ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Засоби захисту кінцевих точок організації на прикладі рішення Trellix»

зі спеціальності *125 Кібербезпека*
(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

_____ Єлизавета СВІТЛИЧНА
(підпис)

Виконав: здобувач вищої освіти групи БСД-41
СВІТЛИЧНА Єлизавєта
(прізвище, ім'я)

Керівник ЧУМАК Надія
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент д.е.н., проф.ЛЕГОМІНОВА Світлана
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

BYOD – bring your own device

EDR – Endpoint Detection and Response

EPP – Endpoint Protection Platform

POLP – principle of least privilege

ETDR – Endpoint Threat Detection and Response

NGFW – Next-Generation Firewall

ZTNA – Zero Trust Network Acces

SSO – Single Sign-On

VPN – Virtual Private Network

ZT – Zero Trust

ZTA – Zero Trust Architecture

ВСТУП

Актуальність дослідження. Використання засобів захисту кінцевих точок у сучасних інформаційних системах, де кіберзагрози стають дедалі складнішими та різноманітнішими, набуває критичного значення. Кінцеві точки, до яких відносяться персональні комп'ютери, ноутбуки, смартфони та сервери, є найбільш вразливими ланками в інфраструктурі будь-якої організації. З огляду на постійне зростання кількості та витонченості кібератак, ігнорування належного захисту може призвести до серйозних фінансових втрат, репутаційних збитків та порушення безперервності бізнес-процесів.

Часті загрози та атаки, показують необхідність захисту кінцевих точок від різного типу атак. Так, програми-вимагачі (Ransomware) залишаються однією з найсерйозніших загроз. Зловмисники шифрують дані на кінцевій точці та вимагають викуп за їх відновлення. Сучасні варіанти програм-вимагачів стають все більш цілеспрямованими та використовують складні методи проникнення та розповсюдження.

Шкідливе програмне забезпечення (Malware), таке як віруси, трояни, черв'яки, шпигунське ПЗ та інші види шкідливого програмного забезпечення постійно еволюціонують. Вони можуть красти конфіденційну інформацію, пошкоджувати файли, надавати зловмисникам віддалений доступ до системи або використовувати обчислювальні ресурси кінцевої точки для здійснення інших атак.

Фішинг та соціальна інженерія також залишаються ефективним способом обману користувачів та отримання їх облікових даних або спонукання до завантаження шкідливого програмного забезпечення. Зловмисники використовують все більш витончені електронні листи, повідомлення та веб-сайти, щоб імітувати легітимні джерела.

Атаки нульового дня (Zero-day attacks) використовують невідомі вразливості в програмному забезпеченні, для яких ще не існує патчів. Захист від таких атак вимагає проактивних та поведінкових методів виявлення.

Сучасні засоби для захисту кінцевих точок відрізняються від традиційних антивірусних програм та розвинулись до комплексних платформ, що використовують передові технології для запобігання, виявлення та реагування на загрози.

До сучасних заходів захисту кінцевих точок включають:

Розширений захист кінцевих точок (Endpoint Detection and Response - EDR), який забезпечує безперервний моніторинг та збір даних з кінцевих точок, що дозволяє виявляти підозрілу активність, аналізувати її та швидко реагувати на інциденти безпеки. Вони часто використовують поведінковий аналіз, машинне навчання та аналітику загроз для виявлення складних атак, які можуть оминути традиційні антивірусні рішення.

Захист нового покоління (Next-Generation Antivirus - NGAV): NGAV використовує просунуті методи виявлення шкідливого програмного забезпечення, такі як машинне навчання, поведінковий аналіз, пісочниці та аналіз репутації файлів, щоб забезпечити більш ефективний захист від сучасних загроз.

Платформи управління безпекою кінцевих точок (Endpoint Security Management Platforms) забезпечують централізоване управління політиками безпеки, моніторинг стану захисту та реагування на інциденти на всіх кінцевих точках в організації.

Trellix пропонує передову сучасну безпеку кінцевих точок за допомогою EPP, EDR, криміналістичних засобів контролю та робочого процесу розслідування під керуванням штучного інтелекту, масштабного керування політикою під керуванням штучного інтелекту та робочих процесів усунення проблем під керуванням штучного інтелекту. Завдяки Trellix організації можуть запобігти зловмисникам атакувати їхні кінцеві точки, виявляти та реагувати на сучасні методи атак за допомогою штучного інтелекту, а також ефективно керувати інфраструктурою кінцевих точок у локальному масштабі та в хмарі.

Враховуючи постійне зростання кількості та складності кіберзагроз, використання сучасних засобів захисту кінцевих точок є не просто бажаним, а абсолютно необхідним заходом для забезпечення безпеки інформаційних активів

будь-якої організації. Інвестиції в ефективні рішення для захисту кінцевих точок допомагають мінімізувати ризики кібератак, запобігти фінансовим втратам та зберегти репутацію компанії.

Об'єкт дослідження – захист кінцевих точок організації.

Предмет дослідження – засоби захисту кінцевих точок організації на прикладі рішення Trellix.

Мета роботи розробити варіант застосування засобів захисту кінцевих точок організації на базі рішення Trellix та рекомендації щодо застосування цих засобів.

Наукові завдання:

дослідити сутність проблеми захисту кінцевих точок організації;

проаналізувати основні підходи захисту кінцевих точок організації;

проаналізувати існуючі рішення захисту кінцевих точок організації;

проаналізувати засоби захисту кінцевих точок організації на базі рішення Trelix;

запропонувати варіант організації захисту кінцевих точок організації на базі рішення Trelix;

розробити рекомендацій щодо застосування засобів захисту кінцевих точок організації.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування засобів захисту кінцевих точок організації, а також розроблено рекомендації фахівцям з кібербезпеки щодо їх реалізації.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ВІДДАЛЕНИХ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

1.1. Аналіз проблеми захисту кінцевих точок організації

Безпека кінцевої точки в організаціях відіграє одну з вирішальних ролей у захисті інформаційної системи від кіберзагроз. Такий захист передбачає впровадження стратегію захисту всіх пристроїв організації, як ноутбуки, смартфони та пристрої Інтернету речей, підключені до інформаційної системи організації.

Саме кінцеві точки є можливим шляхом для зв'язку з інформаційною системою організації, що робить їх привабливими цілями для зловмисників, які хочуть скористатися вразливими місцями. Однією з головних причин націлювання на кінцеві точки є їх легка доступність і часто незахищеність для проведення атаки, що може призвести до несанкціонованого доступу та витоку даних, які є конфіденційними [1].

Зловмисники регулярно намагаються захопити або зламати кінцеві пристрої. Для цього вони можуть мати на увазі будь-яку кількість цілей: зараження пристрою зловмисним програмним забезпеченням , відстеження активності користувача на пристрої, утримання пристрою для отримання викупу, використання пристрою як частини ботнету, використання пристрою як відправної точки для переміщення вбік і компрометації інших пристроїв у мережі тощо [1-2].

У бізнес-контексті зловмисники часто націлюються на кінцеві точки, оскільки скомпрометована кінцева точка може бути точкою входу в безпечну корпоративну мережу. Можливо, зловмисник не зможе пройти крізь корпоративний брандмауер, але ноутбук співробітника може стати легшою ціллю.

Кінцеві точки важко захистити в бізнес-налаштуваннях, оскільки IT-команди мають менше доступу до них, ніж до внутрішньої мережевої інфраструктури. Кінцеві пристрої також значно відрізняються за виробником, моделлю,

операційною системою, встановленими програмами та станом безпеки (готовність до атаки). Заходи безпеки, які успішно захищають смартфони від атак, можуть не працювати, наприклад, для серверів. І хоча один працівник компанії може регулярно оновлювати свій ноутбук і уникати ризикованої поведінки в Інтернеті, інший може уникати оновлення програмного забезпечення та завантажувати незахищені файли на свій ноутбук. Проте компанія має знайти спосіб захистити обидва ноутбуки від атак і запобігти скомпрометації мережі [3-4].

Опитування, в якому прийняло участь 345 фахівців з кібербезпеки, показало, що працює, а що ні для безпеки даних кінцевої точки. Наведені нижче діаграми на рис.1.1 ілюструють виклики та рішення для керівників організацій, бізнесу, технологій і безпеки щодо захисту кінцевих точок [5].

Рис.1.1. Відсоток виявлених загроз кібербезпеки з кінцевими точками

Зловмисники, підбадьорені просторами атак, створеними віддаленою роботою та розподіленими кінцевими точками, зробили останні роки - роком програм-вимагачів, захоплюючи активи та вимагаючи гроші за їх повернення. Понад третина респондентів в опитуванні назвали зловмисне програмне забезпечення та програми-вимагачі найбільшою загрозою безпеці для своєї роботи.

Меншими, але все ж суттєвими загрозами є ті, що є результатом помилок людини. Від надсилання електронної пошти не тій особі до втрачених або вкрадених паролів, люди неминуче роблять необережні помилки, а зловмисники готові накинутися. Майже чверть респондентів назвали помилки співробітників однією з головних проблем безпеки [5].

І хоча зовнішні загрози є найбільшим ризиком для кібербезпеки, небезпеки, що ховаються зсередини, також є проблематичними. П'яту частину респондентів хвилюють ризики, які становлять ненадійні чи зловмисні працівники, які мають особливу мету чи особисту вигоду.

Хоча організації стурбовані кіберзагрозами, вони також стурбовані своєю здатністю впоратися з ними. Близько 36% респондентів вказали на проблеми зі швидкістю реагування на інциденти, а 32% сумнівалися в їх здатності виявляти загрози (рис.1.2).

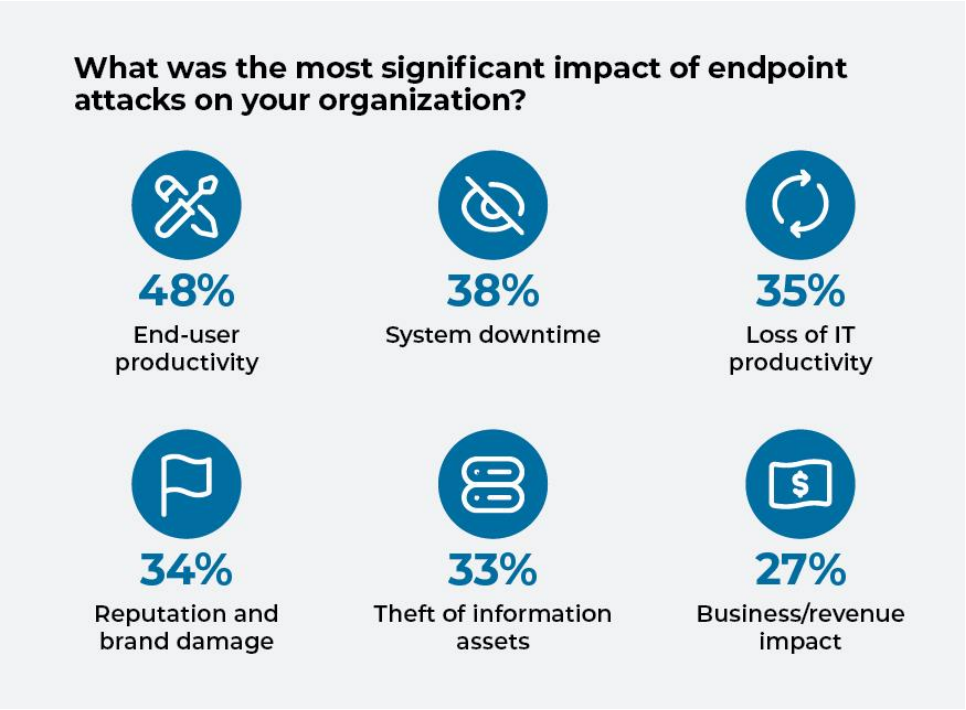


Рис.1.2. Ризики безпеки кінцевої точки

Понад чверть стверджують, що вони не бачать загального стану кібербезпеки. Це проблематично, оскільки три сфери складають основні будівельні блоки хорошого кіберзахисту: це не лише інструменти та процеси, це люди. Третина респондентів кажуть, що їм не вистачає внутрішніх навичок кібербезпеки,

а 38% кажуть, що найбільшою проблемою для них є патрулювання кібербезпеки 24 години на добу.

Атака на кінцеві точки може вплинути на продуктивність кінцевих користувачів і дозволити хакерам отримати вплив на свої цілі. Коли бізнес компанії зупиняється або порушується через кібератаку, власники бізнесу зазвичай обирають найшвидший шлях до відновлення роботи. Якщо це атака програми-вимагача, це часто означає оплату зловмисникам .

Слабка безпека кінцевої точки може надати зловмисникам доступ до конфіденційних організаційних даних, що призведе до фінансових втрат і погіршить їх репутацію. Крім того, зростаюча залежність від політики віддаленої роботи та використання власного пристрою (BYOD) ще більше посилила потребу в комплексних заходах захисту кінцевих точок для забезпечення захищеного мережевого середовища організацій.

Організаціям потрібно інвестувати в складні засоби захисту, які можуть виявляти потенційні загрози, реагувати на них і пом’якшувати їх у реальному часі, захищаючи таким чином свої цінні цифрові активи та ресурси.

Кінцеві точки мають критичне значення в інформаційній системі організації. Це точки дотику, через які дані надходять і виходять з мережі. Відповідно до їх призначення кінцеві точки служать кінцевими пунктами для обміну даними, діючи як інтерфейс між користувачами або процесами та більшою мережевою інфраструктурою організації.

Вони відповідають за:

Ініціювання сеансів спілкування

Обробка запитів на дані

Передача інформації на інші пристрої, що сприяє безперебійній взаємодії в мережі

Підтримка цілісності та ефективності потоку даних

Забезпечення того, щоб пакети інформації досягали призначених місць без втрат або перешкод

Оскільки інформаційні системи є складною інфраструктурою організації,

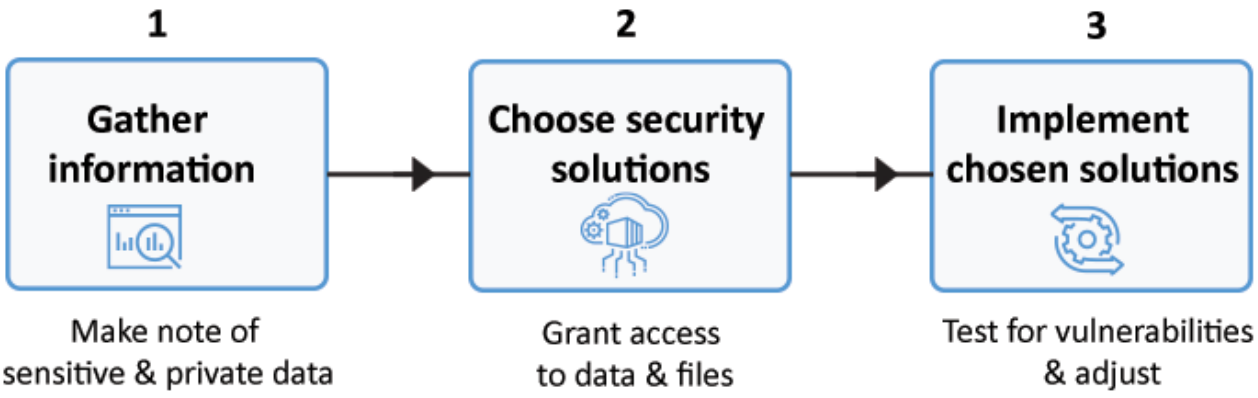
важливість кінцевих точок постійно зростає, що робить їх невід'ємною частиною успішної роботи у складній інфраструктурі інформаційної системи. Таким чином, ефективне управління кінцевими точками покращує підключення та передачу даних, а також підвищує загальну продуктивність і безпеку інформаційної системи організації.

Отже, для вирішення проблеми захисту кінцевих точок, необхідно проаналізувати основні підходи, які використовуються для впровадження відповідних заходів та засобів.

1.2. Аналіз підходів захисту кінцевих точок організації

Для розуміння підходів захисту кінцевих точок організації треба розуміти, як інструменти безпеки кінцевої точки взаємодіють з іншими елементами безпеки, які вже є. Розглянемо елементарний процес впровадження безпеки кінцевих точок, який повинні враховувати підприємства, незалежно від типу їхньої галузі [4].

Процес безпеки кінцевої точки інформаційної системи організації можна представити у вигляді процесу, який складається з трьох кроків, як це показано на рис.1.3.



1.3. Процес роботи захисту кінцевої точки [4]

Крок I : Збір інформації.

На першому етапі організація повинна зібрати всю необхідну інформацію. Щоб краще захистити свою інфраструктуру від потенційних атак, потрібно знати про всі точки доступу, до яких вони підключаються. Це також передбачає запис конфіденційних і приватних даних разом із управлінням ідентифікацією та доступом (IAM) . Ця дія допоможе зрозуміти, яку інформацію вам потрібно захистити та хто має доступ до якого типу даних.

Крок II : Вибір рішення безпеки.

Після огляду та збору відповідної інформації про різні кінцеві точки потрібно вибрати відповідне рішення безпеки для кожного рівня кінцевої точки. Це може включати хмарний захист, захист мережі та захист апаратного та програмного забезпечення.

Крок III : Впровадження рішень безпеки.

На останньому кроці можна запровадити вибране рішення безпеки та почати моніторинг кінцевих точок. Тут потрібно знати продуктивність обраного рішення та визначити, чи все ще існує вразливість в інфраструктурі організації. Якщо відповідь ствердна, потрібно почати весь процес спочатку. Для цього можна перевірити всі вразливості та за потреби налаштувати рішення безпеки.

Тепер ми перейдемо до ключових компонентів безпеки кінцевих точок і того, як вони взаємодіють, щоб забезпечити повну безпеку для мереж організації.

Можна виділити 5 ключових компонентів безпеки кінцевої точки (рис 1.4)

У зв’язку зі зростаючою популярністю культури «принеси свій власний пристрій» (BYOD) і збільшенням кількості використовуваних мобільних пристроїв IoT, як про це повідомлялось раніше, організаціям важливо розглянути, чи є рішення безпеки кінцевих точок достатньо комплексним, щоб протистояти загрозам на всіх фронтах. Таким чином, компанії повинні розуміти фундаментальні компоненти рішення безпеки кінцевої точки. Тому розберемо основні елементи рішення безпеки кінцевої точки.

Отже до компонентів безпеки кінцевої точки відноситься: захист пристрою, контроль мережі, контроль додатків, контроль даних, захист браузера (рис.1.4). Розглянемо кожний компонент.

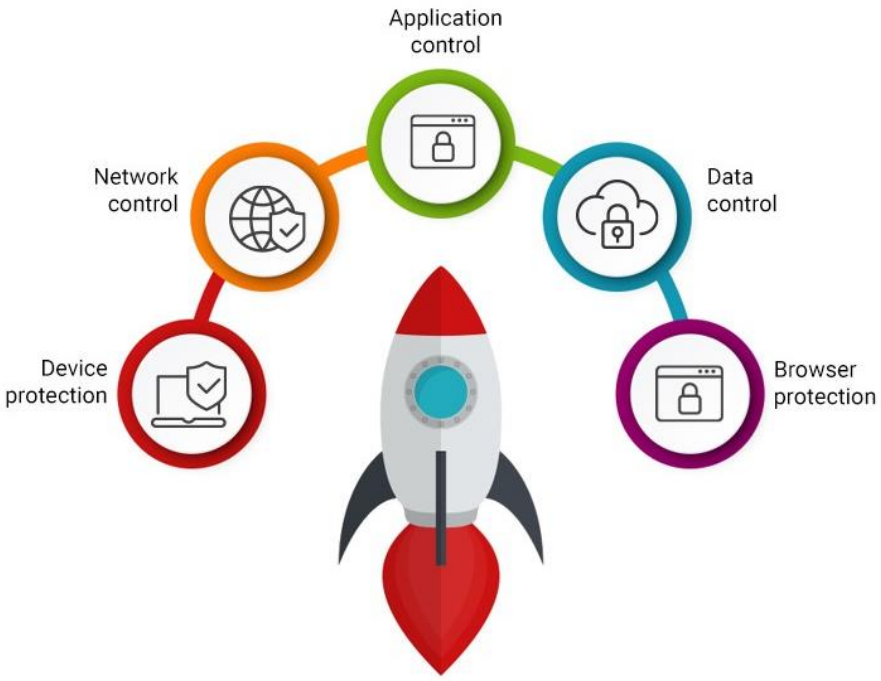


Рис.1.4. Компоненти захисту кінцевих точок [4]

1.Захист пристрою

Компонент захисту пристрою визначає та досліджує підозрілі дії на кінцевих пристроях. До них належать інструменти виявлення та реагування кінцевих точок (EDR - endpoint detection and response), які відстежують події кінцевих точок, від моніторингу та запису до аналізу подій. Це допомагає командам IT-безпеки завчасно ефективно виявляти потенційні загрози та боротися з ними.

Рішення безпеки кінцевих точок забезпечують захист від вірусів (нового покоління) і зловмисного програмного забезпечення для всіх типів пристроїв для видалення нових форм зловмисного програмного забезпечення. Оскільки антивіруси нового покоління використовують розширену аналітику та ML, боротьба з новими програмами-вимагачами та вдосконаленими фішинговими атаками, які обходять традиційне антивірусне програмне забезпечення, стає легшою.

2. Контроль мережі

Компонент керування мережею відстежує, контролює та фільтрує весь вхідний мережевий трафік. Він надає комплексну функцію, подібну до брандмауера, яка допомагає виявляти, ідентифікувати та впоратися з потенційними

ризиками безпеки, які можуть заразити мережу організації.

3. Контроль додатків

Компонент керування додатками означає тип контролю, який кінцеві точки мають над додатками, що використовуються в мережі. Це характеризується інтеграцією з серверами додатків, оскільки це допомагає визначати, контролювати та обмежувати доступ кінцевої точки до цих самих додатків.

Крім того, цей компонент також включає виправлення додатків, коли ризики безпеки, пов'язані з окремими програмними додатками, повністю усуваються. Таким чином, підприємства можуть користуватися покращеним захистом, оновлюючи всі кінцеві точки, включаючи настільні комп'ютери, сервери та програми.

4. Контроль даних

Компонент керування даними керує тим, як дані обробляються в мережі. Це стосується даних, що передаються, а також збережених даних. Інструмент контролю даних запобігає витоку даних і покращує загальну безпеку даних шляхом шифрування конфіденційних або цінних даних. Шифрування робить дані нечитабельними та віддаленими для зловмисників.

5. Захист браузера

Системи безпеки кінцевих точок забезпечують захист браузера або за допомогою веб-фільтрів. Ці фільтри дозволяють вибрати, до чого ваші користувачі можуть отримати доступ або які сайти вони можуть відвідувати, коли вони підключені до вашої мережі.

Цей компонент пропонує функції керування привілеями, також відомі як принцип найменших привілеїв (POLP – principle of least privilege). Це дозволяє підприємствам надавати користувачам і процесам мінімальний набір ресурсів, необхідних для виконання своїх завдань. POLP обмежує права доступу для авторизованих користувачів і програм, видаляючи права локального адміністратора на серверах і ПК. Це значно знижує ризики безпеки корпоративної мережі.

1.3. Аналіз існуючих рішень із кінцевих точок організації

Управління кінцевими точками стає все більш критичним аспектом сучасних IT-середовищ організацій. Поширення різноманітних пристроїв, зростання віддаленої роботи та постійна еволюція загроз безпеці вимагають надійних стратегій для управління та захисту всіх кінцевих точок в організації. В даному підрозділі буде проведено порівняльний аналіз провідних рішень для керування кінцевими точками.. Під час аналізу ці рішення оцінюватимуться на основі їхніх ключових характеристик і можливостей, сильних і слабких сторін (враховуючи продуктивність, масштабованість, зручність використання та підтримку операційної системи), моделей ціноутворення, цільових галузей і розмірів організацій, а також можливостей інтеграції.

Тож розглянемо рішення різних вендорів для вибору кращого рішення за квадрантом гартнера по розподілу гравців на ринку захисту кінцевих точок (рис.1.5), до яких відносяться рішення NinjaOne, Microsoft Intune, Cisco Meraki, і Trellix.

NinjaOne представляє себе як уніфіковану платформу, призначену для централізованого керування всіма робочими процесами, що охоплюють пристрої кінцевих користувачів, сервери, віртуальні машини та мережеві пристрої через єдиний зручний інтерфейс [5]. Основним принципом підходу NinjaOne є автоматизація IT-операцій. Платформа розроблена для автоматизації трудомістких завдань керування кінцевими точками, починаючи від виправлення операційних систем і понад 200 програм до керування конфігураціями, що дозволяє IT-командам ефективно масштабувати свої операції [5]. NinjaOne акцентує увагу на управлінні в реальному часі, пропонуючи такі функції, як моніторинг у реальному часі, сповіщення та можливість негайно вживати заходів для швидкого вирішення проблем1. Ця можливість сприяє швидшому вирішенню проблем і мінімізує вплив на кінцевих користувачів. Платформа підтримує широкий спектр операційних систем, включаючи Windows, macOS і Linux [5].

NinjaOne також пропонує надійні можливості інтеграції з іншими основними

IT-інструментами та платформами, такими як Slack, CrowdStrike та Okta, що сприяє створенню пов’язаного та оптимізованого IT-середовища [5]. Створений на базі хмарної архітектури, NinjaOne забезпечує властиву масштабованість для адаптації до мінливих потреб організаційNinjaOne також пропонує надійні можливості інтеграції з іншими основними IT-інструментами та платформами, такими як Slack, CrowdStrike та Okta, що сприяє створенню пов’язаного та оптимізованого IT-середовища [5]. Створений на базі хмарної архітектури, NinjaOne забезпечує властиву масштабованість для адаптації до мінливих потреб організацій.

Рис.1.5. Гравці захисту кінцевих точок на ринку

Microsoft Intune — це хмарна платформа уніфікованого керування кінцевими точками (UEM), яка дозволяє організаціям керувати та захищати свої кінцеві точки з єдиної консолі [6]. Значною перевагою Intune є його глибока та бездоганна інтеграція з ширшою екосистемою Microsoft, зокрема Microsoft 365 і продуктами безпеки Microsoft [6] Ця інтеграція спрощує керування та підвищує безпеку для організацій, які вже інвестували в технології Microsoft. Intune пропонує широку

підтримку операційної системи, керуючи та захищаючи кінцеві точки, підключені до хмари, у Windows, Android, macOS, iOS і Linux [6]. Платформа зосереджена на трьох основних перевагах: спрощенні керування кінцевими точками шляхом уніфікації рішень і робочих процесів, зміцненні безпеки за допомогою сигналів Microsoft Security і розширених можливостей, а також зниженні загальних витрат за рахунок консолідації постачальників і оптимізації ліцензування [6]. Intune надає низку важливих функцій для сучасного керування кінцевими точками, включаючи політики відповідності пристроїв, політики конфігурації та комплексне керування оновленнями Windows [7]. Microsoft Intune Suite додатково розширює свої можливості за допомогою розширених функцій, таких як Remote Help для безпечних з'єднань підтримки та Endpoint Privilege Management, щоб дозволити стандартним користувачам виконувати адміністративні завдання, схвалені IT. Основний дизайн Microsoft Intune як хмарної платформи UEM, інтегрованої в екосистему Microsoft, позиціонує її як сильного конкурента для організацій, які мають значною мірою перейняв продукти Microsoft. Широка підтримка операційної системи робить його універсальним рішенням для керування різноманітними ландшафтами пристроїв. Включення розширених функцій у Intune Suite вказує на те, що платформа здатна задовольняти складні вимоги до керування кінцевими точками.

Cisco Meraki пропонує першочергове хмарне рішення для керування мобільними пристроями (MDM), розроблене для безперебійного та безпечного віддаленого керування кінцевими точками [8]. Ключовою особливістю Meraki є його тісна інтеграція з іншими продуктами безпеки Meraki та Cisco, що створює міцну основу для моделі безпеки [8] із нульовою довірою. Платформа надає низку функцій, спрямованих на спрощення керування кінцевими точками, включаючи ефективне віддалене керування пристроями. розгортання додатків і надійне застосування політики безпеки [8]. Meraki підтримує різноманітні операційні системи, включаючи iOS, macOS, Windows, Android і ChromeOS, обслуговуючи різноманітні середовища пристроїв [8]. Примітно, що Meraki Systems Manager вбудовано інтегровано з хмарними мережевими пристроями Meraki, пропонуючи

покращену видимість і контроль для організацій, які використовують мережеву інфраструктуру Meraki [8]. Основні цілі платформи включають спрощення процесів керування кінцевими точками та автоматизація безпеки мережі для зменшення витрат на адміністрування. Архітектура, орієнтована на хмару, і глибока інтеграція з екосистемою мереж і безпеки Cisco роблять Meraki привабливим варіантом для організацій, які стандартизували продукти Cisco. Зосередження на простоті керування кінцевими точками пропонує платформу, яку легко розгортати та керувати, що потенційно зменшує потребу в спеціалізованому досвіді. Підтримка поширених операційних систем забезпечує широке охоплення пристроїв у керованому середовищі.

Trellix зосереджується в основному на управлінні безпекою кінцевих точок, надаючи рішення для автентифікації та контролю за доступом кінцевих пристроїв до мережі та застосування політик безпеки для запобігання загрозам [9]. Платформа пропонує багаторівневий захист кінцевих точок, який поширюється на локальні, хмарні та навіть відключені середовища, усіма керовані через єдиного уніфікованого агента [10]. Набір функцій Trellix включає централізоване керування безпекою через ePolicy. Консоль Orchestrator (ePO), яка дозволяє оптимізувати розгортання, конфігурацію політики, моніторинг подій і управління відповідністю [10]. Платформа також надає можливості проактивного керування поверхнею атак, включаючи керування пристроями, керування додатками та функції хост-брандмауера [10]. Trellix використовує багатий і повнофункціональний стек запобігання загрозам, який використовує передове машинне навчання, методи запобігання використанню та евристики для ефективної роботи. виявляти та блокувати загрози на різних етапах. Унікальним аспектом Trellix є його функція Trellix Insights, яка пропонує проактивну інформацію про загрози, прогнозуючи потенційні загрози на основі галузевих тенденцій і географічного розташування, а також оцінюючи стан безпеки організації та надаючи рекомендації щодо покращення [11]. Основна перевага Trellix полягає в її комплексному та інтегрованому підході до безпеки кінцевих точок, використовуючи передові технології, такі як ШІ та машинне навчання, для проактивного керування загрозами

та надійного захисту. Централізована консоль керування спрощує моніторинг за складною системою безпеки.

Складемо за описом основних рішень захисту кінцевих точок оргнізації порівняльну таблицю 1.1 для обрання відповідного рішення.

Таблиця 1.1.

Порівняння рішень захисту кінцевих точок

Категорія функції	**NinjaOne**	**Microsoft Intune**	**Cisco Meraki**	**Трелікс**
Управління кінцевими точками	Реєстрація пристрою, інвентаризація, Windows, macOS, Linux, SNMP, хмарні кінцеві точки	Реєстрація пристрою, інвентаризація, Windows, Android, macOS, iOS, Linux, IoT	Реєстрація пристрою, інвентаризація, iOS, macOS, Windows, Android, ChromeOS, tvOS	Керування пристроями, інвентаризація, Windows, macOS, Linux (через агента)
Керування виправленнями	ОС (Windows, macOS, Linux), програми сторонніх розробників (200+)	ОС (Windows), стороння обмежена через інтеграцію	ОС, програми	Виправлення ОС через інтеграцію з інструментами керування оновленнями
Розгортання програмного забезпечення	Автоматизовані комплексні пакети на основі сценаріїв	Керування програмами, Intune Suite	Загальнодоступні та приватні програми, інсталятори програмного забезпечення, оновлення ОС	Розгортання програмного забезпечення та оновлення керуються централізовано
Віддалений доступ і контроль	Інтегрований (TeamViewer, Splashtop, RDP, Connectwise Control), доступ в один клік	Віддалена допомога (Intune Suite)	Віддалений робочий стіл, командний рядок	Можливості дистанційного розслідування в EDR

Управління мобільними пристроями	В комплекті	Комплексні можливості MDM	Основні функції MDM	Безпека мобільних пристроїв керується як частина загальної стратегії безпеки кінцевої точки
Управління мобільними додатками	В комплекті	Можливості MAM	Базове керування програмами	Функції контролю програми
Функції безпеки	Основні функції безпеки, інтеграція з інструментами безпеки	Відповідність пристроїв, умовний доступ, інтеграція з Microsoft Security	Політики безпеки, обмеження пристроїв, інтеграція з Cisco Security	Багаторівневий захист, антивірус, брандмауер, запобігання загрозам, EDR, керування поверхнею атак, запобігання втраті даних (через окремі модулі)
Звітність і аналітика	Гнучка звітність про пристрій	Аналітика кінцевих точок (Intune Suite), звітність про відповідність	Експорт даних інвентаризації, базова звітність	Детальні звіти, сповіщення, експертиза загроз, настроювані перегляди
Автоматизація та сценарії	Автоматизація завдань кінцевої точки, розгортання	Автоматизація через Intune і Microsoft Power Automate	Розгортання сценарію	Автоматизація робочих процесів безпеки та

	сценаріїв (PowerShell, Batch тощо)			відповідності через ePO

Для подальшого дослідження оберемо рішення Trelix.

Обгрунтування вибору рішення полігає у наступному. Trellix пропонує багаторівневий захист кінцевих точок у різних середовищах за допомогою єдиного агента, яким керує централізована консоль [10]. Він забезпечує проактивне керування поверхнею атак і багатий стек запобігання загрозам, використовуючи передові технології, такі як машинне навчання [10]. Trellix Insights пропонує унікальну проактивну інформацію про загрози та керівництво [10]. Платформа включає автоматичний відкат для швидкого відновлення після загроз [10]. Аналітичні фірми визнають Trellix лідером галузі [10].

Trellix: в першу чергу орієнтовано на організації, які використовують операційні системи Windows, особливо на ті, що мають суворі вимоги до безпеки та, можливо, на ті, що працюють у суворо регульованих галузях.

Організації, які використовують Trellix, можуть швидше реагувати та ефективніше пом’якшувати загрози безпеці завдяки розширеним можливостям виявлення та реагування [9]. Платформа сприяє швидкому розгортанню найновіших функцій і технологій безпеки, гарантуючи, що кінцеві точки завжди захищені від нових загроз [9]. Trellix може покращити зв’язок безпеки в усій організації, забезпечуючи централізоване уявлення про систему безпеки [9].

2 ЗАСОБИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ

2.1. Архітектура Trellix Endpoint Security

Trellix Endpoint Security забезпечує багаторівневий захист кінцевих точок. Дане рішення охоплює локальне, хмарне та відключене середовище в одному агенті та керується з єдиного джерела, забезпечуючи безперебійну роботу всіх компонентів безпеки для забезпечення надійного захисту в усіх векторах.

Trellix відповідно звіту [12] отримав 100% рівень виявлення та нуль помилкових спрацьовувань (FP) в останньому тесті SE Labs Endpoint Security for Enterprise. Цей результат продемонстрував гарну прихильність до ефективності засобів безпеки та операційної ефективності безпеки рішення, і при цьому більше 40 000 компаній у всьому світі довіряють свої ресурси саме Trellix Endpoint Security.

Особливості рішення Trellix Endpoint Security полягає у наступних заходах та функціональних можливостях: централізованому управлінні безпекою, керування поверхнею атаки, стек запобігання загрозам, захист клієнтів і серверів

Централізоване управління безпекою. ePolicy Orchestrator пропонує єдину консоль для керування розгортанням, установкою, встановлення політик безпеки, моніторингу та реагування на події, а також забезпечення відповідності. ePO має сертифікат FedRAMP.

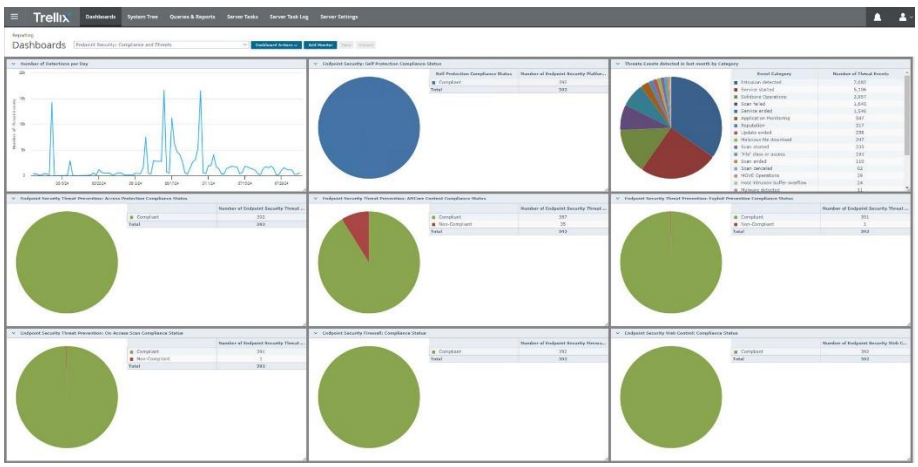


Рис.2.1. Централізоване управління безпекою

Керування поверхнею проактивної атаки. Зміцнює кінцеві точки за допомогою контролю пристроїв, контролю додатків, дозволених/заборонених списків і можливостей брандмауера хоста, щоб зменшити кількість атак.

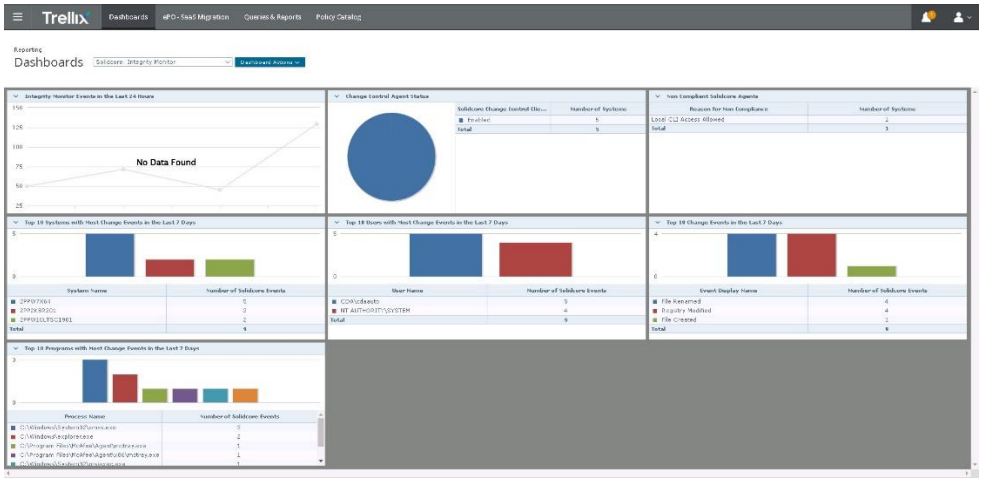


Рис.2.2. Керування поверхнею проактивної атаки

Повнофункціональний стек запобігання загрозам. Дозволяє зупиняйте загрози в будь-якій точці за допомогою багаторівневого захисту від загроз, який використовує вдосконалене машинне навчання, запобігання експлойтам і евристику, щоб захистити вас.

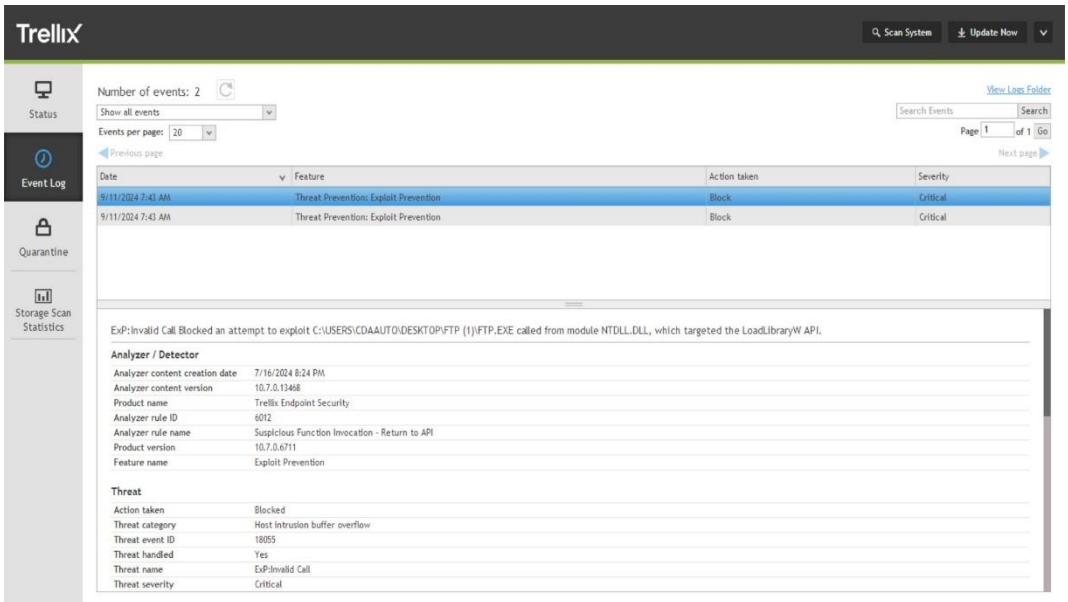


Рис. 2.3. Повнофункціональний стек запобігання загрозам

Захист клієнтів і серверів. Захищає мережеві пристрої зберігання даних (NAS) від загроз. Дозволяє постійно відстежувати пристрої NAS, такі як пристрої зберігання даних NetApp filers ICAP, щоб запобігти небажаним змінам і крадіжці даних.

Erellix Endpoint Security (HX) захищає від сучасних кібератак за допомогою моделі поглибленого захисту. Модульна архітектура Endpoint Security (HX) поєднує механізми за замовчуванням і завантажувані модулі для захисту, виявлення та реагування, а також керування безпекою кінцевих точок (рис. 2.4).

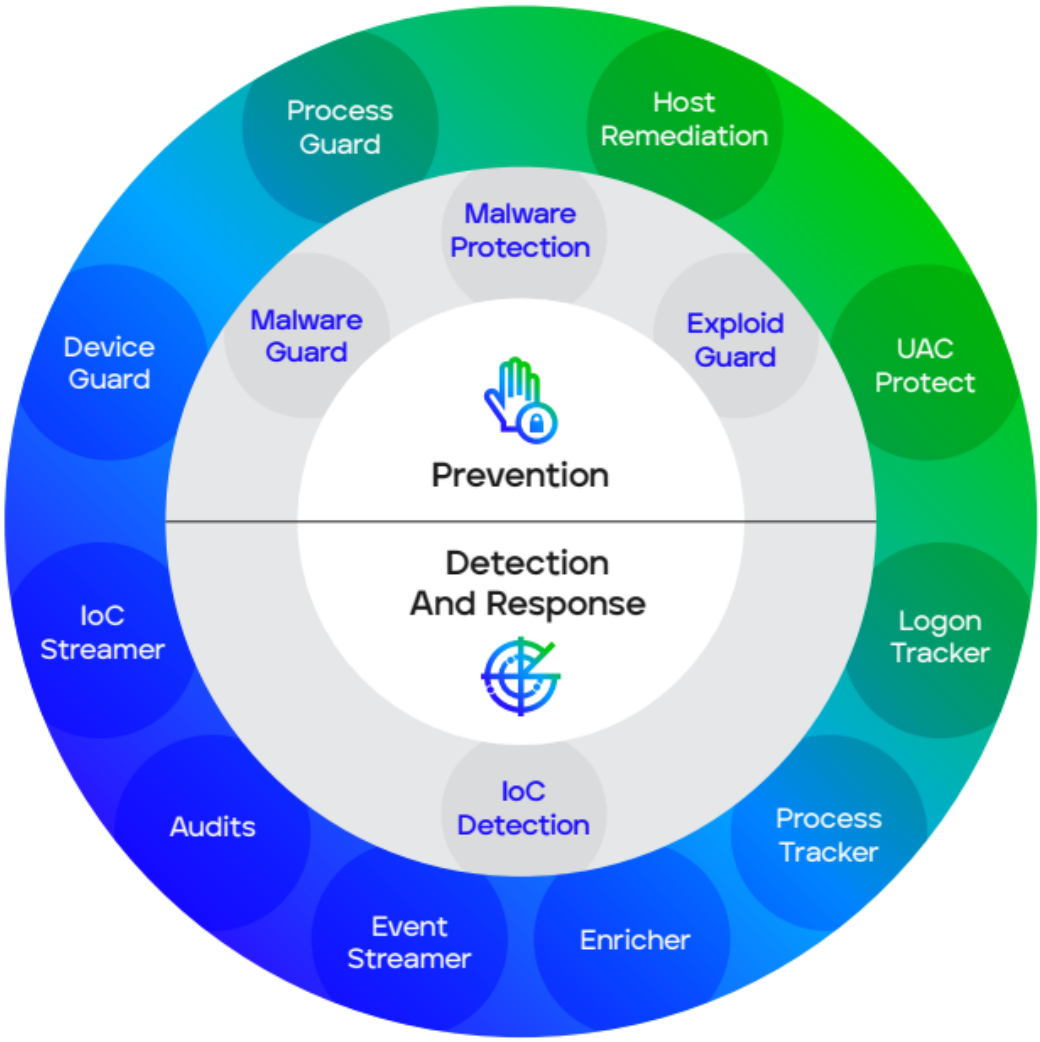


Рис.2.4. Архітектура Trellix Endpoint Security

Щоб запобігти поширеному шкідливому програмному забезпеченню, Endpoint Security (HX) використовує механізм Endpoint Protection Platform (EPP) на основі сигнатур. Щоб знайти загрози, для яких ще не існує сигнатури, MalwareGuard використовує машинне навчання, наповнене знаннями з попередніх

кібератак. Для атак на експлойти у звичайному програмному забезпеченні та браузерах ExploitGuard використовує механізм аналізу поведінки, який визначає, чи використовується експлойт, і зупиняє його виконання. Крім того, Trellix постійно розробляє модулі для виявлення методів атак і прискорення реагування на нові загрози. Наприклад, Process Guard було розроблено, щоб зупинити викрадання облікових даних.

Навіть з найкращим захистом порушення неминучі. Щоб забезпечити суттєве реагування, яке мінімізує збої в бізнесі, Endpoint Security (HX) включає функції виявлення кінцевих точок і реагування, які спираються на індикатори компрометації (IOC) у реальному часі, розроблені за допомогою оперативних служб реагування. Інструменти Trellix також виконують наступні функції:

Шукає та досліджєе відомі та невідомі загрози на десятках тисяч кінцевих точок за лічені хвилини.

Визначає та деталізує вектори атаки, використані для проникнення в кінцеву точку.

Визначає, чи відбулася (і продовжується) атака на конкретну кінцеву точку та куди вона поширилася.

Встановлює графік і тривалість компромісів кінцевих точок і стежить за інцидентом.

Сучасні загрози не зупиняються на одній кінцевій точці, тому виправлення на одній кінцевій точці не вирішить більшість порушень. Повне відновлення ефективно передає дані та вказує на всі пристрої, де може приховуватися загроза, і корелює цю інформацію в режимі реального часу. Endpoint Security (HX) безпосередньо інтегрується з Trellix XDR, який плавно поєднує всі технології та служби Trellix для виявлення та реагування на всі найскладніші загрози.

Системні вимоги до встановлення рішення показані у таблиці 2.1.

Таблиця 2.1.

Системні вимоги до встановлення рішення

Підтримувані операційні системи та середовища	
Windows	Windows 7, 8, 8.1, 10, 11 Server 2008R2, 2012R2, 2016, 2019
Mac	10.9 - 10.15, 11, 12, 13
Linux	RHEL 6.8 - 6.10, 7.2 - 7.9, 8.0 - 8.3 CentOS 6.8 - 6.10, 7.2 - 7.7, 8.0 SUSE 11 SP3, SP4, 12 SP2 - SP5, 15 GA Open SUSE Leap 15.1, 15.2 Ubuntu 14.04, 16.04, 18.04, 19.04, 20.04 LTS Amazon Linux AMI 2018.3, AM2, Amazon Linux 2 Oracle Linux 6.10, 7.6, 8.1, 8.2

Варіанти розгортання: фізичний пристрій, віртуальний пристрій, пристрій, розміщений у хмарі.

2.2. Функції Tellix Endpoint Protection Platform

Для забезпечення безпека кінцевих точок Trellix Endpoint Security використовується Tellix Endpoint Protection Platform, яка використовує фреймворк кібербезпеки, в основу якого покладено п’ять компонент (рис 2.5):

Запобігання (Prevent);

Виявлення (Detect);

Дослідження (Investigate);

Відповідь (Respond);

Керування поверхнею атаки (Manage attacker surface).

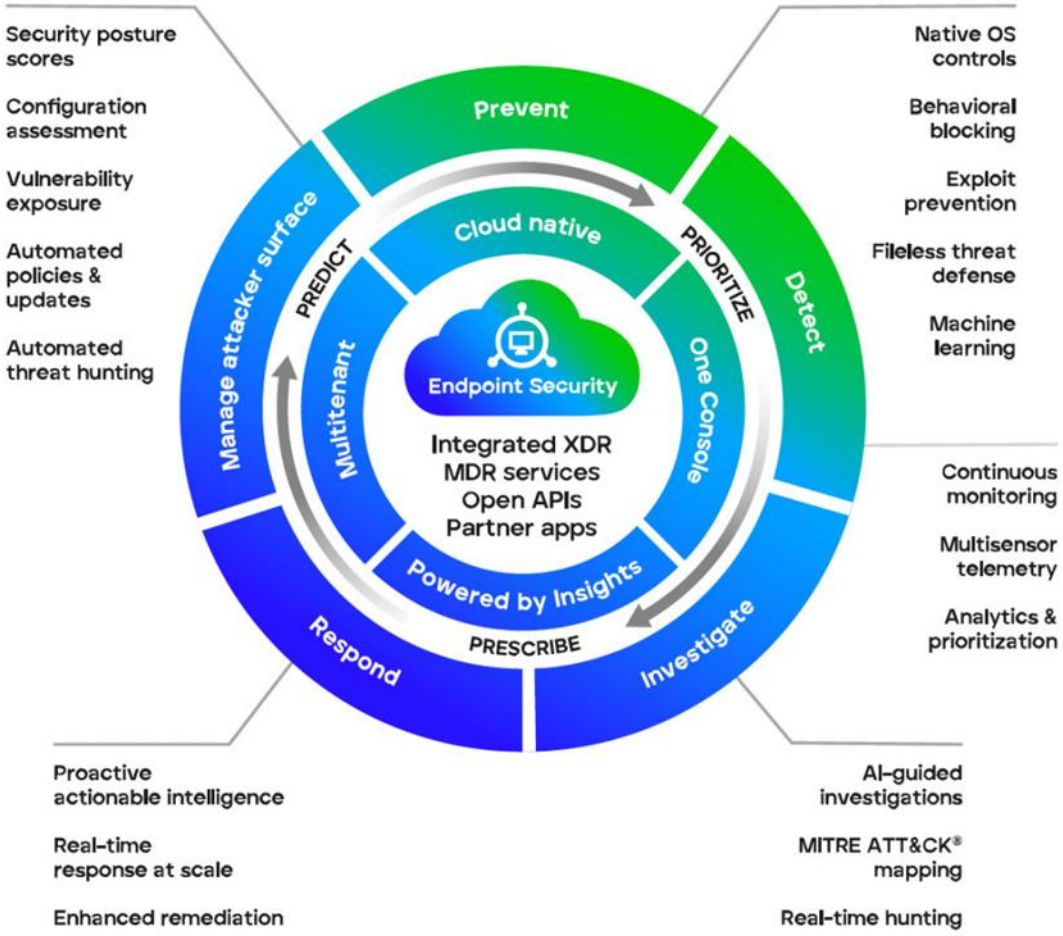


Рис. 2.5. Фреймворк Tellix Endpoint Protection Platform

Trellix Endpoint Protection Platform є ефективною платформою яку використовують фахівці з безпеки для протидії зловмисникам. Це інтелектуальні засоби захисту, що забезпечують спільну роботу, і структура, яка спрощує роботу в складних середовищах. Використання високої продуктивності та ефективності виявлення загроз, яка підтверджено тестами різних розробників, організації можуть використовувати засоби захисту своїх користувачів, підвищувати продуктивність і забезпечувати безпеку своїм системам.

Endpoint Security – це практика захисту кінцевих точок або точок входу пристроїв кінцевих користувачів, Сюди можна віднести настільні комп'ютери, ноутбуки та мобільні пристрої, які захищено від втручань зловмисників та проведення ними різних атак.

До складу Endpoint Security входить три модуля безпеки, які працюють незалежно один від одного та забезпечують кілька 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 та призначення кожної функції представлено у таблиці 2.1.

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 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ КІНЦЕВИХ ТОЧОК ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

3.1 Trellix Endpoint Security ENS для захисту кінцевих точок організації

Trellix ENS для захисту кінцевих точок виявляє загрози, проводить постійний моніторинг за загальною працездатністю системи та складає звіти щодо виявлення та стану захищеності кінцевих точок. Для виконання вказаних завдань клієнтське програмне забезпечення встановлюється у кожну систему.

Як правило, користувач може встановити один або декілька модулів Trellix ENS у клієнтські системи, що дозволяє керувати виявлення загроз та налаштовує параметри, що визначають принцип роботи функцій Trellix ENS.

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. Надалі Trellix ePO – On-prem розгортає ПЗ у клієнтських системах.

Клієнтське програмне забезпечення обмінюється даними з Trellix ePO - On-prem за допомогою Trellix Agent. Це дозволяє отримувати оновлення, 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 кінцевій точці.

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.

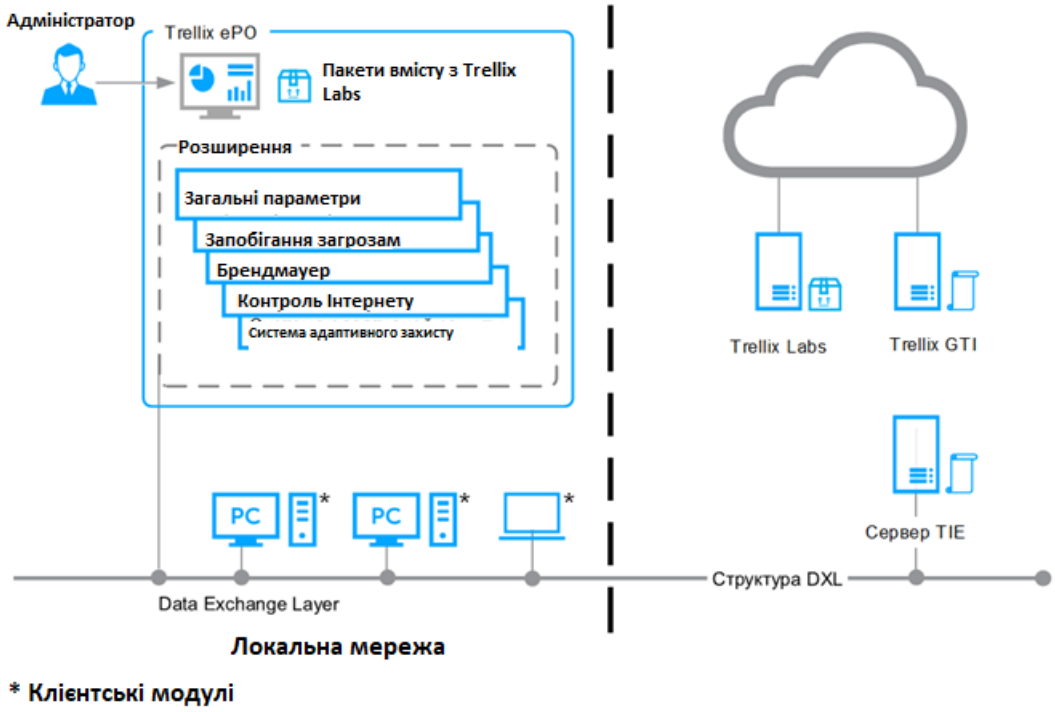


Рис. 3.1. Принцип захисту кінцевих точок Trellix ENS

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 доступних 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 Trellix ENS здійснює захист кінцевих точок та складається з декількох модулів, які дозволяють виявляти і захищати кінцеві точки організації від загроз на основі встановленого Trellix Agent на кінцевих точках.

3.2 Рекомендації налаштування Trellix Agent для кінцевої точки

Забезпечення безпеки кінцевих точок, таких як настільні комп'ютери, ноутбуки та мобільні пристрої, від зловмисних дій та кампаній є критично важливим аспектом сучасної кібербезпеки. Практика захисту кінцевих точок еволюціонувала від традиційного антивірусного програмного забезпечення до комплексних систем, здатних протистояти складним загрозам та експлойтам нульового дня. Організації будь-якого розміру стикаються з ризиками з боку різних зловмисників, включаючи державні структури, хактивістів, організовану злочинність, а також внутрішні загрози, як навмисні, так і випадкові. У зв'язку з цим, захист кінцевих точок часто розглядається як передова лінія кібербезпеки, і організації в першу чергу звертають увагу на забезпечення безпеки своїх корпоративних мереж саме на цьому рівні. З постійним зростанням обсягу та складності кіберзагроз зростає і потреба в більш просунутих рішеннях для захисту кінцевих точок. Trellix Endpoint Security є сучасним програмним забезпеченням для захисту кінцевих точок (антивірусом), яке може виявляти та запобігати зловмисним цифровим загрозам, що проникають на пристрої, перш ніж вони поширяться на найбільш важливі дані. Це рішення об'єднує можливості

запобігання, виявлення та реагування в єдиному агенті, що використовує машинне навчання та автоматизацію. Endpoint security є основою платформи безпеки, забезпечуючи захист активів на кінцевому рівні та надаючи глибше розуміння активності користувачів, ніж будь-яка інша частина стеку безпеки. Trellix Endpoint Security надає багаторівневий захист кінцевих точок, що охоплює локальні, хмарні та ізольовані середовища, використовуючи єдиний агент, керований з єдиного джерела.

Trellix Endpoint Security Agent є клієнтським програмним забезпеченням, яке встановлюється на кожну систему для виконання таких завдань, як перехоплення загроз, моніторинг загального стану системи та повідомлення про виявлення та стан. Зазвичай на клієнтські системи встановлюються один або кілька модулів Trellix ENS, які потім централізовано керуються з використанням Trellix ePolicy Orchestrator (ePO). Trellix Agent є ключовим компонентом, що забезпечує зв'язок між клієнтським програмним забезпеченням та Trellix ePO для конфігурації та застосування політик, оновлень продуктів та звітності. Trellix Endpoint Security поєднує запобігання, виявлення та реагування в одному агенті, використовуючи машинне навчання та автоматизацію для захисту кінцевих точок від вразливостей та потенційних експлойтів безпеки. Trellix ENS збирає інформацію про загрози з багатьох рівнів взаємодії, використовуючи єдиний програмний агент. усуває надмірність, спричинену використанням кількох точкових продуктів 6.

Використання Trellix Endpoint Security Agent надає низку важливих переваг для забезпечення безпеки організації. Однією з ключових переваг є захист важливих даних, таких як особисті дані, медичні записи та фінансова інформація, а також запобігання втраті або зміні дослідницьких даних та інших критичних відомостей. Агент також допомагає захистити критичні системи від кіберзагроз та пов'язаних з ними збоїв, забезпечуючи безперервність бізнес-процесів. Сучасні рішення для захисту кінцевих точок, включаючи Trellix ENS, розроблені для швидкого виявлення, аналізу, блокування та стримування атак до того, як вони зможуть завдати шкоди. Це досягається завдяки роботи різних модулів агента між собою та з іншими технологіями безпеки, що забезпечує адміністраторам

видимість складних загроз та прискорює час виявлення та реагування. Trellix ENS пропонує автоматичне відновлення системи до попереднього справного стану, забезпечуючи продуктивність користувачів та адміністраторів. Агент також забезпечує проактивний захист від програм-вимагачів, запобігаючи знищенню даних організації завдяки унікальній функції відкату. Крім того, Trellix ENS надає аналітикам можливості для прискорення розслідувань за допомогою штучного інтелекту та забезпечує економію часу завдяки низькому рівню хибних спрацьовувань та високоякісним сповіщенням, використовуючи багаторівневий стек захисту. Централізоване управління через єдину консоль у гетерогенних середовищах також сприяє зниженню операційних витрат.

Trellix Endpoint Security Agent забезпечує централізоване управління безпекою через платформу ePolicy Orchestrator (ePO). ePO надає єдину консоль для керування розгортанням, встановленням, налаштуванням політик безпеки, моніторингом подій та забезпеченням відповідності нормативним вимогам 4. ePO також дозволяє автоматизувати щоденні завдання, спрощуючи адміністрування безпеки. Платформа ePO є масштабованою та може керувати сотнями тисяч кінцевих точок, забезпечуючи повну прозорість, економічну ефективність та оптимізовану роботу IT-інфраструктури.

Керування поверхнею атаки є ще однією важливою функцією агента. Trellix ENS допомагає зменшити потенційні точки входу для загроз за допомогою контролю пристроїв, контролю застосунків, списків дозволу/заборони та можливостей брандмауера хоста. Ці функції дозволяють організаціям обмежувати використання потенційно ризикованих периферійних пристроїв, забезпечувати запуск лише довіреного програмного забезпечення та контролювати мережеві з'єднання, мінімізуючи таким чином кількість вразливостей, які можуть бути використані зловмисниками.

Агент Trellix ENS включає багаторівневий стек запобігання загрозам, який використовує передові технології, такі як машинне навчання, запобігання експлойтам та евристичний аналіз, для захисту кінцевих точок на кожному етапі потенційної атаки. Машинне навчання дозволяє виявляти загрози нульового дня,

запобігання експлойтам блокує атаки, що використовують вразливості програмного забезпечення, а евристика виявляє підозрілу поведінку. Модульна архітектура дозволяє інтегрувати конкретні можливості запобігання, такі як брандмауер та веб-контроль, забезпечуючи надійний захист від широкого спектру загроз .

Trellix Endpoint Security Agent забезпечує захист як клієнтських, так і серверних операційних систем, включаючи захист пристроїв мережевого зберігання даних від загроз шляхом постійного моніторингу та запобігання небажаним змінам та крадіжці даних. Це забезпечує всебічний захист IT-інфраструктури організації за допомогою єдиного рішення, спрощуючи управління та підвищуючи загальний рівень безпеки .

Хоча Trellix пропонує окремий продукт EDR, агент Endpoint Security також включає функціональність виявлення та реагування на кінцевих точках (EDR). Це включає постійний моніторинг даних кінцевих точок, можливості автоматизованого аналізу та функції для виявлення, розслідування та реагування на загрози.

Trellix Endpoint Security Agent також пропонує контроль застосунків та змін. Це дозволяє організаціям визначати та застосовувати політики, які обмежують запуск застосунків лише попередньо затвердженим списком. Це значно знижує ризик зараження шкідливим програмним забезпеченням та інших інцидентів безпеки, спричинених неавторизованим програмним забезпеченням. Контроль змін гарантує, що до системи вносяться лише авторизовані модифікації, що ще більше підвищує безпеку та цілісність кінцевих точок.

Trellix Agent — це клієнтський компонент, який забезпечує безпечний зв’язок між Trellix ePolicy Orchestrator — On-prem (Trellix ePO — On-prem) і керованими продуктами.

Агент також виконує функцію оновлення для продуктів Trellix.

Системами можна керувати за допомогою сервера Trellix ePO - On-prem, лише якщо на них встановлено агента. Під час роботи у фоновому режимі агент:

1. Встановлює продукти та їх оновлення в керованих системах.

2. Оновлює вміст безпеки, наприклад файли V3 DAT або пакет вмісту AMCore, пов’язаний із Trellix® Endpoint Security (ENS).

3. Застосовує політики та планує завдання в керованих системах.

4. Збирає інформацію та події з керованих систем і надсилає їх до Trellix ePO - On-prem.

Trellix Agent агент використовується в таких контекстах у Trellix ePO – On-prem:

Агент — основний робочий режим для Trellix Agent, що забезпечує канал зв’язку з Trellix ePO — локальні та локальні служби для керованих продуктів.

SuperAgent — агент, який діє як посередник між Trellix ePO - On-prem та іншими агентами в тому самому широкомовному сегменті мережі. SuperAgent кешує інформацію, отриману від Trellix ePO - On-prem, головного репозиторію або дзеркального розподіленого репозиторію, і розповсюджує її агентам у своїй мережевій підмережі.

Архітектура Trellix Agent є однопотоковою та асинхронною на основі архітектури служб (обміну повідомленнями). В обміні повідомленнями базується структура, послуги комунікації з використанням загальної мови. Це зменшує використання системних ресурсів, так само як число потоків, число дескрипторів, пам'яті і ЦП.

Розглянемо порядок встановлення агента на клієнтських системах, необхідних для керування інформаційною системою організації для захисту кінцевих точок через Trellix ePO - On-prem [13].

На цій рис.3.2 показано, як Trellix Agent працює, якщо його встановлено на клієнтських системах через Trellix ePO - On-prem.

Порядок встановлення та роботи є таким:

1. Встановіть Trellix Agent на клієнті.

2. Trellix Agent встановлює безпечний зв'язок між клієнтом і Треллікс ePO - On-prem .

3. Trellix ePO - On-prem downloads програмний продукт для клієнта над

безпечним з'єднанням.

4. Trellix Agent надає інформацію про клієнтів та інші відомості про Trellix ePO - On-prem.

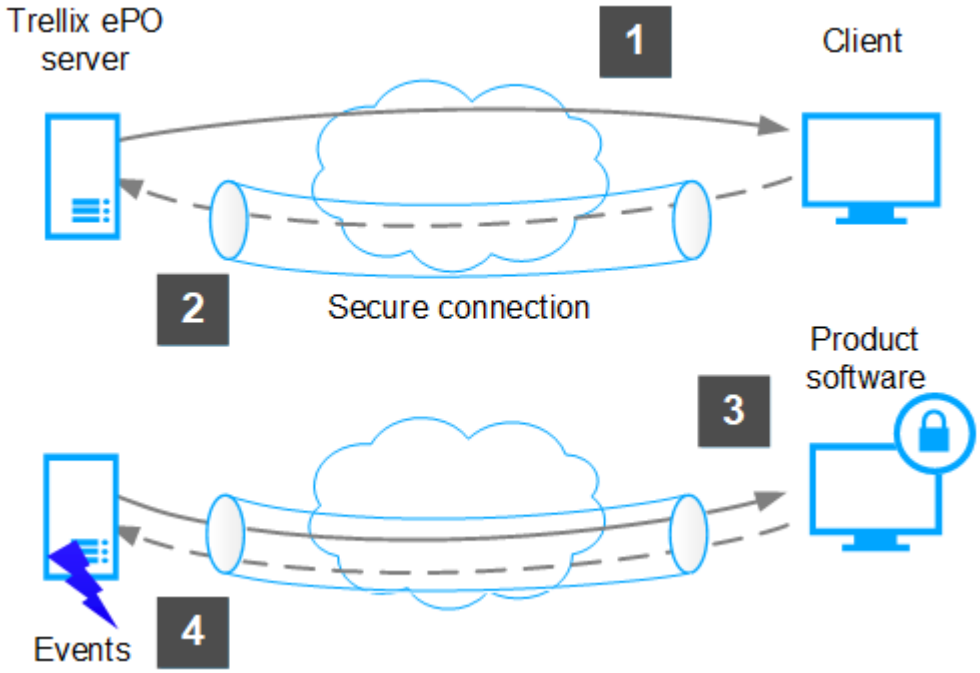


Рис.3.2. Порядок встановлення та роботи Trellix Agent

Розглянемо параметри політик. Trellix Agent надає сторінки конфігурації для налаштування параметрів політики, упорядкованих за такими категоріями: Загальні, Репозиторій, Програма вдосконалення продукту, Усунення несправностей і Спеціальні властивості.

Перш ніж розповсюджувати Trellix Agent для кінцевих точок організації, треба ретельно обдумати, як ви хочете, щоб Trellix Agent поводився в сегментах середовища організації. Можна також налаштувати параметри політики Trellix Agent після їх розповсюдження, але краще налаштувати їх перед розповсюдженням, щоб запобігти непотрібному впливу на ресурси.

Параметри, доступні для загальної політики, розділені на наступні вкладки, які показано у таблиці 3.1.

Таблиця 3.1.

Загальні полтики

Вкладки	Налаштування
General	Інтервал застосування політики Використання піктограми системного лотка в середовищах Windows Значок увімкнення системної іконки в сеансі віддаленого робочого столу. (Trellix ePO - On-prem) Trellix Agent та SuperAgent підтримка пробудження. Чи приймати підключення тільки від Trellix ePO - On-prem. Продуктивність ЦП для інших процесів у середовищі Windows. Обмеження процесів, послуг та реєстрації ключових змін Trellix Agent. Параметри перезавантаження після розгортання продукту в середовищах Windows. Зв'язок агент-сервер. Отримання всіх властивостей системи та продукту.
SuperAgent	Увімкнення RelayServer на Trellix Agent Вимкнення виявлення RelayServers Trellix ePO – Параметри локальної роботи: – Шлях до сховища, куди SuperAgent переходить для продуктів і пакетів оновлень. – Укажіть інтервал для очищення відкладеного кешу. – Укажіть простір на диску для відкладеного кешу. – Вкажіть інтервал видалення файлів з диска. – Трансляція дзвінка пробудження до SuperAgent. – Увімкнення відкладеного кешування.
Events	Увімкнення/вимкнення пересилання пріоритетних подій.

	Рівень пріоритету пересланих подій. Інтервал між завантаженнями подій. Максимальна кількість подій на завантаження.
Logging	Увімкнення/вимкнення журналювання програми. Встановлення ліміту розміру файлу журналу та кількості повторень. Рівень деталізації журналу. (Trellix ePO – локально). (Trellix ePO - On-prem) Параметр для ввімкнення віддаленого доступу до журналів.
Updates	Користувацьке розташування файлу журналу оновлення. Вказівки для параметрів після оновлення (не тільки після успішного оновлення). Пониження версії файлів DAT. Увімкнення автоматичного оновлення продуктів Trellix після розгортання.
Peer-to-Peer	Увімкніть одноранговий зв'язок на Trellix Agent, щоб увімкнути однорангового клієнта. Увімкніть Trellix Agent для доставки оновлень або інсталяційних файлів одноранговим агентам. Вкажіть шлях до сховища. Укажіть дисковий простір для оновлень на одноранговому сервері. Укажіть інтервал видалення файлів із репозиторію однорангового сервера.
Розгортання	Увімкніть Trellix Agent для виконання перевірки несумісності під час розгортання продукту Trellix

Отже для встановлення і розповсюдження Trellix Agent треба обов1язково налаштувати необхідні політики, для коректної роботи агентів у інформаційній системі організації.

Розглянемо зв’язок між агентом і сервером.

Trellix Agent періодично спілкується з Trellix ePO - On-prem, щоб надсилати події та перевіряти, чи всі параметри клієнтської системи оновлені.

Ці зв’язки називають зв’язком агент-сервер. Під час кожного зв’язку між агентом і сервером Trellix Agent збирає поточні системні властивості, а також події, які ще не надіслано, і надсилає їх на сервер. Сервер надсилає нові або змінені політики та завдання Trellix Agent, а також список репозиторію, якщо він змінився після останнього зв’язку між агентом і сервером. Trellix Agent забезпечує виконання нових політик локально в керованій системі та застосовує будь-які зміни завдань або сховища.

Trellix ePO - On-prem використовує мережевий протокол транспортного рівня безпеки (TLS) промислового стандарту для безпечної передачі по мережі.

Після першого встановлення Trellix Agent він звертається до сервера за 45 секунд. Після цього агент Trellix зв’язується, коли станеться одне з наступного:

Інтервал зв’язку між агентом і сервером (ASCI) закінчується.

Дзвінки пробудження надсилаються з Trellix ePO - On-prem або Agent Handlers.

У клієнтських системах виконується заплановане завдання пробудження.

Зв’язок ініціюється вручну з керованої системи (за допомогою монітора статусу агента або командного рядка).

Клієнтське завдання «Запустити негайно» виконується на клієнтських системах.

Отже, налаштований Trellix Agent дозволяє серверу Trellix ePO збирати відповідну інформацію та виявляти загрози кінцевої точки відповідно до налаштованих політик.

Розлянемо процес виявлення загроз для захисту кінцевих точок

Рисунок ілюструє процес захисту від загроз у корпоративній мережі за допомогою платформи Trellix. Опис процесу можна розділити на кілька етапів:

1. Адміністратор (1)

- Керує безпековими політиками через консоль *Trellix ePO*.

- Визначає параметри та налаштовує розширення, такі як:
  - Загальні параметри.
  - Запобігання загрозам.
  - Брендмауер.
  - Контроль Інтернету.
  - Система адаптивного захисту.

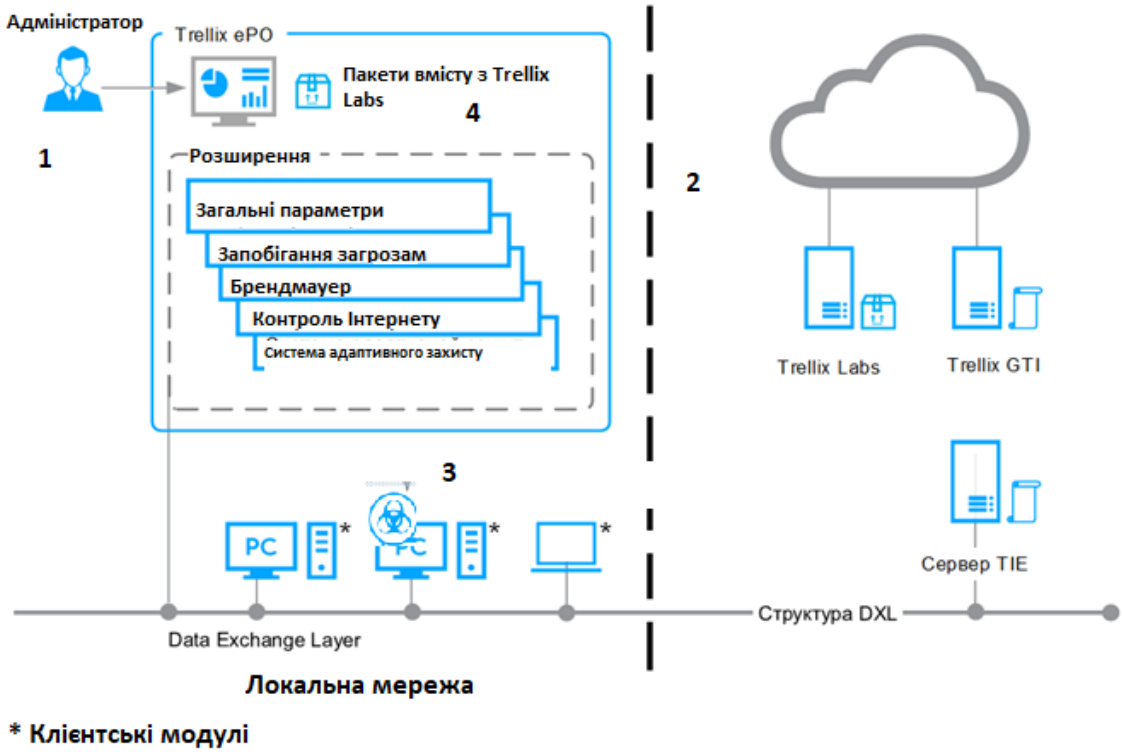


Рис.3.3. Запобігання загроз

2. Зовнішні джерела загроз (2)

- *Trellix Labs та Trellix GTI* збирають і аналізують загрози.
- *Сервер TIE* надає дані про репутацію файлів і програм.
- Інформація передається через *структуру DXL* до корпоративної мережі.

3. Локальна мережа (3)

- Клієнтські пристрої (ПК, сервери) оснащені захисними модулями (*).
- Дані про загрози надходять через *Data Exchange Layer (DXL)*.
- Встановлені політики (брендмауер, контроль Інтернету тощо) захищають кінцеві точки.

4. *Оновлення політик та реакція (4)*

- Адміністратор отримує *пакети вмісту з Trellix Labs* для оновлення політик безпеки.
- Система адаптивного захисту аналізує поведінку та реагує на загрози.
- При необхідності вживаються заходи для блокування загроз або карантину файлів.

Таким чином, система працює у взаємодії між адміністратором, зовнішніми аналітичними службами та клієнтськими модулями для виявлення та нейтралізації загроз у режимі реального часу.

Отже, процес запобігання загрозам кінцевим точкам в організації, представлений на зображенні, включає централізоване керування, отримання актуальної інформації про загрози, налаштування та розгортання засобів захисту на кінцевих точках, а також постійний моніторинг та адаптацію до нових загроз.

3.3. Розробка рекомендацій щодо захисту кінцевих точок інформаційної системи організації

Розглянемо і надаймо рекомендації щодо використання найкращих практик, які організації повинні використовувати під час захисту кінцевих точок кінцевих точок.

Захист кожної кінцевої точки в системі. Це включає в себе всі пристрої, які підключаються до вашої мережі, такі як комп'ютери, ноутбуки, смартфони та сервери. Кінцеві пристрої діють як шлюзи до вашої мережі. Таким чином, захист і відстеження кожного пристрою, який підключається до вашої системи, може служити вашому підприємству добре.

Організації можуть вести інвентаризацію всіх кінцевих точок у мережі та оновлювати його, коли до неї підключаються нові пристрої. Крім того, вони повинні переконатися, що кожен кінцевий пристрій обладнано необхідними засобами захисту від загроз безпеці, і таким чином застосовувати останні виправлення відповідно до потреб.

Застосовуйте принцип найменших привілеїв. Надавайте користувачам лише ті права доступу, які їм необхідні для виконання їхніх робочих обов'язків. Обмеження доступу та привілеїв пристрою є хорошою практикою для забезпечення безпеки кінцевих точок. Права адміністратора не слід призначати звичайним користувачам. Така політика доступу з найменшими привілеями може запобігти неавторизованим користувачам завантажувати виконуваний код на кінцеві точки.

Впроваджуйте автоматизоване встановлення патчів. Регулярно оновлюйте програмне забезпечення на всіх кінцевих точках, щоб усунути відомі вразливості.

Керуйте випадками використання власних пристроїв (BYOD) розсудливо. Встановіть чіткі правила для використання особистих пристроїв на робочому місці та забезпечте їх відповідний захист.

Розумно керуйте справами BYOD. Дозволяючи співробітникам користуватися власними пристроями, компанії повинні мати політику, яка описує необхідні протоколи безпеки. У багатьох випадках організації також можуть розглянути можливість використання політики облікового запису гостьового доступу.

Підприємства повинні наголошувати та зосереджуватися на тому, щоб усвідомлювати кінцевих користувачів про їхні обов’язки та нагадувати їм про правила, що стосуються втрати або крадіжки пристрою. Слабка або неправильна політика BYOD може коштувати компаніям мільярди доларів, оскільки користувачі можуть зламати мережу організації за допомогою власних пристроїв.

Подібний випадок спостерігався в 2017 році, коли стався злам даних найбільшої біржі біткоінів Південної Кореї. Нечітка політика BYOD призвела до цього інциденту, коли 30 мільйонів доларів (у криптовалюті) було вкрадено лише за кілька годин і скомпрометовано дані близько 32 000 користувачів.

Практикуйте сегментацію мережі. Розділіть вашу мережу на менші, ізольовані сегменти, щоб обмежити поширення кібератак.

Загальну продуктивність рішення безпеки кінцевої точки можна подвоїти, якщо розділити мережу на підмережі.

Це можна розпочати, налаштувавши привілейовану область і чітко визначену систему з ієрархією привілеїв. Ви також повинні пам’ятати про міжособистісні, міжвідомчі залежності та організаційні фактори під час сегментації мережі. Це забезпечить відсутність впливу на регулярні бізнес-процеси. Крім того, слід регулярно керувати та оновлювати привілейовані ресурси.

Сегментація мережі є стандартною практикою безпеки, яка відіграє ключову роль у безпеці мережі будь-якої організації.

Впроваджуйте гранульований контроль застосунків. Контролюйте, які програми можуть запускатися на кінцевих точках, щоб запобігти виконанню шкідливого програмного забезпечення.

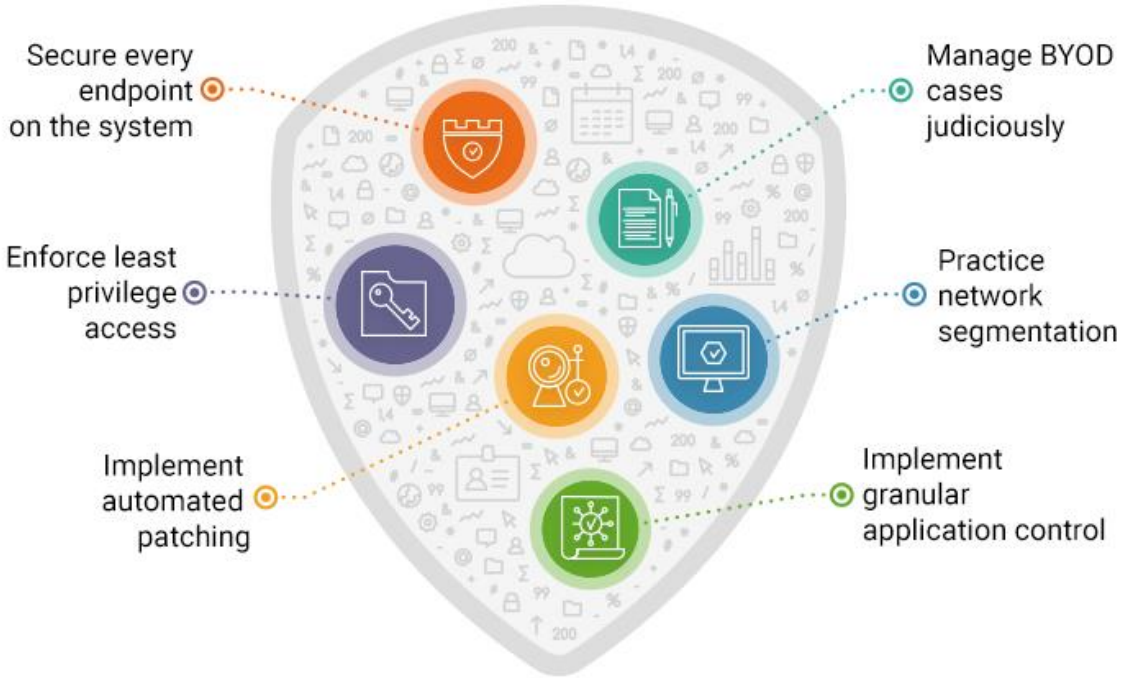


Рис.3.4. Найкращі практики безпеки кінцевих точок організації

Застосуйте надійнішу політику паролів і шифрування кінцевої точки.

Після того, як пристрої кінцевої точки стануть захищеними за допомогою заходів безпеки кінцевої точки, компаніям потрібно заохочувати своїх користувачів застосовувати правильні методи використання паролів.

Компанії можуть зробити довгі та складні паролі обов’язковими для всіх своїх користувачів. Вони також можуть заохочувати практику періодичної зміни

пароля. Крім того, звичка використовувати старі паролі повинна бути заборонена організаціями. Окрім паролів, компаніям може знадобитися додати додатковий рівень захисту за допомогою шифрування.

Одним із найкращих способів може бути шифрування диска або пам'яті кінцевої точки. Це гарантує, що дані пристрою залишатимуться нечитабельними або недоступними під час їх перенесення на інший пристрій або безпечні, навіть якщо пристрій буде вкрадено чи втрачено.

Використовуйте інструменти SIEM і регулярно скануйте кінцеві точки.

Рішення безпеки кінцевих точок повинні легко використовувати інструменти керування інформацією та подіями безпеки (SIEM), щоб забезпечити моніторинг мережі в реальному часі. Оскільки кількість кінцевих пристроїв зростає, рішення SIEM тепер є частиною стандартів компанії для забезпечення загальної безпеки. Хороше рішення SIEM має реєструвати всі мережеві події. Віно також повинно мати політику, яка може позначати потенційні інциденти та негайно вживати заходів щодо них.

Крім того, регулярне сканування кінцевих точок може дозволити організаціям відстежувати всі пристрої, підключені до мережі, у режимі реального часу. Це можна ще більше покращити, використовуючи методи постійної інформації про місцезнаходження для кінцевих пристроїв, таких як смартфони та планшети, які вразливі до втрати або крадіжки.

Впровадити автоматичного виправлення

Безпека кінцевої точки ефективна завдяки автоматизованим процедурам встановлення виправлень. За допомогою них ви можете динамічно надсилати оновлення виправлень під час простоїв. Організації повинні подбати про те, щоб такі автоматизовані системи також застосовувалися до виправлень сторонніх розробників.

Згідно з дослідженням Ponemon Institute, 60% порушень, виявлених у 2023 році, були спричинені невиправленим програмним забезпеченням. Тут уразливості були відомі, але необхідні патчі не були застосовані.

Практикуйте сувору політику доступу до VPN разом із MFA

Сьогодні, коли цільова група звертається до моделі віддаленої роботи, VPN широко використовуються більшістю корпоративних компаній. Однак мережі VPN залишаються вразливими до спуфінгу, сніфінгу, DDoS та інших зовнішніх атак.

Таким чином, доцільніше обмежити використання VPN, таким чином дозволяючи доступ до VPN лише на прикладному рівні. Це може значно зменшити ризик безпеки на рівні мережі.

Крім того, впровадження багатофакторної автентифікації (MFA) може запобігти крадіжці облікових записів з різних джерел. Крім того, запровадження вторинного рівня перевірки, коли система ідентифікує вхід із нерозпізнаних або невідомих місць, може підвищити загальну безпеку.

Практикуйте зміцнення системи та обережно використовуйте хмарне сховище

Організації можуть обмежити доступ до конфігурації та налаштувань пристрою, щоб зменшити вразливості IT, поверхні атак і потенційні вектори атак. Захист системи може встановити еталон для різних пристроїв і операційних систем. Він також може визначати шляхи трафіку між кінцевими точками та мережею. Як наслідок, усі інші відкриті порти (UDP або TCP) можуть бути закриті.

Крім того, компанії повинні пам’ятати, що хмара діє як ще одна кінцева точка, до якої легко отримати доступ зовнішнім особам. Отже, надання окремих облікових даних для кожного користувача є важливим. Крім того, використання TLS (HTTPS) для передачі даних має бути стандартною практикою.

Впровадити детальний контроль додатків

Впровадження цієї практики безпеки дозволить вам зосередитися на обмеженні несанкціонованого виконання програм, які становлять ризиковий елемент для безпеки організації.

Компанії можуть використовувати програми контролю програм, які обмежують виконання програм на основі таких факторів, як хеш, шлях або видавець. Вони можуть підтримувати список дозволених програм, файлів і додатків. Крім того, якщо програмі надано доступ, переконайтеся, що ви також

реалізуєте правила, які блокують зв’язок з іншими невідповідними сегментами мережі.

Отже, сьогодні рішення безпеки кінцевих точок пройшли довгий шлях від традиційних антивірусів і брандмауерів. Вони надають ширший набір засобів захисту для боротьби з відомими та невідомими атаками зловмисного програмного забезпечення, експлойтами безпеки та наслідками після вторгнення.

Зі значним зростанням кількості віддалених і мобільних працівників все більше кінцевих точок піддаються зловмисникам. Це збільшує «захисну поверхню» від традиційних офісних середовищ до кінцевих точок, розподілених по всьому світу. Таким чином, запровадивши систему безпеки кінцевих точок, ви можете гарантувати, що всі кінцеві точки, включаючи пристрої, що належать співробітникам, захищені від несанкціонованого доступу та потенційних кібератак. Це захистить цінні дані вашої компанії та допоможе зберегти її репутацію в галузі.

Отже, впровадження всіх рекомендацій дозволить організаціям захистити свою інформаційну систему організації від різних атак, зловмисного програмного забезпечення шляхом швидкого реагування на інциденти безпеки.

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.

В роботі проведено аналіз обсягу і складності загроз безпеці, які постійно зростають, що спонукає організації впроваджувати досконалі рішення безпеки кінцевих точок, які розроблені для швидкого виявлення, аналізу, блокування та стримування різних атак.

В роботі проведено порівняльний аналіз засобів захисту кінцевих точок, в результаті якого для подальшого дослідження було запропоновано використання Trellix Endpoint Security ENS, що забезпечує високий рівень захисту від сучасних загроз.

Надана архітектура Tellix Endpoint Protection Platform показала, що вона надає різні види послуг захисту кінцевих точок організацій. Така платформа надає автоматичний захист кінцевих точок та відповідає пріоритетам та потребам організацій у сфері безпеки, яке починається з запобігання та пошуку загроз і закінчується індивідуальним налаштуванням засобів захисту.

Досліджено засіб Trellix Endpoint Security ENS, який є комплексом модулів, роботу яких надається у вигляді процесів що забезпечують захист, виявлення та виправлення щодо запобігання загроз, роботи брандмауера, контролю Інтернету та системи адаптивного захисту.

В роботі надано рекомендації щодо використання Trellix Agent, як ключового клієнтського компоненту, який забезпечує безпечний зв’язок. Також запропоновано порядок встановлення агента на клієнтських системах, необхідних

для керування інформаційною системою організації для захисту кінцевих точок через Trellix ePO - On-prem.

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

Таким чином реалізація такого засобу захисту кінцевих точок інформаційної системи організації повинна сприяти розвитку та ефективному захисту інформаційної системи організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Що таке захист кінцевої точки. URL: *https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint#:~:text=Endpoints%20are%20crucial%20in%20network,and%20the%20greater%20network%20infrastructure*.
2. Що таке кінцева точка? URL: https://www.cloudflare.com/learning/security/glossary/what-is-endpoint/ .
3. Повний посібник з рішень та найкращих практик захисту кінцевих точок. URL: https://www.bluevoyant.com/knowledge-center/complete-guide-to-endpoint-security-solutions-and-best-practices .
4. Що таке безпека кінцевих точок? URL: https://www.spiceworks.com/it-security/network-security/articles/what-is-endpoint-security/ .
5. Програмне забезпечення для керування кінцевими точками: моніторинг і керування пристроями. URL: https://www.ninjaone.com/endpoint-management/ .
6. Microsoft Intune—Керування кінцевою точкою | Microsoft Security. URL: https://www.microsoft.com/en-gb/security/business/microsoft-intune .
7. 6 найкращих випадків використання Microsoft Intune для ефективного керування кінцевими точками - ProServeIT. URL: https://www.proserveit.com/blog/microsoft-intune-endpoint-management-6-best-use-cases .
8. Керування мобільними пристроями (MDM) | Системний менеджер | Cisco Meraki. URL: https://meraki.cisco.com/products/systems-manager/ .
9. Що таке керування кінцевими точками? – Trellix. URL: https://www.trellix.com/security-awareness/endpoint/what-is-endpoint-security-management/ .
10. Endpoint Security (ENS) – Trellix. URL: https://www.trellix.com/products/endpoint-security/ .

11. Trellix Endpoint Security (ENS). URL: https://www.trellix.com/assets/data-sheets/trellix-endpoint-security-datasheet.pdf .
12. Звіт роботи Trellix Endpoint Security. URL: https://www.trellix.com/blogs/platform/se-labs-q2-2024-enterprise-endpoint-security-test-results/ .
13. Trellix Agent 5.7.x Product Guide. URL: https://docs.trellix.com/ru-RU/bundle/trellix-agent-5.7.x-product-guide/page/GUID-BC52A070-B597-45A7-A004-A166ACE740CE.html.
14. How agent-server communication works - Trellix Doc Portal. URL: https://docs.trellix.com/bundle/trellix-agent-5.8.x-product-guide/page/UUID-67a3d48c-60f4-856a-6cd8-3fed31210ab0.html .
15. Trellix® Endpoint Security Suite. URL: https://www.trellix.com/assets/solution-briefs/trellix-endpoint-security-suite-solution-brief.pdf .
16. Microsoft Defender for Endpoint vs Trellix Endpoint Security comparison - PeerSpot. URL: https://www.peerspot.com/products/comparisons/microsoft-defender-for-endpoint_vs_trellix-endpoint-security .
17. Module overview - Trellix Doc Portal. URL: https://docs.trellix.com/bundle/fb_1.1.x_ug .
18. Module overview - Trellix Doc Portal. URL: https://docs.trellix.com/bundle/fb_1.0.2_ug/page/UUID-999b3b9a-bf9c-ee0b-000a-00bc1da4125a.html .
19. docs-be.trellix.com. URL: https://docs-be.trellix.com/bundle/agent-hx-data-sheet/raw/resource/enus/agent-hx-data-sheet.pdf?save_local=true .

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)