ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ УПРАВЛІННЯ КІНЦЕВИМИ ТОЧКАМИ ОРГАНІЗАЦІЇ ТА ЇХ ЗАХИСТУ НА ПРИКЛАДІ MICROSOFT INTUNE»

Виконав студент 6 курсу, групи БСДМ-63
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Туриченко Є. А.
(прізвище та ініціали)
Керівник Собчук А. В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н. С.
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ …… 10

ВСТУП ……..…… 10

1 **АНАЛІЗ ПРОБЛЕМИ УПРАВЛІННЯ КІНЦЕВИМИ ТОЧКАМИ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ЇХ ЗАХИСТУ** ……..……. 12

1.1 Дослідження проблеми управління кінцевими точками корпоративних інформаційних систем та їх захисту ……. 12
1.2 Аналіз підходів до управління кінцевими точками корпоративних інформаційних систем та їх захисту ……..... 17
1.3 Аналіз існуючих рішень щодо управління кінцевими точками корпоративних інформаційних систем та їх захисту ……..... 30

2 **АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ КІНЦЕВИМИ ТОЧКАМИ ОРГАНІЗАЦІЇ НА ПРИКЛАДІ MICROSOFT INTUNE** ……. 36

2.1 Призначення та основні функції рішення Microsoft Intune …… 36
2.2 Високорівнева архітектура рішення Microsoft Intune ……..….. 43
2.3 Зміст керування життєвим циклом мобільних пристроїв та додатків Microsoft Intune …….…… 46

3 **ТЕХНОЛОГІЯ УПРАВЛІННЯ КІНЦЕВИМИ ТОЧКАМИ ОРГАНІЗАЦІЇ ТА ЇХ ЗАХИСТОМ** ……...…….……. 51

3.1 Порядок застосування центру адміністрування Microsoft Endpoint Manager ……..……..… 51
3.2 Концепції застосування рішення Microsoft Intune …….. 56
3.3 Рекомендації щодо управління кінцевими точками організації та їх захисту …….…… 58

ВИСНОВКИ …….. 62

ПЕРЕЛІК ПОСИЛАНЬ 64

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 66

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп’ютер

ЦОД – центр обробки даних

AOSP – Android Open Source Project

ACL – Access Control List

API – Application Programming Interface

APT – Advanced Persistent Threat

BYOD – Bring-Your-Own-Device

CDN – Content Delivery Network

DDoS – Distributed Denial of Service

DNS – Domain Name System

EDR – Endpoint Detection and Response

EPP – Endpoint Protection Platform

IaaS – Infrastructure as a Service

ICMP – Internet Control Message Protocol

MAM – Mobile Application Management

MDM – Mobile Device Management

MFA – Multi-Factor Authentication

RDP – Remote Desktop Protocol

SSO – Single Sign-On

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

ВСТУП

Актуальність дослідження. Ключовим завданням будь-якого адміністратора безпеки є захист інформаційних ресурсів організації. Це завдання безпосередньо пов’язано з керування пристроями. Користувачі отримують і надсилають електронні листи з особистих облікових записів, переглядають веб-сайти з дому та інших місць, а також встановлюють додатки та ігри. На своїх пристроях вони хочуть отримати доступ до робочих і навчальних ресурсів, таких як електронна пошта та OneNote, і отримати до них швидкий доступ.

Керування пристроями дозволяє організаціям захищати свої ресурси та дані на різних пристроях. Використовуючи постачальника послуг керування пристроями, організація може гарантувати, що лише авторизовані люди та пристрої отримають доступ до конфіденційної інформації. Так само користувачі пристроїв можуть відчувати себе спокійно, отримуючи доступ до робочих даних зі свого телефону, оскільки вони знають, що їхній пристрій відповідає вимогам безпеки їх організації.

Багато організацій, у тому числі Microsoft, використовують рішення Intune для захисту конфіденційних даних, до яких користувачі отримують доступ із пристроїв, що належать їхнім компаніям та особам. Вищесказане визначає актуальність теми даної магістерської роботи, основний зміст якої становлять дослідження технології управління кінцевими точками організації та їх захисту на прикладі Microsoft Intune.

Об’єкт дослідження – управління кінцевими точками організації.

Предмет дослідження – технологія управління кінцевими точками організації та їх захисту на прикладі Microsoft Intune.

Мета роботи – розробити порядок застосування технології управління кінцевими точками організації та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми управління кінцевими точками організації та

їх захисту;

проаналізувати підходи до управління кінцевими точками організації та їх захисту;

проаналізувати існуючі рішення із управління кінцевими точками організації та їх захисту;

проаналізувати методи та засоби кінцевими точками організації та їх захисту на прикладі Microsoft Intune;

розкрити порядок реалізації технології кінцевими точками організації та їх захисту.

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

Практичне значення одержаних результатів: запропоновано порядок застосування технології кінцевими точками організації та їх захисту на прикладі Microsoft Intune, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати магістерської роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ [17].

1 АНАЛІЗ ПРОБЛЕМИ УПРАВЛІННЯ КІНЦЕВИМИ ТОЧКАМИ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ЇХ ЗАХИСТУ

1.1. Дослідження проблеми управління кінцевими точками корпоративних інформаційних систем та їх захисту

Кінцеві точки, такі як робочі станції користувачів, ноутбуки, сервери та хмарні системи, є найпоширенішим типом активів в організаціях, а також тими, на які зловмисники найбільше націлені. Кінцеві точки містять дані, зберігають облікові дані користувача та підключаються до інших частин мережі. Одна кінцева точка може бути вектором входу, формою стійкості та точкою виходу зловмисників [2].

Таким чином, організації наполегливо працюють, щоб захистити свої кінцеві точки. Одним із способів захисту кінцевих точок організації є інвестиції в технології, орієнтовані на кінцеві точки, включаючи традиційні антивірусні засоби та інструменти виявлення та реагування на кінцеві точки (EDR). Позиції безпеки зазвичай зосереджені насамперед навколо технології кінцевих точок і часто включають інші типи телеметрії для підтримки кінцевих точок.

Згідно з результатами дослідження Adaptiva [1] фахівці з кібербезпеки вважають найбільшою загрозою для кібербезпеки для своєї організації шкідливе програмне забезпечення (у тому числі програми-вимагачі, трояни, набори експлойтів тощо) (38%), за ним йдуть людські помилки (23%) та експлойти нульового дня (18%). Це підтверджує відповідне дослідження, що наголошує на зростаючій загрозі з боку шкідливих програм, особливо програм-вимагачів.

Зацікавленість організацій у переході на рішення захисту кінцевих точок нового покоління обумовлена низкою чинників. Основним фактором є те, що багато встановлених застарілих продуктів безпеки (AV, NGAV, HIPS, EPP тощо) не можуть зупинити зростаючу кількість нових загроз (46%). І навіть організації, які вважають, що у них є надійні інструменти та процеси, як і раніше, стурбовані

тим, що загрози вислизають від захисту (41%) [1]. Ключові фактори для розгляду рішення для захисту кінцевих точок нового покоління показано на рис. 1.2.

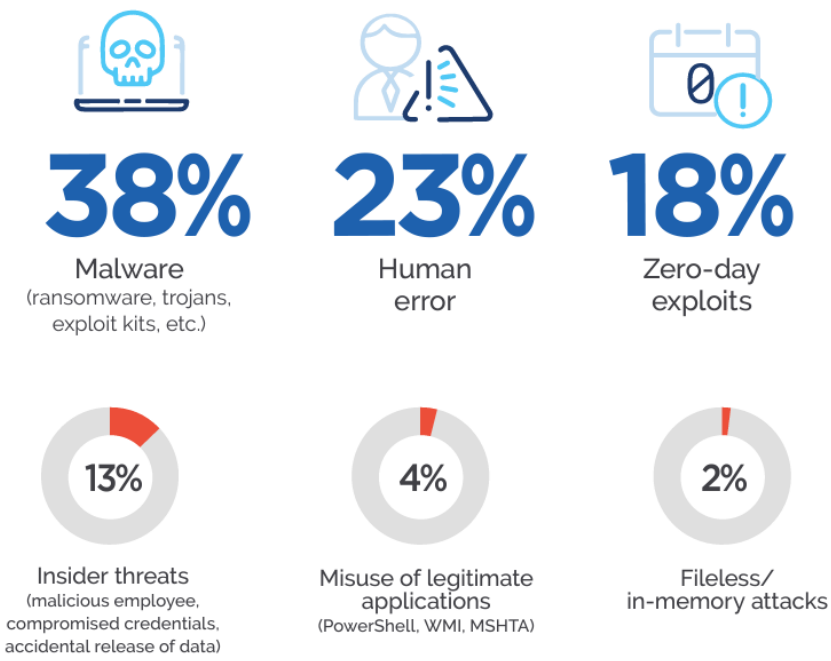

Рис. 1.1. Найбільші загрози для кібербезпеки організації [1]

Рис. 1.2. Ключові фактори для розгляду рішення для захисту кінцевих точок нового покоління [1]

Більшість організацій відчули збільшення кіберзагроз для своїх кінцевих точок (66%). Двадцять відсотків фахівців з кібербезпеки повідомляють, що протягом останніх 12 місяців їхня організація зазнала «успішної» атаки на кінцеву точку, яка скомпрометувала дані та/або IT-інфраструктуру. Кількість невиявлених атак, ймовірно, значно вища [1].

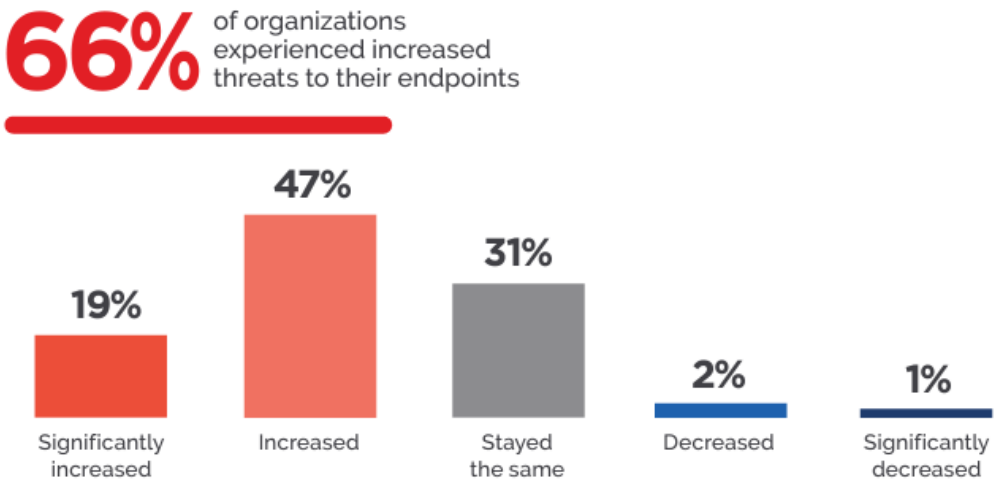

Рис. 1.3. Як змінився ризик безпеки кінцевої точки для вашої організації за останні 12 місяців? [1]

У світлі загроз, що погіршуються, організації досить прагматичні щодо кібератак і усвідомлюють, що вони, ймовірно, стають ціллю. Понад вісім із 10 респондентів вважають, що компрометуюча атака ймовірно відбудеться в найближчі 12 місяців (85%) [1].

Одна з найбільших загроз для кінцевих точок випливає з того факту, що кінцеві точки є останньою лінією захисту. Ще однією загрозою, яка мучила багато організацій протягом багатьох років, були вразливості. Враховуючи функцію кінцевих точок, цю категорію загроз може бути важко класифікувати та захистити. Уразливості можуть стосуватися операційної системи, апаратного забезпечення у фізичній системі або стороннього програмного забезпечення. Як показав останній час, іноді уразливості містяться в бібліотеках, вбудованих у стороннє програмне забезпечення, що наражає кінцеву точку на загрозу [2].

Рис. 1.4. Яка, на вашу думку, ймовірність того, що ваша організація буде скомпрометована успішною кібератакою протягом наступних 12 місяців? [1]

Функція кінцевої точки також може змінити її профіль ризику. Наприклад, уявіть зовнішній сервер проти внутрішньої системи з повітряним зазором. З точки зору кінцевої точки, вони можуть бути одним типом активів, але їхній профіль ризику дуже відрізняється з точки зору вразливості. Зловмисники можуть шукати діри у зовнішньому програмному забезпеченні, такому як веб-сервер, допоміжна бібліотека або відкритий порт [2].

Як видно з останніх виявлень уразливостей, зловмисники абсолютно не витрачають час на масове сканування Інтернету, коли з'являється нова вразливість. Інші вразливі місця, які становлять ризик, – це їх здатність підвищувати показники успіху зловмисників.

Однією з загроз, яка часто впливає на кінцеві точки, є використання широко відомих і добре зарекомендованих наборів для пост-експлуатації. Звичайно, перше, що спадає на думку, це незмінні Cobalt Strike і Metasploit. Хоча продаються як інструменти симуляції супротивника або агресивні засоби безпеки, комплексні комплекти після експлуатації є одними з найпоширеніших

інструментів зловмисника.

У статті Threatpost за червень 2021 року повідомлялося, що використання Cobalt Strike зросло на 161% порівняно з роком у кібератаках1, причому інструмент використовувався як APT, так і учасниками загальних товарів або програм-вимагачів. Набори інструментів після експлуатації також становлять значну загрозу для кінцевих точок організації, оскільки вони постачаються в комплекті з десятками (якщо не сотнями) можливостей експлуатації [2].

Зловмисники можуть отримати початковий доступ до системи та проходити через десятки атак, експлойтів, ескалації привілеїв і спроб бокового переміщення, поки не знайдуть щось, що працює. Ці набори інструментів також містять елемент автоматизації, який, як ми бачили, використовують багато загрозливих суб’єктів на свою користь. Cobalt Strike, наприклад, має можливість для зловмисників завантажувати сценарії агресора, які є автоматизованою серією дій, які виконуються в системі жертви. Це може дати зловмисникам значну перевагу, якщо вони зможуть зібрати сценарій, який переносить їх від 0 до 100 за мінімальний час [2].

Як зазначається в [2], розгортання рішення для кінцевої точки нелегка справа. Команди безпеки мають враховувати багато факторів, у тому числі використання системних ресурсів, способи споживання та дії з даними, а також те, як кінцеве рішення вплине на користувачів.

Незважаючи на це, організації повинні вибрати рішення, яке найкращим чином дозволить їхній групі безпеки виконати вимогу щодо захисту організації, її даних і користувачів. Деякі ключові міркування щодо безпеки кінцевих точок, особливо на тлі сучасних загроз, включають [2]:

рішення кінцевих точок повинні використовувати переваги нових технологічних тенденцій, таких як AI/ML, розширене виявлення та захист від рухомих цілей (moving target defenses, MTD);

рішення для кінцевих точок повинні інформувати та підтримувати команди безпеки. Просте повідомлення про виявлення без додаткового контексту чи пов’язаної телеметрії не надає командам необхідної переваги;

захист кінцевих точок має поєднуватися з можливостями виявлення та реагування, щоб команди могли сортувати, аналізувати, зберігати та блокувати за допомогою однієї платформи.

1.2. Аналіз підходів до управління кінцевими точками корпоративних інформаційних систем та їх захисту

Керування кінцевими точками – це практика автентифікації та контролю прав доступу кінцевих пристроїв до мережі та застосування політик безпеки, які запобігають будь-яким зовнішнім або внутрішнім загрозам, спричиненим цим доступом. Власники мереж зазвичай використовують програмне забезпечення для керування безпекою кінцевих точок, щоб [3]:

обмежити доступ до мережі лише для авторизованих кінцевих пристроїв і їх користувачів у приміщенні або через широку мережу (наприклад, глобальну мережу чи Інтернет);

застосовувати та контролювати політики безпеки кінцевих точок у всій мережі за допомогою невеликих додатків на кожному керованому пристрої (агентах). Це дозволяє адміністраторам безпеки керувати цими пристроями та процесами з однієї центральної консолі або додатка.

Комп’ютери, ноутбуки, планшети та смартфони, які мають доступ до мереж у приміщенні або через віддалене/інтернет-з’єднання, є найпоширенішими пристроями, які потребують керування кінцевими точками. Спеціалізоване апаратне забезпечення кінцевої точки та вбудоване програмне забезпечення також використовуються для захисту та керування пристроями Інтернету речей (IoT), такими як дистанційні датчики та промислові засоби керування [3].

У всьому світі існують мільярди кінцевих точок у корпоративних, інтернет-, інтранет- та мобільних мережах. Крім того, зазвичай один користувач має доступ до мереж через кілька пристроїв – комп’ютер в офісі, ноутбук або планшет у дорозі та смартфон практично з будь-якого місця. Чим більше кінцевих пристроїв розгорнула організація, тим більша потреба керувати ними всіма.

Політики керування кінцевими точками. Перше завдання для захисту кінцевих точок полягає в тому, щоб лише авторизовані пристрої та користувачі могли підключатися до мережі. Як правило, це передбачає налаштування автентифікації імені користувача та пароля на затверджених пристроях, щоб авторизовані учасники мережі могли входити та виконувати роботу.

У багатьох організаціях через великий обсяг кінцевих точок і широкий діапазон прав дозволів для користувачів налаштування кожного пристрою окремо не є доцільним. Це створює потребу в політиках керування безпекою кінцевих точок. Керівництво може вирішити, які дозволи та навіть типи пристроїв можуть використовувати мережу. Завдяки політикам керування безпекою кінцевих точок адміністратори можуть ефективно надавати (або забороняти) певні права в мережі, обмежуючи, до яких областей, робочих навантажень і програм користувач може отримати доступ. Наприклад, користувачам відділу продажів потрібен доступ до додатків для створення потенційних клієнтів, системи відстеження замовлень, внутрішніх комунікацій тощо.

Установивши та створивши шаблон політики безпеки продажів, адміністратори безпеки можуть використовувати програмне забезпечення для керування безпекою кінцевих точок, щоб налаштувати та контролювати багато пристроїв, у тому числі кілька дозволених пристроїв, для кожного користувача в групі продажів. Коли в мережі вносяться зміни, адміністратори та менеджери безпеки можуть змінювати політики та поширювати зміни серед усіх учасників групи [3].

Оскільки захист доступу до мережі стає дедалі важливішим, а паролі можуть бути зламані, керування безпекою кінцевих точок також може спричинити за собою вбудовування маркерів пристрою (наприклад, зашифрованих програмних ідентифікаторів) на пристрої, щоб переконатися, що пристрій (і його користувач) є автентичними та уповноважений. Також широко використовуються такі біометричні дані, як сканування відбитків пальців і сітківки ока, особливо на смартфонах [3].

Однак безпечний вхід є лише першим кроком у безпеці кінцевої точки.

Щойно користувачі отримують доступ до мережі, їхні дії та пристрої створюють постійну проблему безпеки. Після успішного авторизованого входу в мережу програмне забезпечення безпеки кінцевої точки вмикається, щоб забезпечити захист.

Програмне забезпечення безпеки кінцевих точок та керування ними.

Безпека кінцевої точки та керування безпекою кінцевої точки працюють найкраще, коли вони працюють разом. Кінцеві точки – це робочі інструменти та мережеві інтерфейси, і тому вони постійно створюють дані та обмінюються ними. Кожна зміна на пристрої кінцевої точки або даних, до яких він отримує доступ у будь-якій мережі, є потенційною загрозою для безпеки. Це функція програмного забезпечення безпеки кінцевих точок, щоб аналізувати та перевіряти всі зміни та переміщення даних, сканувати на наявність зловмисного програмного забезпечення та вірусів, а також застосовувати виправлення та оновлення за потреби.

Управління безпекою кінцевої точки має координувати та визначати пріоритети оновлень, консолідувати та передавати моніторингові сповіщення та звіти, а також надавати уніфіковані служби безпеки через єдину консоль.

У той час як програмне забезпечення безпеки кінцевих точок виконує величезну роботу з виявлення та захисту кінцевих точок і мережі від загроз, керування безпекою кінцевих точок уніфікує, спрощує та посилює загальну безпеку організації та щоденну готовність до загроз. Організації, які розгортають керування безпекою кінцевих точок, зазвичай отримують такі переваги [4]:

швидше реагування та пом’якшення загроз безпеці;

швидке розгортання новітніх функцій і технологій безпеки;

покращений зв’язок безпеки в усій організації;

нижчі витрати, але надійніший захист;

шлях до майбутніх удосконалень і автоматизації.

Завдяки стрімкому прогресу програмного забезпечення безпеки та розгортання Інтернету речей, системи керування безпекою кінцевих точок, засновані на відкритій архітектурі, є найкращою платформою для майбутнього,

щоб забезпечити ще більше переваг.

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 складних зловмисних програм і нових загроз нульового дня [4].

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 вони повинні співпрацювати один з одним та з іншими технологіями безпеки, щоб надати адміністраторам бачення передових загроз, щоб пришвидшити час виявлення та реагування на виправлення.

Платформа захисту кінцевої точки є важливою частиною кібербезпеки підприємства з кількох причин. 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 ускладнюються політиками віддаленої роботи та BYOD, які роблять безпеку периметра дедалі недостатньою та створюють уразливості. Ландшафт загроз також ускладнюється: хакери завжди винаходять нові способи отримати доступ, викрасти інформацію або змусити

співробітників надати конфіденційну інформацію.

Безпека кінцевої точки – це практика захисту даних і робочих процесів, пов'язаних з окремими пристроями, які підключаються до вашої мережі. 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 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 [4].

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 [4].

Якщо пристрій підключено до мережі, він вважається кінцевою точкою. З ростом популярності BYOD (принесіть свій власний пристрій) та IoT (Інтернет речей) кількість окремих пристроїв, підключених до мережі організації, може швидко досягати десятків (і сотень) тисяч.

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. Згадайте найновіші 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.

Як правило, програмне забезпечення безпеки кінцевої точки включає в себе такі ключові компоненти [4]:

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;

платформи захисту кінцевих точок проти традиційного антивірусу.

Безпека кінцевої точки проти безпеки мережі: антивірусні програми розроблені для захисту окремої кінцевої точки, пропонуючи видимість лише для цієї кінцевої точки, у багатьох випадках лише з цієї кінцевої точки. Однак програмне забезпечення безпеки кінцевих точок розглядає мережу підприємства в цілому та може запропонувати видимість усіх підключених кінцевих точок з одного місця.

Адміністрування: застарілі антивірусні рішення покладалися на те, що користувач міг оновлювати бази даних вручну або дозволяти оновлення в попередньо встановлений час. EPP пропонують взаємопов'язану безпеку, яка передає відповідальність за адміністрування корпоративній команді IT або кібербезпеки.

Захист: традиційні антивірусні рішення використовували виявлення на основі сигнатур для пошуку вірусів. Це означало, що якщо ваш бізнес був «нульовим пацієнтом» або якщо ваші користувачі останнім часом не оновлювали свою антивірусну програму, ви все ще могли бути під загрозою. Завдяки використанню хмари сучасні рішення EPP оновлюються автоматично. А за допомогою таких технологій, як поведінковий аналіз, можна виявити раніше невідомі загрози на основі підозрілої поведінки [4].

Якщо пристрій підключено до мережі, він вважається кінцевою точкою. Із зростанням популярності «Принеси свій власний пристрій» (BYOD) та «Інтернет речей» (IoT) кількість окремих пристроїв, підключених до мережі організації, швидко зросла. Оскільки вони є точками входу для загроз і зловмисного програмного забезпечення, кінцеві точки є легкою мішенню для атак. Мобільні

кінцеві пристрої стали набагато більше, ніж просто телефони.

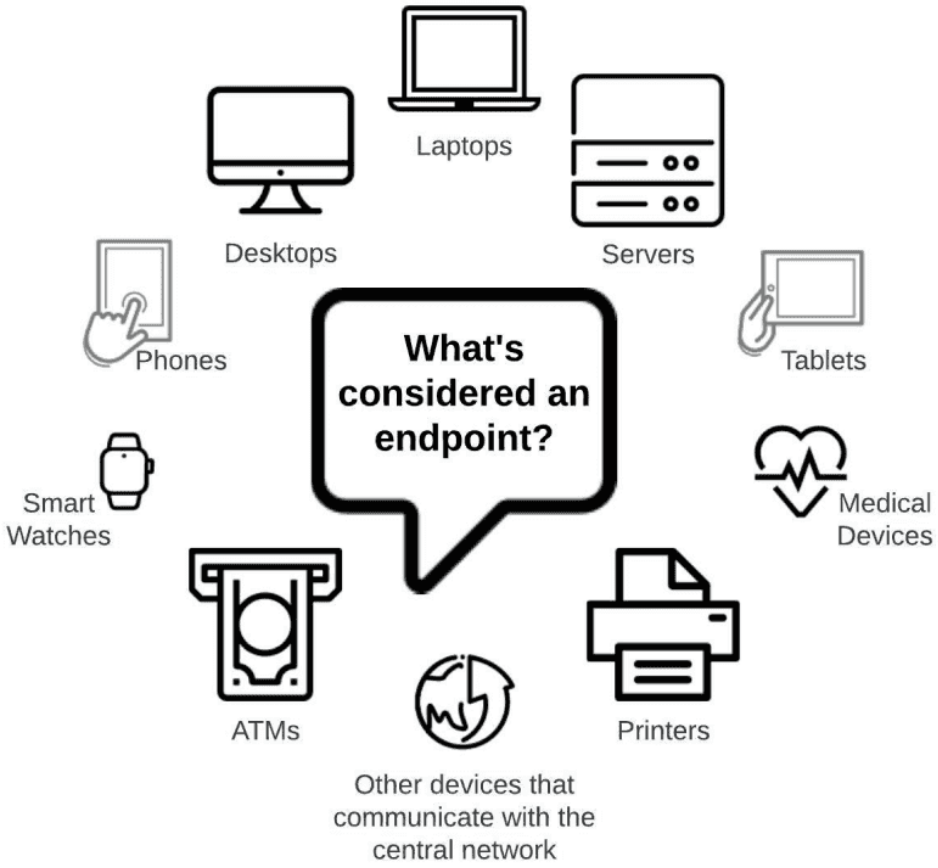

Рис. 1.5. Кінцеві точки [5]

Переносні пристрої, розумні годинники, цифрові помічники, такі як Alexaта інші розумні пристрої з підтримкою IoT також вважаються мобільними кінцевими точками. Тепер у наших автомобілях, літаках, лікарнях і майже в будь-якому іншому місці, яке тільки можна придумати, є підключені до мережі датчики. Кінцеві точки служать точками доступу до корпоративної мережі та створюють точки входу, якими можуть скористатися зловмисники. Рішення безпеки для кінцевих точок потребують адаптації, оскільки різні типи кінцевих точок розвиваються та розширюються [5].

Організаціям будь-якого розміру загрожує організована злочинність, загрози кібербезпеці, різні типи атак, а також зловмисні або випадкові внутрішні загрози. Коли компанії захищають свої кінцеві точки, вони можуть підтримувати більший контроль над точками доступу. Безпека кінцевих точок часто розглядається як передовий рубіж кібербезпеки та є одним із перших місць, де

організації прагнуть захистити свої корпоративні мережі [5].

Оскільки загрози кібербезпеці стають все більш поширеними та складними, більш досконалі рішення безпеки кінцевих точок стали необхідністю. Більшість популярних сьогодні систем захисту кінцевих точок розроблено для швидкого виявлення, аналізу, блокування та стримування поточних атак. Для цього їм потрібно співпрацювати з різними технологіями безпеки та надати адміністраторам видимість. Поширені загрози потрібно швидко виявляти та повідомляти адміністраторам, а час відповіді на виправлення має бути якомога коротшим.

У сучасному діловому світі найціннішим надбанням компанії є дані. Втрата самих даних або втрата доступу до цих даних послаблює весь бізнес. Підприємства та їхні працівники впроваджують методи, щоб зробити доступ до даних більш доступним. Це спричиняє збільшення таких політик, як BYOD, і підвищує ризик нападу зловмисників на доступ до мобільних пристроїв і мереж, створюючи вразливі місця кінцевих точок. Крім того, співробітники працюють вдома або підключаються до мереж Wi-Fi, щоб працювати в дорозі. Зі зміною пандемії кількість кінцевих точок тільки збільшується.

Згідно з кількома дослідженнями, переважна більшість працівників США працювали віддалено в 2020 році, а більше половини продовжували працювати віддалено в квітні 2021 року. Незахищені кінцеві точки створюють великі ризики, і конфіденційні дані, що містяться в них, потрібно надійно захищати [5].

Раніше більшість порушень безпеки відбувалися через мережу. Сьогодні загрози все частіше надходять від кінцевих точок, і використання лише централізованого захисту мережі недостатньо. Вимірювання безпеки повинні контролювати точки доступу та запобігати вразливості, яка може виникнути через віддалені пристрої.

Ці фактори самі по собі означають важливість кінцевої точки підприємства. Окрім них, слід зазначити, що ландшафт загроз ускладнюється. Хакери винаходять нові способи отримати доступ до ресурсів і заволодіти ними, викрасти інформацію або змусити співробітників ділитися конфіденційною інформацією.

Кожна віддалена кінцева точка може легко стати поверхнею атаки, а підприємства будь-якого розміру є привабливими цілями для кібератак [5].

Інструменти безпеки кінцевих точок, які забезпечують безперервне запобігання порушенням, повинні інтегрувати фундаментальні елементи, які показано на рисунку 1.6.

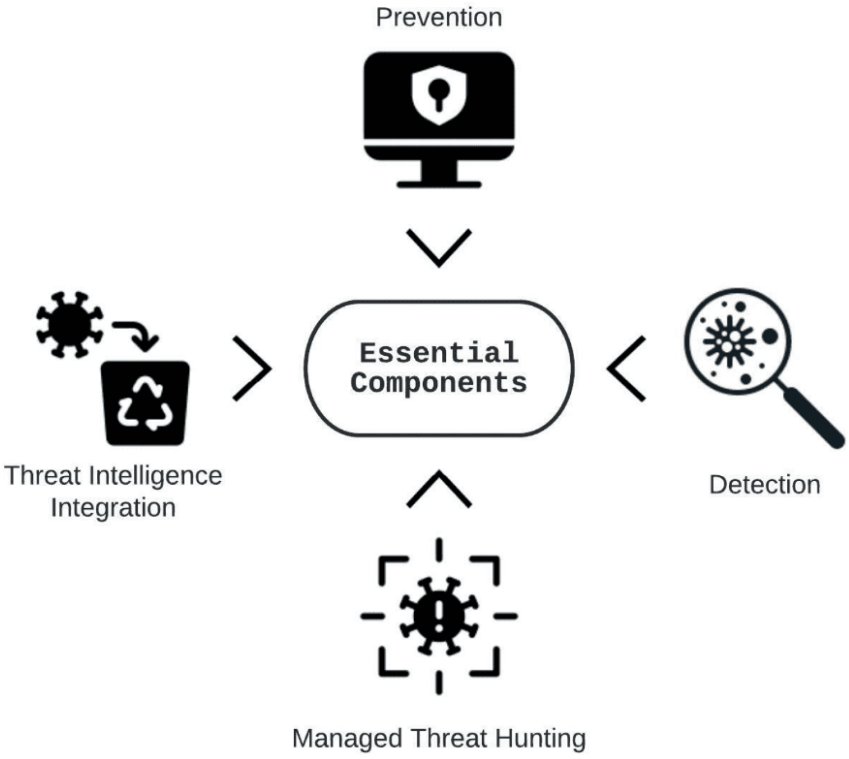

Рис. 1.6. Складові безпеки кінцевих точок [5]

Розглянемо більш детально складові безпеки кінцевих точок (рис. 1.6).

Профілактика. Традиційних антивірусних рішень недостатньо для захисту кінцевих точок. Вони функціонують шляхом порівняння зловмисних сигнатур, наприклад бітів коду, з базою даних, яка постійно оновлюється. Ці бази даних оновлюються щоразу, коли виявляється нова сигнатура зловмисного програмного забезпечення. Такі системи виявляють менше половини всіх атак. Основна проблема цієї схеми полягає в тому, що якщо шкідливе програмне забезпечення ще не виявлено, воно не буде знайдено в базі даних. Час, коли зловмисне програмне забезпечення виходить у світ, і час, коли його можна ідентифікувати традиційними антивірусними рішеннями, відрізняються.

Антивірусні рішення наступного покоління допомагають програмному забезпеченню для керування кінцевими точками усунути цю прогалину, використовуючи передові технології. Ці технології включають штучний інтелект і машинне навчання, ідентифікуючи нове зловмисне програмне забезпечення шляхом вивчення додаткових елементів, таких як хеші файлів, URL-адреси та IP-адреси [5].

Виявлення. Профілактики самої по собі недостатньо для забезпечення безпеки кінцевих точок. Захист програмного забезпечення не є досконалим, і деякі атаки завжди проходять через них і проникають у мережу. Традиційний підхід безпеки не реагує достатньо швидко, коли це відбувається. Це дозволяє зловмисникам вільно блукати в середовищі днями, тижнями, можливо, навіть довше. Підприємствам потрібне рішення, щоб швидше реагувати на ці атаки, швидко знаходячи та видаляючи зловмисників.

Щоб швидко реагувати на таких зловмисників, потрібне рішення Endpoint Detection and Response (EDR). EDR забезпечує постійну та надійну видимість кінцевих точок у режимі реального часу. Компанії повинні шукати рішення, які пропонують розширене виявлення загроз і дослідження. Модуль Qualys EDR є хорошим кандидатом [5].

Керований пошук загроз. Автоматизація не може виявити всі атаки. Досвід фахівців із безпеки необхідний для виявлення потенційних помилкових спрацьовувань і виявлення складних атак.

Кероване полювання на загрози здійснюється групами, до складу яких входять ці професіонали. Використовуючи старі випадки та краудсорсингові дані, відповідальна команда вказує нам, як виявляти зловмисну активність і реагувати на неї [5].

Інтеграція аналізу загроз. Загрози у світі кібербезпеки постійно розвиваються. Щоб не відставати від зловмисників, компанії повинні розуміти загрози в міру їх розвитку. Складні, просунуті загрози можуть переміщатися швидко та непомітно, і команди безпеки повинні переконатися, що їх захист є достатнім для запобігання, виявлення та реагування на ці загрози.

Типове рішення для інтеграції аналізу загроз включає автоматизацію для розслідування всіх інцидентів і використання їх для отримання інформації. Він генерує спеціальні індикатори безпосередньо з кінцевих точок; і використовує їх для проактивної реакції на майбутні атаки. Людський елемент для інтеграції аналізу загроз складається з експертів-дослідників безпеки, аналітиків загроз, культурологів і лінгвістів. Включивши таку команду, можна інтерпретувати нові загрози в різних контекстах [5].

Безпека кінцевої точки – це практика захисту даних і робочих процесів, пов'язаних із пристроями, які підключаються до керованої мережі. Терміни захист кінцевої точки, безпека кінцевої точки та платформа захисту кінцевої точки описують рішення безпеки з централізованими рішеннями. Платформи захисту кінцевих точок захищають такі кінцеві точки, як сервери, робочі станції, мобільні пристрої та робочі навантаження, від загроз кібербезпеці. Рішення для захисту кінцевих точок працюють, перевіряючи файли, процеси та активність системи та використовуючи їх для виявлення підозрілої чи зловмисної поведінки [5].

Платформи забезпечують централізовану консоль, яка встановлюється на мережевий шлюз або сервер і дозволяє дистанційно керувати кожним пристроєм. Кожній кінцевій точці призначається клієнтське програмне забезпечення . Його можна доставити віддалено або встановити безпосередньо на пристрій. Після завершення налаштування клієнтське програмне забезпечення можна використовувати для надсилання оновлень на кінцеві точки, автентифікації спроб входу з кожного пристрою та призначення корпоративних політик. За допомогою контролю програм можна блокувати небезпечні або неавторизовані програми. За допомогою шифрування можна запобігти втраті даних.

Рішення для захисту кінцевих точок можна розглянути за трьома категоріями: *традиційний підхід, гібридний підхід або хмарна модель* (рис. 1.7). Хоча хмарні продукти є більш масштабованими та можуть легко інтегруватися з вашою архітектурою, певні нормативні/відповідні правила можуть вимагати локальної безпеки.

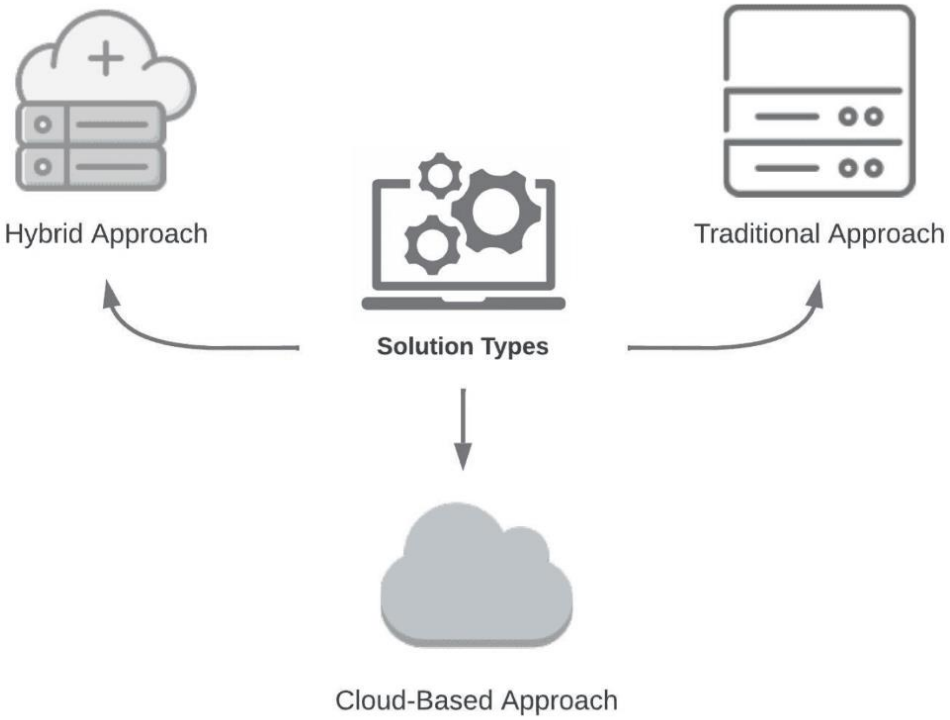

Рис. 1.7. Підходи до захисту кінцевих точок [5]

Традиційний підхід описує стан безпеки на місці. Він покладається на локальний центр обробки даних. Центр обробки даних діє як концентратор для консолі керування, і концентратор зв’язується з кінцевими точками через агента для забезпечення безпеки. У цій моделі адміністратори можуть керувати лише кінцевими точками в межах досяжності концентратора.

Зі збільшенням моделі «робота з дому» використання стаціонарних настільних пристроїв для багатьох організацій значно скоротилося. Разом із глобалізацією робочої сили виявилися обмеження локального підходу. У результаті деякі платформи рішень для захисту кінцевих точок перейшли на *гібридний підхід*. Цей підхід використовує застарілу архітектуру та вносить до неї зміни з метою надання їй деяких хмарних можливостей.

Третій підхід – це *хмарне рішення*. У цій моделі адміністратори можуть віддалено контролювати та керувати кінцевими точками за допомогою централізованої консолі керування. Консоль використовує хмару для віддаленого підключення до пристроїв через агента на них. Агент може працювати незалежно, щоб забезпечити безпеку кінцевої точки, поки вона не в мережі. Сучасні

платформи часто базуються на хмарі, використання хмари допомагає їм зберігати велику, зростаючу базу даних інформації про загрози. У результаті кінцевим точкам не потрібно зберігати всю цю інформацію локально та підтримувати її в актуальному стані. Зберігання цих даних у хмарі забезпечує більшу швидкість і масштабованість [5].

1.3. Аналіз існуючих рішень щодо управління кінцевими точками корпоративних інформаційних систем та їх захисту

Безпека кінцевих точок складається з технологій кібербезпеки, спрямованих на захист кінцевих точок від зловмисного програмного забезпечення та програм-вимагачів. Кінцева точка – це будь-який підключений пристрій, наприклад настільні комп'ютери, ноутбуки, мобільні пристрої, операційні технології (OT) і вузли IoT. Загальні рішення безпеки кінцевих точок включають платформи захисту кінцевих точок (EPP), виявлення та реагування на кінцеві точки (EDR), розширене виявлення та реагування (XDR) і кероване виявлення та реагування (MDR).

Розглянемо рішення Qualys Endpoint Security. У Qualys є все необхідне для виявлення, захисту та керування різноманітною мережею IT, IoT та OT кінцевих точок вашого підприємства. Використання хмарної платформи Qualys. Платформа та її обширна екосистема рішень Qualys охопить ваші кінцеві точки.

Захист активів від майбутніх атак за допомогою найповнішого в галузі виявлення поведінки, аналізу загроз і машинного навчання за допомогою рішень Qualys Multi-Vector EDR або Qualys Context XDR.

Qualys Multi-Vector EDR, який поєднує традиційні можливості EPP із багатовекторним підходом до захисту кінцевих точок, є динамічним рішенням для виявлення та реагування на базі Qualys Cloud Platform. Рішення EDR об'єднує численні контекстні вектори, як-от керування активами, виявлення вразливостей, відповідність політикам, керування виправленнями та моніторинг цілісності файлів – усе це надається за допомогою єдиного агента та хмарної служби.

Для існуючих користувачів Qualys VMDR, CyberSecurity Asset Management (CSAM) або рішень Patch Management перехід на Qualys Multi-Vector EDR з поточного рішення EDR або EPP є переконливим з трьох основних причин.

Консолідація інструментів безпеки: за допомогою Qualys Multi-Vector EDR користувачі можуть скористатися інтеграцією між рішеннями VMDR, CSAM і Patch Management. Це забезпечує більшу автоматизацію та координацію між програмами керування вразливістю (VM) і програмами виправлення та їхніми рішеннями безпеки кінцевих точок.

Threat Intelligence: Qualys Multi-Vector EDR використовує комплексну інформацію про загрози з бази даних Qualys Threat Database, яка надає інформацію про понад 185 000 уразливостей, отриманих із більш ніж 25 джерел загроз, і ця інформація постійно зростає.

Масштабованість: Qualys Multi-Vector EDR легко розгортається одним клацанням миші; Оновлення Qualys Multi-Vector EDR до Qualys Context XDR також є швидким і легким. Переходячи на Qualys Multi-Vector EDR, спеціалісти з безпеки можуть бути впевнені, що масштабування можливостей безпеки кінцевих точок і захисту від загроз у міру їх розвитку може бути безболісним, економічно ефективним і швидким.

Зниження загальної вартості володіння (TCO). Завдяки одному агенту, одній інформаційній панелі та розгортанню в один клік ваша команда з кібербезпеки отримує організоване прогнозування, запобігання, виявлення та реагування за допомогою єдиного рішення безпеки кінцевої точки.

Надання пріоритету найважливішому. Зосередьте свою реакцію на зловмисне програмне забезпечення з найбільшим потенційним впливом на ваш унікальний бізнес і конкретне IT-середовище, визначивши пріоритетність реагування на вразливості та загрози, націлені на критичні активи, позначені Qualys CyberSecurity Asset Management .

Скорочення середнього часу для відповіді (MTTR). Встановіть пріоритетність реагування на інцидент загрози, співвідносячи ступінь серйозності загрози з критичністю активів, використовуючи Qualys CyberSecurity Asset

Management і контекстуалізовані загрози.

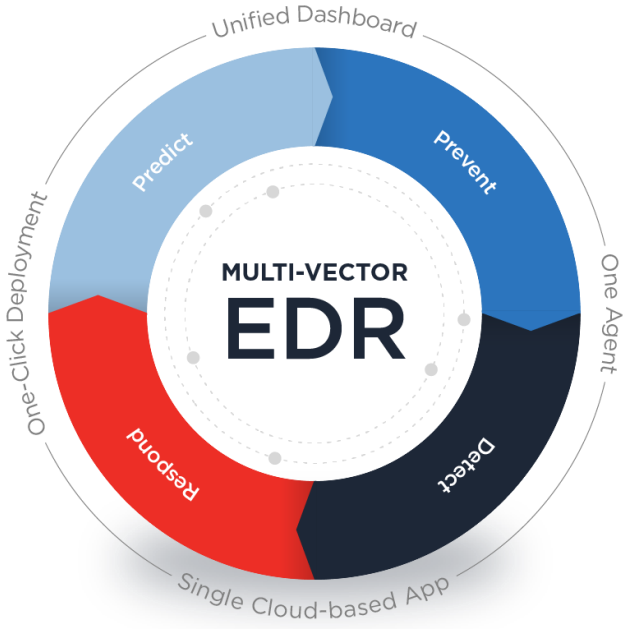

Рис. 1.8. Функції Qualys Multi-Vector EDR

Qualys Multi-Vector EDR – це динамічне рішення для виявлення та реагування на базі хмарної платформи Qualys. Рішення Qualys EDR об'єднує кілька векторів контексту, як-от керування активами, виявлення вразливостей, відповідність політикам, керування виправленнями та можливості моніторингу цілісності файлів – усе це надається за допомогою одного агента та хмарної програми.

За допомогою Qualys Multi-Vector EDR спеціалісти з безпеки досягають розширеного захисту від загроз кінцевої точки, покращеного контексту загроз і визначення пріоритетів сповіщень за нижчої загальної вартості володіння порівняно з традиційним EDR.

У той час як EDR виявляє на кінцевій точці, XDR виходить за рамки виявлення кінцевої точки та реагування на виявлення девіантної та потенційно зловмисної активності на таких пристроях, як сервери, хмари, користувачі та мережі, для додаткового контексту загроз.

Для практиків кібербезпеки, які шукають щось крім EPP та EDR, Qualys пропонує Context XDR. За допомогою Qualys Context XDR клієнти можуть

отримати контекстну пріоритезацію та отримати значущу інформацію про свої активи, що дозволить командам швидко приймати найефективніші рішення для покращеного захисту.

Надто часто рішення XDR і SIEM важко реалізувати, вони покладаються на складні інтеграції та створюють надмірне навантаження на SOC. Розуміння рівня ризиків підприємства, яке є таким важливим для операцій безпеки, рідко є рідною можливістю більшості рішень, а натомість припинено як запальна думка. Те саме стосується критичності активів під час аналізу потенційного впливу загроз, вразливостей і експлойтів на бізнес.

Qualys Context XDR вирішує ці проблеми, надаючи орієнтоване на ризик єдине скло для виявлення загроз у масштабах підприємства та реагування на інциденти. Це забезпечує видимість, контекстний пріоритет і значущу інформацію про активи, що дозволяє командам швидко приймати найефективніші рішення для покращеного захисту [9].

RMM означає Remote Monitoring and Management. Це програмні інструменти, які використовуються постачальниками IT-послуг для віддаленого керування всією інфраструктурою клієнта. Datto RMM – це повнофункціональна безпечна хмарна платформа. Він включає основні компоненти платформи кінцевих точок, що дозволяє віддалено захищати, контролювати, керувати та підтримувати кінцеві точки. Пропонуючи централізоване керування всіма кінцевими точками, включаючи ті, що розміщені на хмарних платформах, Datto дозволяє оптимізувати витрати та підвищити ефективність доставки.

Datto RMM оснащений:

автоматизоване керування виправленнями для забезпечення керування виправленнями на основі політики для захисту кінцевих точок від останніх загроз;

Моніторинг, автоматизація та створення сценаріїв, у тому числі виявлення програм-вимагачів, перевірених сторонніми розробниками, які відстежують і зменшують вплив програм-вимагачів,

Microsoft Endpoint Manager допомагає організаціям використовувати переваги хмарних засобів, зокрема розгортати всі програми, захищати й

контролювати їх, а також кінцеві пристрої та користувачів і забезпечувати безперебійну реалізацію поточних процесів [11].

Забезпечує безпеку в хмарі на кінцевих точках. Захист пристроїв користувачів від загроз здійснюється завдяки унікальним можливостям моделі нульової довіри Microsoft.

Комплексне керування програмами у Windows 11. Забезпечується автоматична підготовка, керування конфігурацією й оновлення програмного забезпечення для всіх кінцевих точок.

Максимальна користь від інвестицій. Модернізація взаємодії з користувачами завдяки хмарній телеметрії Microsoft 365, використовуючи наявні інвестиції.

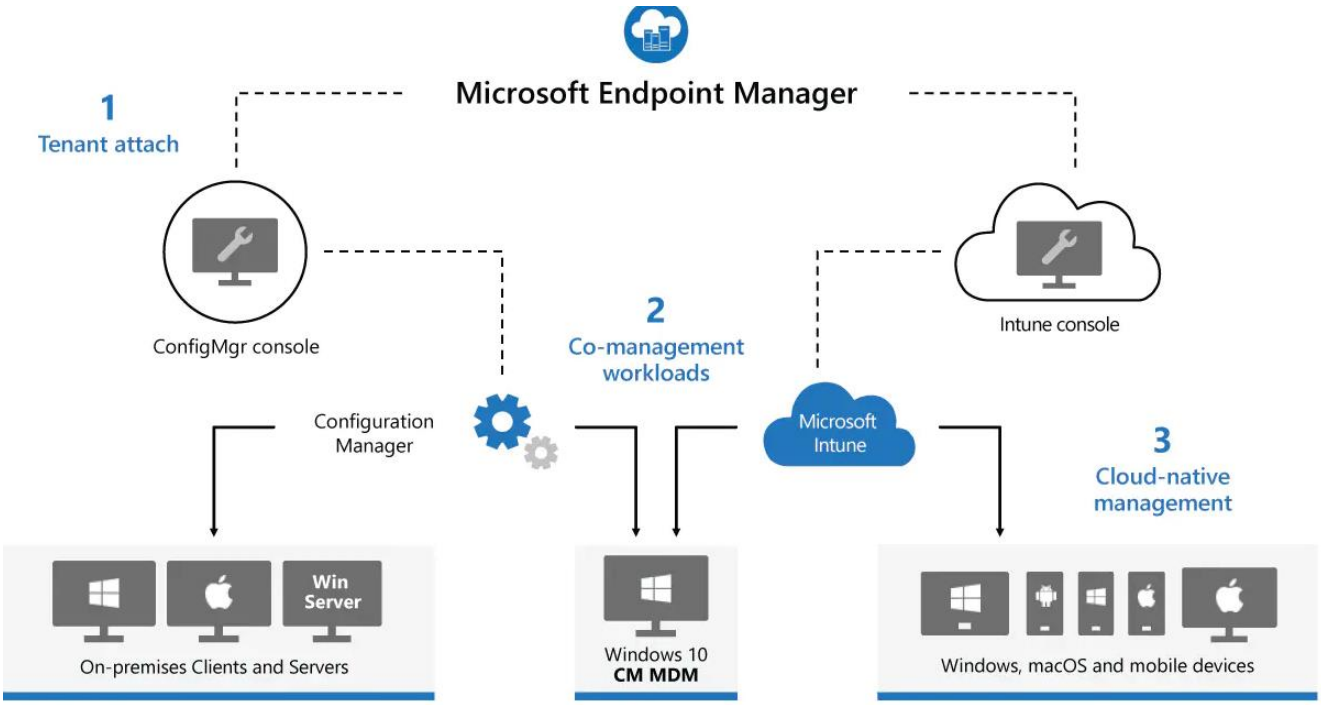

Рис. 1.9. Архітектура Microsoft Endpoint Manager [11]

На рис. 1.9 використання Microsoft Endpoint Manager зображено три етапи керування в хмарі за допомогою Configuration Manager та Intune, об’єднаних у єдине централізоване рішення для керування кінцевими точками.

Під час першого етапу користувачі, у яких є Configuration Manager, можуть користуватися всіма перевагами хмарних засобів завдяки закріпленим за клієнтом функціям. При цьому клієнтів Windows не потрібно реєструвати в Intune.

Підключивши сайт Configuration Manager до хмари, ви відразу отримаєте доступ до віддалених дій і аналітики.

Якщо організація готова до наступного кроку, то її працівники зможуть використовувати засоби спільного керування Windows у Configuration Manager й Intune. Під час другого етапу за пристроєм із Windows 10 можна стежити за допомогою Configuration Manager та систем керування мобільними пристроями.

Рекомендуємо новим клієнтам і тим, що мають нові кінцеві точки, переходити в хмару з Intune. Під час третього етапу наявні клієнти можуть поступово переносити більше робочих процесів у хмару.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ КІНЦЕВИМИ ТОЧКАМИ ОРГАНІЗАЦІЇ НА ПРИКЛАДІ MICROSOFT INTUNE

2.1. Призначення та основні функції рішення Microsoft Intune

Головним завданням фахівців з кібербезпеки є захист інформаційних ресурсів організації. Це завдання безпосередньо пов’язано з керування пристроями. Користувачі отримують і надсилають електронні листи з особистих облікових записів, переглядають веб-сайти з дому та інших місць, а також встановлюють додатки та ігри. На своїх пристроях вони хочуть отримати доступ до робочих і навчальних ресурсів, таких як електронна пошта та OneNote, і отримати до них швидкий доступ.

Керування пристроями дозволяє організаціям захищати свої ресурси та дані на різних пристроях. Використовуючи постачальника послуг керування пристроями, організація може гарантувати, що лише авторизовані люди та пристрої отримають доступ до конфіденційної інформації. Так само користувачі пристроїв можуть відчувати себе спокійно, отримуючи доступ до робочих даних зі свого телефону, оскільки вони знають, що їхній пристрій відповідає вимогам безпеки їх організації.

Багато організацій, у тому числі Microsoft, використовують рішення Intune для захисту конфіденційних даних, до яких користувачі отримують доступ із пристроїв, що належать їхнім компаніям та особам.

Microsoft Intune – це хмарне рішення для керування кінцевими точками. Воно керує доступом користувачів і спрощує керування додатками та пристроями на багатьох пристроях, включаючи мобільні пристрої, настільні комп'ютери та віртуальні кінцеві точки [6].

Ви можете захистити доступ та дані на особистих пристроях, що належать організації та користувачам. Крім того, Intune має функції відповідності вимогам та звітності, що підтримують модель безпеки Zero Trust (нульової довіри).

Microsoft Intune є хмарною службою та пропонує керування мобільними пристроями (Mobile device management, MDM) і керування мобільними додатками (Mobile application management, MAM). Ключовими завданнями будь-якого рішення MDM або MAM є [7]:

підтримання різноманітного мобільного середовища та безпечне керування пристроями iOS/iPadOS, Android, Windows і macOS;

підтвердження відповідності того, що пристрої та додатки відповідають вимогам безпеки організації;

створення політик безпеки, які допоможуть захистити дані організації на корпоративних і особистих пристроях;

використання єдиного уніфікованого гнучкого рішення, щоб забезпечити виконання цих політик і допомогти керувати пристроями, додатками, користувачами та групами;

захист інформації компанії, допомагаючи контролювати те, як співробітники отримують доступ до своїх даних і передають їх.

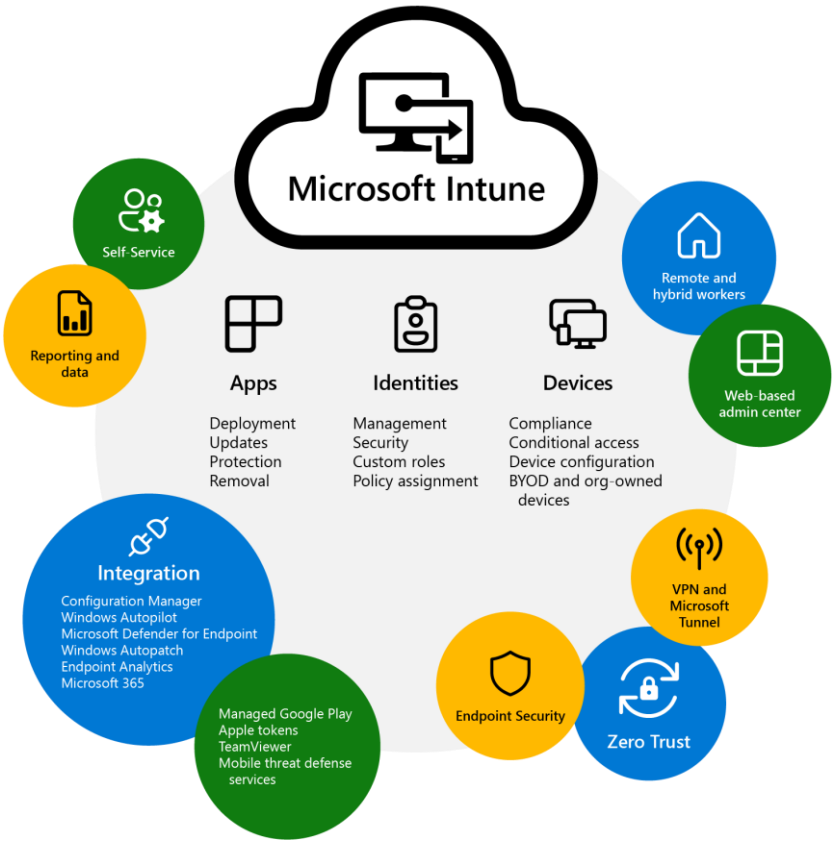

Рис. 2.1. Основні функції рішення Microsoft Intune [6]

Рішення Intune входить до складу Microsoft Azure, Microsoft 365 та інтегрується з Azure Active Directory (Azure AD). Azure AD допомагає контролювати, хто має доступ і до чого вони мають доступ.

Є кілька способів підійти до керування пристроєм. По-перше, можна керувати різними аспектами пристроїв за допомогою функцій, вбудованих в Intune. Цей підхід називається керування мобільними пристроями (MDM). Користувачі «реєструють» свої пристрої та використовують сертифікати для зв'язку з Intune. Як адміністратор ви розміщуєте додатки на пристроях, обмежуєте пристрої певною операційною системою, блокуєте особисті пристрої тощо. Якщо пристрій буде втрачено або викрадено, ви також можете видалити всі дані з пристрою.

У другому підході можна керувати додатками на пристроях. Цей підхід називається керуванням мобільними додатками (MAM). Користувачі можуть використовувати свої особисті пристрої для доступу до організаційних ресурсів. Під час відкриття додатки, наприклад електронної пошти або SharePoint, користувачам може бути запропоновано пройти автентифікацію. Якщо пристрій колись буде втрачено або викрадено, ви можете видалити всі дані організації з додатків, якими керує Intune. Також можна використовувати комбінацію MDM і MAM разом.

Microsoft Intune інтегрується з іншими продуктами та службами Microsoft, орієнтованими на керування кінцевими точками, у тому числі [6]:

Configuration Manager для локального керування кінцевими точками та Windows Server, включаючи розгортання оновлень програмного забезпечення та керування центрами обробки даних.

Ви можете використовувати Intune та Configuration Manager разом у сценарії спільного управління, використовувати підключення клієнта або використовувати обидва варіанти. За допомогою цих параметрів ви отримаєте переваги веб-центру адміністрування та зможете використовувати інші хмарні функції, доступні в Intune.

Windows Autopilot для розгортання та підготовки сучасних ОС. За

допомогою Windows Autopilot можна налаштувати нові пристрої та надсилати ці пристрої безпосередньо користувачам від виробника обладнання або постачальника пристроїв. Для наявних пристроїв ці пристрої можна створити заново, щоб використовувати Windows Autopilot та розгорнути останню версію Windows.

Endpoint analytics для видимості та створення звітів про взаємодію з кінцевими користувачами, включаючи продуктивність та надійність пристрою. Endpoint analytics можна використовувати для виявлення політик або проблем з обладнанням, що уповільнює роботу пристроїв. У ньому також містяться рекомендації, які допоможуть вам заздалегідь покращити взаємодію з кінцевими користувачами та скоротити кількість запитів до служби підтримки.

Microsoft 365 для додатків Office для підвищення продуктивності користувачів, включаючи Outlook, Teams, Sharepoint, OneDrive тощо. За допомогою Intune можна розгорнути Microsoft 365 додатків для користувачів та пристроїв в організації. Ви також можете розгорнути ці додатки під час першого входу користувачів.

Microsoft Defender for Endpoint, які допомагають підприємствам запобігати, виявляти, досліджувати загрози та реагувати на них. У Intune можна створити підключення між Intune та Microsoft Defender for Endpoint. Коли вони підключені, ви можете створювати політики, які сканують файли, виявляють загрози та повідомляють про рівні загроз Microsoft Defender for Endpoint. Ви також можете створити політики відповідності, які визначають допустимий рівень ризику. У поєднанні з умовним доступом можна заблокувати доступ до ресурсів організації для пристроїв, які не відповідають вимогам.

Windows Autopatch для автоматичного виправлення Windows, Microsoft 365 додатків для підприємств, Microsoft Edge та Microsoft Teams. Windows Autopatch – це хмарний сервіс. Він підтримує програмне забезпечення в актуальному стані, надає користувачам новітні засоби підвищення продуктивності, мінімізує локальну інфраструктуру та допомагає звільнити IT-адміністраторів, щоб зосередитись на інших проектах. Windows Autopatch використовує Microsoft

Intune для керування виправленнями для зареєстрованих Intune пристроїв або пристроїв за допомогою спільного керування (Intune + Configuration Manager).

Розглянемо питання керування кінцевими точками організації.

Пристрої, що належать організації, реєструються в Intune для керування мобільними пристроями (MDM). MDM орієнтований на пристрої, тому функції пристроїв настроюються залежно від того, кому вони потрібні. Наприклад, ви можете налаштувати пристрій так, щоб дозволити доступ до Wi-Fi, але тільки в тому випадку, якщо користувача, що увійшов, є обліковим записом організації [6].

У Intune ви створюєте політики, які налаштовують параметри компонентів і забезпечують захист. Пристрої повністю керуються вашою організацією, включаючи посвідчення користувачів, які входять до системи, встановлені додатки та дані, до яких здійснюється доступ.

Під час реєстрації пристроїв ви можете розгорнути політики під час реєстрації. Після завершення реєстрації пристрій буде готовий до використання.

Для особистих пристроїв у сценаріях використання власних пристроїв (BYOD) можна використовувати Intune для керування мобільними додатками (MAM). MAM орієнтований на користувачів, тому ці додатки захищені незалежно від пристрою, який використовується для доступу до цих даних. Основна увага приділяється додаткам, включаючи безпечний доступ до додатків та захист даних у них [6].

За допомогою MAM здійснюється [6]:

публікація мобільних додатків для користувачів;

налаштування додатків та їх автоматичне оновлення;

перегляд звітів про дані, присвячені інвентаризації додатків та їх використання.

Ви також можете використовувати MDM та MAM разом. Якщо ваші пристрої зареєстровані і є додатки, які потребують додаткової безпеки, ви також можете використовувати політики захисту додатків MAM.

Розглянемо, як здійснюється захист даних на будь-якому пристрої.

За допомогою Intune можна захистити дані на керованих пристроях

(зареєстрованих у Intune) та на некерованих пристроях (не зареєстрованих у Intune). Intune може ізолювати дані організації від персональних даних. Ідея полягає в тому, щоб захистити інформацію про компанію, контролюючи спосіб доступу користувачів до інформації та спільного доступу до неї.

Для пристроїв, що належать до організації, потрібен повний контроль над пристроями, особливо безпека. Коли пристрої реєструються, вони отримують правила та параметри безпеки.

На пристроях, зареєстрованих у Intune, ви можете [6]:

створювати та розгортати політики, які налаштовують параметри безпеки, встановлюють вимоги до паролів, розгортають сертифікати тощо;

використовувати мобільні служби захисту від загроз для сканування пристроїв, виявлення загроз та усунення загроз;

переглядати дані та звіти, які вимірюють відповідність параметрам безпеки та правилам;

використовувати умовний доступ, щоб дозволити доступ до ресурсів, додатків та даних організації лише керованим та відповідним пристроям;

видаляти дані організації у разі втрати або крадіжки пристрою.

Для власних пристроїв користувачі можуть не захотіти, щоб їх IT-адміністратори мали повний контроль. Щоб забезпечити підтримку гібридного робочого середовища, надайте користувачам варіанти. Наприклад, користувачі реєструють свої пристрої, якщо їм потрібний повний доступ до ресурсів організації. Або, якщо ці користувачі хочуть отримати доступ тільки до Outlook або Microsoft Teams, використовуйте політики захисту додатків, що вимагають багатофакторної автентифікації (MFA) [6].

На пристроях, які використовують керування додатками:

використовуйте мобільні служби захисту від загроз для захисту даних додатків сканування пристроїв, виявлення загроз та оцінки ризику;

необхідно заборонити копіювання та вставку даних організації в особисті додатки;

використовуйте політики захисту додатків у додатках та на некерованих

пристроях, зареєстрованих у сторонньому або партнерському MDM;

використовуйте умовний доступ, щоб обмежити додатки, які можуть отримувати доступ до електронної пошти та файлів організації;

видаляйте дані організації у додатках.

Intune допомагає організаціям підтримувати співробітників, які можуть працювати з будь-якого місця. Існують функції, які можна налаштувати, які дозволяють користувачам підключатися до організації, де б вони не були.

Використання Windows Hello для бізнесу замість паролів. Windows Hello для бізнесу допомагає захиститись від фішингових атак та інших загроз безпеці. Це також допомагає користувачам швидше та простіше виконувати вхід до своїх пристроїв та додатків.

Windows Hello для бізнесу замінює паролі за допомогою ПІН-коду або біометрії, наприклад відбитків пальців, розпізнавання обличь. Ці біометричні дані зберігаються локально на пристроях і ніколи не надсилаються на зовнішні пристрої або сервери.

Створення підключення VPN для віддалених користувачів. Політики VPN надають користувачам безпечний віддалений доступ до мережі організації. Використовуючи спільних партнерів VPN-підключень, включаючи Check Point, Cisco, Microsoft Tunnel, NetMotion, Pulse Secure тощо, ви можете створити політику VPN з параметрами мережі. Коли політика буде готова, ви розгорнете її для користувачів та пристроїв, яким потрібно віддалено підключитися до мережі.

У політиці VPN можна використовувати сертифікати для перевірки автентичності підключення VPN. У разі використання сертифікатів користувачам не потрібно вводити імена користувачів та паролі.

Створення з'єднання Wi-Fi для локальних користувачів. Для користувачів, яким потрібно підключитися до локальної мережі організації, можна створити політику Wi-Fi з параметрами мережі. Ви можете підключитися до певного SSID, вибрати метод автентифікації, використовувати проксі-сервер і багато іншого. Ви також можете налаштувати політику автоматичного підключення до Wi-Fi, коли пристрій знаходиться в зоні дії [6].

У політиці Wi-Fi можна використовувати сертифікати для автентифікації Wi-Fi підключення. У разі використання сертифікатів користувачам не потрібно вводити імена користувачів та паролі.

Коли політика буде готова, ви розгорнете її для локальних користувачів та пристроїв, яким необхідно підключитися до локальної мережі.

Увімкнення єдиного входу до додатків та служб. При увімкненні єдиного входу користувачі можуть автоматично входити до додатків і служб за допомогою облікового запису Azure AD організації, включаючи деякі мобільні партнерські додатки для захисту від загроз.

Це означає таке [6]:

на пристроях Windows єдиний вхід автоматично вбудований і використовується для входу в додатки та веб-сайти, які використовують Azure AD для перевірки автентичності, включаючи Microsoft 365 додатків. Ви також можете включити єдиний вхід до VPN і Wi-Fi політики;

на пристроях iOS/iPadOS та macOS ви можете використовувати модуль єдиного входу Microsoft Enterprise для автоматичного входу в додатки та веб-сайти, які використовують Azure Active Directory (AD) для перевірки автентичності, включаючи додатки Microsoft 365;

на пристрої Android можна використовувати бібліотеку автентифікації Microsoft (Microsoft Authentication Library, MSAL), щоб увімкнути єдиний вхід до Android.

2.2. Високорівнева архітектура рішення Microsoft Intune

Microsoft Intune є частиною пакету Enterprise Mobility + Security (EMS) від Microsoft. Intune інтегрується з Azure AD, щоб контролювати, хто має доступ і до чого вони можуть отримати доступ (рис. 2.2). Рішення також інтегрується з Azure Information Protection для захисту даних. Його можна використовувати з пакетом продуктів Microsoft 365. Наприклад, можна розгорнути Microsoft Teams, OneNote та інші додатки Microsoft 365 на пристроях. Ця функція дозволяє користувачам

організації працювати продуктивно на всіх своїх пристроях, захищаючи при цьому інформацію організації за допомогою створених політик.

Високорівнева архітектура (рис. 2.2) показує варіанти інтеграції Microsoft Intune у корпоративне середовище Azure з Azure AD.

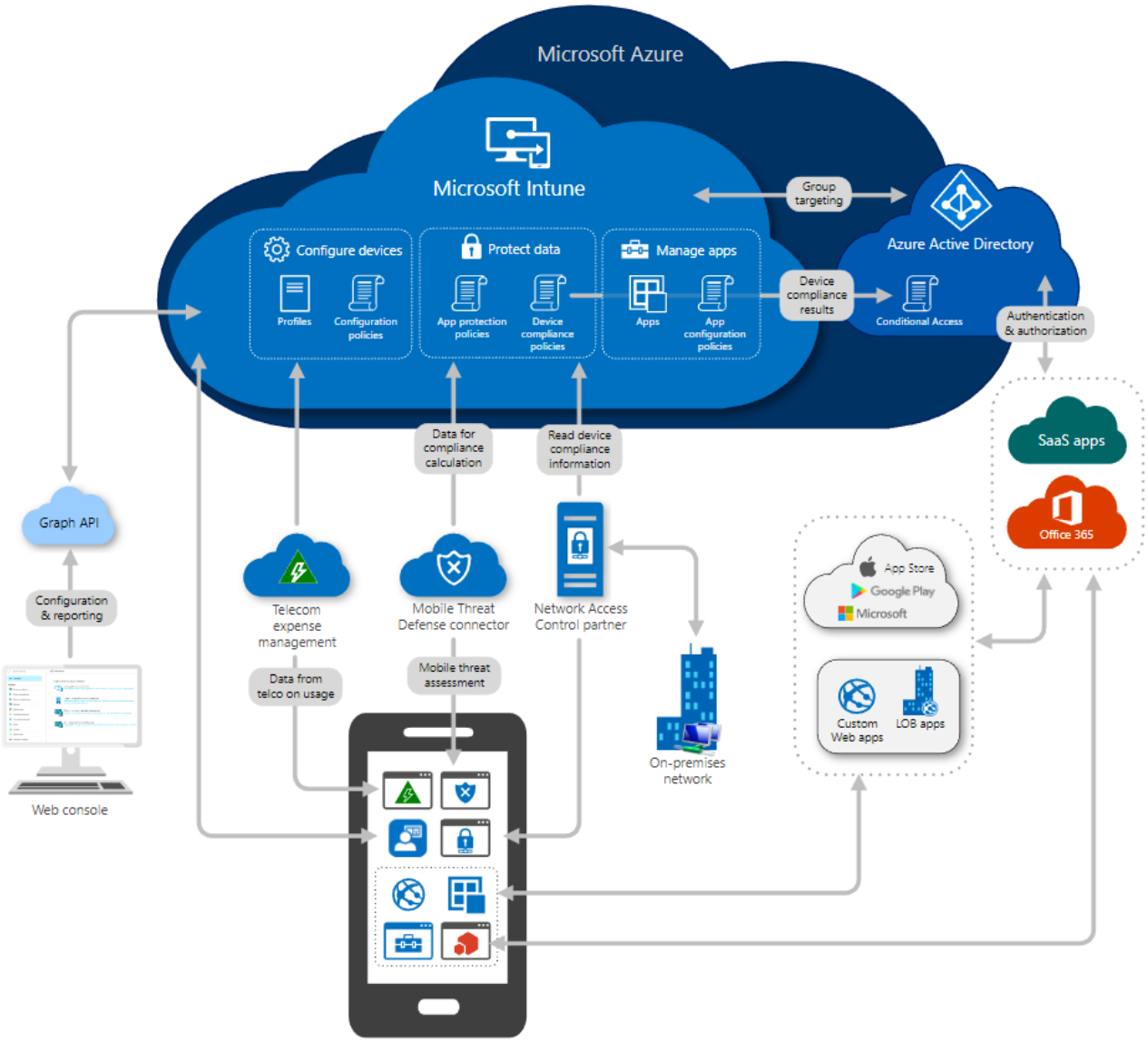

Рис. 2.2. Високорівнева архітектура Microsoft Intune [2]

Розглянемо зміст технології управління кінцевими точками організації та їх захисту на прикладі Microsoft Intune [8] більш детальніше.

В Intune адміністратор керує пристроями, використовуючи підхід, який підходить саме даній організації. Для пристроїв, що належать організації, може знадобитися повний контроль над пристроями, включаючи налаштування, функції

та безпеку. У такому підході пристрої та користувачі цих пристроїв «реєструються» в Intune. Після реєстрації вони отримають встановлені правила та налаштування через політики, налаштовані в Intune. Наприклад, адміністратор може встановити вимоги до пароля та PIN-коду, створити з’єднання VPN, налаштувати захист від загроз тощо.

Користувачі можуть не захотіти, щоб адміністратори їхніх організацій мали повний контроль щодо персональних пристроїв або пристроїв, які можна взяти з собою (BYOD). У такому підході користувачам надаються варіанти. Наприклад, користувачі реєструють свої пристрої, якщо хочуть отримати повний доступ до ресурсів організації. Або, якщо цим користувачам потрібен лише доступ до електронної пошти чи Microsoft Teams, то застосовуються політики захисту додатків, які потребують багатофакторної автентифікації (MFA) для використання цих додатків.

Коли пристрої зареєстровано та керовано в Intune, адміністратори можуть [8]:

переглядати зареєстровані пристрої та отримати перелік пристроїв, які мають доступ до ресурсів організації;

налаштовувати пристрої так, щоб вони відповідали встановленим стандартам безпеки. Наприклад, необхідно заблокувати зламані пристрої;

надсилати сертифікати на пристрої, щоб користувачі могли легко отримувати доступ до корпоративної мережі Wi-Fi або використовувати VPN для підключення до мережі;

переглядати звіти про відповідність користувачів і пристроїв;

видаляти дані організації, якщо пристрій загублено, викрадено або більше не використовується.

Таким чином, рішення Microsoft Intune – хмарний сервіс у корпоративному середовищі, яких підвищує ефективність роботи співробітників та захищає корпоративні дані. Технологія управління кінцевими пристроями організації та їх захисту, яка реалізована в Microsoft Intune дозволяє керувати мобільними пристроями, додатками та комп'ютерами з хмари, зводячи до мінімуму проблеми

із захистом корпоративних даних та запобігаючи витоку інформації.

2.3. Зміст керування життєвим циклом мобільних пристроїв та додатків Microsoft Intune

Усі пристрої, якими ви керуєте, мають життєвий цикл (рис. 2.3). Intune може допомогти керувати цим життєвим циклом: від реєстрації, налаштування та захисту до виведення пристрою з експлуатації, коли він більше не потрібен. Ось приклад: iPad, придбаний вашою компанією, спочатку має бути зареєстрований у вашому обліковому записі Microsoft Intune, щоб ваша компанія могла ним керувати; потім його потрібно налаштувати відповідно до потреб вашої компанії; потім, дані, які зберігаються на ньому користувачем, повинні бути захищені; і, нарешті, коли цей iPad більше не потрібен, ви повинні вийти з експлуатації або стерти всі конфіденційні дані на ньому [12].

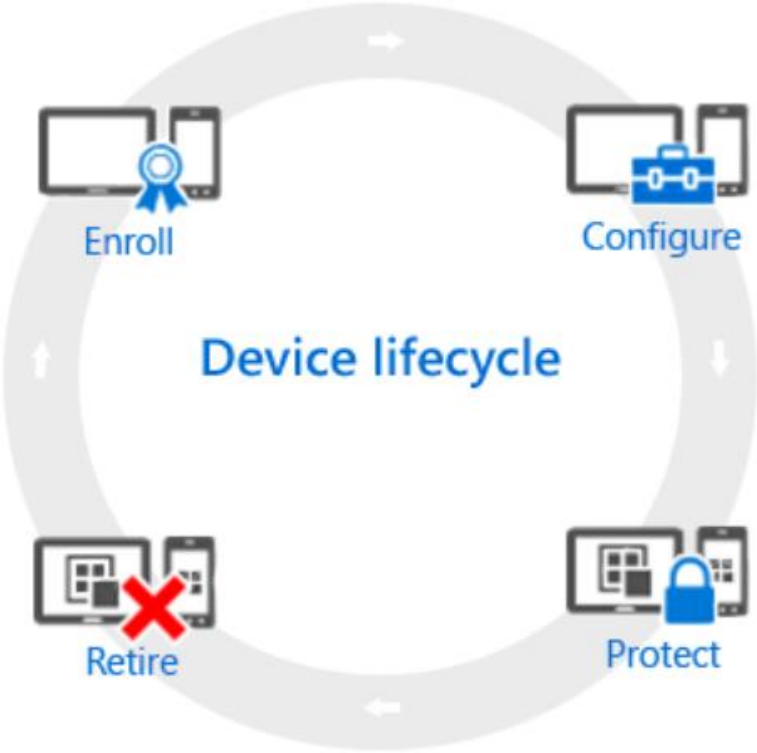

Рис. 2.3. Життєвий цикл мобільних пристроїв [12]

Реєстрація. Сучасні стратегії керування мобільними пристроями (MDM) стосуються різноманітних телефонів, планшетів і ПК (iOS/iPadOS, Android, Windows і macOS). Якщо вам потрібно мати можливість керувати пристроєм, що зазвичай буває для корпоративних пристроїв, спочатку потрібно налаштувати реєстрацію пристрою. Ви також можете керувати ПК з Windows, зареєструвавши їх у Intune (MDM).

Налаштування. Зареєструвати пристрої – це лише перший крок. Щоб скористатися перевагами всіх пропозицій Intune і переконатися, що ваші пристрої безпечні та відповідають стандартам компанії, ви можете вибрати з широкого спектру політик. Вони дозволяють налаштувати майже всі аспекти роботи керованих пристроїв. Наприклад, чи повинні користувачі мати пароль на пристроях, які мають дані компанії? Ви можете вимагати один. У вас є корпоративний Wi-Fi? Ви можете автоматично налаштувати його. Ось типи доступних параметрів конфігурації [12]:

конфігурація пристрою. Ці політики дозволяють налаштовувати функції та можливості пристроїв, якими ви керуєте. Наприклад, ви можете вимагати використання пароля на телефонах Android або вимкнути використання камери на iPhone;

доступ до ресурсів компанії. Коли ви надаєте своїм користувачам доступ до своєї роботи на своїх особистих пристроях, це може поставити перед вами проблеми. Наприклад, як переконатися, що всі пристрої, яким потрібен доступ до корпоративної електронної пошти, налаштовано правильно? Як можна переконатися, що користувачі можуть отримати доступ до мережі компанії за допомогою VPN-з'єднання без необхідності знати складні налаштування? Intune може допомогти зменшити цей тягар шляхом автоматичного налаштування пристроїв, якими ви керуєте, для доступу до загальних ресурсів компанії;

політики керування ПК Windows (з клієнтським програмним забезпеченням Intune). Хоча реєстрація ПК з Windows у Intune дає вам більше можливостей керування пристроями, Intune продовжує підтримувати керування ПК з Windows за допомогою клієнтського програмного забезпечення Intune.

Захист. У сучасному світі IT захист пристроїв від несанкціонованого доступу є одним із найважливіших завдань, які ви виконуєте. Окрім елементів на етапі налаштування життєвого циклу пристрою, Intune надає такі можливості, які допомагають захистити пристрої, якими ви керуєте, від несанкціонованого доступу чи зловмисних атак [12]:

багатофакторна автентифікація. Додавання додаткового рівня автентифікації до входу користувачів може допомогти зробити пристрої ще більш безпечними. Багато пристроїв підтримують багатофакторну автентифікацію, яка вимагає другого рівня автентифікації, наприклад телефонного дзвінка чи текстового повідомлення, перш ніж користувачі зможуть отримати доступ;

параметри Windows Hello для бізнесу. Windows Hello для бізнесу – це альтернативний метод входу, який дозволяє користувачам використовувати жест , наприклад відбиток пальця або Windows Hello, щоб входити без пароля;

політики захисту ПК з ОС Windows (з клієнтським програмним забезпеченням Intune). Коли ви керуєте комп’ютерами Windows за допомогою клієнтського програмного забезпечення Intune, доступні політики, які дають змогу контролювати параметри захисту кінцевої точки, оновлення програмного забезпечення та брандмауера Windows на комп’ютерах, якими ви керуєте.

Виключення зі складу. Коли пристрій втрачено або викрадено, коли його потрібно замінити або коли користувачі переходять на інше місце, зазвичай настає час вилучити або стерти пристрій. Це можна зробити кількома способами, зокрема скинути налаштування пристрою, вилучити його з-під керування та видалити на ньому корпоративні дані.

Життєвий цикл додатків (рис. 2.4) Microsoft Intune починається з додавання додатку та проходить додаткові етапи, доки ви не видалите додаток. Розуміючи ці етапи, ви матимете деталі, необхідні для початку роботи з керуванням додатками в Intune.

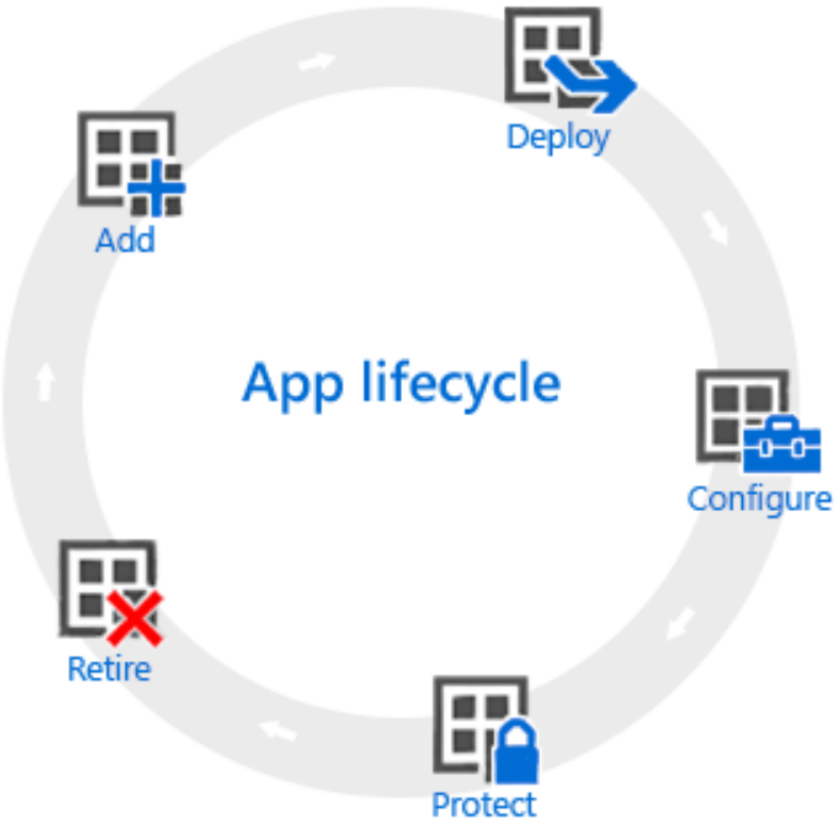

Рис. 2.4. Життєвий цикл додатків [13]

Додавання додатка. Першим кроком у розгортанні додатка є додавання додатків, якими ви хочете керувати та призначати їх, до Intune. Хоча ви можете працювати з багатьма різними типами додатків, основні процедури однакові. За допомогою Intune ви можете додавати різні типи додатків, зокрема додатки, написані власними силами (бізнес-програми), додатки з магазину, вбудовані додатки та додатки в Інтернеті.

Розгортання. Додавши додаток до Intune, ви зможете призначити його користувачам і пристроям, якими ви керуєте. Intune полегшує цей процес, і після розгортання додатка ви можете відстежувати успішність розгортання з Intune на порталі. Крім того, у деяких магазинах додатків, наприклад у магазинах додатків Apple і Windows, ви можете купувати ліцензії на додатки оптом для своєї компанії. Intune може синхронізувати дані з цими сховищами, щоб ви могли розгортати та відстежувати використання ліцензій для цих типів програм прямо з консолі адміністрування Intune.

Налаштування. У рамках життєвого циклу додатка регулярно випускаються нові версії додатків. Intune надає інструменти для легкого оновлення додатків, які ви розгорнули, до новішої версії. Крім того, ви можете налаштувати додаткові функції для деяких додатків, наприклад [13]:

політики конфігурації додатків для iOS/iPadOS надають параметри для сумісних додатків для iOS/iPadOS, які використовуються під час запуску додатка. Наприклад, додаток може вимагати певних налаштувань брендингу або імені сервера, до якого вона має підключитися;

керовані політики браузера допомагають налаштувати параметри для Microsoft Edge, який замінює браузер пристрою за замовчуванням і дозволяє обмежити веб-сайти, які можуть відвідувати ваші користувачі.

Захист. Intune пропонує багато способів захисту даних у додатках. Основні методи захисту [13]:

умовний доступ, який контролює доступ до електронної пошти та інших служб на основі умов, які ви визначаєте. Умови включають типи пристроїв або відповідність політиці відповідності пристроїв, яку ви розгорнули;

політика захисту додатків працює з окремими програмами, щоб захистити дані компанії, які вони використовують. Наприклад, ви можете обмежити копіювання даних між некерованими додатками та додатками, якими ви керуєте, або ви можете запобігти запуску додатків на пристроях, які були зламані або рутовані.

Виключення зі складу. Згодом імовірно, що додатки, які ви розгорнули, застаріють і їх потрібно буде видалити. Intune спрощує видалення додатків.

Таким чином, рішення Microsoft Intune – хмарний сервіс у корпоративному середовищі, яких підвищує ефективність роботи співробітників та захищає корпоративні дані. Технологія управління кінцевими пристроями організації та їх захисту, яка реалізована в Microsoft Intune дозволяє керувати мобільними пристроями, додатками та комп'ютерами з хмари, зводячи до мінімуму проблеми із захистом корпоративних даних та запобігаючи витоку інформації.

3 ТЕХНОЛОГІЯ УПРАВЛІННЯ КІНЦЕВИМИ ТОЧКАМИ ОРГАНІЗАЦІЇ ТА ЇХ ЗАХИСТОМ

3.1. Порядок застосування центру адміністрування Microsoft Endpoint Manager

Microsoft Intune, який є частиною Microsoft Endpoint Manager, забезпечує хмарну інфраструктуру, хмарне керування мобільними пристроями (MDM), хмарне керування мобільними програмами (MAM) і хмарне керування ПК для організації. Intune допомагає переконатися, що пристрої, додатки та дані компанії відповідають вимогам безпеки вашої компанії. Ви можете контролювати, які вимоги потрібно перевірити та що станеться, якщо ці вимоги не виконуються. У центрі адміністрування Microsoft Endpoint Manager можна знайти службу Microsoft Intune, а також інші налаштування, пов’язані з керуванням пристроєм. Розуміння функцій, доступних в Intune, дозволяє виконувати різні завдання керування мобільними пристроями (MDM) і керування мобільними додатками (MAM) [14].

Microsoft Endpoint Manager – це єдина інтегрована платформа для керування всіма кінцевими точками. Цей центр адміністрування Microsoft Endpoint Manager інтегрує ConfigMgr і Microsoft Intune.

Розглянемо центр адміністрування Microsoft Endpoint Manager. Інтерфейс центра адміністрування Microsoft Endpoint Manager показано на рис. 3.1.

Коли ви відкриваєте Microsoft Endpoint Manager, служба відображається на панелі вашого браузера. Деякі з перших робочих навантажень, які ви можете використовувати в Intune, включають пристрої, додатки, користувачів і групи. Робоче навантаження – це просто частина послуги. Коли ви вибираєте робоче навантаження, це вікно відкривається як повна сторінка. Інші панелі висуваються з правого боку панелі, коли вони відкриваються, і закриваються, щоб відкрити попередню панель.

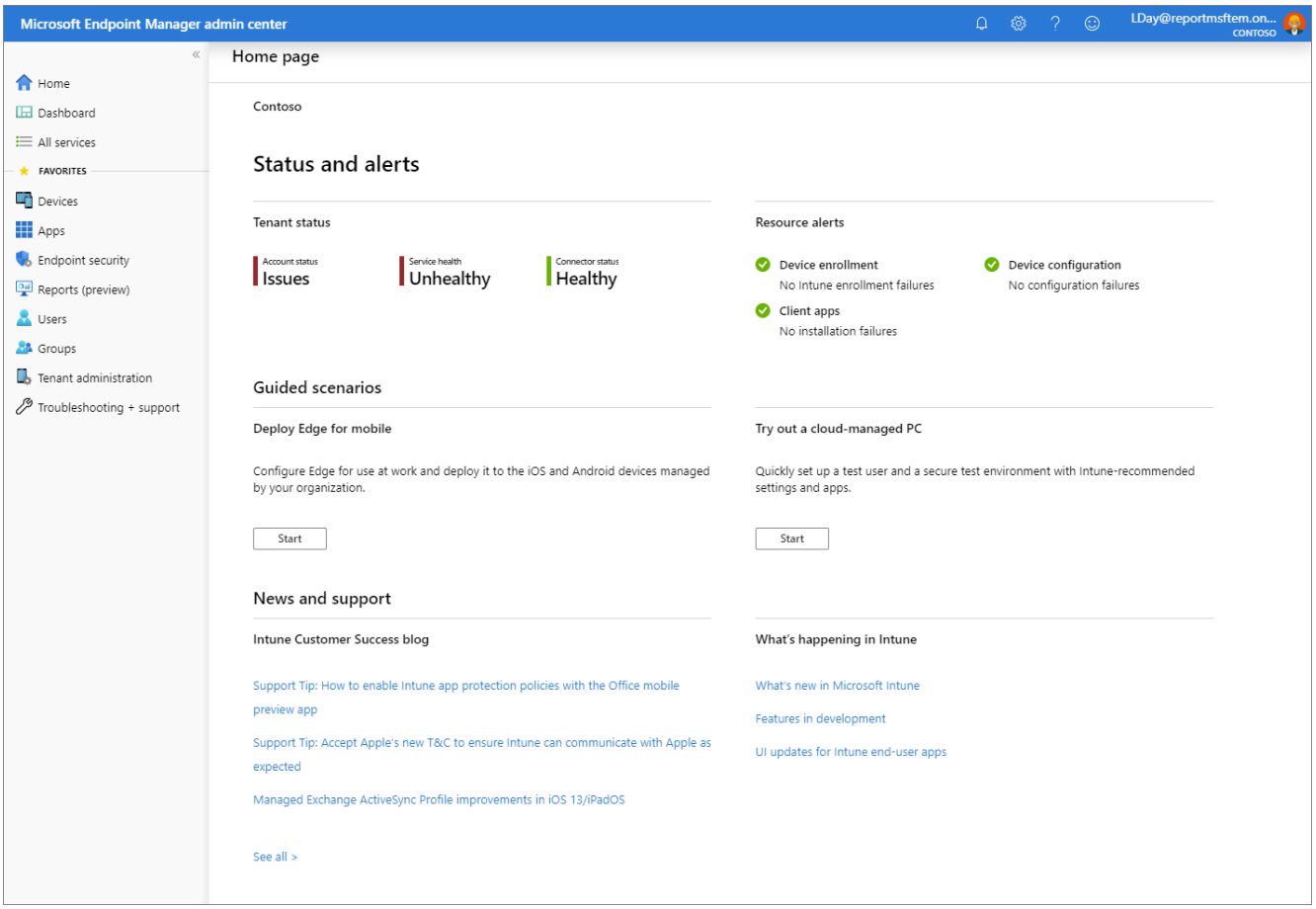

Рис. 3.1. Інтерфейс Microsoft Endpoint Manager [14]

За замовчуванням, коли ви відкриваєте Microsoft Endpoint Manager, ви побачите панель домашньої сторінки. Ця панель надає загальний візуальний знімок стану клієнта та статусу відповідності, а також інші корисні відповідні посилання.

На панелі навігації виберіть *Інформаційна панель*, щоб відобразити загальні відомості про пристрої та клієнтські додатки у вашому клієнті Intune. Якщо ви починаєте роботу з новим клієнтом Intune, у вас ще не буде зареєстрованих пристроїв.

Intune дає змогу керувати пристроями (рис. 3.2) та додатками ваших співробітників, зокрема тим, як вони отримують доступ до даних вашої компанії. Щоб користуватися цією службою керування мобільними пристроями (MDM), пристрої потрібно спочатку зареєструвати в Intune. Коли пристрій зареєстровано, йому видається сертифікат MDM. Цей сертифікат використовується для зв’язку зі службою Intune.

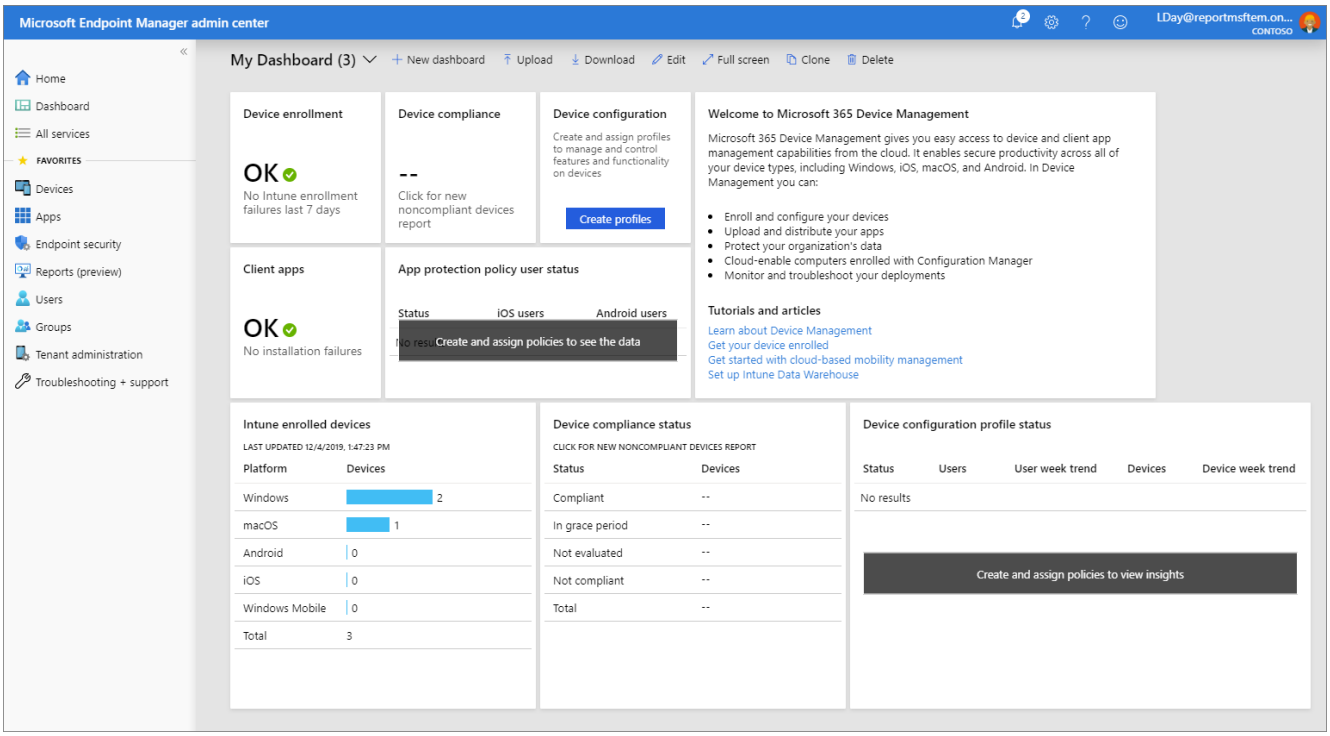

Рис. 3.2. Панель керування додатками [14]

Є кілька способів зареєструвати пристрої вашої робочої сили в Intune. Кожен метод залежить від власника пристрою (особистого чи корпоративного), типу пристрою (iOS/iPadOS, Windows, Android) і вимог до керування (скидання, зв'язок, блокування). Однак перш ніж увімкнути реєстрацію пристрою, потрібно налаштувати інфраструктуру Intune. Зокрема, для реєстрації пристрою потрібно налаштувати повноваження MDM [14].

На панелі «Пристрої – огляд» є кілька вкладок, на яких можна переглянути підсумок таких станів і сповіщень:

Статус реєстрації. Перегляньте відомості про зареєстровані пристрої Intune за платформою та помилками реєстрації.

Сповіщення про реєстрацію – дізнайтеся більше про непризначені пристрої за платформою.

Статус відповідності – переглядайте стан відповідності на основі пристрою, політики, налаштувань, загроз і захисту. Крім того, на цій панелі представлено список пристроїв без політики відповідності.

Статус конфігурації – перегляд статусу конфігурації профілів пристрою, а

також розгортання профілю.

Статус оновлення програмного забезпечення. Перегляньте візуальне зображення стану розгортання для всіх пристроїв і для всіх користувачів.

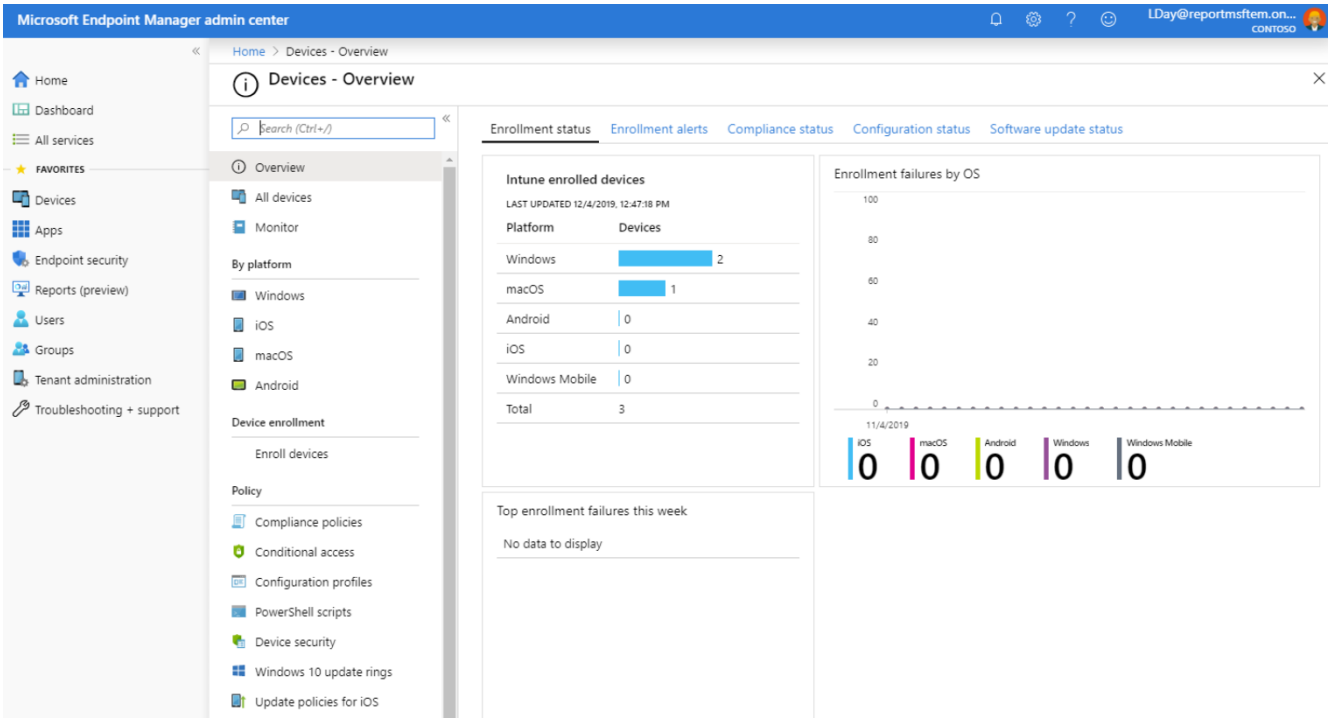

Рис. 3.3. Панель «Пристрої – огляд» [14]

Як адміністратор ви можете використовувати Microsoft Intune для керування клієнтськими додатками, якими користуються працівники вашої компанії. Ця функція є доповненням до керування пристроями та захисту даних. Одним із пріоритетів адміністратора є забезпечення доступу кінцевих користувачів до програм, необхідних для роботи. Крім того, ви можете призначити та керувати додатками на пристроях, які не зареєстровані в Intune. Intune пропонує низку можливостей, які допоможуть вам отримати потрібні додатки на потрібних пристроях.

Розглянемо порядок налаштування центра адміністрування Microsoft Endpoint Manager. Центр адміністрування Microsoft Endpoint Manager дозволяє налаштовувати та налаштовувати вигляд порталу.

Інформаційна панель для відображення загальних відомостей про пристрої та клієнтські програми у вашому клієнті Intune (рис. 3.4). Інформаційні панелі

дають змогу створити цілеспрямоване й упорядковане подання в центрі адміністрування Microsoft Endpoint Manager. Використовуйте інформаційні панелі як робочий простір, де можна швидко запускати завдання для повсякденних операцій і контролювати ресурси. Створюйте спеціальні інформаційні панелі, наприклад, на основі проектів, завдань або ролей користувачів. Центр адміністрування Microsoft Endpoint Manager пропонує інформаційну панель за замовчуванням як початкову точку. Ви можете редагувати інформаційну панель за замовчуванням, створювати та налаштовувати додаткові інформаційні панелі, а також публікувати та ділитися інформаційними панелями, щоб зробити їх доступними для інших користувачів [14].

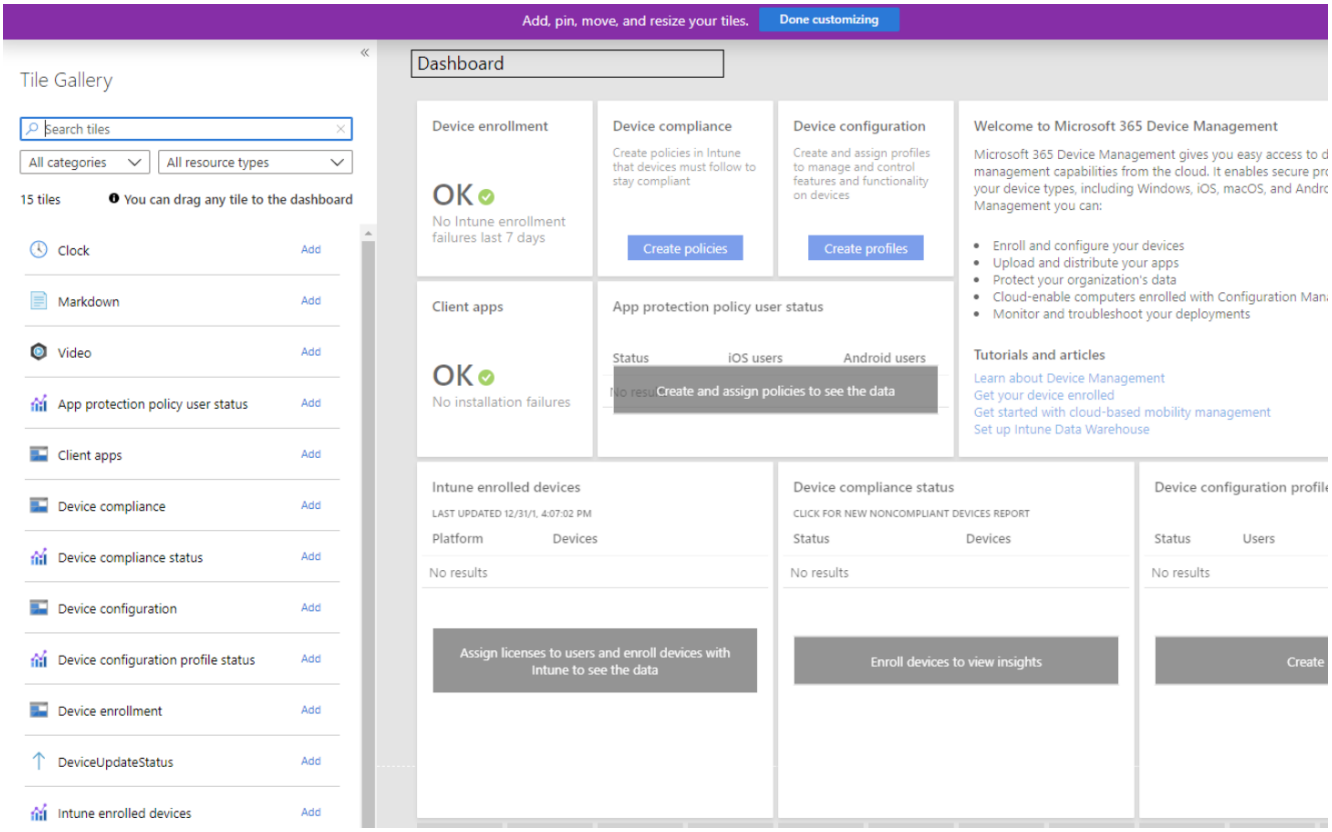

Рис. 3.4. Центр адміністрування Microsoft Endpoint Manager [14]

Щоб змінити поточну інформаційну панель, виберіть *Редагувати*. Якщо ви не хочете змінювати інформаційну панель за замовчанням, ви також можете створити нову інформаційну панель. Створення нової інформаційної панелі дає вам порожню приватну інформаційну панель із галереєю плиток, яка дозволяє

додавати або змінювати порядок плиток. Ви можете знайти плитки за категоріями або типами ресурсів. Ви також можете шукати певні плитки. Виберіть *Моя інформаційна панель*, щоб вибрати будь-яку з наявних настроюваних інформаційних панелей.

3.2. Концепції застосування рішення Microsoft Intune

Розглянемо відмінності застосування рішення Intune for Education для галузі освіти. Так, Intune for Education дозволяє викладачам і студентам бути продуктивними, захищаючи дані закладу освіти. Intune for Education (рис. 3.5) базується на службі Microsoft Intune, хмарній службі керування корпоративною мобільністю (EMM) [15].

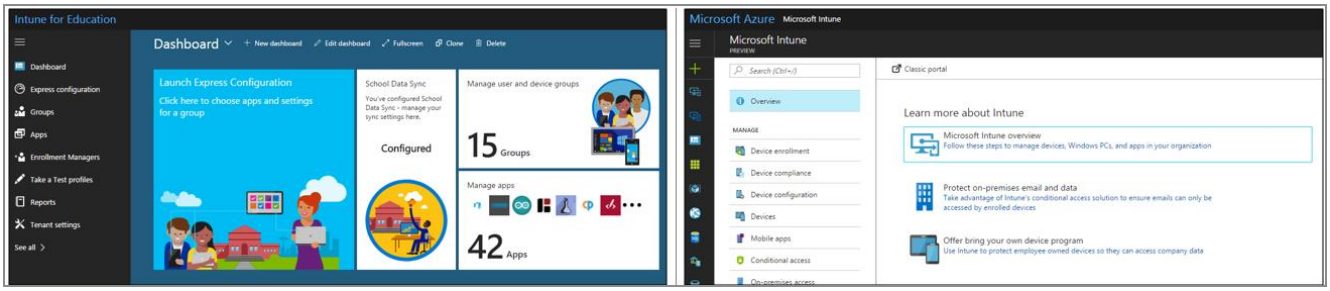

Рис. 3.5. Інтерфейс рішення Intune for Education [15]

Intune for Education дозволяє керувати пристроями Windows 10 і iOS/iPadOS за допомогою повних можливостей MDM, доступних в Intune. Повний досвід керування пристроями дозволяє керувати пристроями Windows, iOS/iPadOS та Android.

Intune for Education можна використовувати як окремо, так і в гармонії з повним керування пристроєм, доступним у Intune. Його також можна використовувати разом з іншими інструментами, доступними в Microsoft Education, що спрощує використання Intune для освіти з іншими корисними освітніми інструментами від Microsoft.

За допомогою Intune і Intune for Education ви можете [15]:

керувати мобільними пристроями, які ваші співробітники та студенти використовують для доступу до даних;

керувати мобільними додатками, до яких ваші користувачі мають доступ щодня;

захистити свою організаційну інформацію, допомагаючи контролювати те, як ваші користувачі отримують доступ до неї та обмінюються нею.

переконайтеся, що пристрої та додатки відповідають вимогам безпеки.

Розглянемо відмінності застосування рішення Intune for Government для урядових організацій. Intune for Government – це додаток та платформа керування мобільними пристроями, розроблена для забезпечення безпеки, конфіденційності та контролю, відповідності та прозорості. Він відповідає потребам федерального, штатного та місцевого уряду США за допомогою фізичних і логічних мережевих ізольованих екземплярів Azure. Ці екземпляри призначені для уряду США з усіма клієнтськими даними, додатками та апаратним забезпеченням, які проживають у континентальній частині Сполучених Штатів [16].

Intune for Government включає фізично ізольований екземпляр Microsoft Intune, який підтримує вимоги безпеки та відповідності, критичні для уряду США. Intune – це хмарна сервіс керування корпоративною мобільністю (EMM), яка є основою для Intune for Government. Державні установи матимуть доступ до тих самих функцій, які доступні комерційним клієнтам. До них належать сертифікати відповідності FedRAMP і Міністерства оборони, а також управління перевіреними особами США [16].

За допомогою Intune for Government ви можете керувати пристроями Windows 10, iOS і Android, використовуючи всі можливості MDM, доступні в Intune. Наприклад, ви можете [16]:

керувати мобільними пристроями державних службовців, які використовуються для доступу до даних;

керувати мобільними додатками, до яких мають доступ ваші користувачі;

захищати державні дані, контролюючи спосіб доступу користувачів до них і обміну ними;

переконатися, що пристрої та програми відповідають вимогам безпеки.

3.3. Рекомендації щодо управління кінцевими точками організації та їх захисту

Загальний стан і безпека кожного пристрою впливають на загальну організацію, і якщо кінцева точка не справна, це може становити значний ризик для безпеки. Наприклад, IDC виявив, що кінцеві точки, такі як ноутбуки, настільні ПК або мобільні пристрої, є джерелом 70% успішних зломів. Оскільки ці кінцеві точки часто служать шлюзами для порушення безпеки, надійне керування кінцевими точками є важливим для сучасних організацій. Керування кінцевими точками включає дії з надання, моніторингу, захисту, виправлення та оновлення кінцевих точок для захисту IT-середовища.

Завдяки політиці безпеки кінцевих точок організації можуть забезпечити захист корпоративних активів і даних. Щоб розробити цю політику, компаніям слід запитати себе, який рівень безпеки потрібен для їхніх конкретних кінцевих точок, а також чи повинні інструменти безпеки кінцевих точок тримати пристрої сильно заблокованими чи забезпечувати менший захист, щоб надати співробітникам деяку особисту свободу.

Розглянемо основні рекомендації з керування та захисту кінцевих точок організації.

Оскільки все більше співробітників працюють у дорозі чи віддалено, використання BYOD і несанкціонованих пристроїв IoT стає все більш поширеним. Щоб зрозуміти, що підключається до їхніх мережевих ресурсів, IT-команди повинні почати з *інвентаризації всіх пристроїв*. Зауважте, що деякі пристрої можуть ніколи не торкатися самої корпоративної мережі, а натомість спрямовуватися прямо в хмару для інтеграції з програмами SaaS. У цьому випадку може знадобитися брокер безпеки доступу до хмари або еквівалент.

Необхідно отримати *повну видимість* усіх кінцевих пристроїв, які підключаються до корпоративних програм і даних, перш ніж робити що-небудь

інше – зрештою, неможливо захистити те, про що ви не знаєте.

Наступним кроком є розуміння *способів роботи цих різних кінцевих точок*. Задокументуйте, до яких серверів і додатків вони підключаються, а також коли та які дані вони обмінюються та збирають. Також важливо вказати, як програмне забезпечення *оновлюється* на цих кінцевих точках і як часто. Нарешті, оцініть, які *ризики безпеці* кожна кінцева точка потенційно може представляти, а також їхній вплив на бізнес у разі порушення або компрометації.

Після ідентифікації та профілювання кінцевих точок необхідно зрозуміти, як можна використовувати існуючі продукти безпеки для їх захисту. Антивірус наступного покоління все ще широко розгортається, оскільки він використовує комбінацію порівняння сигнатур для виявлення відомих загроз та штучного інтелекту та машинного навчання для нових загроз. Ця технологія перетворилася на виявлення та реагування на кінцеву точку, яка забезпечує оповіщення консолі, звітування, реагування на інциденти безпеки та розширене покриття місцезнаходження, а також забезпечує інтеграцію сторонніх розробників. Це необхідний механізм захисту для керування пристроями кінцевих користувачів.

Однак зауважте, що доведеться розробити інший план для пристроїв, які належать працівникам. Для цього може знадобитися інсталяція агента на їхніх пристроях або використання VPN перед отриманням доступу до активів компанії.

Необхідно дотримуватися принципу найменшого привілею доступу з використанням нульової довіри. Оскільки в організаціях поширюється цілий ряд кінцевих точок, принцип нульової довіри «ніколи не довіряй, завжди перевіряй» має вирішальне значення для контролю поверхні ризику та забезпечення точного доступу співробітників до корпоративних активів.

Завдяки централізованому контролю політиками ці кінцеві точки постійно перевіряються на відповідність стандартним конфігураціям пристроїв, запитам на доступ, тимчасовим підвищенням привілеїв, відкликанню привілеїв і прав доступу. Завдяки добре розробленій структурі ідентифікації та керування доступом більшість із цих завдань можна виконувати автоматизовано, а дорогоцінне людське втручання можна зарезервувати для аномальних випадків,

які цього вимагають.

Необхідно забезпечувати безпеку IoT пристроїв. IoT охоплює широкий спектр пристроїв, від сканерів райдужної оболонки до розумних колонок і датчиків ядерної енергії. Наведені нижче найкращі методи безпеки зазвичай застосовуються до всіх пристроїв IoT:

Дотримання рамок безпеки. Конкретні найкращі методи безпеки кінцевих точок Інтернету речей залежатимуть від впливу та ризику пристрою. Дотримання системи безпеки є важливим першим кроком. Наприклад, структура NIST Interagency/Internal Report 8259 застосовується до виробників IoT.

Як покупець, переконайтеся, що постачальники дотримуються цієї основи, що забезпечує надійну основу для оцінки ризиків інвентаризації апаратного та програмного забезпечення, стандартизованого та доступного журналювання подій, інтегрованого керування ідентифікацією та ключами, стандартизованого керування конфігурацією та централізованих можливостей усунення вразливостей. Це також підтверджує, що постачальники несуть відповідальність за своєчасне розкриття інформації у разі порушення або вразливості.

Необхідно забезпечувати парольну політику пристроїв IoT. Одним із найбільш використовуваних атак проти пристроїв IoT є комбінації імені користувача та пароля виробника за замовчуванням, які часто можна знайти в Інтернеті. IT-команди повинні перевірити пароль кожного пристрою та змінити його на щось унікальне.

Виявлення пристроїв Інтернету речей і застосування політики. Пристрої IoT набагато частіше, ніж ноутбуки, будуть встановлені без дозволу. Таким чином, проведення регулярних аудитів пристроїв IoT є обов’язковим. Будь-які виявлені нові або невідомі пристрої мають бути заблоковані за замовчуванням, і має бути введено процес ескалації та автентифікації. Маючи цю інформацію, IT-спеціалісти можуть відстежити власника пристрою, щоб не тільки забезпечити легітимність, але й змінити паролі за замовчуванням, перш ніж буде надано подальший доступ до мережі.

Отже, забезпечення безпеки кінцевих точок організації залишається такою

ж важливою, як і раніше. Вважаємо, що запропоновані рекомендації забезпечать хорошу базову позицію пристрою кінцевого користувача та елементарну кібергігієну.

Також, у сучасному ландшафті загроз, який постійно змінюється, спеціалісти з кібербезпеки повинні залишатися пильними, навіть після впровадження рекомендацій та застосування методів безпеки кінцевих точок. Оскільки все більше організацій переглядають, як часто співробітникам потрібно бути в офісі, а запровадження Інтернету речей продовжує стрімко розвиватися, більше кінцевих точок залишатиметься поза мережею та піддаватиметься підвищеному ризику атак.

ВИСНОВКИ

В роботі проаналізовано проблему управління кінцевими точками корпоративних інформаційних систем, визначено його мету та завдання.

Керування кінцевими точками – це практика автентифікації та контролю прав доступу кінцевих пристроїв до мережі та застосування політик безпеки, які запобігають будь-яким зовнішнім або внутрішнім загрозам, спричиненим цим доступом. Власники мереж зазвичай використовують програмне забезпечення для керування безпекою кінцевих точок.

Безпека кінцевої точки – це практика захисту даних і робочих процесів, пов'язаних із пристроями, які підключаються до керованої мережі. Терміни захист кінцевої точки, безпека кінцевої точки та платформа захисту кінцевої точки описують рішення безпеки з централізованими рішеннями. Платформи захисту кінцевих точок захищають такі кінцеві точки, як сервери, робочі станції, мобільні пристрої та робочі навантаження, від загроз кібербезпеці.

Проведено аналіз існуючих технологій управління кінцевими точками організації. Рішення для захисту кінцевих точок можна розглянути за трьома категоріями: традиційний підхід, гібридний підхід або хмарна модель. Загальні рішення безпеки кінцевих точок включають платформи захисту кінцевих точок (EPP), виявлення та реагування на кінцеві точки (EDR), розширене виявлення та реагування (XDR) і кероване виявлення та реагування (MDR).

Досліджено методи та засоби управління кінцевими точками організації на прикладі Microsoft Intune. Microsoft Intune – це хмарне рішення для керування кінцевими точками. Microsoft Intune пропонує керування мобільними пристроями (MDM) і керування мобільними додатками (MAM).

Визначено призначення, основні функції та склад рішення з управління кінцевими точками організації на прикладі Microsoft Intune. Рішення Microsoft Intune входить до складу Microsoft Azure, Microsoft 365 та інтегрується з Azure AD. Azure AD допомагає контролювати, хто має доступ і до чого вони мають

доступ. Високорівнева архітектура показує варіанти інтеграції Microsoft Intune у корпоративне середовище Azure з Azure AD.

В роботі розглянуто зміст керування життєвим циклом мобільних пристроїв та додатків в Microsoft Intune.

Розглянуто порядок застосування центру адміністрування Microsoft Endpoint Manager. Microsoft Endpoint Manager – це єдина інтегрована платформа керування кінцевими точками для керування всіма кінцевими точками. Цей центр адміністрування Microsoft Endpoint Manager інтегрує ConfigMgr і Microsoft Intune.

Розглянемо відмінності застосування рішень Intune for Education для галузі освіти та Intune for Government для урядових організацій.

Розроблено рекомендації фахівцям з кібербезпеки щодо застосування технології управління кінцевими точками організації.

Таким чином, правильна реалізація управління кінцевими точками корпоративних інформаційних систем має забезпечити ефективний захист корпоративних даних та кібербезпеку інформаційної системи організації в цілому.

ПЕРЕЛІК ПОСИЛАНЬ

1. 2022 Endpoint security report. Adaptiva. [Електронний ресурс] – Режим доступу: https://adaptiva.com/resources/report/endpoint-security-report.

2. Matt Bromiley. 2022 SANS Protects: The Endpoint. Whitepaper, April 2022. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/dam/en/us/products/collateral/security/endpoint-security/sans-protects-endpoint-wp.pdf.

3. What Is Endpoint Management? Trellix. [Електронний ресурс] – Режим доступу: https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-security-management.html.

4. What Is Endpoint Security? Trellix. [Електронний ресурс] – Режим доступу: https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-security.html.

5. What is Endpoint Security? April 13, 2022. [Електронний ресурс] – Режим доступу: https://www.prplbx.com/resources/blog/what-is-endpoint-security/.

6. Microsoft Intune securely manages identities, manages apps, and manages devices. Article 10/31/2022. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune.

7. Device management overview. Microsoft. Article, 09/01/2022. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-device-management.

8. Microsoft Intune is an MDM and MAM provider for your devices. Article, 01/09/2022. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-gb/mem/intune/fundamentals/what-is-intune.

9. Qualys Context XDR (Extended Detection & Response) [Електронний ресурс] – Режим доступу: https://www.qualys.com/apps/extended-detection-response/.

10. Effortless & Effective Endpoint Detection and Response for MSPs. [Електронний ресурс] – Режим доступу: https://www.datto.com/products/datto-edr/.

11. Microsoft Endpoint Manager [Електронний ресурс] – Режим доступу: https://www.microsoft.com/uk-ua/security/business/microsoft-endpoint-manager.

12. Overview of the Microsoft Intune mobile device management (MDM) lifecycle. Article 25/01/2022. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-gb/mem/intune/fundamentals/device-lifecycle.

13. Overview of the app lifecycle in Microsoft Intune. Article 30/03/2022. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-gb/mem/intune/apps/app-lifecycle.

14. Tutorial: Walkthrough Intune in Microsoft Endpoint Manager. Article 17/12/2021. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-gb/mem/intune/fundamentals/tutorial-walkthrough-endpoint-manager.

15. How is Intune for Education different from the full device management experience in Intune? Article 25/06/2020. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-gb/mem/intune/fundamentals/introduction-intune-education.

16. What is Intune for Government? Article 13/01/2022. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-gb/mem/intune/fundamentals/introduction-intune-government.

17. Туриченко Є. А. Технологія управління кінцевими точками організації та їх захисту на прикладі Microsoft Intune. Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». Державний Університет Телекомунікацій. 27 жовтня 2022. Тези доповідей. С. 38-41. [Електронний ресурс] – Режим доступу: https://dut.edu.ua/uploads/p_2121_20358827.pdf.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)