвитку за допомогою Machine Learning та вбудованого кіберінтелекту. Основні компоненти платформи включають:

Trellix Endpoint Security (ENS) — Датчики запобігання

ENS ATP + IVX (Sandbox) — Датчики розширеного запобігання

Trellix EDR — Датчики розширеного виявлення

Trellix HX — Криміналістика

Trellix Agent — Єдиний агент для всіх вищезазначених датчиків

EPO / XConsole — Централізоване управління та звітність

Trellix XDR — Платформа Trellix XDR з інтеграцією з AI

Insights — Аналітика

Trellix Advanced Research Center — Дослідницький відділ.

Компанія Trellix досягла дуже високого рівня захисту від зловмисного програмного забезпечення протягом 2023 року з виявленням 99,7% у бізнес-тесті за серпень-листопад 2023 року.

Trellix також демонструвала стабільно «дуже низькі» хибні спрацьовування протягом циклів тестування протягом 2023 року. Знову ж таки, важливість забезпечення виняткового захисту без генерування непотрібних попереджень через хибні спрацьовування є критичним результатом, який перетворюється на покращення показників MTTD і MTTR для команд безпеки [1].

2 МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ

2.1. Архітектура Tellix Endpoint Protection Platform

Організації будь-якого розміру наражаються на небезпеку з боку національних держав, хактивістів, організованої злочинності, а також зловмисних і випадкових інсайдерських загроз. Для зловмисників успішний злам забезпечує мотивацію та ресурси для подальших атак. Розрив у знаннях та можливостях між зловмисниками та захисниками вимагає фундаментальних змін у захисті кінцевих точок.

Фахівці з безпеки перебувають під дедалі більшим тиском, щоб захистити свої організації. Щоб подолати супротивників, засоби захисту кінцевих точок повинні співпрацювати одна з одною і з іншими технологіями безпеки, швидко виявляти, аналізувати, блокувати та стримувати поточні атаки. Вони повинні представляти криміналістичну інформацію швидко та інтуїтивно зрозуміло. Більше того, вони повинні робити все це, не ускладнюючи середовище для IT-команд і не впливати на продуктивність користувачів організації

Платформа захисту кінцевих точок Trellix дозволяє клієнтам реагувати та керувати життєвим циклом захисту від загроз. Це розширювана платформа для спільної роботи, що дозволяє зменшити складність традиційних середовищ захисту кінцевих точок від різних постачальників. Вона також надає адміністраторам можливість бачити сучасні загрози, щоб прискорити час виявлення та усунення загроз. Глобальні дані про загрози та локальні події в режимі реального часу надаються кінцевим точкам, що сприяє швидкому виявленню та реагуванню на них. Керування спрощується завдяки використання централізованої консолі і зручній для читання інформаційній панелі та звітів.

Tellix Endpoint Protection Platform створена для обміну інформацією в режимі реального часу між засобами захисту від загроз. Обмін подіями та інформацією про загрози з декількома технологіями, щоб ваша організація могла негайно вжити

заходів проти підозрілих програм, завантажень, веб-сайтів і файлів. Надлишкові дані, спричинені продуктами або засобами захисту для різних точок, можна знайти та усунути, а загальна архітектура кінцевих точок інтегрує кілька рівнів захисту, щоб обмінюватися інформацією про загрози для швидшого їх виявлення та аналізу.

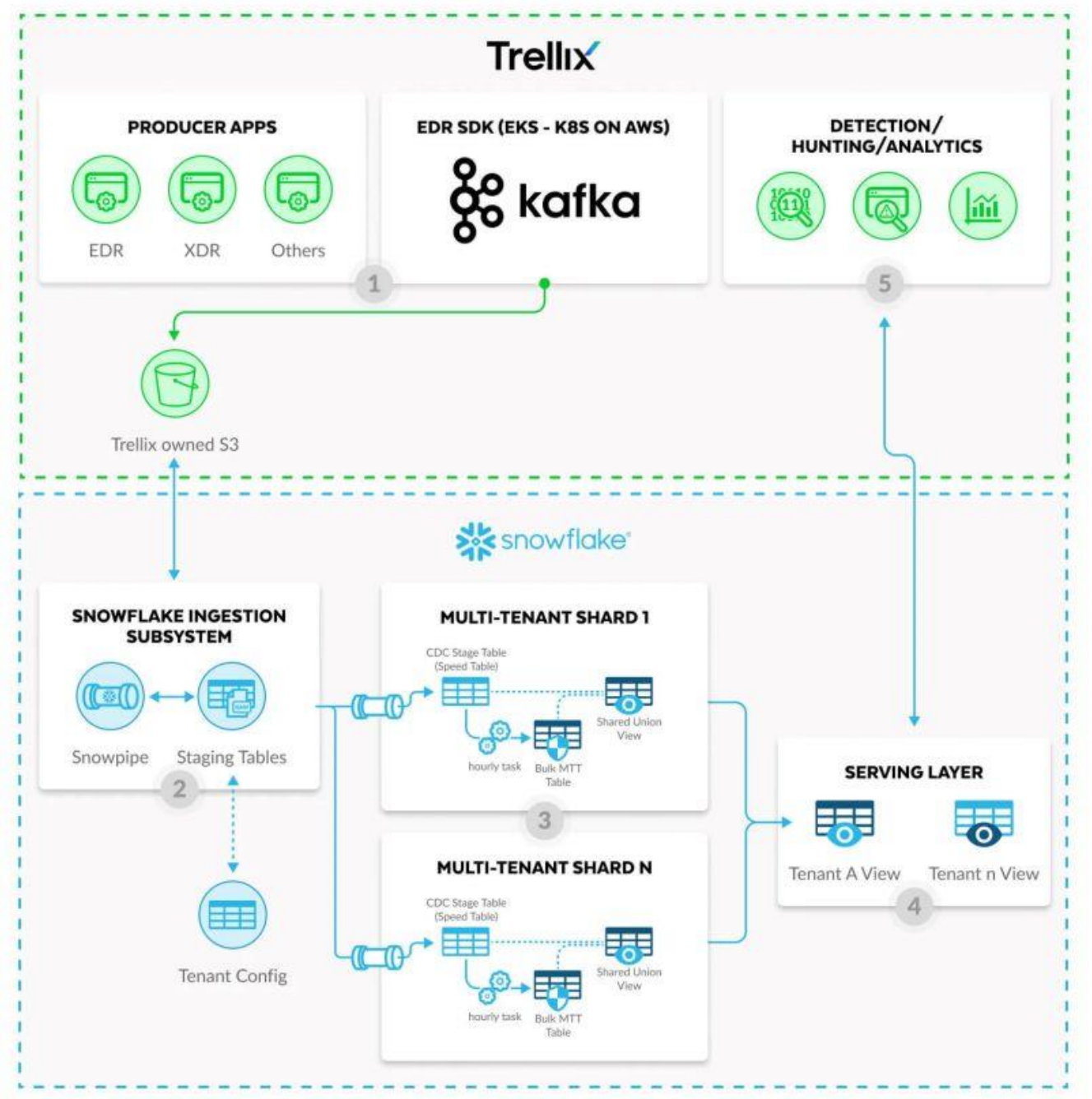

Рис.2.1. Архітектура даних Trellix [8]

Продукти та послуги, які надає Trellix для захисту кінцевих точок є наступні.

Trellix Endpoint Security (ENS)

Дозволяє оцінити переваги рішення для автоматичного захисту кінцевих точок, яке відповідає організаційним пріоритетним потребам у сфері безпеки, починаючи з запобігання та пошуку загроз і закінчуючи індивідуальним налаштуванням засобів захисту.

Trellix Endpoint Security (HX)

Надає можливості для віддаленого виявлення та розслідування кібератак на кінцеві точки, у тому числі атак прихованих шкідливих програм. Автоматизація сортування шляхом інтеграції з іншими системами виявлення дозволяє визначити першопричину та швидко усунути інцидент безпеки.

Trellix Endpoint Detection and Response

Це вдосконалене рішення EDR допомагає зменшити кількість хибних оповіщень та надати аналітикам можливість скоротити середній час виявлення та реагування на загрози за рахунок використання потужних засобів автоматизації.

Trellix Application and Change Control

Рішення забезпечує функціонування лише довірених програм на пристроях, серверах та настільних комп'ютерах.

Trellix Mobile Security

Рішення гарантує постійний захист незалежно від того, яким чином пристрій підключено до Інтернету — через корпоративну мережу, публічну точку доступу або оператора стільникового зв'язку — і чи він підключений взагалі.

Trellix MOVE AntiVirus

Єдине рішення для захисту віртуальних серверів та робочих столів призначене для всіх основних гіпервізорів.

Trellix Advisory Services

Підписка Trellix Advisory Services дає можливість скористатися послугами профільних фахівців, які пліч-о-пліч з вашою командою працюватимуть над впровадженням рішення EDR.

2.2. Ключові аспекти архітектури безпеки кінцевої точки Tellix Endpoint Protection Platform

Безпека кінцевих точок забезпечується в Tellix Endpoint Protection Platform завдяки використанню фреймворка кібербезпеки, який складається з п’яти компонент (рис 2.2):

Запобігання (Prevent);

Виявлення (Detect);

Дослідження (Investigate);

Відповідь (Respond);

Керування поверхнею атаки (Manage attacker surface).

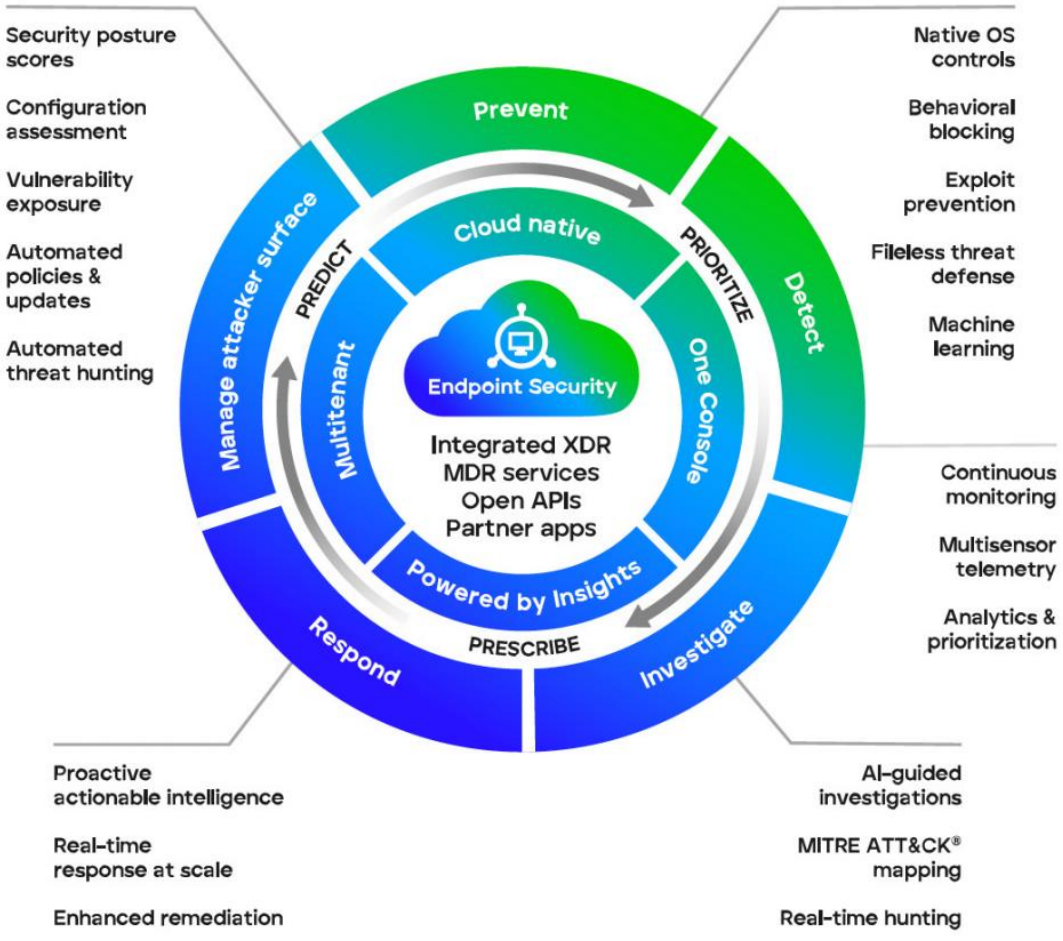

Рис. 2.2. Фреймворк Tellix Endpoint Protection Platform

2.3. Функції безпеки кінцевої точки Tellix Endpoint Protection Platform

Trellix Endpoint Protection Platform є ефективною платформою для сучасних фахівців з безпеки для подолання переваг зловмисників: інтелектуальні засоби захисту, що забезпечують спільну роботу, і структура, яка спрощує роботу в складних середовищах. Завдяки високій продуктивності та ефективності виявлення загроз, підтвердженій тестами сторонніх розробників, організація зможе захистити своїх користувачів, підвищити продуктивність і забезпечити безпеку своїй системі.

Endpoint Security – це практика захисту кінцевих точок або точок входу пристроїв кінцевих користувачів, таких як настільні комп'ютери, ноутбуки та мобільні пристрої, від використання зловмисниками та проведення шкідливих кампаній.

Endpoint Security складається з трьох модулів безпеки, які працюють незалежно один від одного для забезпечення кількох рівнів захисту.

Threat Prevention не дозволяє загрозам проникнути в систему, автоматично перевіряє файли при доступі та виконує цільові перевірки на наявність шкідливих програм у клієнтських системах.

Брандмауер – відстеження передачі даних між комп'ютером, мережевими ресурсами та Інтернетом. Перехоплює підозрілі повідомлення.

Контроль Інтернету – відстежує пошук та перегляд сторінок в Інтернеті у клієнтських системах та блокує веб-сайти та завантаження на основі рейтингу та вмісту безпеки.

Система адаптивного захисту від загроз – аналізує вміст у корпоративному середовищі користувача та визначає, які дії виконувати, використовуючи дані про репутацію файлів, правила та порогові значення репутації.

Основні функції платформи представлено у таблиці 2.1, де показано призначення кожної функції.

Таблиця 2.1.

Опис функцій Tellix Endpoint Protection Platform

Захист	•Класифікація поведінки за допомогою машинного навчання виявляє загрози нульового дня в режимі, близькому до реального часу, що дозволяє: • Автоматично розроблювати класифікацію поведінки для ідентифікації поведінки і додати правила для виявлення майбутніх атак. • Негайно відновлює кінцеву точку до останнього відомого працездатного стану щоб запобігти зараженню та зменшити навантаження на адміністратора.
Захист кінцевих точок від цільових атак	• Закриває проміжок часу від зіткнення до локалізації від днів до мілісекунд • Trellix Threat Intelligence Exchange збирає дані з різних джерел, дозволяючи компонентам системи безпеки миттєво інформувати один одного про нові та багатофазні сучасні атаки.
Інтелектуальне, адаптивне сканування	• Покращує продуктивність і продуктивність, оминаючи сканування довірених процесів і надаючи пріоритет підозрілим процесам і програмам. • Адаптивне поведінкове сканування відстежує підозрілу активність, націлюється на неї та ескалує її, якщо це виправдано.
Удосконалений захист від шкідливих програм	• Швидко захищає, виявляє та усуває шкідливе програмне забезпечення за допомогою нового антивірусного движка, який ефективно працює на різних пристроях і операційних системах.
Динамічне утримання додатків	• Захищає від програм-вимагачів і "сірого" ПЗ та забезпечує нульовий рівень захисту.

Блокування мережевих атак	• Інтегрований брандмауер використовує оцінки репутації на основі GTI для захисту кінцевих точок від бот-мереж, DDoS, складних постійних загроз, та підозрілі веб-з'єднання. • Брандмауер дозволяє тільки вихідний трафік під час запуску системи, захищаючи кінцеві точки, коли вони не знаходяться в корпоративній мережі
Дієва експертиза загроз	• Адміністратори можуть швидко побачити, де знаходяться заражені файли, чому вони виникають, а також тривалість впливу, щоб зрозуміти загрозу і швидко відреагувати. Централізоване управління (платформа Trellix ePO) з декількома варіантами розгортання. • Централізоване управління забезпечує більшу прозорість, спрощує операції, підвищує продуктивність IT, уніфікує безпеку та зменшує витрати. • Інтегрована архітектура дозволяє системам захисту кінцевих точок співпрацювати та взаємодіяти для посилення захисту.
Відкрита, розширювана система захисту кінцевих точок	• Оптимізація процесів та усунення дублювання призводять до зниження операційних витрат. • Безшовна інтеграція з іншими продуктами Trellix.

Trellix пропонує повний спектр рішень, які забезпечують глибокий захист, поєднуючи потужні засоби захисту з ефективним управлінням. Скорочення часу на захист, підвищення продуктивності та ефективне управління дають змогу командам безпеки швидше протистояти більшій кількості загроз, використовуючи менше ресурсів.

3 ТЕХНОЛОГІЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ

3.1 Технологія захисту кінцевих точок організації на прикладі Trellix Endpoint Security ENS

Trellix ENS перехоплює загрози, стежить за загальною працездатністю системи та складає звіти щодо виявлення та стану. Для виконання цих завдань клієнтське програмне забезпечення встановлюється у кожну систему.

Як правило, користувач встановлює один або кілька модулів Trellix ENS у клієнтські системи, керує виявленнями та налаштовує параметри, що визначають принцип роботи функцій продукту.

Trellix ePO - On-prem

Розгорнути модулі Trellix ENS у клієнтських системах та керувати ними можна за допомогою Trellix ePO – On-prem.

Кожен модуль включає розширення і пакет ПЗ, які встановлюються на сервер Trellix ePO - On-prem. Потім Trellix ePO – On-prem розгортає ПЗ у клієнтських системах. Trellix ePO - On-prem .

Клієнтське програмне забезпечення обмінюється даними з Trellix ePO - On-prem за допомогою Trellix Agent , щоб отримувати оновлення продукту, звіти та конфігурацію політик, а також примусово застосовувати ці політики.

Модулі клієнта

Клієнтське програмне забезпечення захищає системи завдяки регулярним оновленням, безперервному відстеженню та докладній звітності.

Це програмне забезпечення надсилає дані про виявлення на комп'ютерах користувачів на сервер Trellix ePO - On-prem. Ці дані використовуються при складанні звітів про виявлення та проблеми безпеки на вашому комп'ютері.

Сервер TIE та Trellix DXL

При використанні Adaptive Threat Protection платформа Trellix ENS інтегрується з Trellix Threat Intelligence Exchange (TIE) та Trellix® Data Exchange Layer. Ці додаткові продукти дозволяють користувачам локально керувати

репутацією файлів та миттєво надавати загальний доступ до інформації в усьому середовищі.

Trellix GTI

Модулі Запобігання загрозам, Брандмауер, Контроль Інтернету та Adaptive Threat Protection надсилають запит Trellix Global Threat Intelligence , щоб отримати інформацію про репутацію та визначити, як слід обробляти файли в клієнтській системі.

Trellix Labs

Клієнтське програмне забезпечення обмінюється даними з Trellix Labs, щоб отримувати файли вмісту та оновлення ядра. Trellix Labs регулярно випускає оновлені пакети вмісту.

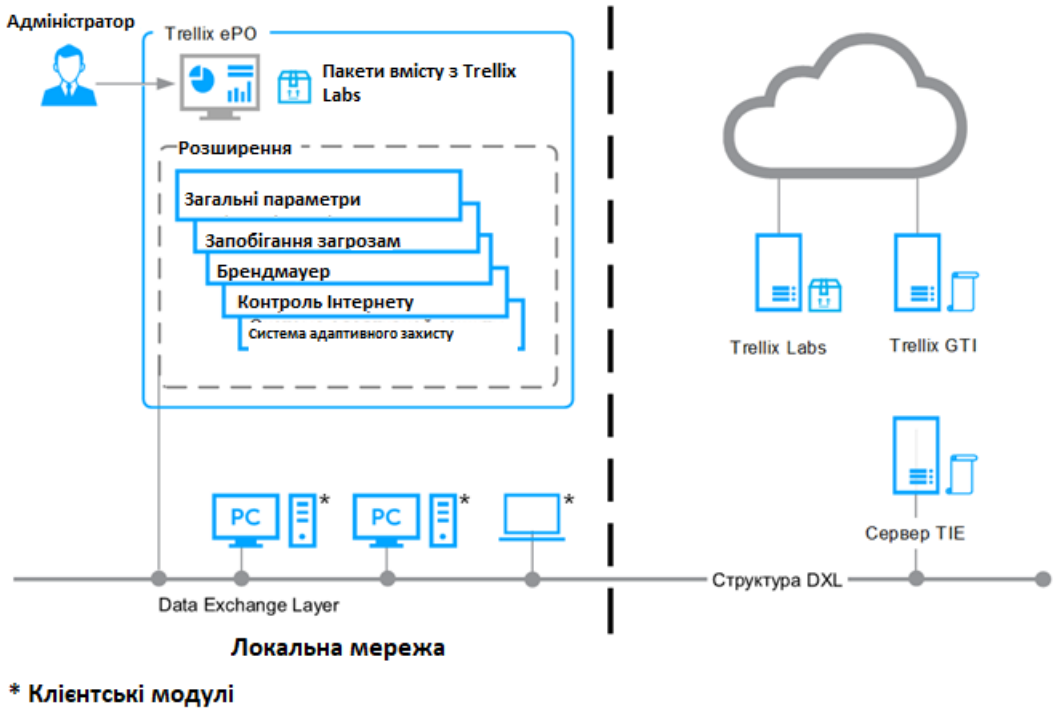

Рис. 3.1. Принцип технології Trellix ENS

Регулярне оновлення Trellix ENS дозволяє захистити комп'ютери користувачів від нових загроз.

Клієнтське програмне забезпечення з'єднується з локальним або віддаленим сервером Trellix ePO - On-prem або безпосередньо з сайтом в Інтернеті, щоб здійснити оновлення. Trellix ENS перевіряє наявність наступних оновлень.

Оновлення файлів вмісту, які використовуються для виявлення загроз. Файли вмісту містять опис загроз, наприклад, вірусів та шпигунських програм. З виявленням нових загроз ці описи оновлюються.

Оновлення компонентів програмного забезпечення, наприклад, різного роду виправлення.

Отже технологія захисту кінцевих точок складається з комплексу технологій, які дозволяють виявляти і захищати кінцеві точки організації від загроз. Розглянемо кожну з цих технологій в наступних підрозділах.

3.2. Принцип роботи модуля запобігання загрозам технології Trellix ENS

Першою складовою технології Trellix ENS є модуль запобігання загрозам (рис.3.1).

Trellix Endpoint Security (ENS) Threat Prevention блокує загрози, не дозволяючи їм проникнути в систему, автоматично перевіряє файли при доступі та виконує цільові перевірки на наявність шкідливих програм у клієнтських системах.

Модуль Запобігання загрозам виявляє загрози на основі файлів вмісту безпеки. Оновлення вмісту безпеки завантажуються автоматично, щоб забезпечувати захист від конкретних вразливостей та блокувати загрози, що виникають.

Модуль Запобігання загрозам захищає середовище організації від наступних загроз:

Віруси, черв'яки та троянські коні.

Порушення захисту точки доступу (небажані зміни файлів, загальних ресурсів, розділів реєстру, параметрів реєстру). Цей модуль також запобігає або обмежує підозрілу поведінку процесів та служб.

Засоби використання уразливостей, пов'язані з переповненням буфера.

Неприпустиме використання API – захист від зловмисних викликів API, що виконуються невідомою або скомпрометованою програмою.

Вторгнення в мережу, наприклад атаки, націлені на зниження пропускної спроможності, та мережеві атаки типу "відмова в обслуговуванні".

Потенційно небажані коди та програми.

Загрози, пов'язані з уразливістю.

Засоби використання вразливостей нульового дня.

Загрози у сценаріях, створених не на основі браузера, наприклад PowerShell, JavaScript та VBScript.

Розгорнути модуль Запобігання загрозам клієнтських систем і керувати ним можна за допомогою Trellix ePO - On-prem.

Основні функції модуля Запобігання загрозам спрямовано на захист середовища організації від загроз, виявлення в ньому шкідливих програм, а також виправлення помилок шляхом очищення або відновлення заражених файлів.

До основних функцій модуля Запобігання загрозам, який забезпечить захист систем від вторгнень до того, як вони отримають доступ до середовища відносяться:

ЗАХИСТ

1. Захист доступу – захист від внесення небажаних змін до клієнтських систем шляхом обмеження доступу до певних файлів, загальних ресурсів, розділів реєстру, параметрів реєстру, а також запобігання або обмеження загрозливої поведінки процесів та служб.

2. Запобігання дії засобів використання вразливостей – модуль Запобігання загрозам використовує сигнатури в оновленнях вмісту для захисту від наведених нижче вразливостей:

– захист від переповнення буфера – зупиняє виконання довільного коду при переповненні буфера внаслідок атаки;

– неприпустиме використання API – захист від зловмисних викликів API, які виконуються невідомими або шкідливими програмами в системі.

– запобігання вторгненням в мережу (мережева IPS) – захист від атак, націлених на зниження пропускної спроможності, та мережевих атак типу "відмова в обслуговуванні", які знижують працездатність мережі.

– розширені правила – надаються додаткові параметри і збільшується гнучкість порівняно з правилами модуля "Захист доступу". Однак, щоб створити розширені правила, потрібно розуміти власний синтаксис Trellix .

3. Інтерфейс командного рядка – повну перевірку, швидку перевірку, вибіркові перевірки та оновлення вмісту безпеки можна виконувати з командного рядка або в рамках розгортання пакетного файлу.

ВИЯВЛЕННЯ

Наведені нижче функції модуля Запобігання небезпеці дозволять виявляти загрози при їх виникненні в середовищі.

1. Перевірка доступу - перевірка на наявність загроз при читанні файлів з диска або їх запису на диск. Перевірка інтегрується з інтерфейсом Antimalware Scan Interface (AMSI), щоб забезпечити покращену перевірку наявності загроз у сценаріях, не пов'язаних із браузером.

2. Перевірка на вимогу – запуск або планування визначених перевірок, включаючи перевірку наявності записів у реєстрі для шпигунських програм, які раніше не були очищені. Перевірки виконуються лише при бездіяльності системи. Щоб оптимізувати продуктивність перевірки, слід обмежити завантаження ЦП.

3. Потенційно небажані програми – виявлення потенційно небажаних програм (наприклад, шпигунських програм та програм для показу реклами), а також запобігання їх запуску у вашому середовищі.

4. Карантин - поміщення в карантин заражених елементів, спроба їх очищення або відновлення або автоматичне видалення.

5. Панелі моніторингу та монітори – відображення статистики модуля Запобігання загрозам , включаючи тривалість перевірки, стан оновлення вмісту, а також програми з найбільшою кількістю вразливостей. (Керовані системи)

6. Запити та звіти – отримання докладних відомостей про модуль Запобігання загрозам , включаючи інформацію про кількість загроз, виконання

перевірки, відповіді на виявлені загрози, події скорочення кількості помилкових позитивних результатів, а також відомості про рівень чутливості Trellix GTI . (Керовані системи)

7. Захист від шкідливих програм із раннім запуском – підтримує функцію ELAM, доступну у Windows 8 та пізніших випусках. ELAM збирає список драйверів пристроїв, завантажених під час циклу завантаження, та перевіряє їх після запуску служб перевірки.

ВИПРАВЛЕННЯ

Наведені нижче функції модуля Запобігання загрозам дозволяє усувати проблеми безпеки, обробляти виявлені загрози, покращити продуктивність та посилити захист.

1. Дії – виконання певних дій у разі виявлення погроз.

2. Попередження – повідомлення у разі виявлення загроз, а також обмеження трафіку за допомогою фільтрів.

3. Файли Extra.DAT – захист від нових загроз (наприклад, масштабної вірусної епідемії). Trellix ePO - On-prem.

4. Заплановані перевірки – запуск перевірок у періоди низьких навантажень дозволяє підвищити продуктивність системи та перевірок.

5. Репозиторії вмісту – зниження мережного трафіку через Інтернет чи внутрішню мережу підприємства шляхом переміщення репозиторію файлів вмісту ближче до клієнтських систем. (Керовані системи).

6. Файли журналу (Trellix Endpoint Security (ENS) Client) – надання історії виявлених елементів, яку можна використовувати для визначення потреби змінити налаштування, щоб посилити захист або підвищити продуктивність системи.

7. Панелі керування та монітори – відстеження операцій та використання цієї інформації для налаштування параметрів модуля Запобігання загрозам . (Керовані системи).

Модуль Запобігання загрозам складається з двох компонентів: розширення, встановленого на сервері Trellix ePO - On-prem , та ПЗ для захисту (включаючи ядро

сканера та файли вмісту), встановленого в клієнтській системі. Модуль Запобігання загрозам містить програмне забезпечення для захисту, а також ядро сканера та файли вмісту, встановлені в клієнтській системі.

Крім того, в клієнтській системі встановлено рішення Trellix Endpoint Security (ENS) Common , яке включає Trellix Endpoint Security (ENS) Client .

За допомогою Trellix Agent клієнтське програмне забезпечення зв'язується з Trellix ePO - On-prem для налаштування та надсилання звітів, з Trellix Global Threat Intelligence для отримання інформації про репутацію, а також із Trellix Labs для оновлення файлу вмісту та ядра.

За допомогою Trellix Agent клієнтське програмне забезпечення зв'язується з Trellix Global Threat Intelligence для отримання інформації про репутацію, а також Trellix Labs для оновлення файлу вмісту та ядра.

Робочий процесу – захист доступу загрозам слід виконувати за базовою процедурою при захисті файлів, розділів реєстру, значень реєстру, процесів і служб.

Крок процедури наступні (Рис.3.2).

1. Якщо система керована, адміністратор налаштовує правила захисту у політиці модуля Захист доступу та застосовує її у клієнтській системі.

2. Адміністратор налаштовує правила захисту у політиці Захист доступу до Trellix ePO – On-prem та примусово застосовує її у клієнтській системі.

3. Адміністратор завантажує останні версії файлів вмісту в Trellix Labs .

4. Користувач завантажує безпечну (не шкідливу) програму, MyProgram.exe, в Інтернеті та запускає її. MyProgram.exe запускається сама та запускає дочірній процес під назвою AnnoyMe.exe. AnnoyMe.exe робить спробу внести зміни до операційної системи, щоб переконатися, що AnnoyMe.exe завжди завантажується під час запуску. Модуль Запобігання загрозам обробляє запит і зіставляє дію з існуючим правилом захисту, визначеним Trellix або користувачем. Модуль Запобігання загрозам не дає AnnoyMe.exe внести зміни до операційної системи.

5. Модуль Запобігання загрозам реєструє відомості. Модуль Запобігання загрозам реєструє відомості, а потім створює подію та надсилає її до Trellix ePO - On-prem .

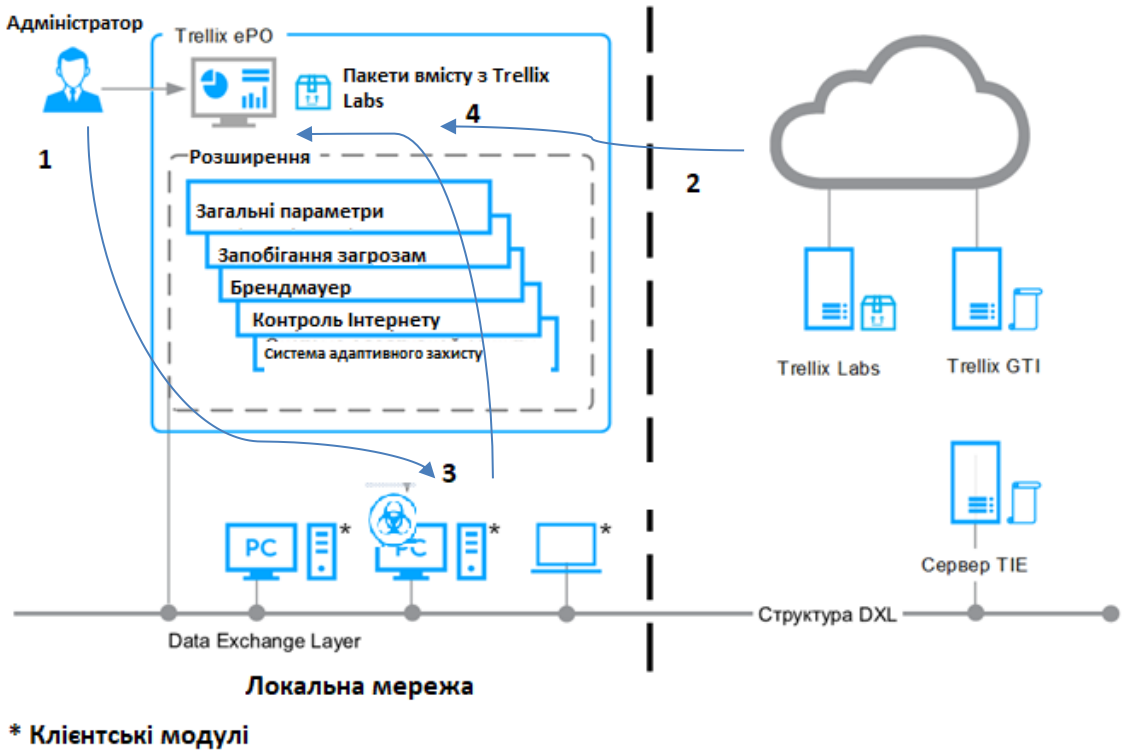

Рис. 3.2. Робочий процесу – захист загрозам

Клієнтська система

Крім модуля Запобігання загроз клієнтська система включає такі компоненти:

Файли вмісту (включаючи вміст AMCore, що також називається сигнатурами шкідливих програм , захист доступу та вміст функції запобігання діям засобів уразливостей) – спільно з ядром сканера вони відповідають за виявлення загроз та виконання відповідних дій щодо їх усунення.

Ядро сканера – перевіряє файли, папки та диски клієнтської системи та порівнює результати з інформацією про відомі віруси та файли вмісту.

Trellix Agent – забезпечує безпечний зв'язок між керованими продуктами та сервером Trellix ePO-On-prem.

Trellix Endpoint Security (ENS) Common – надаються такі послуги, як оновлення, ведення журналу, звіти про події та властивості, планування завдань, зв'язок та зберігання параметрів.

Trellix ePO - On-prem

Сервер Trellix ePO - On-prem використовує такі компоненти для віддаленого керування та оновлення клієнтських систем:

Trellix ePO - On-prem – забезпечує централізоване адміністрування та примусове застосування політик модуля Запобігання загрозам , а також за допомогою запитів та панелей моніторингу відстежує активність та виявлення загроз.

Репозиторій вмісту – завантажує оновлення файлів вмісту із сайту завантаження Trellix . Використовуючи репозиторій вмісту у своїй організації, ви зможете копіювати файли вмісту автоматично та максимально скоротити навантаження на смугу пропускання.

Сервер Trellix

Компанія Trellix, до якої входить Trellix Labs і служба технічної підтримки Trellix, надає такі послуги.

Trellix Labs (бібліотека загроз) – досліджує та зберігає докладну інформацію про шкідливі та потенційно небажані програми та способи їх нейтралізації.

Trellix GTI (евристична перевірка мережі на підозрілі файли) – здійснює пошук підозрілих програм та бібліотек DLL, запущених у клієнтських системах, захищених модулем Запобігання загрозам . Trellix GTI відправляє відбиток кожного підозрілого файлу в Trellix Labs для аналізу та прийняття рішення про подальші дії.

Оновлення вмісту та ядра – забезпечують захист від конкретних уразливостей та блокують виконання нових і виникаючих загроз (включаючи атаки з переповненням буфера).

3.3. Принцип роботи брандмауера технології Trellix ENS

Trellix Endpoint Security (ENS) Firewall захищає системи, мережеві ресурси та програми від зовнішніх та внутрішніх атак.

Брандмауер перевіряє весь вхідний та вихідний трафік і порівнює його зі списком правил брандмауера, який є набором критеріїв зі зв'язаними діями. Якщо пакет відповідає всім критеріям правила, брандмауер діє згідно з цим правилом, блокуючи або дозволяючи пакет через брандмауер.

Розгорнути та адмініструвати Брандмауер у клієнтських системах можна за допомогою Trellix ePO - On-prem.

Основні функції модуля Брандмауер спрямовані на захист від загроз, виявлення проблем з безпекою та виправлення хибних позитивних результатів.

ЗАХИСТ

Захист мережі та програмо організації відбувається за допомогою наведених нижче функцій модуля Брандмауера.

6. Правила – визначає критерії, які Брандмауер буде використовувати для визначення необхідності блокування або дозволу вхідного та вихідного трафіку.

7. Групи правил – організовує правила брандмауера, щоб спростити керування, застосовувати правила вручну або за розкладом, а також обробляти трафік залежно від типу з'єднання.

8. Фільтрування та перевірка пакетів з контролем стану – відстежує стан та характеристики мережного з'єднання у таблиці станів, дозволяючи лише пакети, що відповідають відомому відкритому з'єднанню.

9. Контроль на основі репутації – блокує ненадійні файли або весь трафік з недовіреної мережі на основі репутації.

ВИЯВЛЕННЯ

Наведені нижче функції модуля Брандмауер дозволяють виявляти проблеми з безпекою.

1. Панелі керування та монітори – відображає події вторгнень та виявлень у Trellix GTI та Брандмауер .

2. Запити та звіти – функція відновлює докладну інформацію про модуль Брандмауер , включаючи правила клієнта, помилки, події вторгнення та блокування та зберігає цю інформацію у звітах.

3. Попередження – відображає попередження про заблокований трафік на основі репутації файлу або мережі, що виконується.

4. Журнал трафіку – реєструє весь заблокований та дозволений трафік.

ВИПРАВЛЕННЯ

Наведені нижче функції модуля Брандмауер дозволяють скоротити кількість помилкових позитивних результатів, або зовсім позбутися їх .

1. Адаптивний режим – автоматично створює правила у клієнтській системі, щоб дозволити допустимі дії.

2. Після того, як правила клієнта створені, необхідно їх проаналізувати та вибрати ті, які можна перетворити на політики сервера.

3. Певні мережі – визначте довірені мережі, щоб дозволити трафік із мереж, які ваша організація вважає безпечними.

4. Довірені файли, що виконуються – створює список безпечних виконуваних файлів, щоб скоротити кількість помилкових позитивних результатів.

5. Каталог брандмауера – визначає правила та групи для додавання до кількох політиків, або мережі та програми, які будуть додані до правил брандмауера.

6. Параметри клієнта – дозволяє користувачам тимчасово відключати модуль Брандмауер для усунення несправностей.

7. Панелі керування та монітори – відстежує операції та виявлення вторгнень, а потім використовує цю інформацію для налаштування параметрів модуля Брандмауер.

Брандмауер перевіряє весь вхідний та вихідний трафік на пакетному рівні та порівнює пакети з налаштованими правилами брандмауера, щоб визначити необхідність у вирішенні чи блокуванні трафіку (Рис. 3.3).

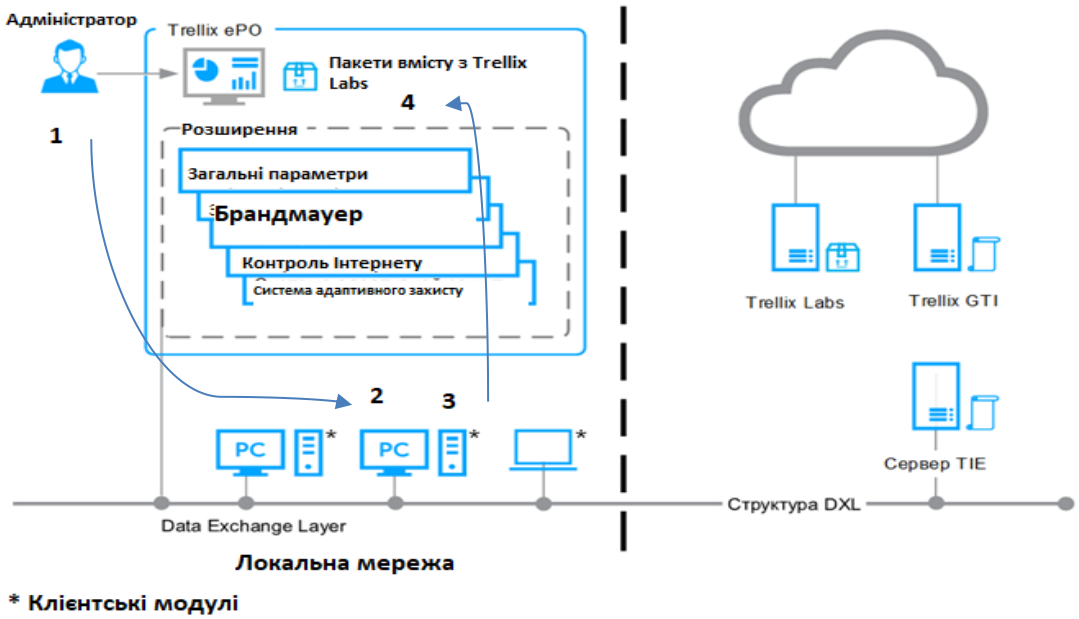

Рис.3.3. Принцип роботи брандмауера

1. Адміністратор налаштовує правила брандмауера Trellix ePO - On-prem і застосовує політику в клієнтській системі.

2. Якщо система керована, адміністратор налаштовує правила брандмауера Trellix ePO - On-prem і застосовує політику в клієнтській системі.

3. Користувач виконує завдання, яке ініціює мережну активність та створює трафік.

4. Брандмауер перевіряє весь вхідний та вихідний трафік і порівнює пакети з налаштованими правилами. Якщо трафік відповідає правилу, Брандмауер блокує чи дозволяє його залежно від критеріїв правила.

5. Брандмауер записує інформацію до журналу. Брандмауер записує в журнал відомості, а потім створює подію і відправляє її в Trellix ePO - On-prem.

3.4. Принцип роботи модуля контролю інтернету технології Trellix ENS

Trellix Endpoint Security (ENS) Контроль Інтернету відстежує пошук в Інтернеті та перегляд веб-сторінок на клієнтських комп'ютерах. Він захищає від загроз на веб-сторінках та завантаження файлів.

Технологія Trellix аналізує всі веб-сайти та на підставі результатів перевірки надає їм колірні рейтинги безпеки. Колір відображає рівень безпеки веб-сайту.

Контроль Інтернету використовує ці результати перевірки визначення загроз в Інтернеті. ПЗ, встановлене в клієнтській системі, надає додаткові функції, які відображаються у вікні браузера та результати пошуку для сповіщення користувачів.

Розгорнути модуль Контроль Інтернету у клієнтських системах та керувати ним можна за допомогою Trellix ePO - On-prem. Параметри дозволяють контролювати доступ до сайтів відповідно до їх рейтингу безпеки, типу вмісту, а також URL-адреси та доменного імені.

Параметри дозволяють контролювати доступ до сайтів відповідно до їх рейтингу безпеки та типу вмісту.

Основні функції модуля Контроль Інтернету спрямовані на захист систем від веб-загроз, виявлення загроз та виправлення помилок, пов'язаних із завантаженням файлів.

ЗАХИСТ

Наведені нижче функції модуля Контроль Інтернету допомагають захистити системи від шкідливих веб-сайтів та завантажень.

1. Список блокувань та дозволів – запобігає відвідуванню користувачами певних URL-адрес або доменів, або завжди дозволяє доступ до сайтів, важливих для вашого бізнесу.

2. Блокування веб-категорій та дій на основі рейтингу – рейтинги безпеки та веб-категорії, визначені Trellix , використовуються для контролю доступу користувачів до сайтів, сторінок та завантажень.

3. Безпечний пошук – автоматичне блокування небезпечних сайтів із результатів пошуку на підставі їхнього рейтингу безпеки.

4. Самозахист – забороняє користувачам вимикати модуль контролю Інтернету, а також видаляти або змінювати файли, розділи реєстру, значення реєстру, служби та процеси модуля Контроль Інтернету .

ВИЯВЛЕННЯ

Наведені нижче функції модуля Контроль Інтернету допомагають виявляти шкідливі веб-сайти.

1. Кнопка Контроль Інтернету у вікні браузера – у модулі Контроль Інтернету , що підключається , відображається кнопка, що вказує рейтинг безпеки сайту. Натисніть цю кнопку, щоб отримати більше інформації про веб-сайт.

2. Контроль Інтернету на сторінках результатів пошуку – відображається біля кожного сайту зі списку. Колір значок вказує на рейтинг безпеки сайту. Наведіть курсор на значок, щоб отримати більше інформації про сайт.

3. Звіти сайту – у них містяться докладні відомості про те, як було вираховано рейтинг безпеки на основі типів виявлених загроз, результатів перевірок та інших даних.

4. Панелі керування та монітори – відображають статистику операцій модуля Контроль Інтернету , включаючи відвідування та завантаження з сайтів за рейтингом, тип вмісту, а також список блокувань та дозволів.

5. Запити та звіти – надання детальної інформації про події у браузері модуля Контроль Інтернету з можливістю її збереження у звітах.

ВИПРАВЛЕННЯ

Наведені нижче функції модуля Контроль Інтернету дозволяють виконувати відстеження та налаштування.

1. Взаємне блокування з іншими продуктами Trellix – автоматично відключає модуль Контроль Інтернету , якщо він виявляє пристрій інтернет-шлюзу або якщо встановлено рішення Skyhigh Client Proxy, а також у режимі перенаправлення.

2. Перевірка файлів, що завантажуються – модуль Контроль Інтернету відправляє файли в модуль Запобігання загрозам для перевірки. У разі виявлення загрози модуль Запобігання загрозам відповідає налаштованим діям (наприклад, очищенням) і повідомляє користувача.

3. Панелі керування та монітори – відстежують операції, щоб зрозуміти, які дії в Інтернеті ви виконуєте, а потім використовують цю інформацію для налаштування параметрів модуля Контроль Інтернету.

4. Винятки – запобігають призначенню рейтингу для певних IP-адрес та їх блокування модулем Контроль Інтернету.

Принцип роботи модулю Контроль Інтернету (рис.3.4) запитує у Trellix GTI інформацію про репутацію, щоб визначити, які дії слід робити при навігації за URL-адресами.

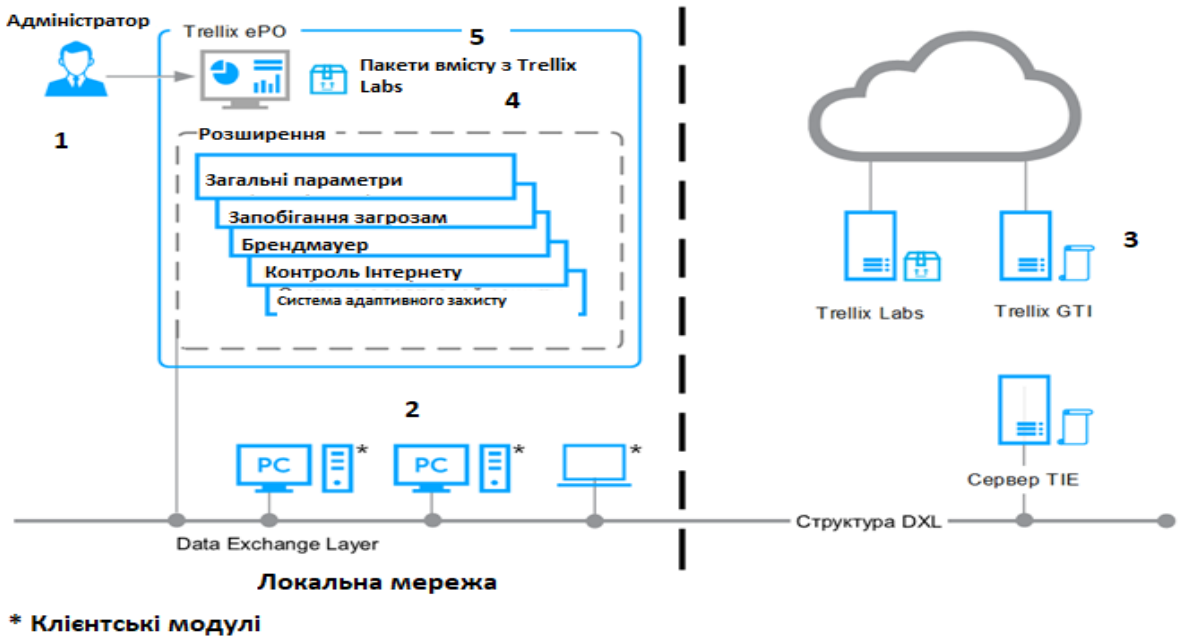

Рис. 3.4. Принцип роботи модуля Контроль Інтернету

1. Адміністратор налаштовує параметри модуля Контроль Інтернету Trellix ePO - On-prem і примусово застосовує політику в клієнтській системі.

2. Адміністратор налаштовує параметри модуля Контроль Інтернету Trellix ePO - On-prem і примусово застосовує політику в клієнтській системі.

3. Користувач заходить на веб-сайт або отримує доступ до його ресурсів.

4. Модуль Контроль Інтернету вимагає репутацію URL-адреси у Trellix GTI .

– якщо репутація URL-адреси зеленого кольору, модуль Контроль Інтернету дозволяє перейти по цій URL-адресі та відображає сторінку. В іншому випадку модуль Контроль Інтернету переходить на сторінку блокування або попередження залежно від налаштувань.

– якщо репутація URL-адреси не має рейтингу, але відповідає категорії Trellix GTI , модуль Контроль Інтернету дозволяє або блокує перехід за URL-адресою залежно від налаштувань розділу Дії на основі вмісту .

5. Якщо це запит на завантаження файлів, а файл не має репутації шкідливого, модуль Контроль Інтернету дозволяє завантаження, навіть якщо URL-адреса має репутацію шкідливого. Якщо репутація файлу невідома, Контроль Інтернету надсилає файл у модуль Запобігання загрозам , щоб перевірити його сканером на вимогу.Модуль Запобігання загрозам порівнює файл із вмістом AMCore. Якщо його вміст відповідає сигнатурі або хешу, завантаження файлу блокується. В іншому випадку файл завантажується.

6. Модуль Контроль Інтернету реєструє інформацію. Модуль Контроль Інтернету реєструє відомості, а потім створює подію та надсилає її до Trellix ePO - On-prem .

3.5. Принцип роботи модуля Adaptive Threat Protection технології Trellix ENS

Trellix Endpoint Security (ENS) Adaptive Threat Protection аналізує вміст у середовищі вашого підприємства та визначає, які дії слід вжити, на основі репутації файлів, правил та порогових значень репутації.

Adaptive Threat Protection надає такі переваги:

1. Швидке виявлення та захист від загроз безпеки та шкідливих програм.

2. Можливість дізнатися, які системи чи пристрої вже скомпрометовані та як загроза поширюється у вашому середовищі.

3. Можливість негайно очистити певні файли на основі репутації загрози та ваших критеріїв ризику.

4. Інтеграція із системою сканування за допомогою Real Protect дозволяє виконувати автоматичний аналіз поведінки у хмарі та клієнтських системах.

5. Функція захисту від крадіжки облікових даних (CTP) захищає службу підсистеми локальних засобів захисту (LSASS.exe) від потенційних загроз з боку хакерів. Процеси, які несподівано намагаються отримати доступ до Microsoft LSASS.exe для отримання облікових даних, будуть заблоковані. Інформація про відповідну подію буде надіслана до Trellix ePO - On-prem .

6. Розширена перевірка сценаріїв, включно з інтерфейсом Antimalware Scan Interface (AMSI).

7. Здатність виявляти методи атак, не пов'язані з використанням файлів, при яких відсутній файл шкідливої програми, що зберігається.

8. Можливість відстеження невідомих процесів та автоматичного виправлення змін, внесених до системи.

9. Інтеграція в режимі реального часу з сервером "Пісочниці", Adaptive Threat Protection та Trellix Threat Intelligence Exchange забезпечує можливість надсилання невідомих файлів під час створення та виконання файлів. Рішення повертає детальну оцінку файлу та дані про репутацію, а також класифікацію шкідливих програм. Така інтеграція дозволяє реагувати на загрози та надавати спільний доступ до інформації у вашому середовищі.

Основні функції модуля ATP спрямовані на захист вашого підприємства від файлів з невідомою репутацією, виявлення шкідливих шаблонів та виправлення хибних позитивних результатів.

ЗАХИСТ

Забезпечує захист шляхом блокування або обмеження файлів з невідомою репутацією, використовуючи функції ATP .

1. Обробка файлів на основі репутації – модуль ATP попереджає про невідомий файл у середовищі.

2. ATP може негайно заблокувати файл, а не надсилати інформацію про нього в Trellix для аналізу.

3. Інтеграція із сервером TIE – сервер TIE (за наявності) надає інформацію про кількість систем, у яких запускався файл. Сервер "Пісочниці" допомагає визначити, чи загрожує файл.

4. Динамічне обмеження додатків дозволяє запуск невідомих файлів у контейнері, обмежуючи їх можливі дії.

Коли компанія вперше використовує файл із невідомою репутацією, модуль ATP може запустити його у контейнері. Правила обмеження визначають, які дії не можуть здійснювати обмежені програми. Динамічне обмеження програм також обмежує процеси, коли вони завантажують PE-файли (переносні виконувані файли) і бібліотеки DLL (бібліотеки, що динамічно підключаються), які знижують репутацію процесу.

ВИЯВЛЕННЯ

Виявлення шкідливих шаблонів і програм у пам'яті завдяки наведеним нижче функціям модуля ATP .

1. Сканування за допомогою Real Protect виконує автоматичний аналіз поведінки.

Real Protect перевіряє підозрілі файли та операції у клієнтській системі та виявляє шкідливі шаблони, використовуючи методи машинного навчання. Перевірки Real Protect на основі клієнта та на основі хмари включають перевірку DLL, що дозволяє не допустити завантаження довіреними процесами недовірених файлів PE і DLL.

2. Захист від крадіжки облікових даних – забезпечує захист від крадіжки облікових даних.

Технологія захисту від крадіжки облікових даних має зупинити атаки, спеціально спрямовані на службу підсистеми локальних засобів захисту (LSASS).

3. Розширена перевірка сценаріїв – інтеграція з AMSI (Antimalware Scan Interface) забезпечує розширену перевірку загроз у сценаріях, створених не на основі браузера, наприклад PowerShell, JavaScript та VBScript.

4. Правила ATP – визначення дозволених та заборонених дій для процесів в окремих контекстах, а також можливість зміни репутації залежно від контексту та поведінки.

ВИПРАВЛЕННЯ

Очищення файлів та усунення хибних позитивних результатів за допомогою описаних нижче функцій модуля ATP .

1. Очищення файлів – модуль ATP може очищати файли, коли репутація файлу досягає встановленого порога.

2. Розширене відновлення – якщо процес невідомий, розширене відновлення відслідковує його поведінку та реєструє у журналі всі файли, які створює процес, і, при необхідності, всі файли, які процес змінює чи видаляє. Якщо процес, що відстежується, демонструє шкідливу поведінку, функція розширеного відновлення зупиняє процес, його дочірні процеси та процеси-предки та виконує відкіт змін, внесених процесом, а також відновлює систему до стану, максимально наближеного до стану, в якому вона знаходилася до запуску процесу.

3. Виключення файлів користувача – якщо файл користувача є довіреним, але за замовчуванням має репутацію шкідливого, він блокується. Можна виключити його з перевірок або змінити репутацію файлу, зробивши його довіреним, і дозволити його запуск в організації без запиту оновленого файлу DAT у Trellix .

4. Скорочення кількості хибних позитивних результатів :

– Якщо модуль ATP отримує відомості про репутацію файлу вище за певний поріг з сервера TIE або Trellix GTI , він може автоматично перевизначити помилковий позитивний результат за допомогою модуля Adaptive Threat Protection або Запобігання загрозам .

– Якщо Adaptive Threat Protection визначає, що виявлення є помилковим позитивним результатом, Trellix Labs може випустити негативний файл Extra.DAT , щоб приховати виявлення до наступного оновлення вмісту.

5. Правила Adaptive Threat Protection – Trellix щомісяця надає оновлення для правил вмісту AMCore.

6. Панелі моніторингу та звіти Trellix ePO - On-prem – демонстрація операцій та виявлень, які можна використовувати для налаштування параметрів Adaptive Threat Protection . (Керовані системи).

Adaptive Threat Protection отримує інформацію про репутацію з локального кешу репутації, з сервера TIE та від Trellix GTI , щоб визначити спосіб обробки файлів та процесів у клієнтській системі. ATP використовує правила для виявлення атак з використанням ресурсів цільової системи та атак без використання файлів, а також розширене відновлення для відкату змін у разі, якщо атака відбудеться.

Принцип роботи. Адміністратор налаштовує параметри ATP у Trellix ePO - On-prem і примусово застосовує модуль у клієнтській системі (рис.3.5).

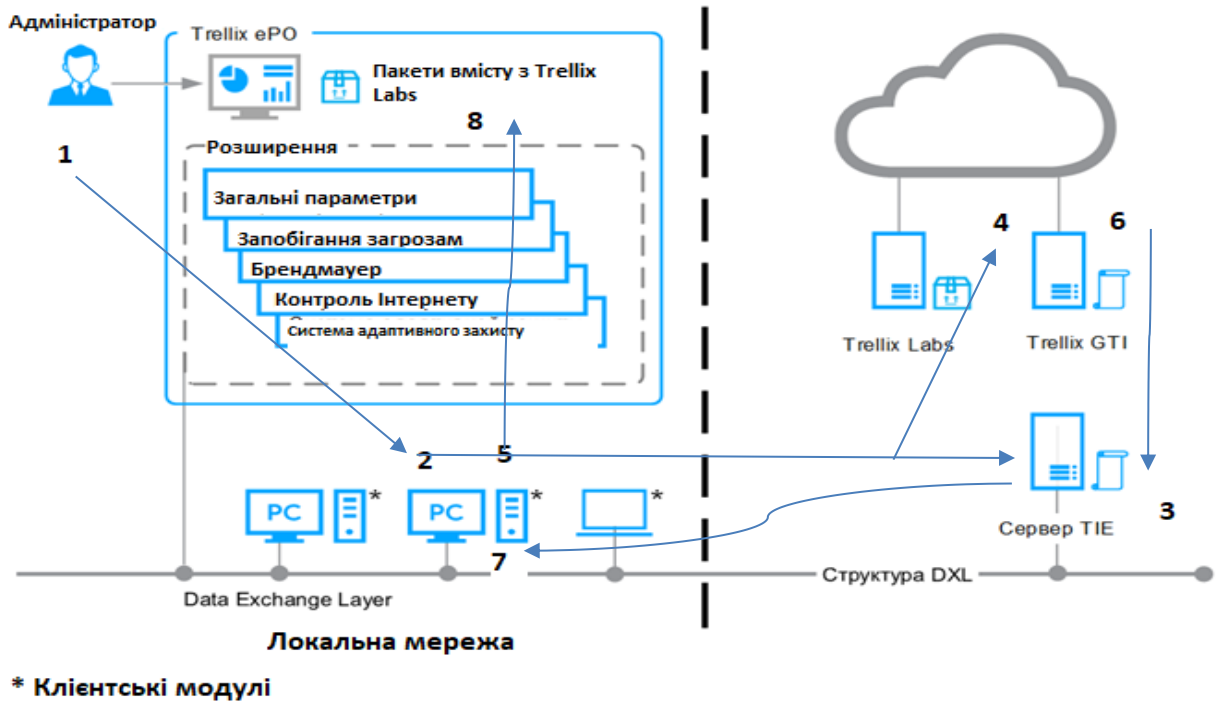

Рис.3.5. Принцип роботи Adaptive Threat Protection

1. Користувач виконує файл у клієнтській системі.

2. Adaptive Threat Protection перевіряє наявність файлу у локальному кеші репутації.

3. Якщо файлу немає в локальному кеші репутації, ATP надсилає запит репутації на сервер TIE (за наявності).

4. Якщо файл відсутній у базі даних сервера TIE , сервер TIE відправляє запит репутації в Trellix GTI . Якщо сервер TIE недоступний, ATP надсилає запит репутації Trellix GTI .

5. Залежно від репутації файлу та параметрів ATP, можливі наступні варіанти дій.

– Дозволяється запуск файлу.

– Файл очищується.

– Файл заблоковано.

– Дозволяється запуск файлу у контейнері.

– Користувачеві пропонується виконати дію.

Для процесу з репутацією Відомий як надійний правила Adaptive Threat Protection визначають відповідні дії. ATP відстежує процес, його дочірні та батьківські процеси з метою виявлення підозрілої поведінки, яка може свідчити про атаку без використання файлів, і при необхідності блокує процес. Якщо репутація процесу Невідомо (50) або нижча, функція розширеного відновлення створює резервну копію змін і виконує відкат, якщо процес демонструє шкідливу поведінку.

6. Trellix GTI надсилає актуальну інформацію про репутацію файлу на сервер TIE .

7. Сервер TIE оновлює базу даних та надсилає оновлену інформацію про репутацію у всі системи з увімкненим модулем ATP для негайного захисту середовища.

8. ATP записує відомості в журнал, а потім, якщо працює в керованій системі, створює подію та відправляє її в Trellix ePO – On-prem.

3.6. Рекомендації використання технологій захисту кінцевих точок технології Trellix ENS

Сучасна безпека кінцевих точок забезпечує багаторівневий захист, щоб зменшити поверхню атаки, виявити загрози, які обійшли елементи керування безпекою, і швидко усунути загрози. Він також включає криміналістику для визначення та локалізації радіусу вибуху, щоб ви могли швидко та впевнено повернутися до завідомо справного стану.

Використання Trellix Endpoint Security ENS надає надійні можливості захисту від загроз. Вони підкреслюють ефективність модулів захисту від загроз, таких як Adaptive Threat Protection і Web Control, у захисті своїх серверів, настільних комп'ютерів і ноутбуків від різних кіберзагроз.

Висока здатность Trellix запобігати атакам від програм-вимагачів, блокувати шкідливі веб-сайти та надавати сповіщення високого рівня серйозності про потенційні загрози.

Trellix Endpoint Security ENS має високу оцінку щодо простоти керування з єдиної консолі та регулярні оновлення, що забезпечують безпеку окремих кінцевих точок. Крім того, Trellix Endpoint Security ENS діє проти внутрішніх і зовнішніх загроз у поєднанні з його здатністю запускати трасування електронної пошти та захищати від крадіжки даних і зловмисного програмного забезпечення що забезпечує високу репутацію надійного рішення для захисту від загроз кінцевих точок організації.

Безпека кінцевих точок є основою вашої розширеної платформи виявлення загроз і реагування на них, захищаючи останню милю активів. Вона надає більше інформації про дії користувачів, ніж будь-яка інша частина стеку безпеки організацій.

Trellix Endpoint Security ENS крім запропонованих модулів пропонує додаткові технології, які розширюють можливості платформи, а саме

- Звіт про відповідність;
- Мобільна безпека;

- Безпека робочого навантаження в хмарі для гібридної хмари;
- Видимість мережі та брандмауер на основі мікросегментації;
- Шифрування кінцевої точки;
- Запобігання втраті даних кінцевої точки;
- Мережева пісочниця.

Отже, Trellix Endpoint Security ENS надає багатошаровий захист кінцевих точок організації від сучасних атак.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було отримано наступні результати:

Проаналізовано роль і місце кінцевих точок організації, в результаті якого визначено, що вони відіграють велику роль для досягнення цілей організацій. Оскільки організації все частіше застосовують віддалені та гібридні моделі робочих місць користувачів, які підключаються до мереж із зовнішніх кінцевих пристроїв і роблять їх захист дедалі важливішим для запобігання кібератакам.

Визначено що обсяг і складність загроз кібербезпеці постійно зростають, що спонукає організації у більш досконалих рішеннях безпеки кінцевих точок. Сучасні системи захисту кінцевих точок розроблені для швидкого виявлення, аналізу, блокування та стримування поточних атак.

В роботі проведено порівняння технологій захисту кінцевих точок, в результаті якого для подальшого дослідження запропоновано використання Trellix Endpoint Security ENS, яке забезпечує високого рівня захист від сучасних атак.

Запропонована архітектура Tellix Endpoint Protection Platform надає різні види послуг захисту кінцевих точок організацій. Тому для захисту кінцевих точок запропоновано послугу на базі технології Trellix Endpoint Security ENS, яка надає автоматичний захист кінцевих точок та відповідає організаційним пріоритетним потребам у сфері безпеки, починаючи з запобігання та пошуку загроз і закінчуючи індивідуальним налаштуванням засобів захисту.

Досліджено технологію Trellix Endpoint Security ENS та запропоновано комплекс модулів, роботу яких надано у вигляді процесів що забезпечують захист, виявлення та виправлення щодо запобігання загроз, роботи брандмауера, контролю Інтернету та системи адаптивного захисту.

В результаті виконання роботи надано рекомендації щодо використання Trellix Endpoint Security ENS для захисту кінцевих точок організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. 1 What Is Endpoint Security? How It Works & Its Importance. URL: https://www.trellix.com/security-awareness/endpoint/what-is-endpoint-security/#definition. (дата звернення: 02.10.2024).

2. What is an Endpoint? Everything You Need to Know. https://www.mcpc.com/insights/blog/what-is-an-endpoint-everything-you-need-to-know/ . (дата звернення: 02.10.2024).

3. Kamruzzaman, A., Ismat, S., Brickley, J. C., Liu, A., & Thakur, K. . A Comprehensive Review of Endpoint Security: Threats and Defenses. 2022 International Conference on Cyber Warfare and Security (ICCWS). IEEE. doi: 10.1109/ICCWS56285.2022.9998470 (дата звернення: 12.10.2024).

4. Davies, V. (2023). The Top 10 risks of remote working. Bizclik Media Ltd. URL: https://cybermagazine.com/articles/the-top-10-risks-of-remote-working (дата звернення: 22.10.2024).

5. Захист кінцевих точок: як не загубитися у різноманітті продуктів. URL: Retrieved from https://trellix.bakotech.com/home/endpoint-protection-how-not-to-get-lost-in-the-variety-of-products (дата звернення: 29.10.2024).

6. 2024 Data Breach Investigations Report. (2024, June 11). URL: https://www.verizon.com/business/resources/reports/dbir (дата звернення: 02.11.2024).

7. The Data Security Risks Of Remote Working and How To Mitigate Them | Metomic. (2024, September 30). Retrieved from https://www.metomic.io/resource-centre/the-challenges-of-dlp-for-remote-working-and-how-to-manage-it (дата звернення: 12.11.2024).

8. Se Top 5 Endpoint Management Software with Pricing. (2024, October 11). Retrieved from https://research.aimultiple.com/endpoint-management-software ntinelOne Reviews, Ratings & Features 2024 | Gartner Peer Insights. URL: https://www.gartner.com/reviews/market/endpoint-protection-platforms/vendor/sentinelone/alternatives?marketSeoName=endpoint-protection-platforms&vendorSeoName=sentinelone (дата звернення: 25.11.2024).

9. Trellix Improves Query Speed While Reducing Costs to Deliver Better Endpoint Security. URL: https://www.snowflake.com/en/customers/all-customers/case-study/trellix. (дата звернення: 26.11.2024).

10. TrustRadius. (2024, October 16). URL: https://www.trustradius.com/products/trellix-endpoint-security/reviews?qs=product-usage (дата звернення: 26.11.2024).

11. Березовський К.В., Рудомьотова М.А. Технологія захисту кінцевих точок організації. Актуальні проблеми кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції (м. Київ, 25 жовтня 2024 року). Київ, 2024. С. 10-12 (дата звернення: 05.11.2024).