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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

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

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека_
(назва)

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

Виконав: здобувач вищої освіти групи БСДМ-61
ДИГАС Максим
(ПРІЗВИЩЕ, Ім'я)

Керівник: БОРСУКОВСЬКИЙ Юрій
к.т.н, доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: ТУРОВСЬКИЙ Олександр
(ПРІЗВИЩЕ, Ім'я)

Київ 2024

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

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___”_____ 2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дигасу Максиму Віталійовичу
(прізвище, ім’я, по батькові)

1. Тема кваліфікаційної роботи:
«Технологія управління кінцевими точками організації та їх захисту на прикладі Microsoft Intune»
керівник кваліфікаційної роботи: БОРСУКОВСЬКИЙ Юрій, к.т.н., доцент,
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145.

2. Строк подання студентом кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
Технологія управління кінцевими точками організації та їх захисту на прикладі Microsoft Intune
наукова та технічна література, нормативні документи
міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження актуальності проблеми захисту хмарних сервісів
2. Аналіз можливостей та функціоналу Microsoft Intune
3. Розробка рішення з імплементація архітектури Zero Trust

5. Перелік ілюстративного матеріалу:
Презентація PowerPoint

6. Дата видачі завдання 19.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Дослідження актуальності проблеми захисту хмарних сервісів для управління та захисту кінцевими точками	19.10.2023 р.	
2.	Аналіз наукової та технічної літератури за темою кваліфікаційної роботи.	22.10.2023 р.	
3.	Аналіз можливостей та функціоналу Microsoft Intune	27.10. 2023р.	
4.	Методи захисту та засоби управління кінцевими точками	03.11.2023 р.	
5.	Розробка рішення з імплементація архітектури Zero Trust	15.11.2023 р.	
6.	Оформлення результатів дослідження. Проходження плагіату.	26.11.2023 р.	
7.	Підготовка доповіді до захисту.	15.12.2023 р.	

Здобувач(ка) вищої освіти _____ Максим ДИГАС
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій Борсуковський
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

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

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Дигас М.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)

За спеціальністю 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Технологія управління кінцевими точками організації та їх захисту на прикладі Microsoft Intune»

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(*підпис*) (*Ім'я, ПРІЗВИЩЕ*)

Висновок керівника кваліфікаційної роботи

Здобувач ***ДИГАС Максим*** обрав тему роботи, метою якої було дослідити зміст технології контролю доступу до мережі організацій. Перелік використаних джерел свідчить про вміння здобувача розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***ДИГАС Максим*** показав гарну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***ДИГАСА Максима*** на оцінку **«добре»** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Юрій БОРСУКОВСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*
"____" _____ 2023 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач(ка) ***ДИГАС Максим*** допускається до захисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну магістерську роботу

студента Дигаса Максим

на тему: «Технологія управління кінцевими точками організації та їх захисту на прикладі Microsoft Intune»

Актуальність:

Наразі глобальний ринок праці проходить фазу динамічної трансформації: з одного боку на драйверами змін є катаклізми (пандемічні обмеження, збройні конфлікти та ін.), а з іншого боку цьому сприяє технологічний розвиток і відповідні адаптивні зміни у політиці роботодавців.

За даними WFH Research, наразі 12,7% повноштатних працівників працюють з дому, що свідчить про швидку нормалізацію віддалених робочих середовищ. Одночасно значна кількість, а саме 28,2% працівників, вибрали гібридну робочу модель, що об'єднує роботу як з дому, так і в офісі, надаючи гнучкість і зберігаючи рівень фізичної присутності на робочому місці. Прогнози компаній вказують на те, що до 2025 року приблизно 32,6 млн американців будуть працювати віддалено, що становитиме приблизно 22% робочої сили, що свідчить про поступовий, проте постійний перехід до віддалених форм роботи

Позитивні сторони:

1. На основі проведеного аналізу в роботі встановлено, що хмарні рішення для забезпечення цифрової та інформаційної безпеки є невід'ємною частиною сучасного бізнесу, і вони допомагають організаціям захищати свої активи та зберігати конфіденційність даних в умовах зростаючих цифрових загроз.

2. Проведено дослідження хмарних рішень з управління та захисту кінцевими точками корпоративних мереж.

3. Розроблено рішення з імплементація архітектури Zero Trust для ідентифікаторів і кінцевих точок за допомогою інструментів Microsoft Intune.

Недоліки:

1. У магістерській роботі доцільно було б розглянути більше функціоналу для управління та безпеки кінцевих точок.

2. Бажано було розглянути ситуацію, як блокувати або видаляти дані на втрачених або вкрадених пристроях

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку «**добре»**, а здобувач **ДИГАС Максим** - присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Рецензент: Олександр ТУРОВСЬКИЙ

д.т.н., професор *підпис* *Ім'я, ПРІЗВИЩЕ*

РЕФЕРАТ

Текстова частина магістерської роботи: 116 сторінок, 86 рисунків, 86 джерел.

Об'єкт дослідження – хмарні сервіси для управління та захисту кінцевими точками кросплатформенної корпоративної мережі.

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

Мета дослідження – розробка рішень з управління кінцевими точками організації та їх захисту з використанням технологій Microsoft Intune.

Методи дослідження – мультилокальний інформаційний пошук, аналітичні висновки, моделювання кросплатформенної корпоративної мережі на засадах технологій Microsoft Intune.

В роботі досліджені хмарні рішення з забезпечення управління та безпеки кінцевими точками корпоративної мережі підприємства.

Встановлено, що серед існуючих наразі рішень, одним з перспективних та ефективних є система Microsoft Intune.

У якості оптимізаційного рішення для безпеки корпоративної мережі на базі системи Microsoft Intune розроблена політика Zero Trust. Результати тестування корпоративної мережі з використанням Microsoft 365 Defender підтверджують, що впровадження політики Zero Trust на базі Microsoft Intune призвело до значного підвищення рівня безпеки контуру (на 76%).

Галузь використання – кібербезпека корпоративної інформаційної системи.

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, ЗАХИСТ КІНЦЕВИХ ТОЧОК, МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК, ТЕХНОЛОГІЯ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК

ABSTRACT

Master's thesis: 116 pages, 86 figures, 86 sources.

Object of research – cloud services for cross-platform endpoint management and protection in the corporate network.

Subject of research – endpoint management technology for organization and its protection using Microsoft Intune as an example.

The aim of research – development of solutions for endpoint management and protection using Microsoft Intune technologies.

Research methods – multi-local information search, analytical conclusions, modeling of cross-platform corporate network based on Microsoft Intune technologies.

The paper explores cloud solutions for managing and securing endpoints in the corporate network of an enterprise.

It is established that among the currently available solutions, one of the promising and effective systems is Microsoft Intune.

As an optimization solution for corporate network security based on the Microsoft Intune system, a Zero Trust policy has been developed. The test results of the corporate network using Microsoft 365 Defender confirm that the implementation of the Zero Trust policy based on Microsoft Intune has led to a significant increase in the security level of the perimeter (by 76%).

Field of use – cybersecurity of corporate information system.

CORPORATE INFORMATION SYSTEM, CYBER SECURITY, ENDPOINT PROTECTION, METHODS AND MEANS OF MANAGEMENT OF ENDPOINT PROTECTION FOR TECHNICS

ЗМІСТ

ВСТУП 9
1 ОГЛЯД ХМАРНИХ РІШЕНЬ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЙ 13
1.1 Архітектура IT-структури організації 13
1.2 Концепція цифрової та інформаційної безпеки IT-структури організації 18
1.3 Огляд хмарних рішень для забезпечення цифрової та інформаційної безпеки IT-структури організації 24
Висновок до 1 розділу 34
2 ОГЛЯД MICROSOFT INTUNE 36
2.1 Загальна характеристика Microsoft Intune 36
2.2 Архітектура Microsoft Intune 40
2.3 Загальна концепція Zero Trust 55
Висновок до 2 розділу 62
3 ІМПЛЕМЕНТАЦІЯ АРХІТЕКТУРИ ZERO TRUST ДЛЯ ІДЕНТИФІКАТОРІВ І КІНЦЕВИХ ТОЧОК ЗА ДОПОМОГОЮ ІНСТРУМЕНТІВ MICROSOFT INTUNE 63
3.1 Процедура розгортання Microsoft Intune 63
3.2 Архітектура Zero Trust 71
3.3 Розгортання та тестування архітектури Zero Trust для ідентифікаторів і кінцевих точок за допомогою інструментів Microsoft Intune 77
Висновок до 3 розділу 94
ВИСНОВОК 95
ПЕРЕЛІК ПОСИЛАНЬ 96

ВСТУП

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

Актуальність. Наразі глобальний ринок праці проходить фазу динамічної трансформації: з одного боку на драйверами змін є катаклізми (пандемічні обмеження [1] – [3], збройні конфлікти [4] – [6] та ін.), а з іншого боку цьому сприяє технологічний розвиток і відповідні адаптивні зміни у політиці роботодавців [7] – [9].

За даними WFH Research [10], наразі 12,7% повноштатних працівників працюють з дому, що свідчить про швидку нормалізацію віддалених робочих середовищ. Одночасно значна кількість, а саме 28,2% працівників, вибрали гібридну робочу модель, що об'єднує роботу як з дому, так і в офісі, надаючи гнучкість і зберігаючи рівень фізичної присутності на робочому місці. Прогнози Upwork [11] вказують на те, що до 2025 року приблизно 32,6 млн американців будуть працювати віддалено, що становитиме приблизно 22% робочої сили, що свідчить про поступовий, проте постійний перехід до віддалених форм роботи. За опитуваннями Buffer [12] 98% працівників висловили бажання працювати віддалено, принаймні частково, що відображає зростаючий інтерес працівників до можливостей гнучкості, автономії та балансу між роботою і особистим життям, які надає віддалена робота. При цьому опитування Indeed [13] вказує 93% роботодавців, які планують продовжувати проведення співбесід інтерв'ю віддалено, що свідчить про готовність адаптуватися до віртуальних методів і сигналізує про визнання віддаленої роботи як стійкого варіанту. Більше того, за даними Apollo Technical LLC [14] вже зараз близько 16% компаній вже повністю функціонують у віддаленому режимі та не мають фізичних офісів. Ці компанії є піонерами в парадигмі віддаленої роботи, відзначаючи можливість таких моделей та відкриваючи шлях для інших.

Визначені тенденції демонструють, що модель організації віддаленої роботи стає все більш стійкою та сприймається роботодавцями як перспективна система організації робочого простору у майбутньому, зокрема за даними Forbes [15] доцільною вважають форму дистанційної праці роботодавці IT-сфери, галузі маркетингу, галузі обліку та аудиту та ін. При цьому формується актуальна проблематика, коли віддалені працівники прагнуть використовувати власні засоби до доступу захищених мереж роботодавця. Така ситуація створює відповідні загрози: за опитуваннями OpenVPN [16] 73% роботодавців сприймають віддалених працівників як загрозу кібербезпеці організації; за даними Gitnux [17] 60% віддалених працівників використовують незахищені особисті пристрої для доступу до мережі свого роботодавця, разом з тим, після переходу на віддалену роботу кількість атак програм-вимагачів зросла на 20%, фішингових атак електронної пошти на 80%, а комплексних кібератак на 67%; при цьому Lancashire Business View [18] фіксує, що 63% підприємств зазнали витоку даних через віддалену роботу співробітників. Все це призводить до необхідності запровадження відповідних рішень, які б сприяли організації продуктивної, гнучкої, а головне безпечної віддаленої роботи, адже саме тому, як вказують Digital [19], майже 60% компаній використовують програмне забезпечення для моніторингу для відстеження віддалених співробітників. Хоча ці інструменти можуть підвищити продуктивність і підзвітність, вони також створюють питання конфіденційності, підкреслюючи необхідність прозорості та згоди на їх використання.

Відтак, формується актуальне завдання у дослідженні, розгортанні та оптимальному використанні програмних засобів і рішень, що сформують збалансований, кросплатформенний та безпечний робочий простір. Провідним рішенням у цьому контексті є Microsoft Intune [20].

Microsoft Intune – це інструментальна хмарна платформа, розроблена компанією Microsoft, призначена для управління кінцевими точками в

корпоративних інформаційних системах (End-Point Management, EPM). Ця платформа надає функціональність централізованого контролю, адміністрування та захисту різноманітних кінцевих пристроїв, включаючи персональні комп'ютери, мобільні пристрої та інші пристрої, що використовуються в організаційному контексті. Microsoft Intune дозволяє організаціям встановлювати та керувати політиками безпеки, віддалено надавати доступ до корпоративних ресурсів, впроваджувати оновлення програмного забезпечення, контролювати використання даних та забезпечувати загальний рівень безпеки для кінцевих точок. Ця платформа також дозволяє інтегрувати рішення для моніторингу та реагування на загрози, що підвищує загальний рівень безпеки організації [20] – [22].

Мета дослідження – розробка рішень з управління кінцевими точками організації та їх захисту з використанням технологій Microsoft Intune.

Завдання дослідження:

- виконати огляд хмарних рішень забезпечення цифрової та інформаційної безпеки організацій;
- дослідити Microsoft Intune;
- розробити рішення з імплементація архітектури Zero Trust для ідентифікаторів і кінцевих точок за допомогою інструментів Microsoft Intune.

Ступінь наукової розробки. Наразі, використання хмарної платформи Microsoft Intune не має достатнього наукового супроводу, серед нечисленних релевантних праць варто виділити J. Trillas Sánchez, J. Kujo, U. H. Park. Проте вони вирішують обмежені аспекти використання досліджуваної платформи та не містять системних рекомендацій щодо її розгортання. Відтак, в даній роботі вперше пропонується інтеграція системного підходу до розгортання архітектури Zero Trust.

Практичне значення одержаних результатів. Використання архітектури Zero Trust в політиці End-Point Management дозволить забезпечити формування безпечної та продуктивної структури організацій.

1 ОГЛЯД ХМАРНИХ РІШЕНЬ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЙ

1.1 Архітектура IT-структури організації

Архітектура IT-структури організації – це визначення та організація компонентів, які створюють інформаційну технологічну інфраструктуру організації. Ця архітектура включає в себе апаратне та програмне забезпечення, комунікаційні системи, бази даних, застосунки, мережі, процеси, політики безпеки та інші складові, необхідні для підтримки бізнес-процесів та завдань організації [23] – [25] – Рисунок 1.

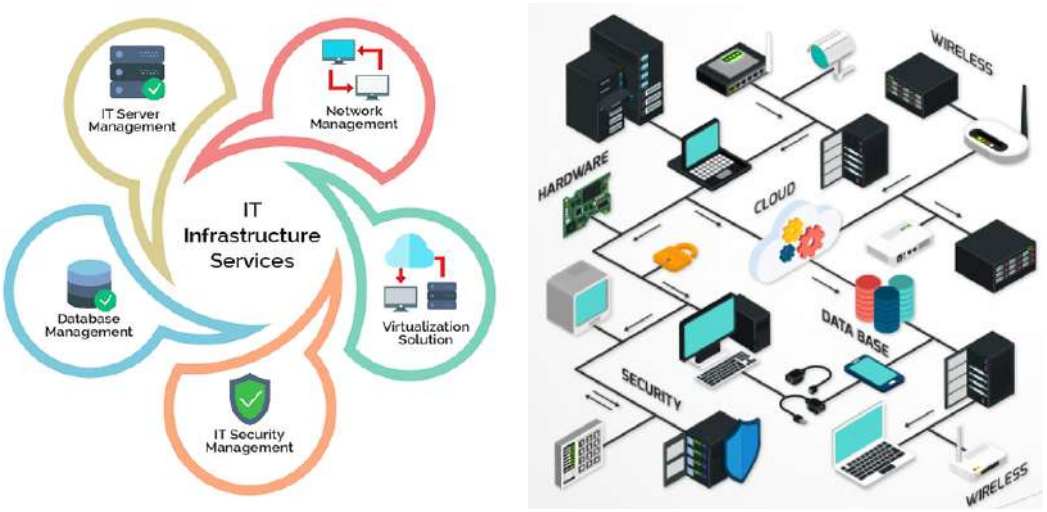


Рисунок 1 – Концептуальна схема IT-інфраструктури підприємства [23] – [25]

Основні аспекти архітектури IT-структури організації включають такі елементи [26] – [28] (Рисунок 1, Рисунок 2):

1. Апаратне забезпечення (Hardware) – сервери, комп'ютери, мережеве обладнання, сховища даних та інші фізичні компоненти, які використовуються для обробки та зберігання інформації.
2. Програмне забезпечення (Software) – операційні системи, додатки, системи управління базами даних та інші програмні рішення, які дозволяють виконувати різні завдання та функції.

3. Мережі та комунікації (Networks and Communications) – комутатори, маршрутизатори, кабельну і бездротову інфраструктуру, яка забезпечує зв'язок між різними пристроями та користувачами.
4. Безпека (Security) – заходи та політики, спрямовані на захист інформації від несанкціонованого доступу та загроз, включаючи аутентифікацію, авторизацію, шифрування і інші методи безпеки.
5. Системи управління (Management Systems) – IT-системи для моніторингу та управління ресурсами та процесами, що забезпечують роботу IT-інфраструктури.
6. Бізнес-застосунки (Business Applications) – додатки та програми, що використовуються для підтримки бізнес-процесів та функцій організації.
7. Бази даних (Databases) – системи для зберігання та управління даними, що використовуються в різних бізнес-процесах.

Архітектура IT-структури організації розробляється з урахуванням потреб, цілей та бізнес-вимог організації і спрямована на оптимізацію використання IT-ресурсів та забезпечення їхньої ефективної та безпечної роботи [26] – [28].

Разом з розвиненою інформаційною інфраструктурою підприємства, що використовує різні цифрові засоби, обладнання та системи виникає проблематика кросплатформенності [29] – [31] (Рисунок 3).

Проблематика кросплатформенності в IT-інфраструктурі підприємства є неоднозначним завданням, викликаним різноманіттям операційних систем та пристроїв, які використовуються в корпоративному середовищі. Зазначені виклики полягають у вирішенні різниці в операційних системах, таких як Windows, macOS, Linux, а також операційних систем для мобільних пристроїв, зокрема Android та iOS.

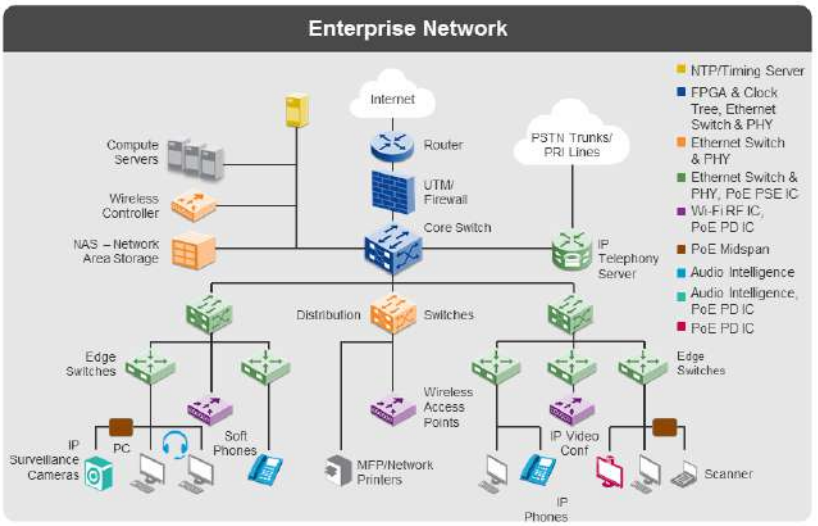


Рисунок 2 – Типова архітектура IT-інфраструктури підприємства [26] – [28]

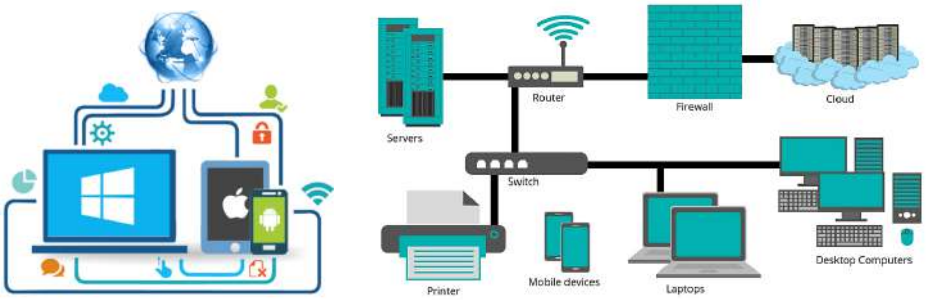


Рисунок 3 – Концепція проблематики кросплатформенності архітектури IT-структури організації [29] – [31]

Ця різноманітність може викликати труднощі в інтеграції систем через різницю в стандартах та протоколах зв'язку, що впливає на ефективність обміну даними. Суттєвим аспектом стають проблеми сумісності додатків та програмного забезпечення, які виникають внаслідок різниці в операційних середовищах, спричиняючи труднощі в їх взаємодії та впливаючи на продуктивність користувачів.

Важливим аспектом також є кібербезпека, оскільки використання різних операційних систем вимагає різних стратегій захисту від потенційних кіберзагроз. Це створює необхідність у впровадженні відмінних заходів забезпечення безпеки та захисту даних на кожній платформі.

Управління кросплатформенностю вимагає великих зусиль у плані навчання персоналу та використання різних інструментів для моніторингу та підтримки. Це може призводити до ускладнення адміністрування та підтримки IT-інфраструктури підприємства та, як наслідок, збільшення витрат на обслуговування.

Розв'язання проблем кросплатформенності вимагає використання технологій, фреймворків та підходів, які дозволяють створювати програми, що працюють ефективно та надійно на різних платформах, забезпечуючи при цьому єдність та безпеку даних та процесів [29] – [31].

Кросплатформенність IT-інфраструктури підприємств, залучення до корпоративних мереж значну кількість цифрових засобів та систем, масштабованість та значне розгалуження мереж організацій, а також використання принципів віддаленої роботи та використання персональних платформ і засобів працівниками створює проблему контролю та забезпечення цифрової безпеки для відповідної архітектури підприємств [32] – [34] – Рисунок 4.

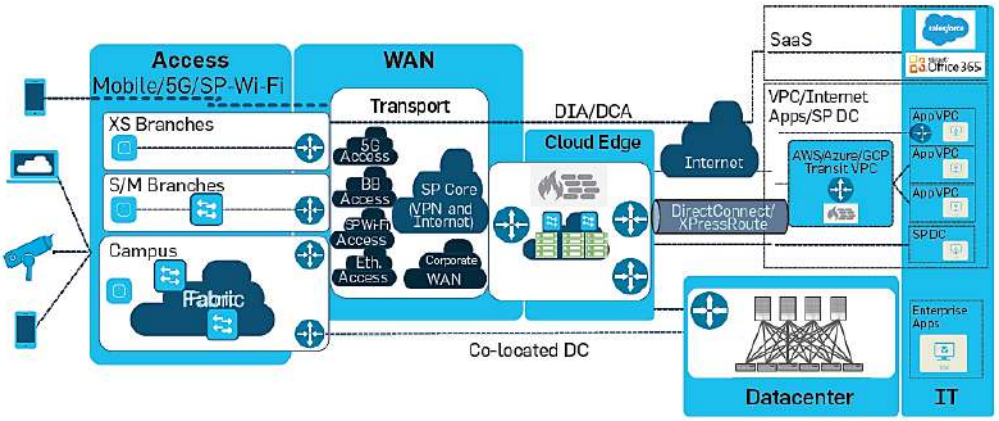


Рисунок 4 – Візуалізація проблематики забезпечення контролю та цифрової безпеки на підприємстві з розгалуженої IT-інфраструктурою, до якої інтегрована кросплатформенні рішення [32] – [34]

Кожен пристрій має свої програми та додатки, які використовуються для виконання різних завдань. Контроль та безпека цих додатків важливі для

запобігання вразливостям та атакам. Співробітники працюють в різних мережах, включаючи корпоративну мережу, віртуальні приватні мережі (VPN), бездротові мережі та громадські мережі. Кожна мережа має свої ризики та вимоги до безпеки.

Одним з дієвих наразі рішень при організації доцільної IT-архітектури підприємств, що засновані на принципах цифрової різноманітності та кросплатформенності є використання централізованих хмарних рішень. Застосування хмарних централізованих рішень для забезпечення контролю та безпеки використання різних засобів та платформ для входу в структуру IT-організації має декілька значущих переваг і може бути досить доцільним [35] – [37] – Рисунок 5.

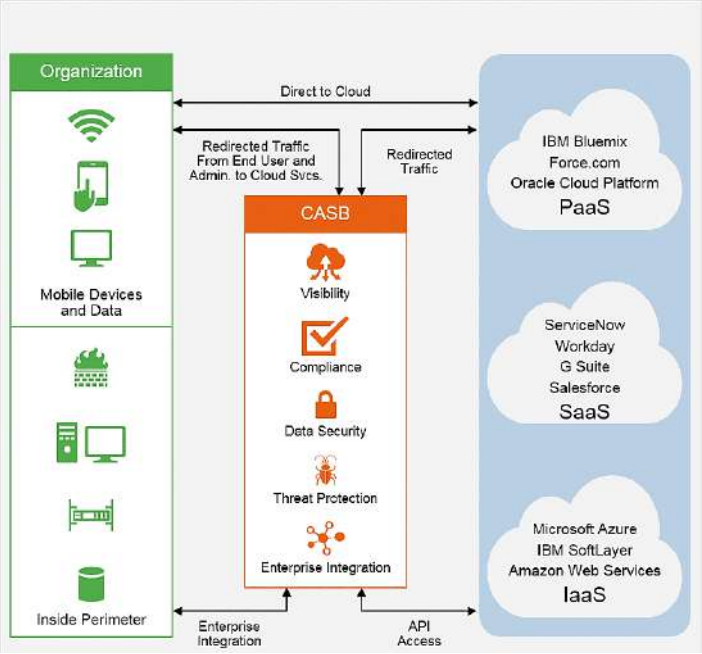


Рисунок 5 – Концепція застосування централізованих хмарних рішень для забезпечення контролю та безпеки IT-архітектури підприємства [35] – [37]

Хмарні централізовані рішення дозволяють адміністраторам керувати безпекою та доступом на різних пристроях та платформах з єдиного інтерфейсу. Це полегшує управління, моніторинг та впровадження політик безпеки. Використання єдиної точки входу (Single Sign-On (SSO)) дозволяє користувачам отримати доступ до різних служб та систем з одним

ідентифікаційним обліковим записом, підвищуючи зручність для користувачів та спрощуючи управління доступом.

1.2 Концепція цифрової та інформаційної безпеки IT-структури організації

Концепція цифрової та інформаційної безпеки IT-структури організації полягає в створенні системи заходів та політик для захисту інформації та інфраструктури в умовах зростаючих цифрових загроз та ризиків. Вона охоплює широкий спектр питань та компонентів, спрямованих на забезпечення конфіденційності, цілісності та доступності даних та ресурсів організації. Основні аспекти концепції цифрової та інформаційної безпеки включають в себе [38] – [40] (Рисунок 6):

1. Ідентифікація та аутентифікація – визначення користувачів та систем, їх ідентифікацію та автентифікацію для забезпечення лише легітимного доступу до ресурсів. Використання сильних паролів, двофакторної аутентифікації та інших методів допомагає захищати ідентифікаційні дані.
2. Авторизація – визначення прав доступу користувачів та систем до різних ресурсів та функцій. Переконання, що користувачі мають обмежений доступ лише до необхідної інформації, допомагає попередити несанкціонований доступ.
3. Шифрування даних – зхист даних шляхом шифрування їх в спокійному стані та під час передачі. Шифрування даних допомагає запобігти несанкціонованому доступу та втраті інформації.
4. Моніторинг та аудит – постійний моніторинг активності користувачів та систем для виявлення незвичайної поведінки та інцидентів безпеки. Проведення аудиту для встановлення інцедентів та порушень безпеки.
5. Захист від malware та загроз – захист від вірусів, троянів, шкідливих програм та інших цифрових загроз. Використання антивірусних

програм, мережевих брандмауерів та інших технічних засобів для захисту від malware.

6. Управління ідентифікацією та доступом – розробка та реалізація процедур керування ідентифікацією, управління правами доступу та ревізії для забезпечення дотримання політик безпеки.
7. Безпека мережі та комунікацій – захист мережевого трафіку та комунікацій від несанкціонованого доступу та перехоплення. Використання захищених протоколів та мережевих засобів для забезпечення безпеки комунікацій.
8. Забезпечення бізнес-процесів – захист інформаційних ресурсів та систем, що використовуються для підтримки бізнес-процесів організації. Забезпечення доступності та цілісності даних усіх бізнес-систем.
9. Навчання та освіта користувачів – навчання та підвищення свідомості користувачів щодо цифрової безпеки та реагування на загрози. Заохочення безпечних практик та усвідомлення ризиків.

10. Управління інцидентами – розробка та впровадження процедур та планів для реагування на інциденти безпеки, виявлення та виправлення вразливостей. Ефективне управління інцидентами допомагає швидко відновити безпеку після інциденту.

Рисунок 6 – Концепція цифрової та інформаційної безпеки IT-структури організацій та підприємств

Запровадження та дотримання концепції цифрової та інформаційної безпеки є необхідним для успішної функціонування організацій та збереження їх репутації та довіри клієнтів та партнерів. Вона допомагає уникати фінансових втрат, витрат на відновлення після інцидентів та збереження даних та інфраструктури в найкращому стані [38] – [40].

Проблематика кросплатформенності в сфері цифрової та інформаційної безпеки IT-організації значним чином впливає на рівень безпеки, що проявляються множиною ризиків [41] – [43] (Рисунок 7).

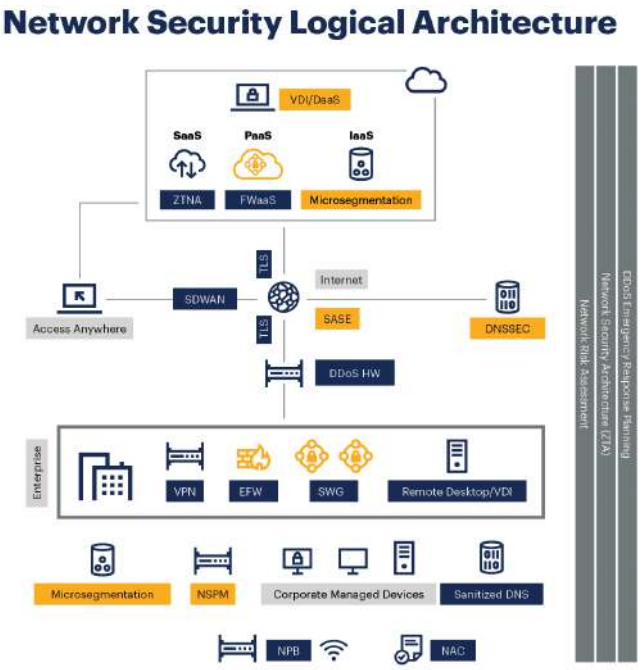


Рисунок 7 – Концепція логічної системи кібербезпеки організації, що демонструє складність улаштування при залученні до корпоративних мереж кросплатформенних систем та засобів [41] – [43]

Різноманітність платформ у контексті кросплатформенності передбачає підтримку різних операційних систем, пристроїв та архітектур. Це спричиняє необхідність експертизи в кількох платформах, що є важливим завданням та вимагає додаткових ресурсів для забезпечення безпеки на всіх рівнях. Різнорідність платформ може призвести до послаблення стандартизації в області безпеки. Кожна платформа вимагає власних інструментів, налаштувань та політик безпеки, ускладнюючи управління.

Для вирішення проблем кросплатформенності у контексті безпеки, організація повинна ретельно аналізувати ризики та визначити ефективні стратегії та інструменти для забезпечення безпеки на всіх платформах. Також важливо регулярно оновлювати політику безпеки та надавати персоналу відповідну навчання та навички для роботи з різними платформами [41] – [43].

Проблематика використання різних засобів та платформ для доступу до ІТ-структури організації суттєво впливає на цифрову та інформаційну

безпеку організації, призводячи до відповідних ризиків і викликів [44] – [46] – Рисунок 8.

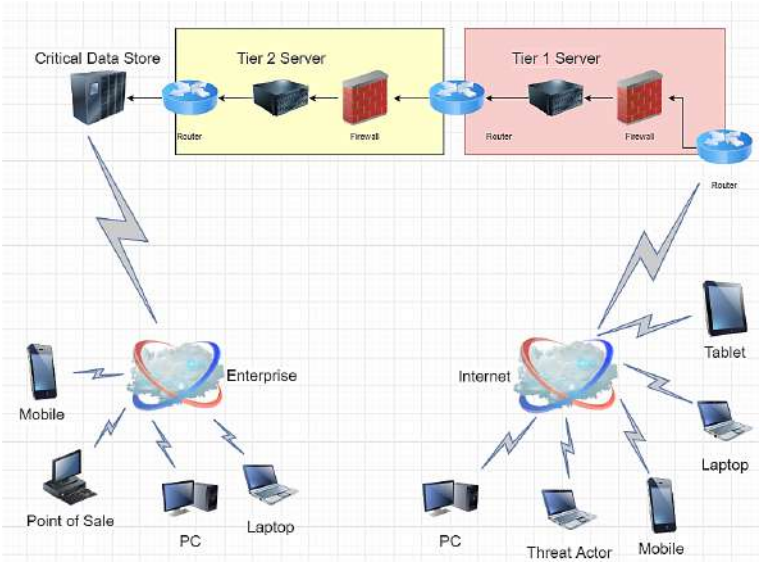


Рисунок 8 – Візуалізація вразливості мультидевайсного та мультисистемного доступу до корпоративних мереж [44] – [46]

Використання різноманітних засобів та платформ, включаючи стаціонарні та мобільні пристрої, розсіює інфраструктуру організації. Дані розподіляються по різних місцях, що може ускладнити не лише моніторинг та управління безпекою, але й взаємодію між різними частинами системи. Персональні мобільні пристрої, такі як смартфони та планшети, є високомобільними, але при цьому піддаються ризикам втрати або крадіжки. Це може призвести до втрати конфіденційної інформації, а також порушення конфіденційності та цілісності даних.

Використання публічних або незахищених мереж для доступу до IT-інфраструктури може експонувати конфіденційні дані ризику перехоплення та несанкціонованого доступу через невідповідність стандартам безпеки. З використанням різних платформ та засобів може виникати складність у впровадженні та управлінні єдиною системою керування доступом та ідентифікацією користувачів через різноманітність технічних параметрів та вимог безпеки [44] – [46].

Для вирішення цих проблем та забезпечення цифрової та інформаційної безпеки, організація повинна розробити та дотримуватися політики безпеки, яка включає в себе [47] – [49]:

- управління мобільними пристроями та персональними пристроями, включаючи політики віддаленого видалення даних у разі втрати або крадіжки;
- встановлення безпечних мережевих з'єднань та використання шифрування даних для захисту комунікацій;
- регулярний аудит та моніторинг активності користувачів на всіх платформах;
- навчання та освіта персоналу щодо безпечних практик та свідомості щодо ризиків.

Необхідно акцентувати увагу на тому, що забезпечення безпеки в сфері цифрової та інформаційної безпеки в сучасному суспільстві вимагає комплексного та цільового підходу, який ураховує всі аспекти використання різноманітних засобів та платформ в організаційному середовищі [47] – [49].

Відповідно до аналізу улаштування оптимальної IT-інфраструктури сучасного підприємства (п. 1.2 поточного дослідження), встановлено, що доцільним засобом вирішення проблематики кросплатформенності, мультидевейсності та мультимережності є імплементація хмарних централізованих рішень менеджменту та кіберзахисту [50] – [52] – Рисунок 9.

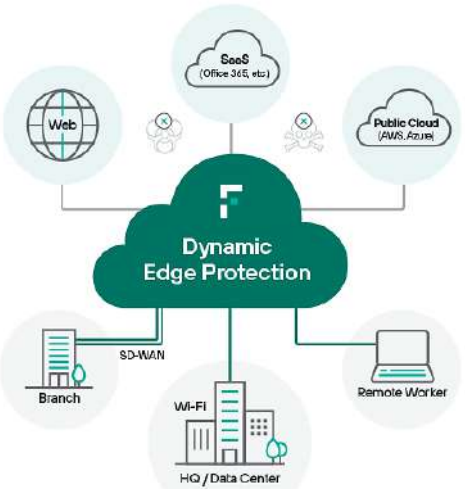


Рисунок 9 – Концепція застосування централізованих хмарних рішень з улаштування системи контролю та безпеки підприємства [50] – [52]

Використання централізованих хмарних платформ контролю доступу та безпеки демонструє здатність здійснювати ефективне централізоване управління ідентифікацією користувачів і керування їхнім доступом до ресурсів. Це спрощає процес управління правами доступу та виконання політики безпеки, що призводить до зменшення ризиків несанкціонованого доступу. Централізовані хмарні платформи вже впроваджують механізми одноразового входу, або SSO, що гарантує той факт, що користувачі можуть здійснювати вхід в систему один раз, отримуючи при цьому доступ до різних ресурсів та додатків без потреби повторного введення пароля. Це сприяє спрощенню процесу використання та, водночас, підвищує рівень безпеки.

1.3 Огляд хмарних рішень для забезпечення цифрової та інформаційної безпеки IT-структури організації

Огляд хмарних рішень для забезпечення цифрової та інформаційної безпеки IT-структури організації включає в себе розгляд різних послуг, платформ та інструментів, які можуть бути використані для забезпечення безпеки в цифровому середовищі. Ось кілька ключових аспектів та хмарних

рішень, які допомагають забезпечити цифрову та інформаційну безпеку організацій та підприємств.

Хмарні платформи для ідентифікації та контролю доступу. Сервіси, такі як Microsoft Azure Active Directory та Okta, надають інструменти для централізованого управління ідентифікацією користувачів та контролю доступу до ресурсів. Вони дозволяють встановлювати політики доступу, включаючи багатофакторну аутентифікацію, SSO та управління правами [53] – Рисунок 10.

Рисунок 10 – Принципова схема Microsoft Azure Active Directory [53]

Хмарні рішення для шифрування даних. Сервіси, як Amazon Web Services (AWS) Key Management Service [54] (Рисунок 11) та Microsoft Azure Information Protection [55] (Рисунок 12), надають можливості для шифрування даних в хмарі та під час їх передачі. Це допомагає забезпечити конфіденційність даних навіть під час їх зберігання та обробки в хмарі.

Хмарні платформи для моніторингу та аудиту безпеки. Сервіси, такі як AWS CloudTrail [56] (Рисунок 13) та Azure Monitor [57] (Рисунок 14), надають засоби для моніторингу активності користувачів та систем в хмарі. Вони дозволяють виявляти незвичайну активність та вести аудит безпеки для виявлення потенційних загроз.

Засоби для виявлення та захисту від загроз. Багато хмарних рішень, включаючи AWS GuardDuty [58] (Рисунок 15) та Microsoft Defender for Cloud [59] (Рисунок 16), надають засоби для виявлення та захисту від цифрових

загроз, таких як вторгнення та малвара. Вони використовують штучний інтелект та машинне навчання для пошуку аномальної активності та вчасного реагування на загрози.

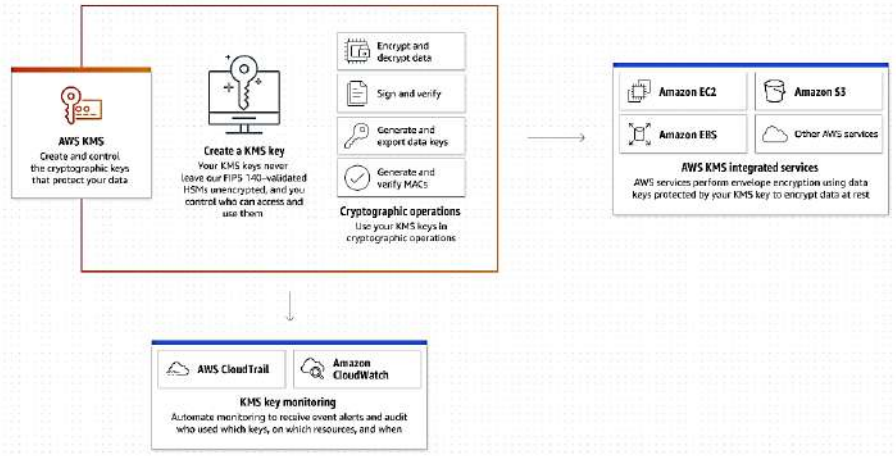


Рисунок 11 – Принципова схема Amazon Web Services (AWS) Key Management Service [54]

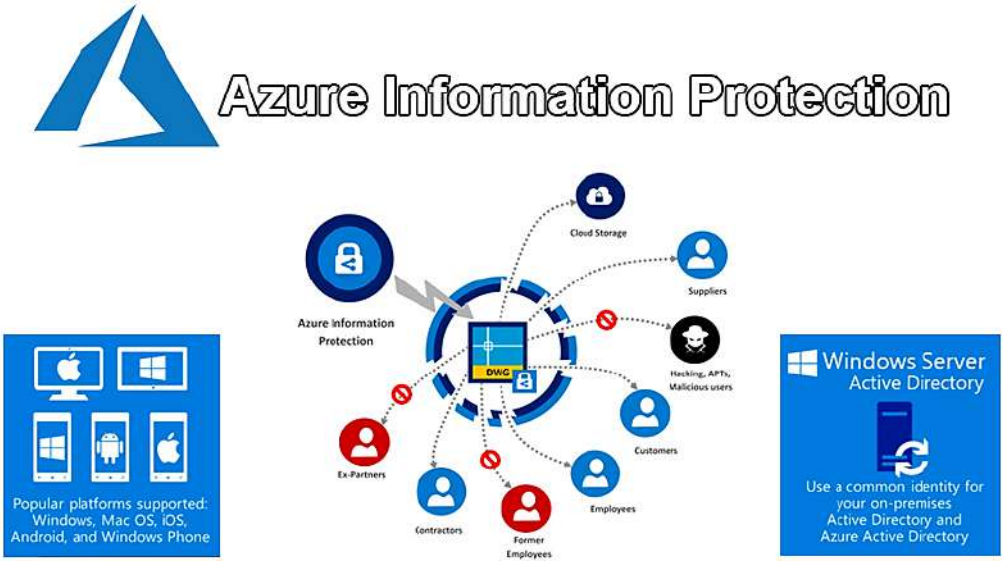


Рисунок 12 – Принципова схема Microsoft Azure Information Protection [55]

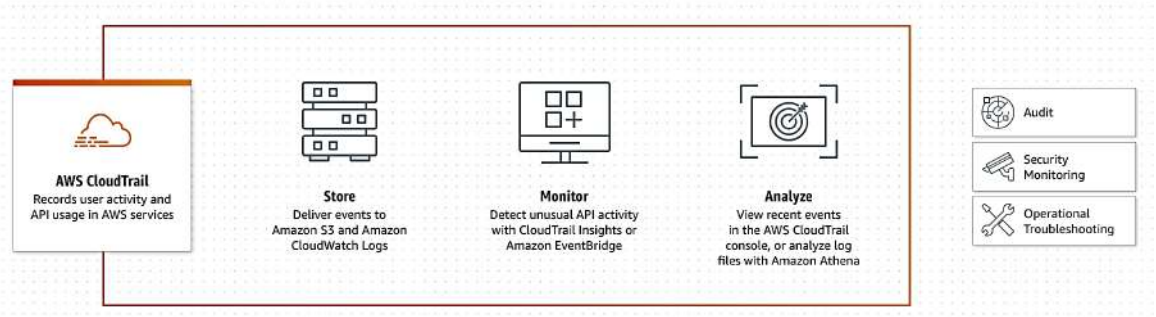


Рисунок 13 – Принципова схема AWS CloudTrail [56]

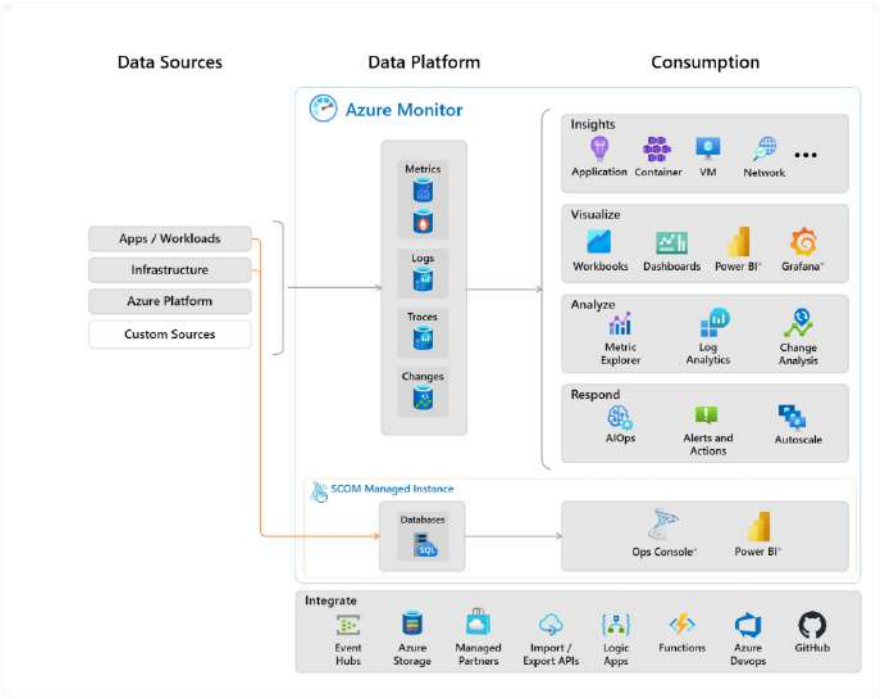


Рисунок 14 – Принципова схема Azure Monitor [57]

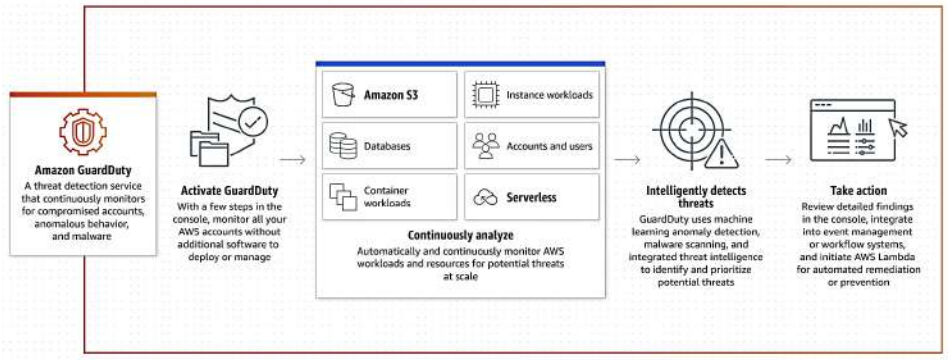


Рисунок 15 – Принципова схема AWS GuardDuty [58]

Рисунок 16 – Принципова схема Microsoft Defender for Cloud [59]

Хмарні рішення для керування мобільними пристроями. Сервіси, такі як Microsoft Intune [20] (Рисунок 17) та VMware Workspace ONE [60] (Рисунок 18), дозволяють керувати мобільними пристроями та надавати їм безпечний доступ до корпоративних ресурсів. Вони дозволяють віддалено вимагати видалення даних у випадку втрати або крадіжки пристрою.

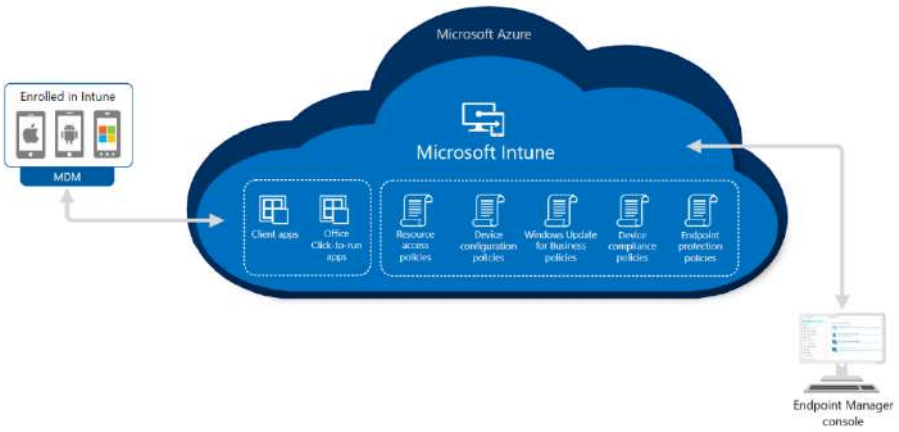


Рисунок 17 – Принципова схема Microsoft Intune [20]

Хмарні резервні копії та відновлення даних. Хмарні послуги для резервного копіювання, такі як AWS Backup [61] (Рисунок 19) та Google Cloud Storage [62] (Рисунок 20), надають можливості для зберігання та відновлення даних в разі аварій або втрати. Це важливий аспект забезпечення інформаційної безпеки.

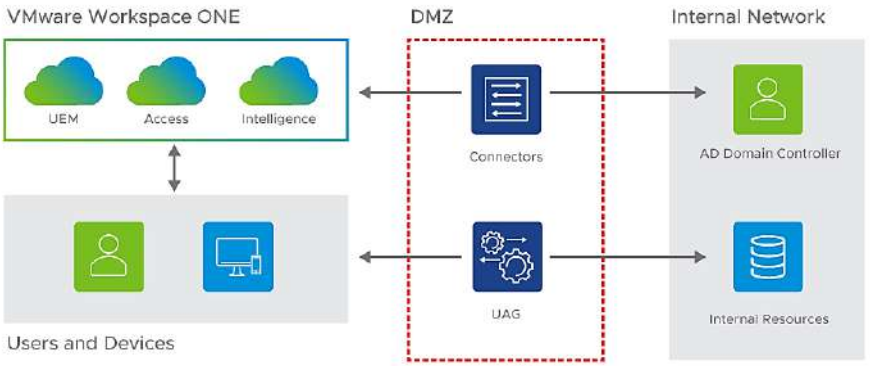


Рисунок 18 – Принципова схема VMware Workspace ONE [60]

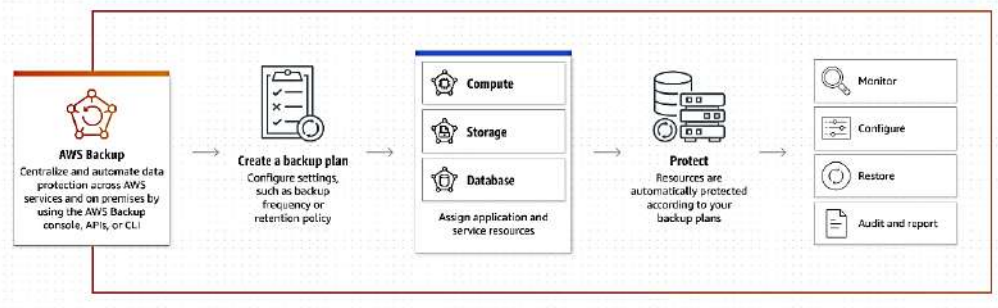


Рисунок 19 – Принципова схема AWS Backup [61]

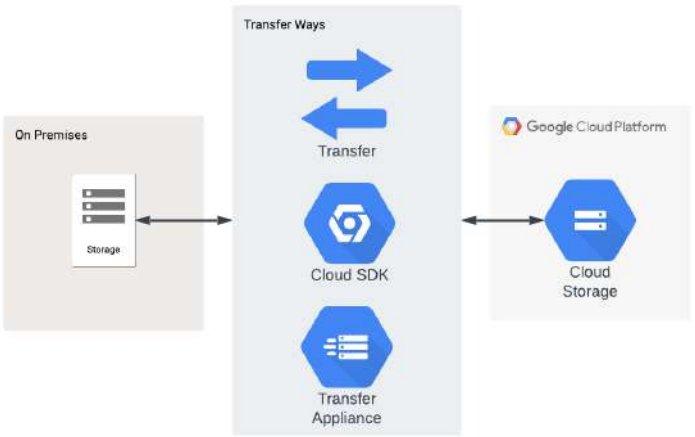


Рисунок 20 – Принципова схема Google Cloud Storage [62]

Спеціалізовані рішення для кіберзахисту. Такі сервіси як Cloudflare [63] (Рисунок 21) та Cisco Umbrella [64] (Рисунок 22) пропонують спеціалізовані

хмарні рішення для кіберзахисту, такі як рішення для захисту від DDoS-атак або захисту від фішингу. Вони допомагають зменшити ризики цифрових атак.

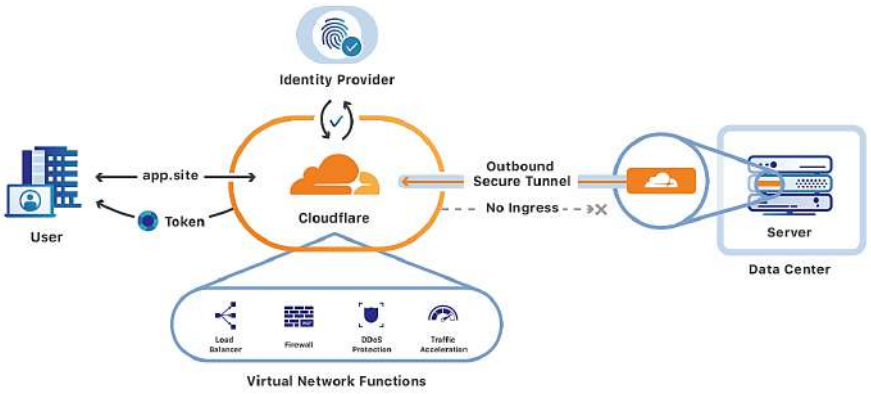


Рисунок 21 – Принципова схема Cloudflare [63]

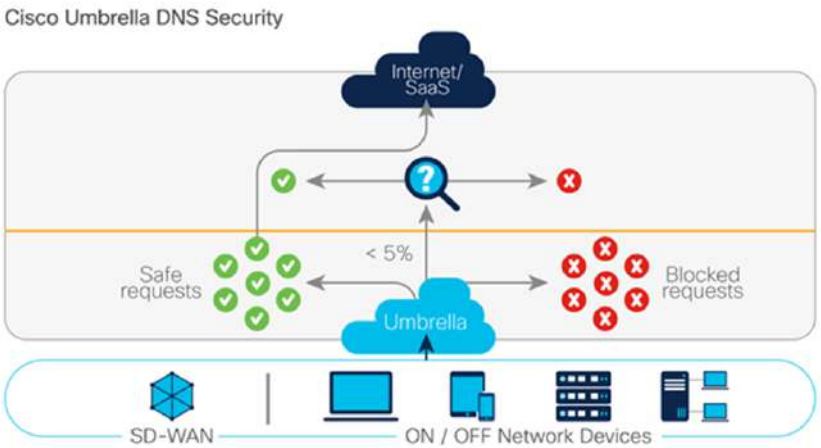


Рисунок 22 – Принципова схема Cisco Umbrella [64]

Важливо відзначити, що вибір конкретних хмарних рішень для забезпечення цифрової та інформаційної безпеки повинен враховувати потреби та характеристики самої організації, а також дотримуватися кращих практик безпеки. Комбінація різних хмарних послуг та інструментів може допомогти організаціям створити комплексну систему захисту в цифровому середовищі.

Зважаючи на фокус дослідження, щодо технології управління кінцевими точками організації та їх захисту, детально розглянемо Microsoft Intune [20].

Microsoft Intune (Рисунок 17) – це хмарний сервіс для управління мобільними пристроями та захисту корпоративних даних. Він дозволяє організаціям централізовано керувати мобільними пристроями (включаючи iOS, Android та Windows), надавати безпечний доступ до корпоративних ресурсів та забезпечувати захист даних. Основні функції Microsoft Intune включають [20] – [22]:

- Intune дозволяє організаціям встановлювати політики безпеки для мобільних пристроїв, віддалено відстежувати, блокувати або видаляти дані на втрачених або вкрадених пристроях, а також надавати користувачам можливість самостійно реєструвати свої пристрої для роботи в корпоративному середовищі;
- Intune дозволяє шифрувати дані на мобільних пристроях та застосовувати політики захисту даних, такі як обмеження копіювання, друку та редагування корпоративних файлів;
- Intune дозволяє керувати додатками на мобільних пристроях, включаючи встановлення, видалення та оновлення додатків з віддаленого доступу. Він також підтримує політики додатків, які визначають, як додатки повинні взаємодіяти з даними та іншими додатками;
- Intune дозволяє налаштовувати VPN-підключення, проксі-сервери та інші налаштування мережі на мобільних пристроях.

Аналогічні хмарні платформи:

1. VMware Workspace ONE [60] (Рисунок 18): ця платформа надає аналогічний функціонал для управління мобільними пристроями та

захисту даних. Вона включає в себе інструменти для централізованого управління пристроями, контролю доступу та управління додатками.

2. Citrix Endpoint Management [65] (Рисунок 23): ця платформа також пропонує рішення для управління мобільними пристроями, захисту даних та контролю доступу до корпоративних ресурсів.
3. MobileIron [66] (Рисунок 24): це інше популярне рішення для управління мобільними пристроями та захисту даних, яке дозволяє організаціям створювати політики безпеки для мобільних пристроїв та додатків.

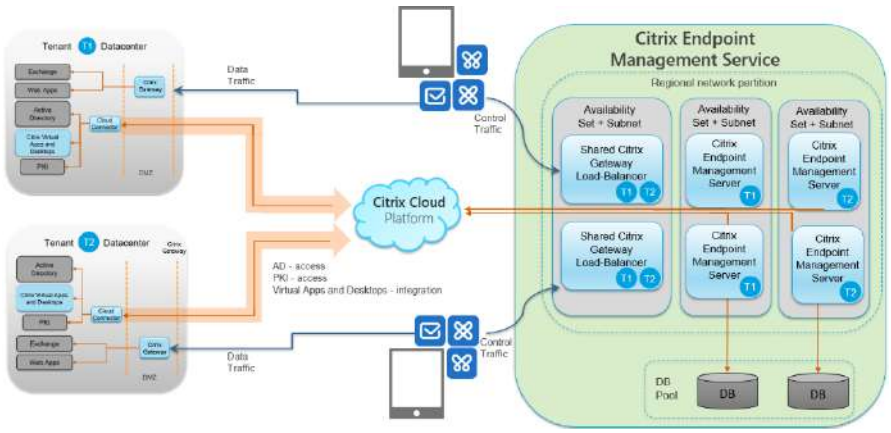


Рисунок 23 – Принципова схема Citrix Endpoint Management [65]

Вибір платформи для управління мобільними пристроями та захисту даних залежить від потреб та інфраструктури конкретної організації, а також від її пріоритетів щодо цифрової та інформаційної безпеки.

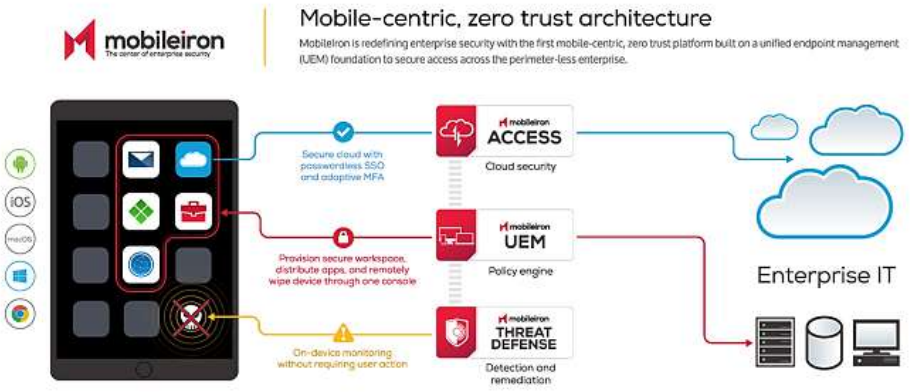


Рисунок 24 – Принципова схема MobileIron [66]

Компаративний аналіз Microsoft Intune порівняно з іншими аналогічними хмарними сервісами, такими як VMware Workspace ONE, Citrix Endpoint Management і MobileIron, допомагає розглянути переваги та недоліки кожної з цих платформ для управління мобільними пристроями та захисту даних. Ось декілька ключових аспектів для порівняння:

1. Функціональність та можливості:

- Microsoft Intune: Intune має багато можливостей для управління мобільними пристроями та захисту даних. Він інтегрується з іншими продуктами Microsoft, такими як Azure AD та Office 365.
- VMware Workspace ONE: Workspace ONE також надає широкий функціонал для управління мобільними пристроями та контролю доступу. Він спрощує інтеграцію з VMware-середовищами.
- Citrix Endpoint Management: Ця платформа пропонує рішення для управління мобільними пристроями та контролю доступу до додатків, інтегрується з рішеннями Citrix для віддаленого доступу.
- MobileIron: MobileIron спеціалізується на управлінні мобільними пристроями та контролі доступу, надаючи широкі можливості для захисту даних.

2. Інтеграція:

- Microsoft Intune: Як частина екосистеми Microsoft, Intune інтегрується з Azure AD та іншими сервісами Microsoft, що спрощує роботу в середовищі Windows та з іншими продуктами Microsoft.
- VMware Workspace ONE: Workspace ONE також добре інтегрується з іншими продуктами VMware та іншими технологіями віртуалізації.
- Citrix Endpoint Management: Ця платформа інтегрується з рішеннями Citrix, такими як Citrix Virtual Apps та Citrix Virtual Desktops.

- MobileIron: MobileIron надає можливості інтеграції з різними додатками та сервісами.

3. Вартість:

- Вартість використання кожної з платформ може значно відрізнятися в залежності від обраного плану та обсягу користувачів. Зазвичай, Microsoft Intune має конкурентоспроможну ціну, особливо для організацій, які вже використовують інші продукти Microsoft.

4. Підтримка та обслуговування:

- Важливо враховувати рівень підтримки та служби підтримки, яку надають постачальники кожної платформи. Microsoft, VMware, Citrix та MobileIron мають різний рівень підтримки, що може вплинути на ефективність вирішення технічних питань та проблем.

5. Спеціалізовані можливості:

- Кожна з платформ може мати свої спеціалізовані можливості та інструменти для конкретних вимог організації, такі як захист від DDoS-атак, контроль мережі або аналіз загроз.

Загалом, вибір між Microsoft Intune та іншими аналогічними хмарними платформами залежить від потреб та інфраструктури конкретної організації. Кожна з них має свої переваги та особливості, і важливо ретельно розглянути їх перед вибором.

Висновок до 1 розділу

Огляд хмарних рішень для забезпечення цифрової та інформаційної безпеки IT-структури організації підкреслює важливість вибору відповідних інструментів та платформ для забезпечення безпеки даних та доступу до корпоративних ресурсів. Хмарні сервіси стають ключовими компонентами

стратегії кіберзахисту організацій, оскільки вони пропонують широкий спектр інструментів та рішень для вирішення сучасних цифрових загроз.

Сервіси, такі як Microsoft Intune, VMware Workspace ONE, Citrix Endpoint Management та MobileIron, пропонують широкий функціонал для управління мобільними пристроями, контролю доступу та захисту даних. Їх вибір залежить від потреб організації, особливостей її інфраструктури та бюджетних можливостей.

Ці платформи дозволяють створити комплексну систему захисту в інформаційному просторі, інтегруючи різні аспекти безпеки, такі як управління пристроями, захист даних, контроль доступу та виявлення загроз. При цьому важливо ретельно аналізувати вартість, рівень підтримки та інтеграційні можливості кожної платформи перед прийняттям рішення.

Хмарні рішення для забезпечення цифрової та інформаційної безпеки є невід'ємною частиною сучасного бізнесу, і вони допомагають організаціям захищати свої активи та зберігати конфіденційність даних в умовах зростаючих цифрових загроз.

2 ОГЛЯД MICROSOFT INTUNE

2.1 Загальна характеристика Microsoft Intune

Microsoft Intune – це хмарна платформа для управління мобільними пристроями та захисту корпоративних даних в цифровому середовищі. Ця платформа розроблена корпорацією Microsoft та надає широкий функціонал для організацій, які бажають ефективно управляти мобільними пристроями та забезпечити безпеку даних [20] – [22] – Рисунок 25.

Рисунок 25 – Концептуальна схема Microsoft Intune [20] – [22]

Основні характеристики та можливості Microsoft Intune [20] – [22] (Рисунок 26 – Рисунок 29):

1. Intune дозволяє організаціям віддалено управляти мобільними пристроями, включаючи смартфони та планшети на різних операційних системах, такі як iOS, Android та Windows. Адміністратори можуть встановлювати політики безпеки, віддалено відслідковувати пристрої та навіть блокувати або видаляти дані на втрачених або вкрадених пристроях.

2. Платформа дозволяє зашифровувати дані на мобільних пристроях та застосовувати політики безпеки для корпоративних даних. Це допомагає захистити конфіденційні інформаційні активи організації.
3. Intune дозволяє адміністраторам керувати додатками на мобільних пристроях, включаючи встановлення, оновлення та видалення додатків. Також існують можливості для створення політик додатків, які контролюють взаємодію додатків з даними.
4. Intune дозволяє організаціям налаштовувати VPN-підключення, проксі-сервери та інші налаштування мережі на мобільних пристроях для забезпечення безпеки та доступу до корпоративних ресурсів.
5. Платформа включає в себе засоби для виявлення та відстеження загроз, такі як віруси та малвара. Вона також надає засоби для реагування на цифрові загрози.
6. Intune легко інтегрується з іншими хмарними продуктами Microsoft, такими як Azure Active Directory та Office 365, що спрощує роботу в єдиній екосистемі.
7. Intune дозволяє адміністраторам управляти комп'ютерами з операційною системою Windows. Вони можуть встановлювати оновлення, налаштовувати політики безпеки та віддалено вирішувати проблеми на цих пристроях.
8. Платформа підтримує також пристрої з операційною системою MacOS, що дозволяє організаціям включати їх до корпоративного середовища та забезпечувати їх безпеку.
9. Intune дозволяє адміністраторам керувати додатками на різних типах пристроїв. Це допомагає забезпечити, що користувачі отримують доступ до необхідних додатків із відповідними політиками безпеки.
10. Intune надає засоби для захисту даних на різних пристроях. Це включає в себе можливість шифрування даних, обмеження копіювання та передачі конфіденційної інформації.

11. Платформа може інтегруватися з іншими хмарними службами для розширення її можливостей. Наприклад, вона підтримує інтеграцію з іншими хмарними послугами Microsoft, такими як Microsoft Defender ATP.

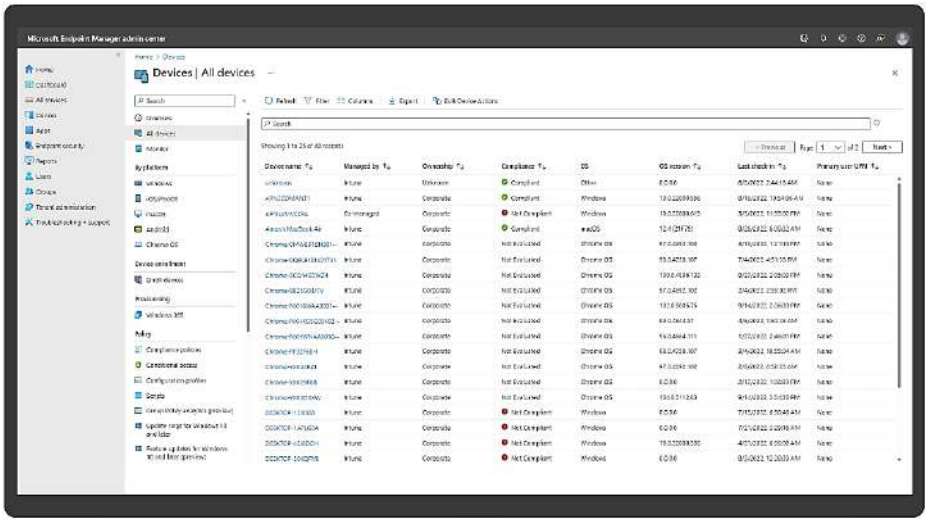


Рисунок 26 – Кросплатформенне керування кінцевими точками [20] – [22]

Microsoft Intune допомагає організаціям створювати безпечне та ефективне робоче середовище для мобільних співробітників та захищати корпоративні ресурси та дані в цифровому світі. Microsoft Intune став важливим інструментом для сучасних організацій, які працюють у цифровому середовищі та мають потребу в ефективному управлінні мобільними пристроями та захисті даних. Він дозволяє організаціям підтримувати безпеку та продуктивність своїх співробітників, незалежно від типу пристрою або операційної системи.

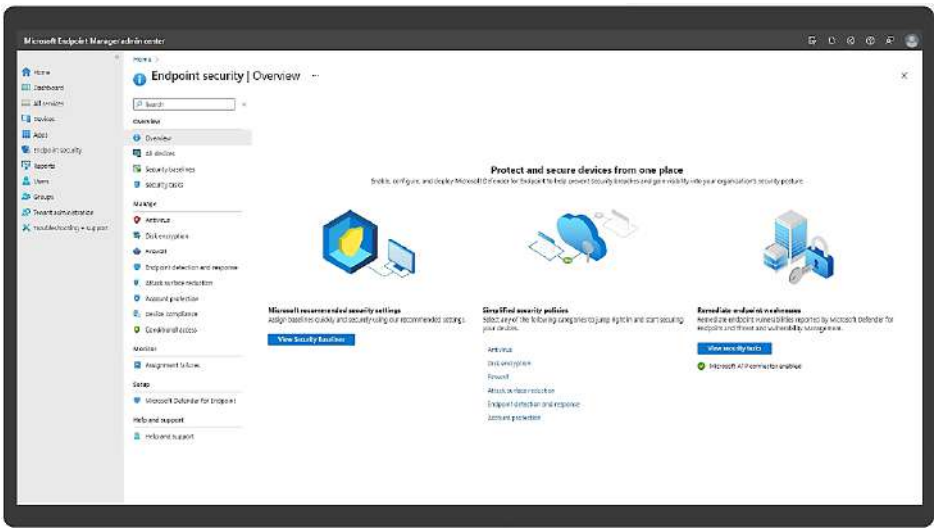


Рисунок 27 – Вбудований захист кінцевих точок [20] – [22]

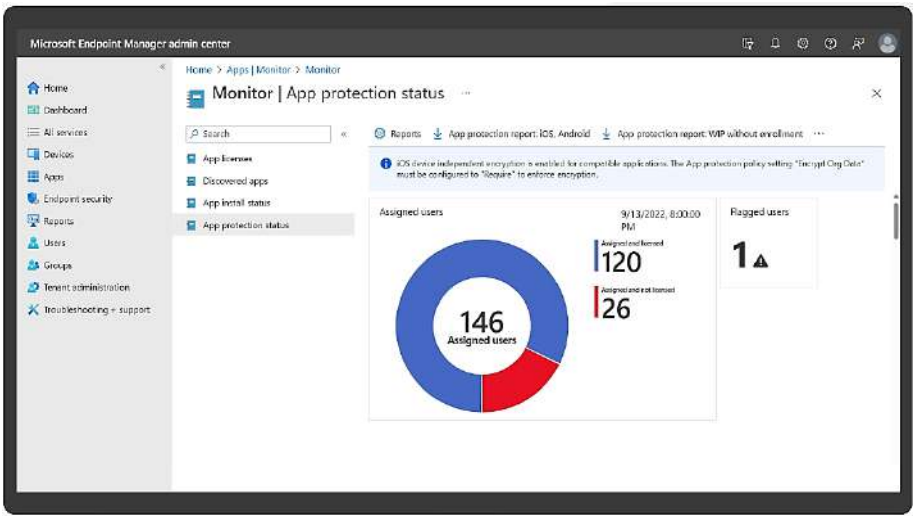


Рисунок 28 – Керування мобільними додатками [20] – [22]

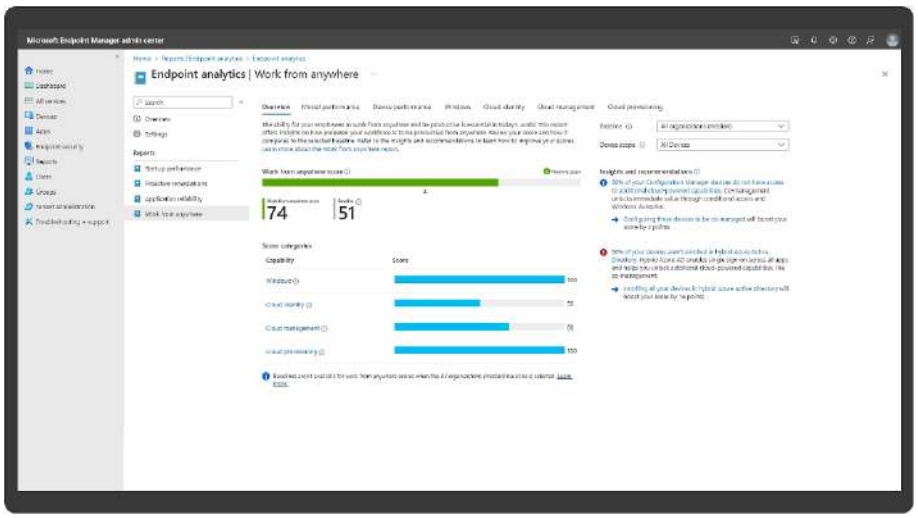


Рисунок 29 – Аналітика кінцевих точок [20] – [22]

Microsoft Intune є важливим компонентом сучасного інфраструктурного управління та цифрової безпеки для організацій. Ця хмарна платформа розроблена корпорацією Microsoft і надає широкий функціонал для управління мобільними пристроями та захисту корпоративних даних в умовах сучасного цифрового середовища.

2.2 Архітектура Microsoft Intune

Архітектура Microsoft Intune складається з ряду ключових компонентів, які спільно дозволяють управляти мобільними пристроями та захищати корпоративні дані в цифровому середовищі. Важливим аспектом архітектури Intune є його хмарна природа, що дозволяє організаціям отримувати доступ до цих функцій через Інтернет. Основні компоненти архітектури Microsoft Intune включають [20] – [22] (Рисунок 30):

1. Intune Service: Це центральна хмарна служба, яка забезпечує основну функціональність Intune. Вона відповідає за управління мобільними пристроями, встановлення політик безпеки, віддалене відстеження та керування додатками на пристроях.

2. Azure Active Directory (Azure AD): Intune інтегрований з Azure AD для ідентифікації та автентифікації користувачів та пристроїв. Це дозволяє забезпечити безпеку доступу до корпоративних ресурсів та даних.
3. Mobile Device Management (MDM): Цей компонент включає в себе функції для управління мобільними пристроями, такі як віддалене встановлення політик, відслідковування пристроїв та блокування або видалення даних на втрачених або вкрадених пристроях.
4. Mobile Application Management (MAM): Цей компонент відповідає за управління додатками на мобільних пристроях. Він дозволяє контролювати доступ та взаємодію додатків з корпоративними даними.
5. Conditional Access: Цей компонент встановлює умови доступу до корпоративних ресурсів на основі різних параметрів, таких як місцезнаходження, тип пристрою та стан безпеки.
6. Azure Information Protection: Цей компонент дозволяє зашифровувати та захищати корпоративні дані, забезпечуючи їхню конфіденційність та цілісність.
7. Microsoft Defender for Endpoint: Інтеграція з цим компонентом дозволяє виявляти та відстежувати загрози на мобільних пристроях та реагувати на них.
8. Intune App Protection Policies: Цей компонент встановлює політики захисту для додатків на мобільних пристроях, контролюючи їхню взаємодію з даними та дозволи доступу.

Архітектура Microsoft Intune дозволяє організаціям ефективно управляти мобільними пристроями та захищати корпоративні дані в умовах сучасного цифрового середовища. Ця хмарна платформа інтегрована з іншими службами Microsoft, створюючи єдину екосистему для цифрового управління та безпеки.

Intune Service (Служба Intune) [20] – [22]: Це ключовий компонент архітектури Microsoft Intune і представляє собою центральну хмарну службу,

що відповідає за надання основної функціональності платформи. Служба Intune дозволяє організаціям ефективно управляти мобільними пристроями та забезпечувати безпеку корпоративних даних в цифровому середовищі.

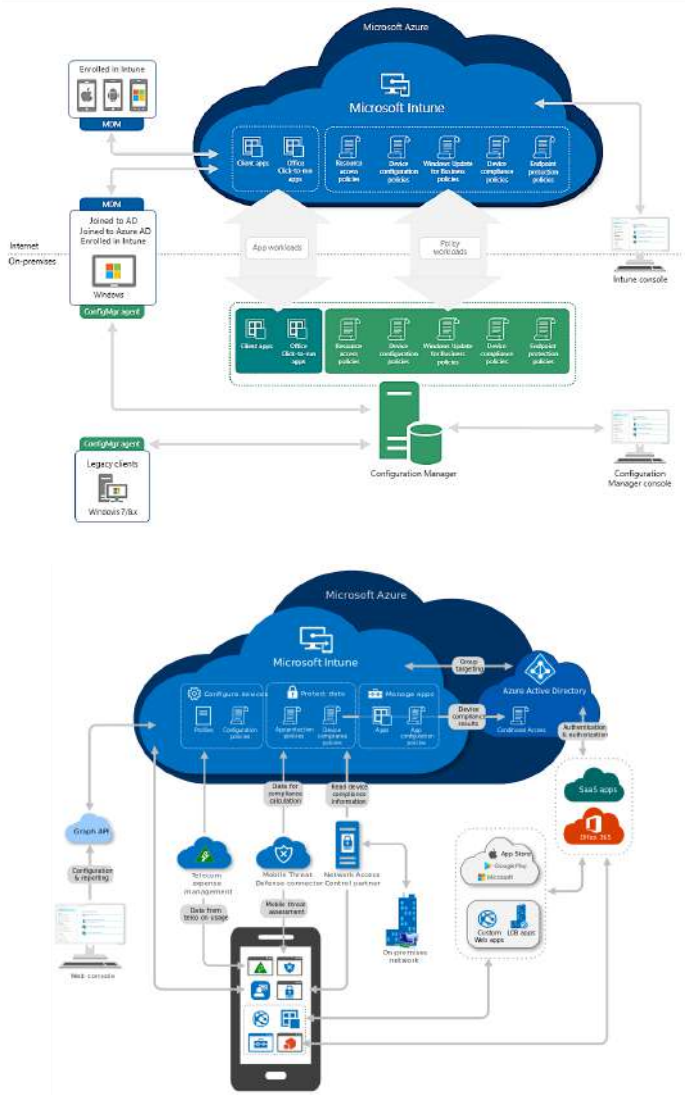


Рисунок 30 – Архітектура Microsoft Intune [20] – [22]

Головні функції та можливості служби Intune включають [20] – [22] (Рисунок 31):

1. Служба Intune надає можливість адміністраторам віддалено керувати мобільними пристроями, такими як смартфони, планшети та ноутбуки, які використовуються співробітниками. Адміністратори можуть встановлювати політики безпеки, моніторити стан пристроїв та

виконувати віддалені дії, такі як блокування або видалення даних на втрачених чи вкрадених пристроях.

2. Intune дозволяє адміністраторам контролювати додатки, які встановлені на мобільних пристроях. Вони можуть визначати, які додатки є дозволеними для користування в корпоративному середовищі та налаштовувати політики безпеки для додатків.
3. Служба Intune допомагає захищати корпоративні дані, що зберігаються на мобільних пристроях, за допомогою шифрування та політик безпеки. Це забезпечує конфіденційність і цілісність інформації.
4. Intune надає засоби для моніторингу стану мобільних пристроїв та виявлення можливих загроз. Адміністратори можуть відстежувати події та реагувати на їхні наслідки.
5. Служба Intune пов'язана з іншими продуктами та службами Microsoft, такими як Azure Active Directory та Microsoft 365. Ця інтеграція дозволяє створювати єдине цифрове робоче середовище та забезпечувати спільний доступ до ресурсів.

Intune Service виступає як центральний елемент управління та захисту мобільних пристроїв та даних в організації, дозволяючи забезпечити безпеку та продуктивність співробітників у цифровому середовищі.

Azure Active Directory (Azure AD) є ключовим компонентом архітектури Microsoft Intune та інших облачних служб Microsoft. Ця служба відіграє важливу роль в ідентифікації та автентифікації користувачів та пристроїв у цифровому середовищі організації [20] – [22] (Рисунок 32).

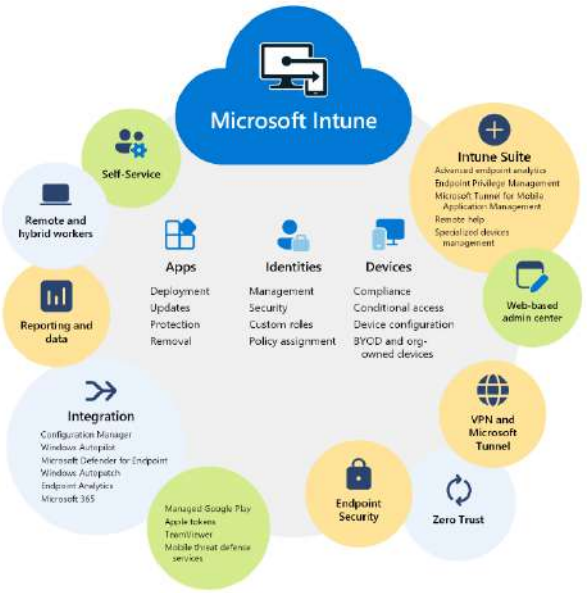


Рисунок 31 – Концептуальна схема Intune Service [20] – [22]

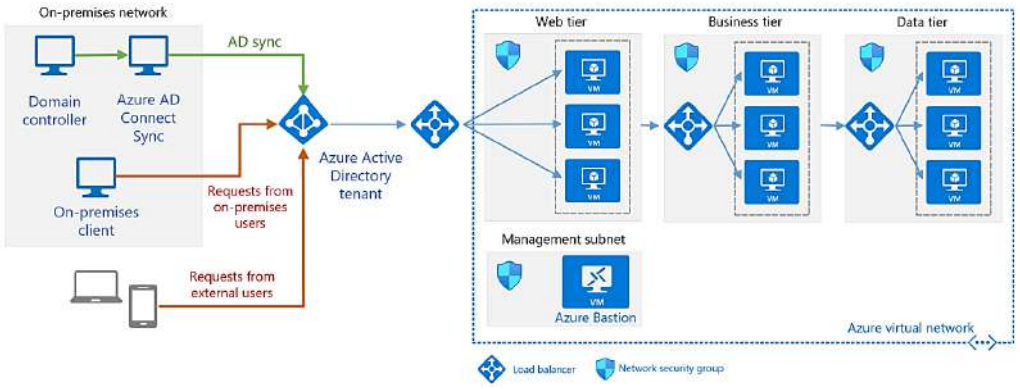


Рисунок 32 – Концептуальна схема Azure Active Directory [20] – [22]

Основні характеристики та можливості Azure Active Directory включають [20] – [22]:

1. Azure AD дозволяє організаціям управляти ідентифікацією користувачів та пристроїв. Вона підтримує різні методи автентифікації, включаючи багатофакторну автентифікацію, одноразовий доступ та інші засоби забезпечення безпеки входу в систему.
2. Azure AD дозволяє використовувати одноразові паролі для безпечного входу в систему. Це зменшує ризик несанкціонованого доступу до корпоративних ресурсів.

3. За допомогою Azure AD можна налаштувати багатофакторну автентифікацію, що вимагає введення двох або більше факторів для підтвердження ідентифікації, забезпечуючи вищий рівень безпеки.
4. Azure AD інтегрована з іншими хмарними службами Microsoft, такими як Microsoft 365 та Microsoft Intune. Ця інтеграція дозволяє забезпечити єдиний вхід та управління доступом до різних ресурсів.
5. Azure AD дозволяє налаштовувати умови доступу до різних корпоративних ресурсів, контролюючи, хто, коли і звідки може отримувати доступ.
6. Azure AD співпрацює з іншими компонентами Microsoft, такими як Azure Information Protection та Microsoft Defender, для захисту корпоративних даних в цифровому середовищі.

Azure Active Directory виступає як ключовий елемент в архітектурі безпеки та ідентифікації в сучасних організаціях, дозволяючи забезпечити безпеку та продуктивність користувачів в умовах цифрового середовища.

Mobile Device Management (MDM) – це важливий компонент архітектури Microsoft Intune та інших подібних рішень. MDM дозволяє організаціям ефективно керувати мобільними пристроями, які використовуються співробітниками, і забезпечувати безпеку корпоративних даних на цих пристроях [20] – [22] (Рисунок 33).

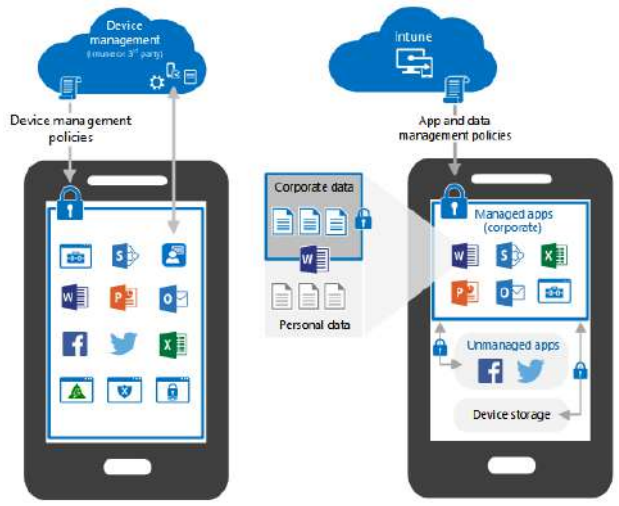


Рисунок 33 – Концептуальна схема Mobile Device Management [20] – [22]

Основні функції та можливості Mobile Device Management включають [20] – [22]:

1. MDM дозволяє адміністраторам віддалено керувати налаштуваннями та політиками безпеки на мобільних пристроях. Це включає в себе встановлення паролів, шифрування даних та інші заходи безпеки.
2. Адміністратори можуть встановлювати політики безпеки для мобільних пристроїв, щоб забезпечити конфіденційність та цілісність корпоративних даних. Це включає в себе вимоги до паролів, блокування пристроїв та інші заходи.
3. MDM надає можливість відслідковувати місцезнаходження мобільних пристроїв та виконувати дії, такі як віддалене блокування або видалення даних на втрачених або вкрадених пристроях.
4. MDM дозволяє адміністраторам керувати доступом до корпоративних додатків на мобільних пристроях. Вони можуть вимагати встановлення обов'язкових додатків та налаштовувати політики безпеки для них.
5. MDM вимагає реєстрації та прив'язки мобільних пристроїв до корпоративного середовища, щоб забезпечити безпеку та контроль.

6. MDM надає можливість збирати інформацію про конфігурацію та стан мобільних пристроїв, що спрощує моніторинг та аналіз їхнього стану.

Mobile Device Management є важливим інструментом для організацій, які дозволяють співробітникам використовувати мобільні пристрої в робочих цілях. Він допомагає забезпечити безпеку та ефективне управління цими пристроями в цифровому середовищі.

Mobile Application Management (MAM) – це важливий компонент архітектури Microsoft Intune та інших подібних рішень. MAM дозволяє організаціям управляти додатками на мобільних пристроях, забезпечуючи безпеку корпоративних даних і контроль над їхнім використанням [20] – [22] (Рисунок 34).

Рисунок 34 – Концептуальна схема Mobile Application Management [20] – [22]

Основні функції та можливості Mobile Application Management включають [20] – [22]:

1. MAM дозволяє адміністраторам встановлювати політики доступу до додатків на мобільних пристроях. Вони можуть визначити, які додатки є дозволеними для користування в корпоративному середовищі та контролювати їх доступність.
2. MAM дозволяє налаштовувати політики безпеки для додатків на мобільних пристроях. Це включає в себе шифрування даних, вимоги до

паролів, обмеження обміну даними між додатками та інші заходи безпеки.

3. MAM дозволяє відокремити корпоративні дані від особистих на мобільних пристроях. Це забезпечує конфіденційність корпоративної інформації та дозволяє видаляти лише корпоративні дані з пристроїв, коли співробітник покидає організацію.
4. MAM дозволяє віддалено видаляти корпоративні дані з пристроїв у випадку втрати, крадіжки або виходу співробітника з організації. Це допомагає забезпечити безпеку даних.
5. MAM дозволяє адміністраторам встановлювати політики безпеки для окремих додатків, контролюючи їхню поведінку та доступ до корпоративних даних.
6. MAM надає засоби для моніторингу використання додатків на мобільних пристроях та аналізу поведінки користувачів.

Mobile Application Management є важливим інструментом для забезпечення безпеки та контролю над додатками на мобільних пристроях в організаціях. Він дозволяє інтегрувати корпоративні додатки та дані в цифровому середовищі, забезпечуючи безпеку та продуктивність співробітників.

Conditional Access – це стратегічний компонент архітектури безпеки, який дозволяє організаціям контролювати, коли і як користувачі мають доступ до ресурсів та даних в цифровому середовищі, в залежності від різних умов та обставин [20] – [22] (Рисунок 35).

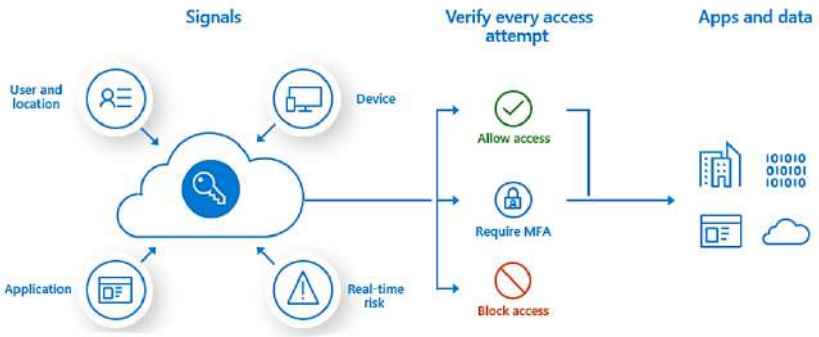


Рисунок 35 – Концептуальна схема Conditional Access [20] – [22]

Основні характеристики та можливості Conditional Access включають [20] – [22]:

1. Conditional Access дозволяє налаштовувати різні умови, які користувачі повинні виконувати для отримання доступу. Це може включати в себе багатофакторну автентифікацію, геолокаційні умови, стан пристрою та інші параметри.
2. Conditional Access дозволяє визначити, які ресурси та додатки доступні для користувачів. Це може бути доступ до файлів, веб-сайтів, хмарних служб та інших цифрових ресурсів.
3. Conditional Access допомагає визначити ризики та потенційні загрози доступу. Наприклад, він може вимагати багатофакторну автентифікацію для доступу з незахищених мереж або незнайомих пристроїв.
4. Conditional Access надає можливість моніторити та журналювати всі спроби доступу, а також реагувати на аномальну поведінку чи потенційні загрози.
5. Conditional Access інтегрований з іншими службами безпеки, такими як Azure Active Directory, Microsoft Intune та інші, для забезпечення комплексного підходу до безпеки та доступу.

Conditional Access допомагає організаціям забезпечити безпеку та контроль над доступом до ресурсів в цифровому середовищі. Він дозволяє реагувати на різні сценарії та забезпечити безпеку корпоративних даних та ресурсів, зменшуючи ризик несанкціонованого доступу та загроз безпеці.

Azure Information Protection (AIP) – це рішення для забезпечення захисту та управління конфіденційністю даних та інформацією в організації. Це компонент архітектури безпеки, який дозволяє класифікувати, мітити та захищати дані на всіх етапах їхнього життєвого циклу [20] – [22] (Рисунок 36).

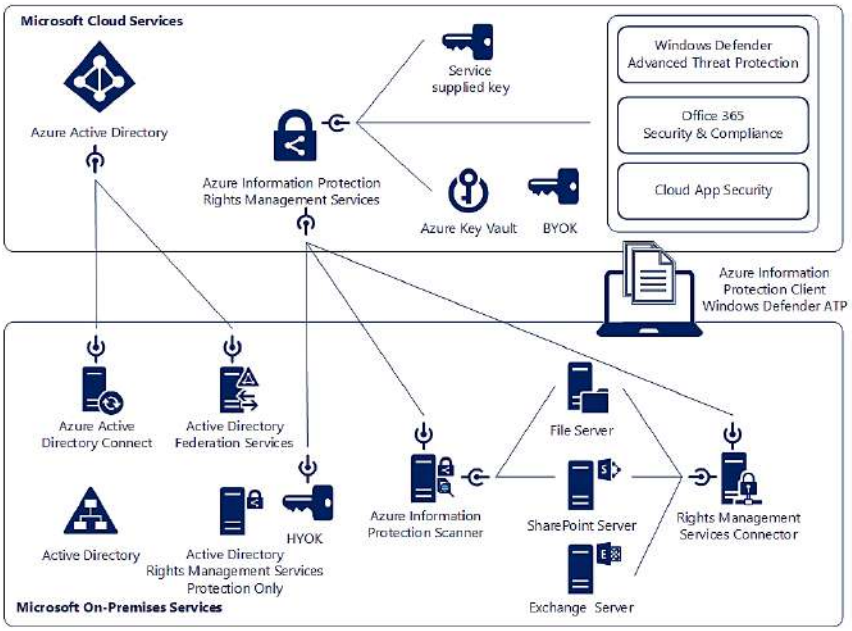


Рисунок 36 – Концептуальна схема Azure Information Protection [20] – [22]

Основні характеристики та можливості Azure Information Protection включають [20] – [22]:

1. AIP дозволяє організаціям класифікувати дані в залежності від їхньої важливості та конфіденційності. Це включає в себе надання категорій та міток, які вказують на рівень конфіденційності.
2. AIP надає можливість шифрувати дані на різних рівнях, забезпечуючи захист від несанкціонованого доступу та розповсюдження.
3. Організації можуть встановлювати політики безпеки для управління доступом до конфіденційних даних. Це включає в себе обмеження доступу, аудит та інші заходи безпеки.

4. AIP допомагає запобігти витоку конфіденційних даних шляхом обмеження можливості копіювання, друку та розповсюдження даних.
5. AIP інтегрований з іншими службами Microsoft, такими як Microsoft 365 та Azure Active Directory, для забезпечення єдиного підходу до захисту даних та інформації.
6. AIP надає можливість моніторити використання та розповсюдження конфіденційної інформації та аналізувати події, пов'язані з безпекою даних.

Azure Information Protection є важливим інструментом для організацій, які прагнуть забезпечити безпеку та конфіденційність своїх даних та інформації. Воно дозволяє класифікувати, захищати та контролювати доступ до даних, забезпечуючи високий рівень безпеки в цифровому середовищі.

Microsoft Defender for Endpoint є інтегрованим рішенням для захисту кінцевих точок (комп'ютерів, ноутбуків, мобільних пристроїв) в організаціях. Воно надає широкий спектр захисних можливостей для виявлення, запобігання та відновлення від кіберзагроз, зокрема, від вірусів, троянців, атак рейдерів та інших загроз безпеці [20] – [22] (Рисунок 37).

Основні характеристики та можливості Microsoft Defender for Endpoint включають:

1. Антивірусний захист: Рішення включає антивірусний захист, який допомагає виявляти та блокувати віруси та шкідливі програми на кінцевих точках.
2. Захист від загроз в реальному часі: Microsoft Defender for Endpoint надає захист в реальному часі, виявляючи та реагуючи на кіберзагрози миттєво.
3. Захист від рейдерів та шкідливих програм: Він виявляє та блокує атаки рейдерів та шкідливі програми, які можуть використовувати вразливості в системі.

4. Аналітика та інтелігентний виявлення загроз: Microsoft Defender for Endpoint використовує штучний інтелект і машинне навчання для виявлення складних та розширених загроз.
5. Інтеграція з іншими службами Microsoft: Воно інтегроване з іншими рішеннями Microsoft, такими як Azure Active Directory, для забезпечення єдиного підходу до безпеки та доступу.
6. Моніторинг та аналітика: Microsoft Defender for Endpoint надає можливість моніторити та аналізувати події, пов'язані з безпекою кінцевих точок, для виявлення потенційних загроз.

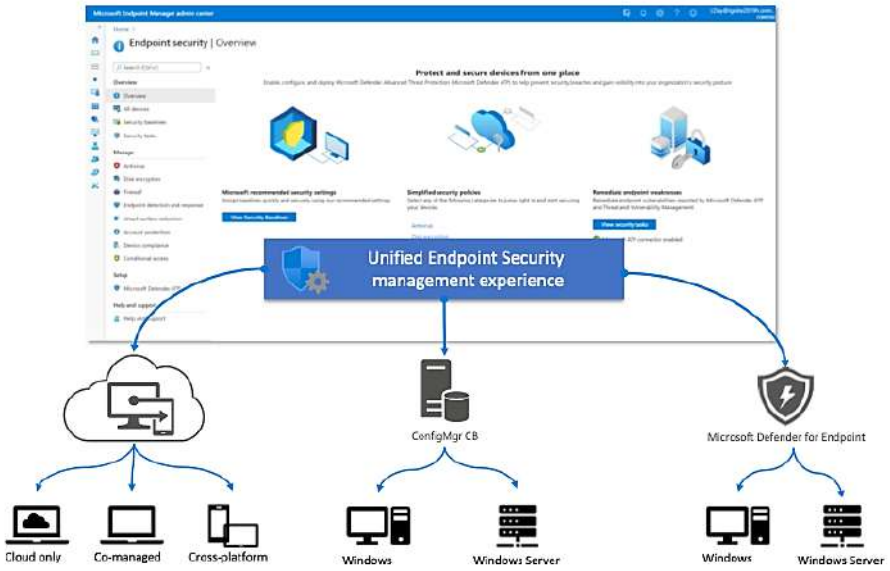


Рисунок 37 – Концептуальна схема Microsoft Defender for Endpoint [20] – [22]

Microsoft Defender for Endpoint допомагає організаціям забезпечити захист та безпеку їхніх кінцевих точок в цифровому середовищі. Воно дозволяє виявляти та запобігати кіберзагрозам, зменшуючи ризик компрометації даних та інфраструктури.

Intune App Protection Policies – це компонент рішення Microsoft Intune, який дозволяє організаціям захищати корпоративні дані та додатки на мобільних пристроях, забезпечуючи безпеку та контроль над їхнім використанням [20] – [22] (Рисунок 38).

Рисунок 38 – Концептуальна схема Intune App Protection Policies [20] – [22]

Основні характеристики та можливості Intune App Protection Policies включають [20] – [22]:

1. Політики захисту додатків Intune дозволяють класифікувати дані, вказуючи, які дані вважаються конфіденційними та які необхідно захищати.
2. Політики дозволяють встановлювати обмеження на доступ до конфіденційних даних з мобільних додатків. Наприклад, можна визначити, що користувачі можуть відкривати певні додатки тільки після аутентифікації.
3. Intune App Protection Policies дозволяє шифрувати дані в конфіденційних додатках та відслідковувати їх розповсюдження.
4. У випадку втрати мобільного пристрою або виходу співробітника з організації, Intune дозволяє віддалено видалити конфіденційні дані з пристрою.
5. Політики дозволяють інтегрувати корпоративні додатки з Intune, забезпечуючи захист корпоративних даних та інформації.

Intune App Protection Policies допомагає організаціям забезпечити безпеку та контроль над корпоративними даними та додатками на мобільних пристроях. Воно дозволяє інтегрувати безпеку в мобільні додатки та

захищати конфіденційні дані, зменшуючи ризик витоку інформації та порушення безпеки.

Таким чином, архітектура Microsoft Intune – це комплексний інформаційно-технічний структурний фреймворк, спроектований для забезпечення комплексного управління та безпеки кінцевих точок в організаціях. Вона включає в себе різні компоненти та функціональні можливості, що дозволяють організаціям ефективно управляти мобільними пристроями, додатками та даними, забезпечуючи безпеку та контроль над цифровим середовищем.

Архітектура Intune включає в себе такі ключові елементи [20] – [22]:

- Mobile Device Management (MDM) для управління мобільними пристроями та їхніми налаштуваннями.
- Mobile Application Management (MAM) для контролю та безпеки мобільних додатків.
- Conditional Access для встановлення умов доступу до ресурсів та даних.
- Azure Information Protection для захисту та управління конфіденційністю даних.
- Microsoft Defender for Endpoint для захисту кінцевих точок від кіберзагроз.
- Intune App Protection Policies для контролю доступу та захисту корпоративних даних в мобільних додатках.

Архітектура Intune дозволяє організаціям забезпечити цифрову безпеку та контроль над ресурсами та даними, незалежно від типу пристрою або місця роботи. Вона інтегрована з іншими рішеннями Microsoft та надає єдиний підхід до управління та безпеки в сучасному цифровому середовищі. Архітектура Intune є важливою для забезпечення безпеки та продуктивності співробітників у сучасних організаціях.

2.3 Загальна концепція Zero Trust

Zero Trust – це стратегічний підхід до кібербезпеки, який передбачає, що нікому або нічому не слід автоматично довіряти, навіть якщо вони вже перебувають в межах мережі. Ця концепція визначається тим, що доступ до ресурсів та інформації повинен бути надано лише після успішної ідентифікації та автентифікації, а потім надавати мінімальний необхідний рівень доступу, усі інші спроби доступу розглядаються як потенційно небезпечні та вимагають додаткової перевірки. Ключові принципи Zero Trust включають перевірку ідентичності та авторизації для кожного запиту на доступ, мінімізацію прав доступу та постійний моніторинг та аналіз активності для виявлення підозрілих або аномальних змін [67] – [69] – Рисунок 53.

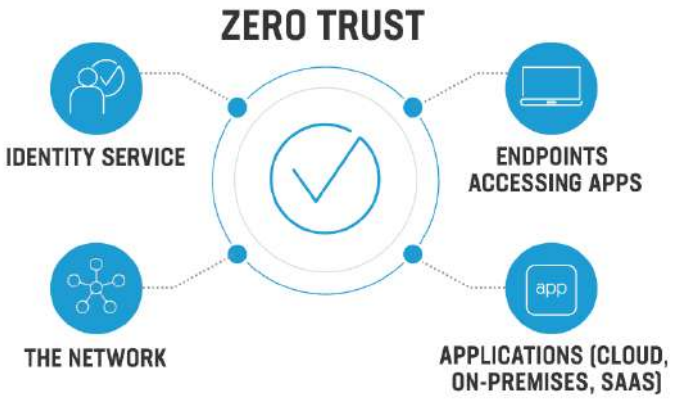


Рисунок 53 – Загальна концепція Zero Trust [67] – [69]

Концепція Zero Trust у сфері кібербезпеки передбачає відмову від традиційної моделі периметра та припускає, що нікому, навіть вже присутнім в мережі користувачам чи пристроям, не слід автоматично довіряти. У рамках цієї концепції доступ до ресурсів та інформації надається тільки після успішної перевірки ідентифікації та автентифікації, при цьому надається лише мінімально необхідний рівень доступу. Основні принципи Zero Trust включають неперервну перевірку та авторизацію для кожного запиту,

мінімізацію прав доступу та постійний моніторинг активності для виявлення небезпечних або підозрілих дій [70] – [72] – Рисунок 54.

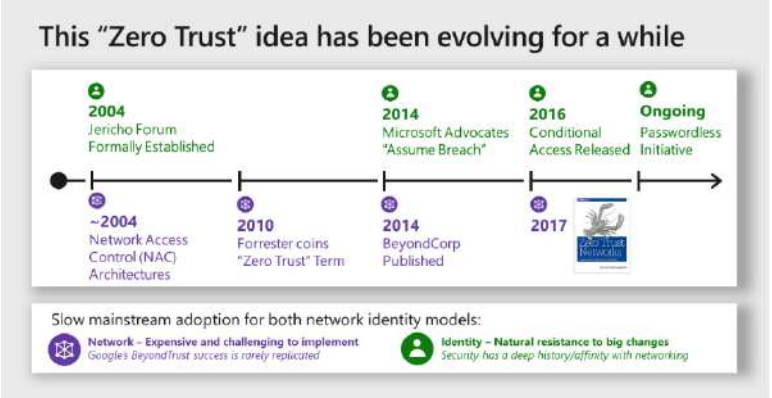


Рисунок 54 – Еволюція концепції Zero Trust [70] – [72]

Використання концепції Zero Trust передбачає перехід від традиційної довірчої моделі, де користувачі та пристрої, які перебувають всередині мережі, автоматично вважаються довіреними, до більш суворої системи перевірки ідентифікації та авторизації (Рисунок 55) [70] – [72].

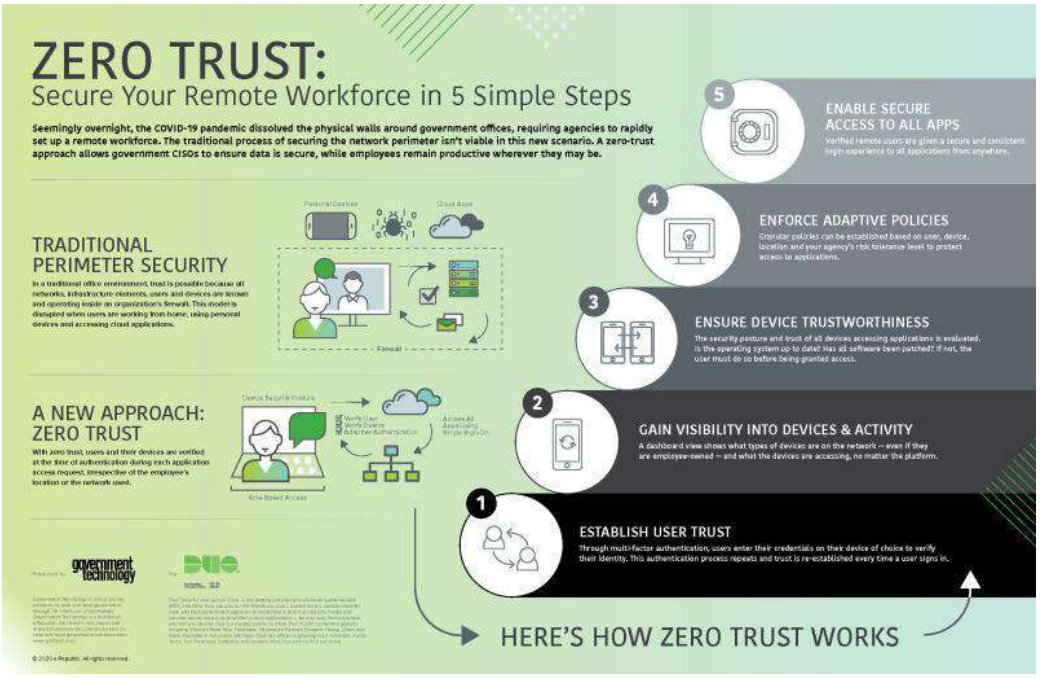


Рисунок 55 – Алгоритм переходу на систему безпекової організації Zero Trust [70] – [72]

Zero Trust виключає ідею великих довірчих зон всередині мережі. Замість цього, доступ до ресурсів базується на конкретних характеристиках користувача, пристрою, мережі та інших факторах. Принцип найменшого дозволу (Least Privilege) використовується для забезпечення того, що користувачеві чи пристрою надається лише той рівень доступу, який необхідний для виконання конкретної роботи чи завдання.

Всі запити на доступ періодично перевіряються, ідентифікуючи користувача чи пристрій. Це включає в себе багатофакторну аутентифікацію та інші методи перевірки. Здатність виявляти незвичайну чи підозрілу активність є ключовою частиною концепції Zero Trust. Мережева активність постійно моніториться для вчасного виявлення можливих загроз.

Захищений обмін інформацією між користувачами та ресурсами за допомогою шифрування сприяє забезпеченню конфіденційності та цілісності даних. Розгортання додатків у вигляді мікросервісів дозволяє ізолювати та захищати окремі компоненти додатку, зменшуючи вплив можливих атак [70] – [72].

Здатність ідентифікувати та контролювати доступ пристроїв, які підключаються до мережі, є важливою частиною Zero Trust для запобігання компрометацій від нещасних пристроїв.

Ці практики дозволяють створити більш ефективну та безпечну кібербезпекову модель, особливо в умовах зростаючого обсягу та різноманітності кіберзагроз.

Компаративний аналіз концепцій традиційної довірчої моделі та моделі Zero Trust (Рисунок 56) [73] – [75]:

1. Традиційна Довірча Модель:
    - *Принцип:* Парадигма внутрішнього захисту, де сховища ресурсів вважаються довіреними, надаючи широкий доступ внутрішнім користувачам.

- *Доступ:* Внутрішні користувачі мають значний обсяг доступу без інтенсивної перевірки.
- *Мінімізація:* Мінімальна обмеженість прав, спрямована на захист периметру мережі.

2. Zero Trust Модель:
   - *Принцип:* Заснована на неприпущенні довіри навіть внутрішнім користувачам чи пристроям, і вимагає інтенсивної аутентифікації для обмеженого доступу.
   - *Доступ:* Рішуче обмежений доступ лише до необхідних ресурсів, піддається строгому контролю.
   - *Мінімізація:* Акцент на принципі найменшого дозволу, що передбачає обмеження прав на необхідний мінімум.
3. Переваги Zero Trust:
   - *Захист від внутрішніх загроз:* Забезпечує високий рівень захисту від інсайдерських загроз та випадків компрометації.
   - *Гнучкість:* Спроможність адаптуватися до розподіленої та гібридної інфраструктур, що стає більш поширеним явищем.
   - *Мінімізація поверхні атак:* Активно зменшує можливість атак, концентруючи доступ лише на конкретних аутентифікаційних факторах.
4. Обмеження Zero Trust:
   - *Складність впровадження:* Імплементація вимагає ретельного планування та розгляду і може виявитися витратною та часоємкою.

- *Можливий вплив на продуктивність:* Забезпечення високого рівня безпеки може призвести до додаткових етапів аутентифікації, що потенційно впливає на продуктивність.

5. Застосування:
   - *Традиційна модель:* Зазвичай ефективна в менших організаціях з менш складними мережами.
   - *Zero Trust:* Зокрема ефективна в умовах великих корпорацій, де розподілена робота та збільшення кількості зовнішніх загроз є актуальними.
6. Засоби використання:
   - *Традиційна модель:* Базується на традиційних мережевих файрволах та стандартних системах безпеки.
   - *Zero Trust:* Використовує різноманітні засоби, включаючи багатофакторну аутентифікацію, активний моніторинг та сучасні засоби кіберзахисту.
7. Майбутнє:
   - *Традиційна модель:* Може стикатися з викликами в умовах зростаючих кіберзагроз та еволюції корпоративних інфраструктур.
   - *Zero Trust:* Очікується, що вона буде домінуючою в контексті зростаючої популярності хмарних технологій та розподіленого робочого середовища.

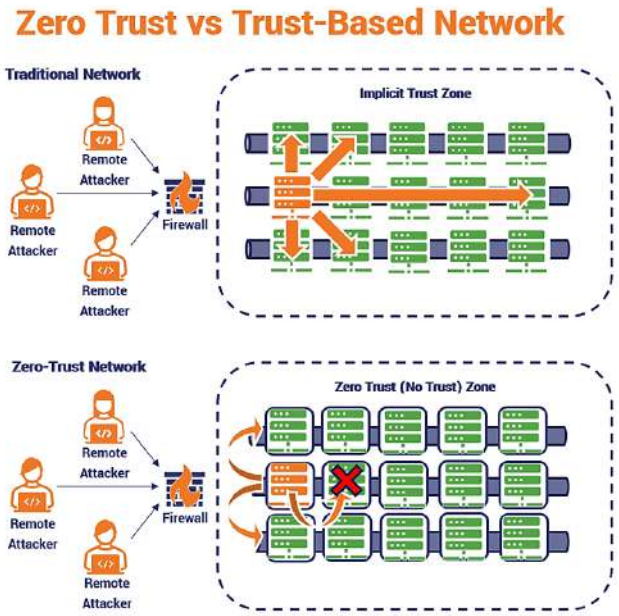


Рисунок 56 – Компаративний аналіз довірчої моделі та моделі Zero Trust [73] – [75]

Комплексний аналіз відзначає переваги концепції Zero Trust у забезпеченні вищого рівня безпеки в умовах динамічного кіберзагроз та еволюції корпоративних інфраструктур.

Zero Trust – це концепція безпеки, яка визначає, що ніякий користувач чи пристрій не повинен автоматично довірятися всередині корпоративної мережі, навіть якщо вони перебувають в межах цієї мережі. У рамках Microsoft Intune, рішення для управління мобільними пристроями та захисту корпоративних даних, принципи Zero Trust втілені для максимізації кібербезпеки [76] – [79] (Рисунок 57).

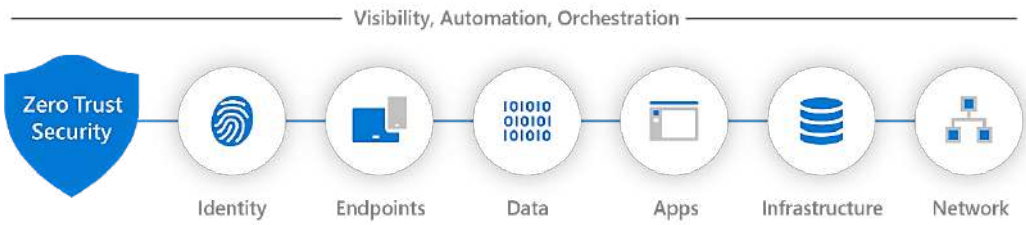


Рисунок 57 – Загальна концепція Zero Trust Microsoft Intune [76] – [79]

Одним із ключових аспектів впровадження Zero Trust в Microsoft Intune є строге управління доступом та аутентифікацією. Застосовуються принципи

мінімізації дозволів, а також використання багатофакторної аутентифікації (MFA), що робить можливим підтвердження ідентифікації користувача в безпечний спосіб.

Microsoft Intune надає централізоване управління конфігураціями пристроїв та застосуванням політик безпеки, що спрощує управління профілем та політикою. Крім того, реалізується дистанційне видалення даних з втрачених чи вкрадених пристроїв.

Ще однією важливою складовою є захист інформації. Intune використовує шифрування для забезпечення конфіденційності даних під час їх передачі та зберігання. Активний моніторинг та аналітика безпеки дозволяють виявляти незвичайну активність та вчасно реагувати на потенційні загрози.

Також слід відзначити інтеграцію Microsoft Intune з іншими рішеннями Microsoft 365 та Azure, що створює єдиний екосистемний підхід до безпеки, забезпечуючи тим самим комплексний захист організаційних ресурсів [76] – [79].

Таким чином, загальна концепція Zero Trust визначає новий стандарт підходу до кібербезпеки, в якому перевірка та автентифікація користувачів та пристроїв вважаються обов'язковими, незалежно від їхнього місцезнаходження в мережі. Вимагаючи від кожного елемента мережі постійного підтвердження своєї ідентичності та намагаючись мінімізувати довіру, Zero Trust вирізняється своєю передовою стратегією захисту.

У концепції Zero Trust важливу роль відіграють принципи мінімізації дозволів, використання багатофакторної аутентифікації та активний моніторинг безпеки. Впровадження цієї концепції в контексті Microsoft Intune дозволяє створити надійне та ефективне середовище управління мобільними пристроями та захисту корпоративних ресурсів.

Застосування Zero Trust не лише високоефективно забезпечує кібербезпеку, але й стає важливим етапом у відповіді на постійно зростаючі

цифрові загрози, демонструючи потужний та передовий підхід до захисту інформації та інфраструктури.

Висновок до 2 розділу

Microsoft Intune – це інтегрована платформа для управління кінцевими точками та забезпечення цифрової безпеки в організаціях. Вона дозволяє організаціям ефективно управляти мобільними пристроями, додатками та даними, забезпечуючи безпеку та контроль над цифровим середовищем. Основні характеристики включають Mobile Device Management (MDM), Mobile Application Management (MAM), Conditional Access, Azure Information Protection, Microsoft Defender for Endpoint та Intune App Protection Policies.

Процедура розгортання Microsoft Intune включає кілька кроків, які включають в себе реєстрацію в службі, налаштування параметрів, реєстрацію кінцевих точок, створення політик безпеки, моніторинг та аналіз, навчання та оптимізацію. Ця процедура вимагає глибоких знань інформаційно-технічної безпеки та системного адміністрування. Правильно розгорнутий Microsoft Intune допомагає зменшити ризики і забезпечує безпеку даних та пристроїв, що використовуються в організації, і підвищує загальну продуктивність користувачів.

3 ІМПЛЕМЕНТАЦІЯ АРХІТЕКТУРИ ZERO TRUST ДЛЯ ІДЕНТИФІКАТОРІВ І КІНЦЕВИХ ТОЧОК ЗА ДОПОМОГОЮ ІНСТРУМЕНТІВ MICROSOFT INTUNE

3.1 Процедура розгортання Microsoft Intune

Процедура розгортання Microsoft Intune є складним технічним процесом, спрямованим на забезпечення безпеки та ефективного управління кінцевими точками, даними та додатками в організаціях. Ця процедура передбачає реєстрацію та налаштування служби Intune, реєстрацію кінцевих точок, створення та налаштування політик безпеки, моніторинг та аналіз безпеки та продуктивності, а також навчання користувачів та адміністраторів.

Розглянемо типову схему розгортання Microsoft Intune на підприємстві. Microsoft Intune розгортається для певних категорій користувачів, що адмініструються профільними менеджерами організації [20] – [22] – Рисунок 39.

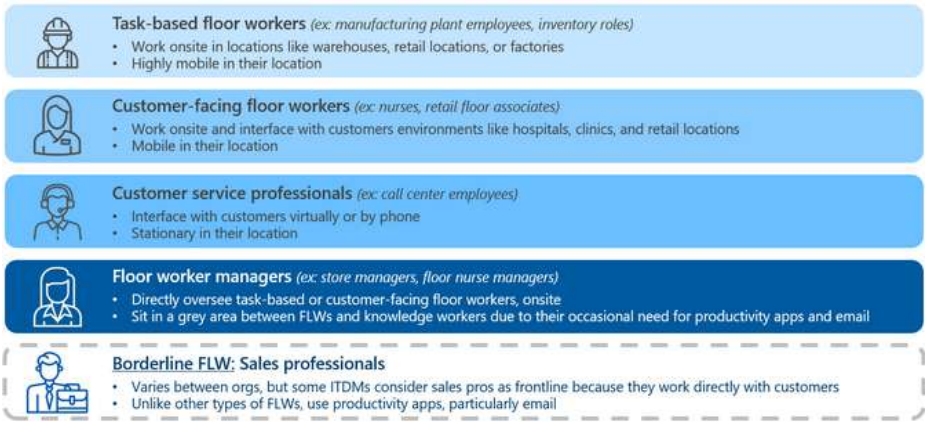


Рисунок 39 – Типові категорії користувачів системи Microsoft Intune

Відповідні категорії інфраструктури Microsoft Intune використовуються відповідні коросплатформенні цифрові засоби [20] – [22] – Рисунок 40.

Рисунок 40 – Кросплатформенний взаємозв’язок між окремими категоріями користувачів інфраструктури Microsoft Intune [20] – [22]

Варіації розгортання Microsoft Intune передбачають 4 архітектурні принципи [20] – [22] – Рисунок 41.

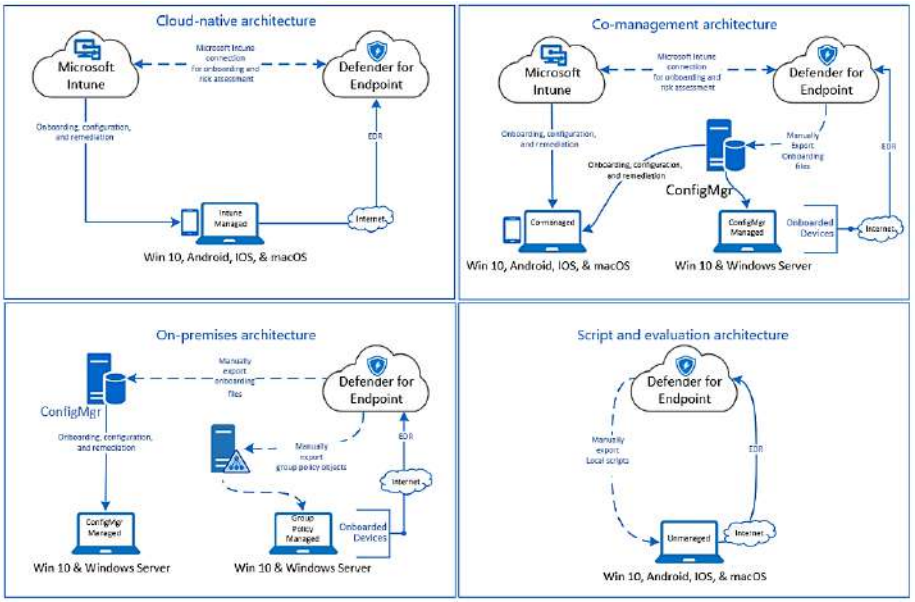


Рисунок 41 – Варіація розгортання Microsoft Intune на підприємстві

Розгортання Microsoft Intune вимагає глибоких знань у сфері інформаційно-технічної безпеки та системного адміністрування. Важливо дотримуватися кращих практик та рекомендацій, щоб забезпечити безпеку та ефективність цього процесу.

Правильно розгорнутий Microsoft Intune допомагає організаціям забезпечити захист конфіденційних даних та оптимальне управління

кінцевими точками, зменшуючи ризики та підвищуючи продуктивність користувачів.

Процедура розгортання Microsoft Intune включає наступні кроки [20] – [22] (Рисунок 42):

1. Реєстрація в службі Microsoft Intune: Реєстрація в системі виконується через входження в адміністративний обліковий запис Microsoft 365 або Azure, після чого доступні відповідні опції реєстрації служби Microsoft Intune.
2. Конфігурація налаштувань: Встановлення налаштувань розгортання включає параметри, такі як обмеження доступу, налаштування політик безпеки і визначення параметрів користувачів.
3. Реєстрація кінцевих точок: Реєстрація мобільних пристроїв, комп'ютерів і ноутбуків в системі Microsoft Intune виконується за допомогою різних методів, включаючи відправлення запрошень користувачам та використання автоматичних методів, таких як Mobile Device Management (MDM).
4. Налаштування політик безпеки: Створення і налаштування політик безпеки для різних типів пристроїв та додатків, включаючи Conditional Access, Mobile Application Management (MAM) і Intune App Protection Policies.
5. Моніторинг та аналіз: Налаштування системи моніторингу та аналізу для відстеження безпеки та продуктивності в цифровому середовищі.
6. Навчання та підтримка: Проведення навчання користувачів і адміністраторів щодо використання Microsoft Intune та забезпечення безпеки даних та пристроїв.
7. Тестування і оптимізація: Проведення тестування розгорнутої системи та оптимізація політик та налаштувань відповідно до потреб організації.

8. Супровід та оновлення: Регулярне оновлення політик та моніторинг для забезпечення актуальності та ефективності заходів безпеки.

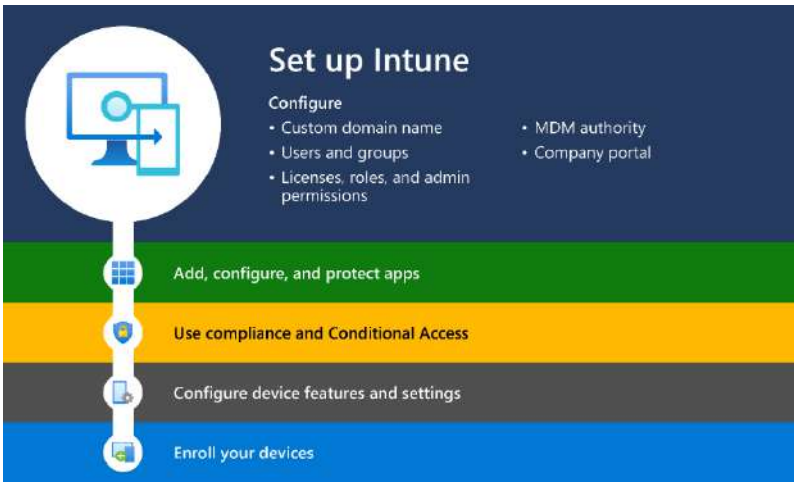


Рисунок 42 – Узагальнений алгоритм розгортання Microsoft Intune [20] – [22]

Процедура розгортання Microsoft Intune (Рисунок 42) дозволяє організаціям забезпечити безпеку та управління кінцевими точками, даними та додатками в цифровому середовищі, зменшуючи ризики та забезпечуючи продуктивність користувачів.

Відповідно формується централізована система контролю та безпеки мультидивайсних та кросплатформерних корпоративних мереж, що формується від концептуальної (Рисунок 43) до розгорнутої (Рисунок 44) схеми.

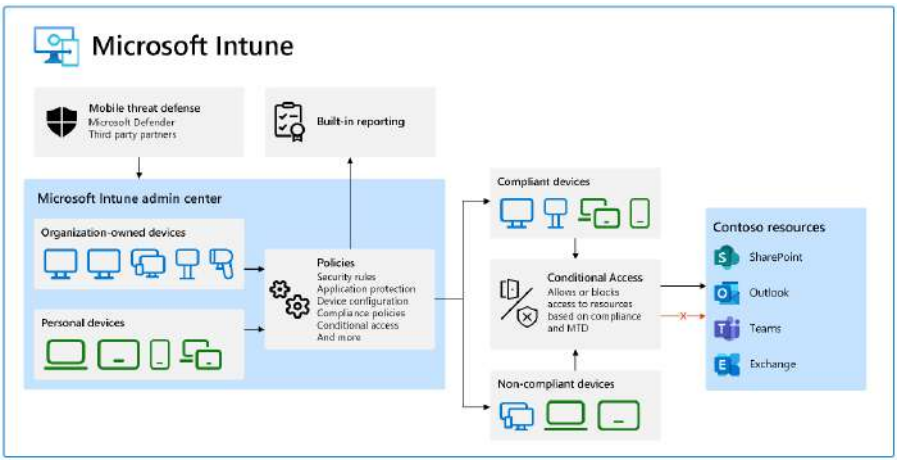


Рисунок 43 – Концептуальна схема розгортання Microsoft Intune [20] – [22]

Запроваджена система Microsoft Intune дозволяє отримувати широкі можливості до аналітики, контролю та забезпечення кібербезпеки корпоративної мережі, що відображено на рисунках нижче – Рисунок 45 –

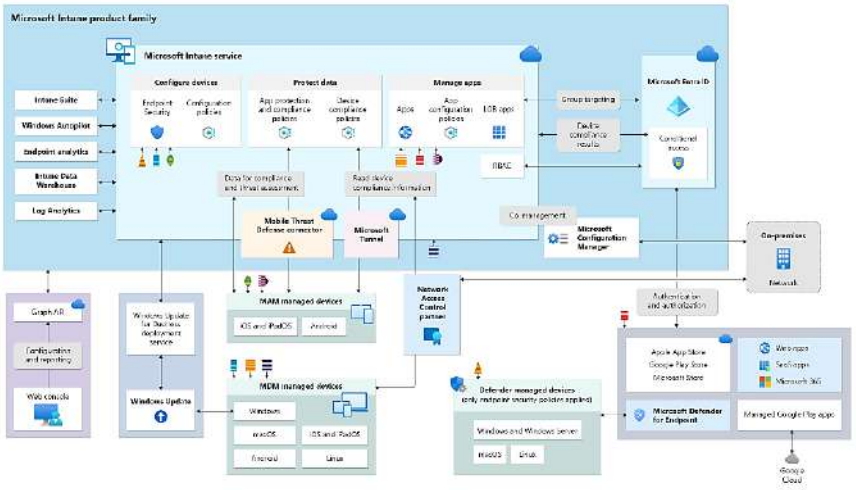


Рисунок 44 – Розгорнута схема корпоративної мережі організації, сформована на базі хмарних рішень Microsoft Intune [20] – [22]

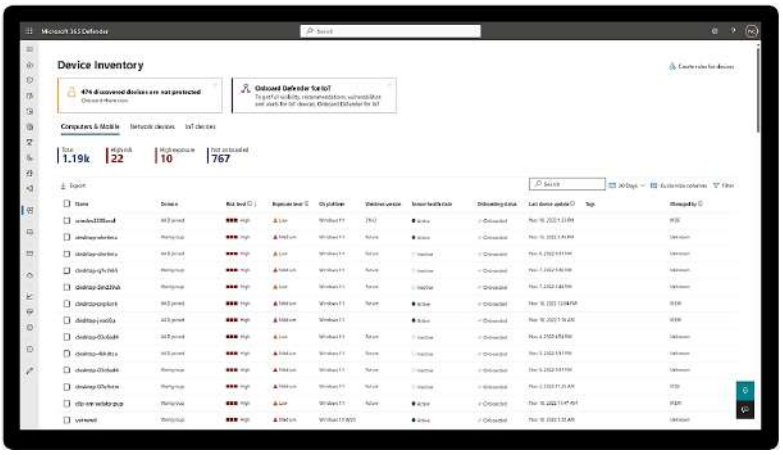


Рисунок 45 – Ризик-менеджмент мультидевайсної корпоративної мережі

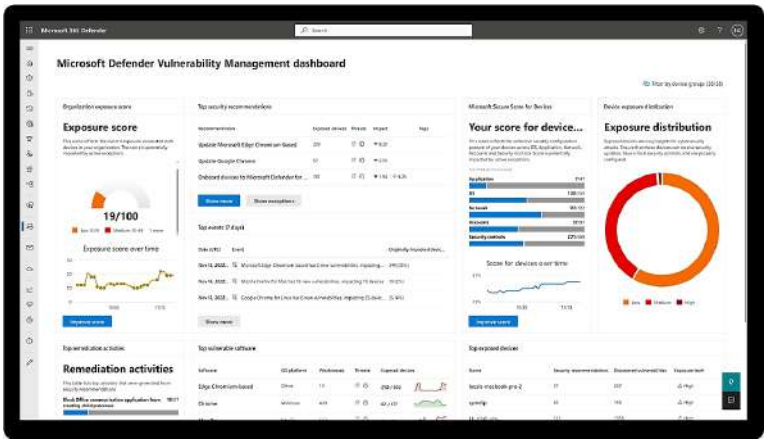


Рисунок 46 – Потоковий аналіз та контроль стану кібербезпеки корпоративної мережі організації [20] – [22]

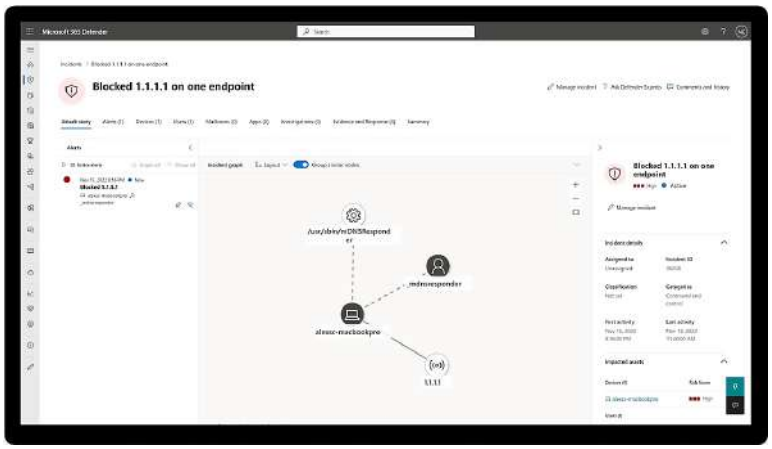


Рисунок 47 – Автоматизовані алгоритму усунення вразливостей та атак за допомогою системи Microsoft Intune в корпоративній мережі підприємства

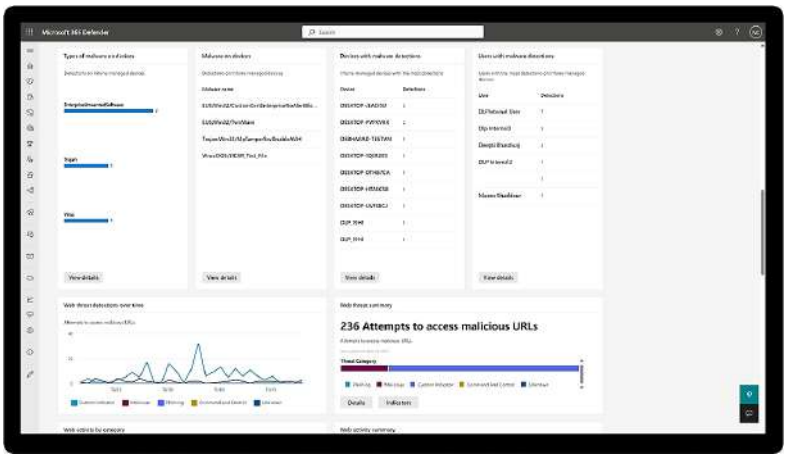


Рисунок 48 – Контроль вразливостей програмних засобів та додатків, що інтегровані до корпоративної мережі [20] – [22]

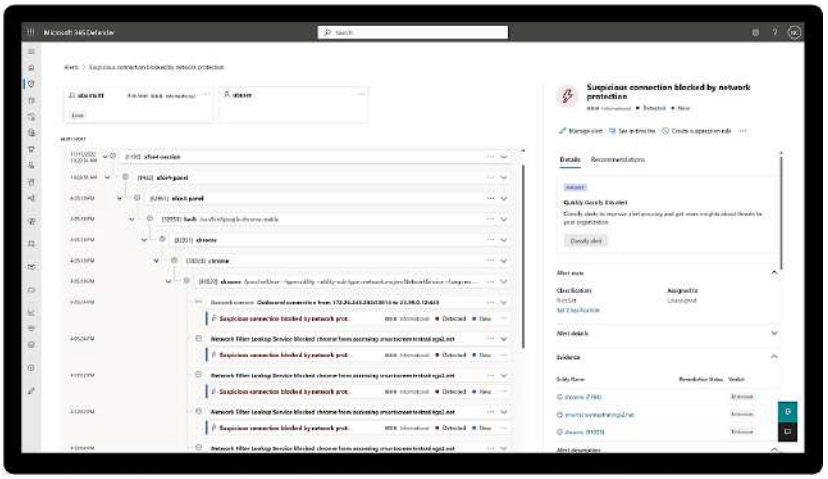


Рисунок 49 – Застосування генеративних алгоритмів з виявлення вразливостей корпоративної мережі [20] – [22]

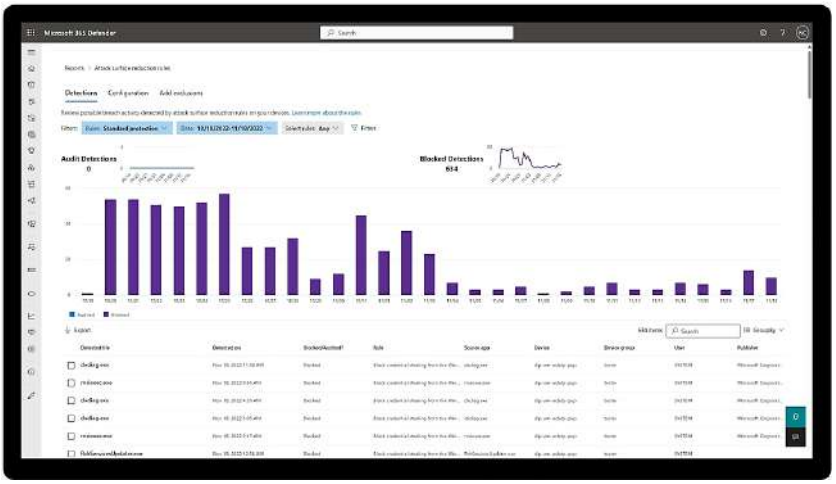


Рисунок 50 – Моніторинг та аналіз вразливостей корпоративної мережі

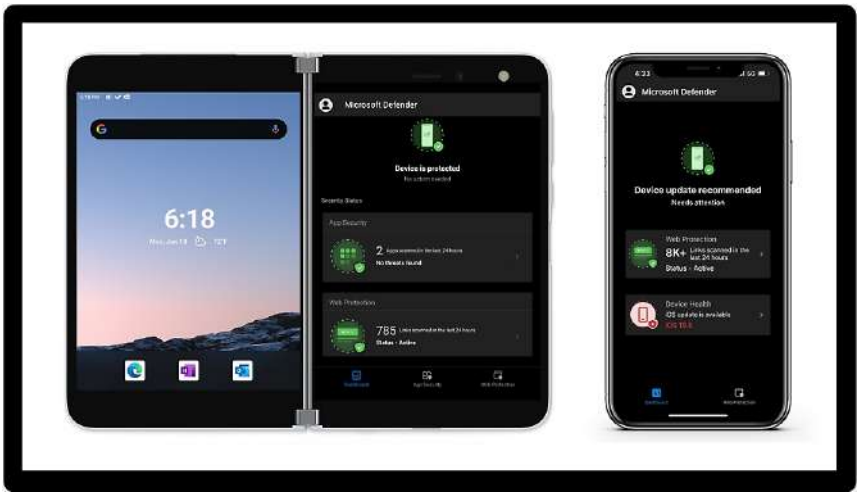


Рисунок 51 – Контроль та захист мобільних платформ корпоративної мережі

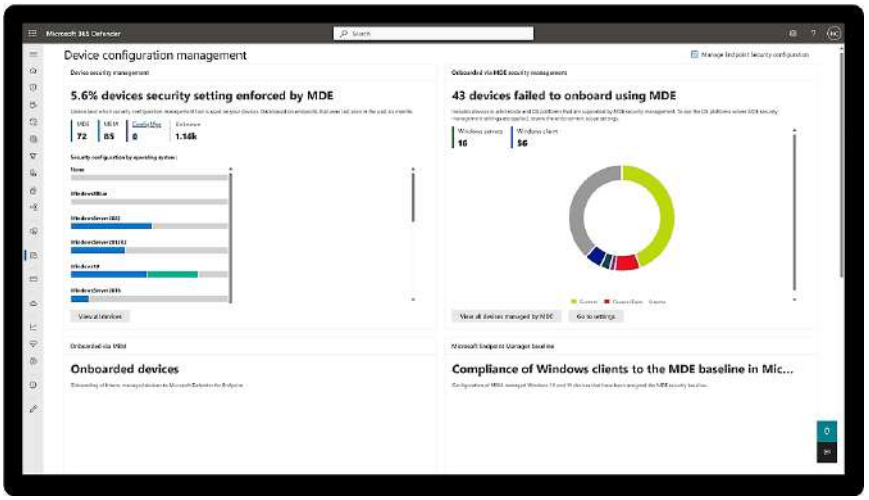


Рисунок 52 – Контроль та аналіз функціонування мультидевайсної кросплатформенної корпоративної мережі [20] – [22]

Таким чином, процедура розгортання Microsoft Intune є важливим кроком для організацій, які бажають забезпечити безпеку та контроль над кінцевими точками, даними та додатками в своєму цифровому середовищі. Вона включає в себе кілька кроків, включаючи реєстрацію, налаштування, реєстрацію кінцевих точок, створення політик безпеки, моніторинг, навчання та оптимізацію.

3.2 Архітектура Zero Trust

Архітектура Zero Trust представляє собою комплексний підхід до кібербезпеки, орієнтований на мінімізацію довіри та постійну перевірку ідентичності кожного елемента мережі. Вона включає в себе ряд ключових принципів та компонентів, спрямованих на забезпечення високого рівня безпеки в умовах постійно зростаючих цифрових загроз.

Основний принцип Zero Trust полягає в обмеженні доступу до мережевих ресурсів лише тим користувачам та пристроям, які безперечно потребують цього доступу для виконання своїх завдань. Застосування багатофакторної аутентифікації підвищує рівень безпеки шляхом використання кількох методів перевірки ідентичності, таких як пароль, фізичний ключ або біометричні дані. Активний моніторинг мережі дозволяє виявляти незвичайну активність та надзвичайні події, вчасно реагуючи на потенційні загрози безпеки. Розділення мережі на мікропериметри допомагає обмежувати зони доступу, ускладнюючи рух по мережі для потенційних зловмисників [80] – [82] – Рисунок 58.

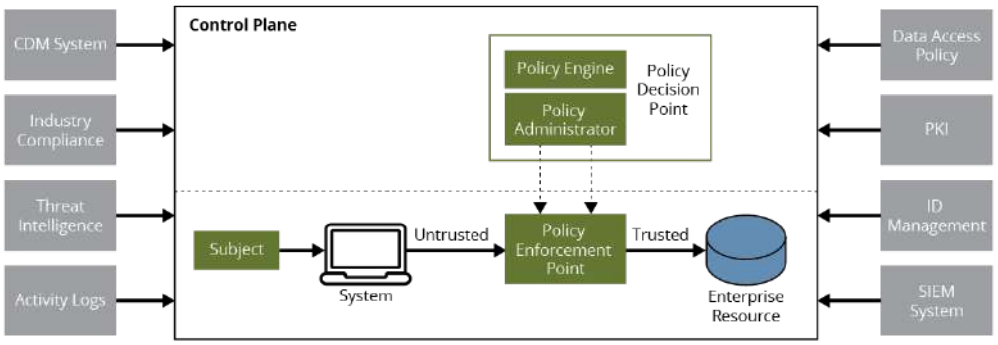


Рисунок 58 – Концептуальна схема архітектури Zero Trust [80] – [82]

Елементи архітектури Zero Trust включають різні компоненти, які працюють у взаємодії для забезпечення високого рівня кібербезпеки (Рисунок 58) [80] – [82]:

1. Policy Engine – відповідає за розробку та визначення політик безпеки, які контролюють доступ до ресурсів та взаємодію з ними. Політичний рушій визначає, які дії та обмеження встановлюються для кожного користувача чи пристрою.
2. Policy Administrator – відповідає за управління та адміністрування політик безпеки. Адміністратор політики налаштовує та підтримує політики, забезпечуючи їх актуальність та відповідність поточним вимогам безпеки.
3. Policy Enforcement Point – відповідає за фактичне застосування політик безпеки. Точка виконання політики визначає, чи має конкретний користувач чи пристрій доступ до конкретного ресурсу відповідно до встановлених політик.
4. Continuous Diagnostics and Mitigation (CDM) System – використовується для постійного моніторингу та діагностики стану системи, а також для зменшення ризиків шляхом виявлення та виправлення потенційних проблем безпеки.
5. Industry Compliance System – відповідає за забезпечення відповідності до стандартів та вимог конкретної галузі чи регуляторного органу.
6. Threat Intelligence Feed – використовує дані про поточні кіберзагрози для посилення безпекових заходів та реакції на нові загрози.
7. Network and System Activity Logs – записують дії та активності в мережі та системі для подальшого аналізу та виявлення аномальної активності.
8. Data Access Policies – визначають умови та обмеження для доступу до конкретних даних, забезпечуючи конфіденційність та цілісність інформації.
9. Enterprise Public Key Infrastructure (PKI) – забезпечує безпеку комунікацій та ідентифікацію за допомогою шифрування на основі відкритих ключів.

10. ID Management System – відповідає за ефективне управління ідентифікацією користувачів та пристроїв.
11. Security Information and Event Management (SIEM) System – забезпечує централізований аналіз та реагування на події, пов'язані з безпекою.
12. Control Plane – забезпечує керування всіма аспектами мережі, включаючи політики безпеки та розподіл ресурсів.

Ці елементи працюють узгоджено, створюючи комплексну систему Zero Trust, яка відзначається високим рівнем безпеки та відсутністю довіри до будь-яких елементів мережі чи користувачів.

Забезпечення єдиного централізованого механізму ідентифікації та управління доступом спрощує впровадження та моніторинг політик безпеки. Акцент на безпеці кінцевих точок допомагає уникнути атак та захищає важливі дані від втрати або незаконного доступу. Zero Trust передбачає, що користувачі та пристрої мають довіреність на будь-якій мережі, враховуючи потенційні ризики та забезпечуючи захист навіть на ненадійних мережах. Система Zero Trust повинна бути інтегрованою частиною всієї стратегії кібербезпеки, взаємодіючи з різними засобами захисту та аналізу [80] – [82].

Ця комплексна архітектура створює надійний захист від сучасних цифрових загроз, допомагаючи організаціям долати виклики та забезпечувати безпеку в умовах динамічного кіберландшафту.

Архітектура Zero Trust включає низку ключових логічних складових та елементів, спрямованих на створення надійного і безпечного середовища для обробки даних та взаємодії користувачів у кіберпросторі [83] – [85] (Рисунок 59):

1. Централізована ідентифікація та управління доступом (CIAM) – відповідає за забезпечення централізованої системи ідентифікації користувачів і керування доступом до різних ресурсів в мережі. Використання CIAM дозволяє встановлювати та змінювати права доступу в реальному часі в залежності від контексту.

2. Багатофакторна аутентифікація (MFA) – забезпечує використання двох або більше методів ідентифікації для підтвердження особи користувача. Це може включати паролі, біометричні дані, фізичні токени, чи інші фактори.
3. Мережевий моніторинг та аналітика (Network Monitoring and Analytics) – відповідає за систематичний моніторинг мережі для виявлення аномальної або підозрілої активності. Використання аналітики дозволяє реагувати на потенційні загрози в реальному часі.
4. Сегментація мережі та мікропериметрия (Network Segmentation and Micro-Perimeter Security) – дозволяють розділити мережу на сегменти та створити мікропериметри для обмеження доступу до ресурсів та данних, зменшуючи поверхню атак.
5. Політика безпеки на рівні додатків (Application-Level Security Policies) – застосування політик безпеки на рівні додатків дозволяє забезпечити захист окремих додатків та сервісів, надаючи ретельний контроль над доступом до них.
6. Безпека кінцевих точок (Endpoint Security) – цей компонент орієнтований на захист пристроїв, які використовуються користувачами для доступу до мережі. Включає заходи безпеки, що забезпечують ідентифікацію, шифрування, та захист від загроз на рівні кінцевих точок.
7. Надійне інтернет-з'єднання (Secure Internet Connections) – включає заходи для забезпечення безпечного інтернет-з'єднання, включаючи використання VPN, захист від фішингу та інші технології.
8. Централізований моніторинг та управління подіями (Centralized Event Monitoring and Management) – для ефективності та швидкості реакції на потенційні загрози важливо мати централізовану систему моніторингу та управління подіями.

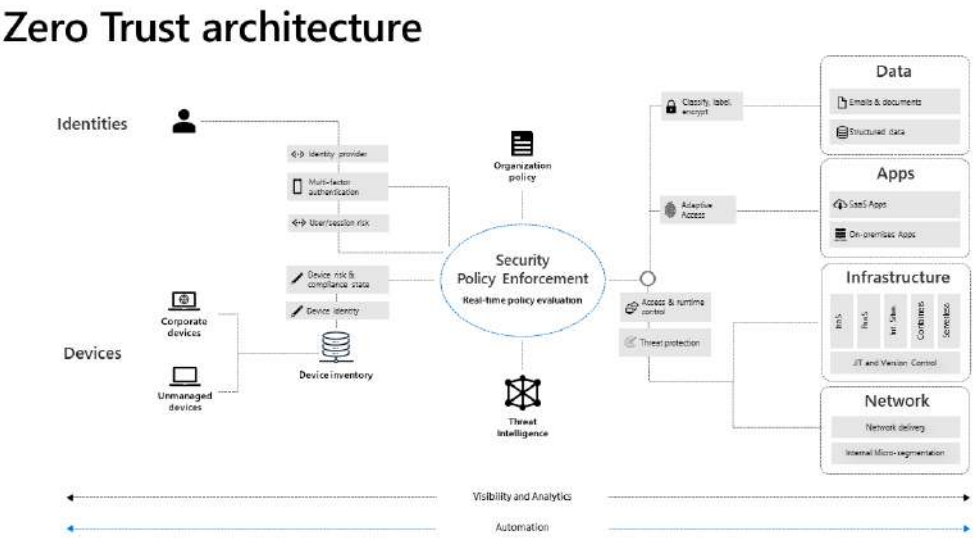


Рисунок 59 – Типова архітектура Zero Trust [83] – [85]

Ці складові взаємодіють між собою, створюючи повністю інтегровану та комплексну систему Zero Trust, яка забезпечує високий рівень безпеки в сучасному кіберпросторі.

Microsoft Intune – це рішення для управління мобільними пристроями та захисту корпоративних даних в хмарному середовищі. Архітектура Zero Trust в Microsoft Intune включає наступні компоненти [76] – [79] (Рисунок 60):

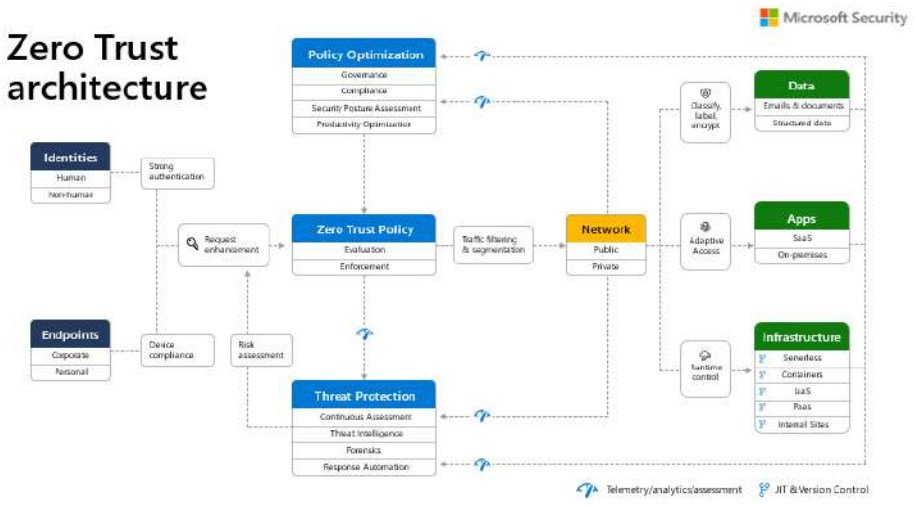


Рисунок 60 – Архітектура Zero Trust Microsoft Intune [76] – [79]

1. Security Policy Enforcement – включає в себе багатофакторну аутентифікацію з умовним доступом, який враховує ризик облікового

запису користувача, стан пристрою та інші критерії та політики, встановлені адміністратором.

2. Identities, Devices, Data, Apps, Network, and Other Infrastructure Components – усі ці аспекти, включаючи ідентифікацію, пристрої, дані, додатки, мережу та інші компоненти інфраструктури, конфігуруються з відповідними заходами безпеки. Кожен компонент має свої політики, які координуються зі загальною стратегією Zero Trust.
3. Device Policies – визначають критерії для здорових пристроїв. Вони враховуються при умовному доступі, що вимагає наявність здорових пристроїв для доступу до конкретних додатків та даних.
4. Conditional Access Policies – використовуються для забезпечення умовного доступу на основі різних факторів, таких як стан пристрою, ризик облікового запису користувача та інші критерії, що визначаються адміністратором.
5. Threat Protection and Intelligence – здійснює моніторинг оточення, виявляє поточні загрози та вживає автоматизованих заходів для ліквідації атак. Використовується система захисту від загроз та розуміння, щоб надавати інформацію про поточні ризики та вживати заходів для їх врегулювання.

Сформована в Microsoft Intune архітектура дозволяє реалізувати концепцію Zero Trust, де доступ до ресурсів надається на основі конкретних умов і оцінки безпеки пристрою та користувача. Всі компоненти працюють разом для створення безпечного та гнучкого оточення для користувачів та пристроїв у хмарному середовищі.

Таким чином встановлено, що архітектура Zero Trust представляє сучасний підхід до кібербезпеки, який ґрунтується на принципах недовіри до всіх елементів в мережі та неперервного моніторингу та перевірці ідентичності, доступу та активності. У цій архітектурі, нічого не вважається

автоматично надійним, навіть якщо пристрій або користувач раніше успішно автентифікувалися.

Основні складові Zero Trust включають в себе централізоване керування політикою безпеки, ідентифікацію та автентифікацію, захист від загроз та аналіз діяльності для виявлення аномалій. Взаємодія цих компонентів створює ефективний захисний бар'єр, що забезпечує безпеку даних та інфраструктури в умовах постійно зростаючого рівня кіберзагроз.

Архітектура Zero Trust представляє передовий стандарт у сфері кібербезпеки, надаючи високий рівень захисту в умовах постійно зростаючого рівня кіберзагроз. Зокрема, інтеграція рішень Microsoft Intune в цей концепт додає ефективність та гнучкість до області політики безпеки, ідентифікації, та захисту від загроз. За допомогою Microsoft Intune, вирішення проблем Zero Trust стає більш адаптивним та пристосованим до вимог сучасного користувача. Механізми мультифакторної аутентифікації, умовного доступу, та автоматизованого реагування на поточні загрози стають ключовими компонентами цієї архітектури, забезпечуючи комплексний захист для організацій у всіх сферах їхньої діяльності. Такий підхід не лише підвищує безпеку, але і дозволяє ефективно впроваджувати інновації, забезпечуючи високий рівень захисту у сучасному цифровому середовищі.

3.3 Розгортання та тестування архітектури Zero Trust для ідентифікаторів і кінцевих точок за допомогою інструментів Microsoft Intune

Відповідно до рекомендацій Microsoft для рішення Intune [76] – [79] розгортання архітектури Zero Trust виконується на базі хмарного рішення Microsoft 365 за наступним алгоритмом.

Крок 1: налаштування початкових політик безпеки Zero Trust – Рисунок 61.

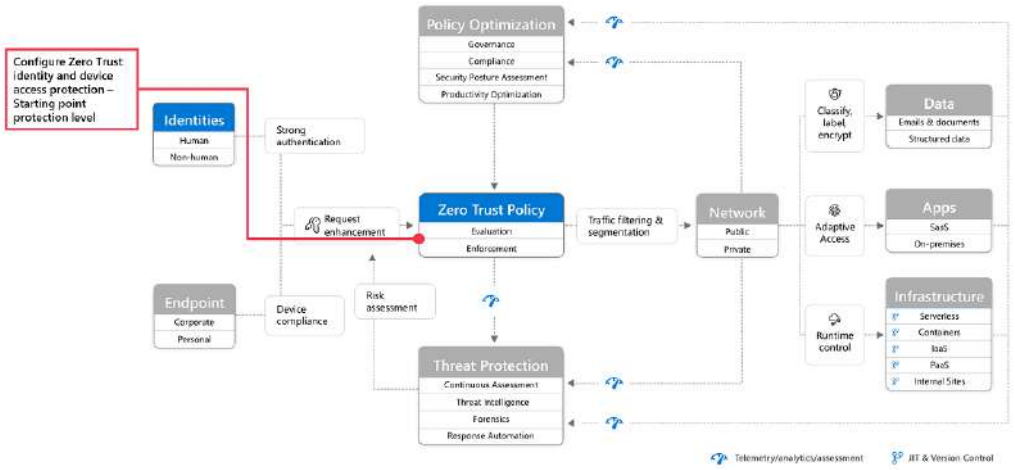


Рисунок 61 – Крок 1: налаштування початкових політик безпеки Zero Trust [76] – [79]

Початковий етап впровадження архітектури Zero Trust передбачає налаштування базових політик для ідентифікації та захисту доступу до кінцевих точок. Це включає в себе встановлення багатофакторної аутентифікації, політик умовного доступу, вимог до відповідності пристроїв та оцінки ризику облікових записів користувачів. Також реалізується аналітика поведінки користувачів та сутностей для виявлення аномалій, а управління призначеними правами обмежує доступ до привілейованих ролей. Встановлення базових конфігурацій безпеки для пристроїв та програм допомагає стандартизувати середовище та зменшити ризики. Цей етап є ключовим для створення міцної основи архітектури безпеки Zero Trust [76] – [79].

Крок 2: управління кінцевими точками за допомогою Intune – Рисунок 62.

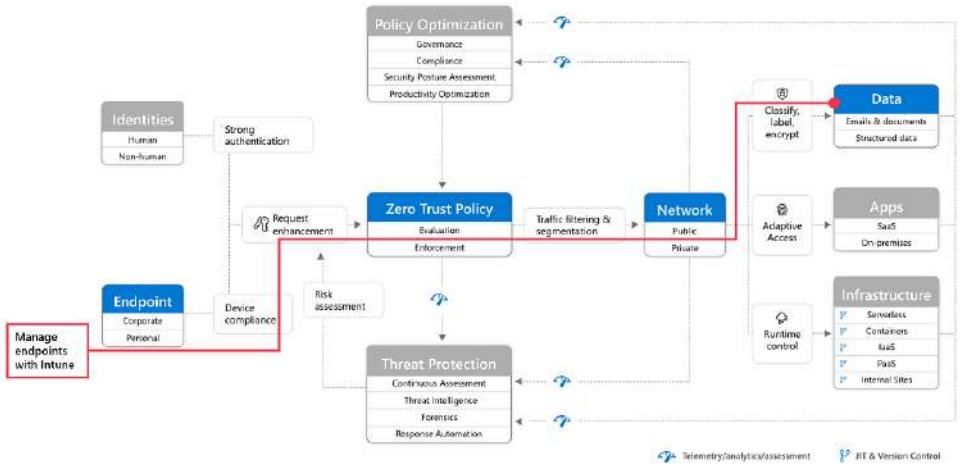


Рисунок 62 – Крок 2: управління кінцевими точками за допомогою Intune [76] – [79]

Другий крок впровадження архітектури Zero Trust передбачає управління кінцевими точками за допомогою інструментів Microsoft Intune. Intune забезпечує централізоване управління політиками безпеки для пристроїв, включаючи комп'ютери, смартфони та планшети. Це включає конфігурацію політик умовного доступу, вимог до відповідності та встановлення заходів безпеки, таких як шифрування даних та встановлення антивірусів. Платформа також надає моніторинг стану пристроїв, виявлення та вирішення проблем безпеки, що допомагає забезпечити сталу безпеку ідентифікованих кінцевих точок відповідно до принципів Zero Trust [76] – [79].

Крок 3: додавання пристроїв та налаштування корпоративних політик безпеки – Рисунок 63.

Третій крок впровадження архітектури Zero Trust передбачає додавання підприємницьких політик для захисту ідентифікаторів та доступу пристроїв. Це включає конфігурацію політик, які визначають стандарти безпеки для ідентифікаторів користувачів та умов доступу до корпоративних ресурсів. Політики умовного доступу, які враховують ризики облікового запису користувача та стан пристрою, встановлюють критерії доступу до інформації та додатків. Це допомагає створити міцний захист для ідентифікаційних

даних і забезпечити високий рівень безпеки для користувачів та їх пристроїв у відповідності з принципами Zero Trust [76] – [79].

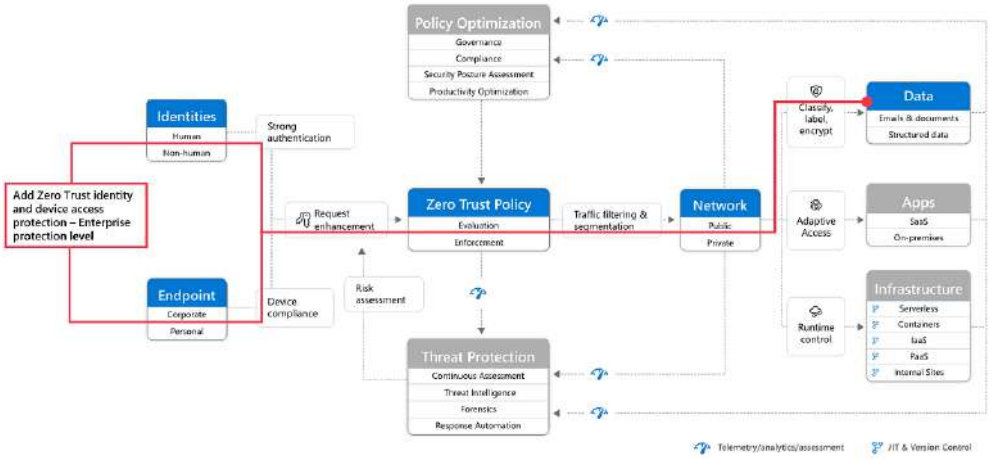


Рисунок 63 – Крок 3: додавання пристроїв та налаштування корпоративних політик безпеки [76] – [79]

Крок 4: розгортання Microsoft Defender XDR – Рисунок 64.

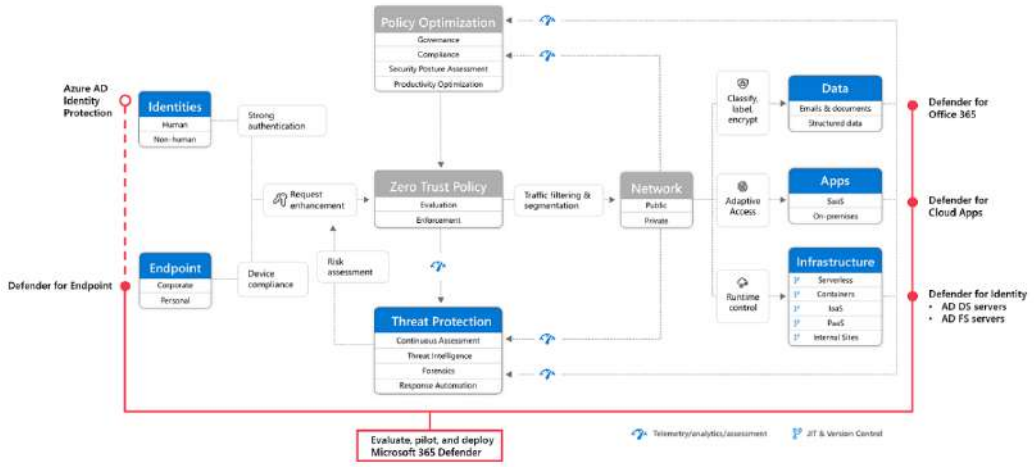


Рисунок 64 – Крок 4: розгортання Microsoft Defender XDR [76] – [79]

Четвертий крок впровадження архітектури Zero Trust передбачає оцінку, пілотування та впровадження Microsoft Defender Extended Detection and Response (XDR). Це включає в себе вивчення ефективності та можливостей Microsoft Defender XDR, впровадження його в обмеженому пілотному режимі для оцінки його впливу на безпеку, а також повноцінне впровадження у випадку позитивних результатів пілотування. Microsoft Defender XDR

забезпечує розширений виявлення та реагування на загрози, інтегруючи аналіз безпеки та реагування в єдину систему для забезпечення найвищого рівня захисту від сучасних кіберзагроз.

Крок 5: захист та конфігурування конференційними даними – Рисунок 65.

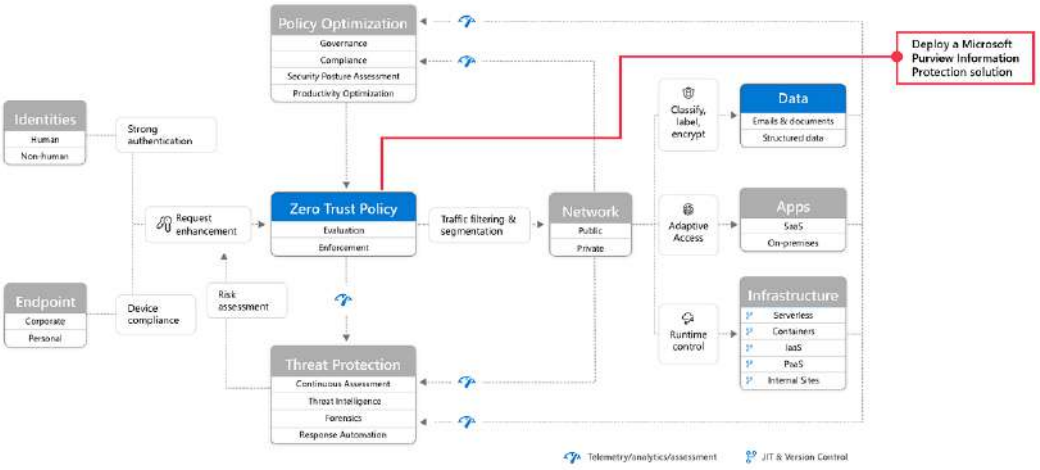


Рисунок 65 – Крок 5: захист та конфігурування конференційними даними [76] – [79]

П'ятий етап впровадження архітектури Zero Trust передбачає захист та управління чутливими даними. На цьому етапі важливо визначити та застосувати ефективні політики захисту конфіденційної інформації, а також механізми управління доступом, щоб забезпечити, що тільки авторизовані користувачі мають доступ до чутливих даних. Використання інструментів для виявлення та моніторингу небезпечних дій у реальному часі дозволяє оперативно реагувати на будь-які спроби незаконного доступу чи витоку інформації. Також важливо впровадити механізми автоматизованої класифікації даних для ефективного виявлення та захисту різних типів конфіденційної інформації.

Щоб налаштувати ідентифікацію та доступ для архітектури Zero Trust, потрібно виконати кілька кроків. Спочатку слід налаштувати необхідні

функції ідентифікації та їх параметри. Далі слід налаштувати загальні політики умовного доступу для ідентифікації та доступу. Також важливо налаштувати політики умовного доступу для гостей та зовнішніх користувачів. Останнім етапом є налаштування політик умовного доступу для хмарних додатків Microsoft 365, таких як Microsoft Teams, Exchange та SharePoint, а також політик для Microsoft Defender для Cloud Apps. Ці заходи допоможуть забезпечити надійну і безпечну ідентифікацію та доступ до різних ресурсів відповідно до принципів Zero Trust – Рисунок 66.

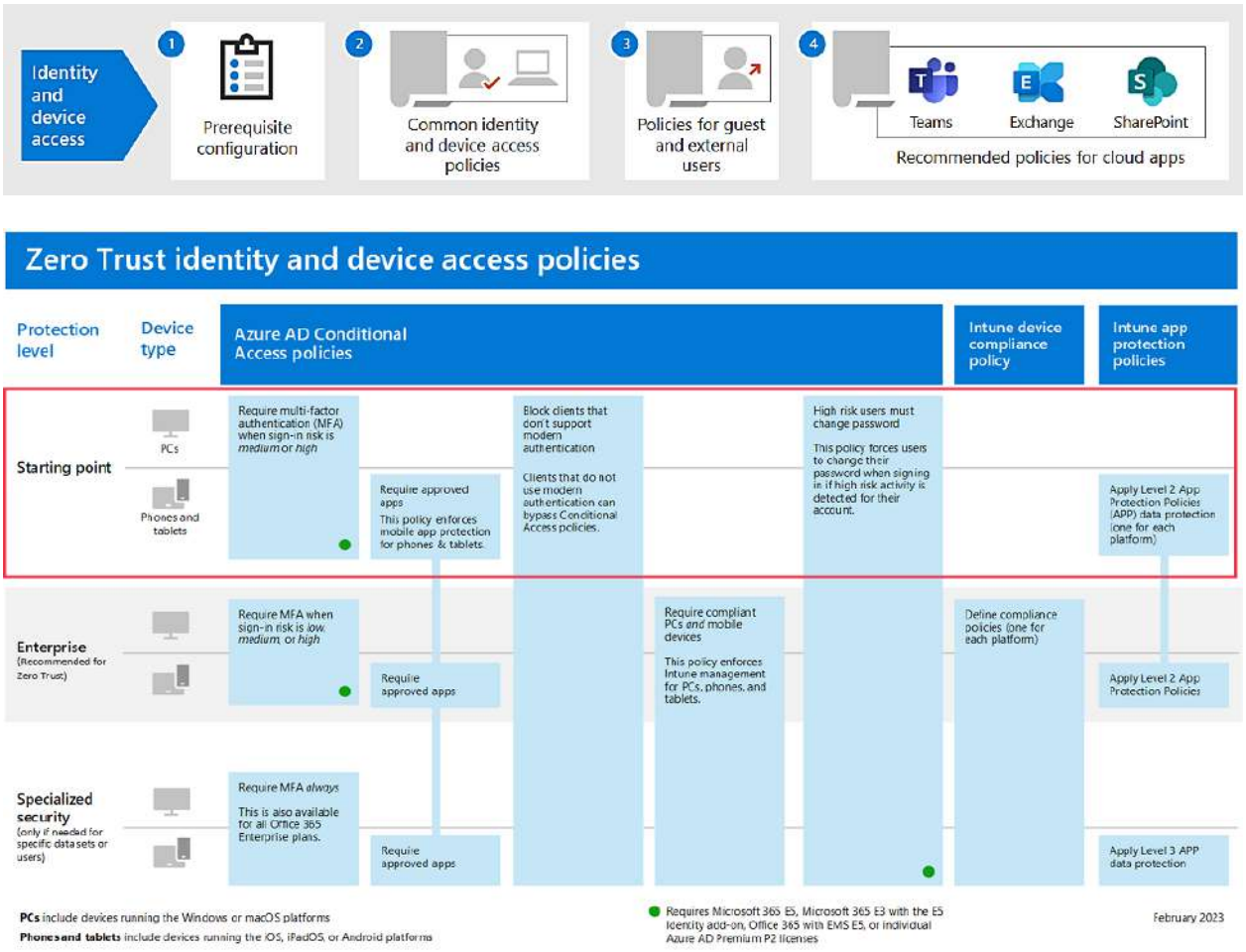


Рисунок 66 – Алгоритм налаштування та ідентифікації політики Zero Trust для ідентифікаторів і кінцевих точок за допомогою інструментів Microsoft Intune [76] – [79]

Таким чином, встановлено, що алгоритм розгортання архітектури Zero Trust для ідентифікаторів і кінцевих точок з використанням інструментів Microsoft Intune є комплексним та деталізованим процесом. На перших етапах, конфігуруються ідентифікаційні функції та встановлюються відповідні параметри. Далі, налаштовуються загальні політики умовного доступу, включаючи політики для гостей та зовнішніх користувачів. Ключовий пункт - це конфігурація політик умовного доступу для хмарних додатків Microsoft 365 та Microsoft Defender для Cloud Apps.

Методика враховує всі аспекти захисту від ідентифікації до захисту даних і надійності кінцевих точок. Використання інструментів Microsoft Intune дозволяє впроваджувати та керувати цими політиками ефективно, забезпечуючи цільовий захист, відповідно до концепції Zero Trust. Висновок полягає в тому, що процес розгортання є стратегічно розробленим та деталізованим, спрямованим на гармонійне поєднання безпеки та ефективності використання ідентифікаційних ресурсів та кінцевих точок в організації.

Відповідно до рекомендованого алгоритму виконаємо розгортання політики Zero Trust для ідентифікаторів і кінцевих точок за допомогою інструментів Microsoft Intune. Досліджувана архітектура Zero Trust на базі Microsoft Intune формується у відповідності до рекомендацій та типових рішень Microsoft [76] – [79] – Рисунок 67.

Зважаючи на значну деталізованість впровадження політики та архітектури Zero Trust на базі Microsoft Intune, нижче наводимо лише ключові кроки налаштування дослідної системи – Рисунок 68 – Рисунок 76.

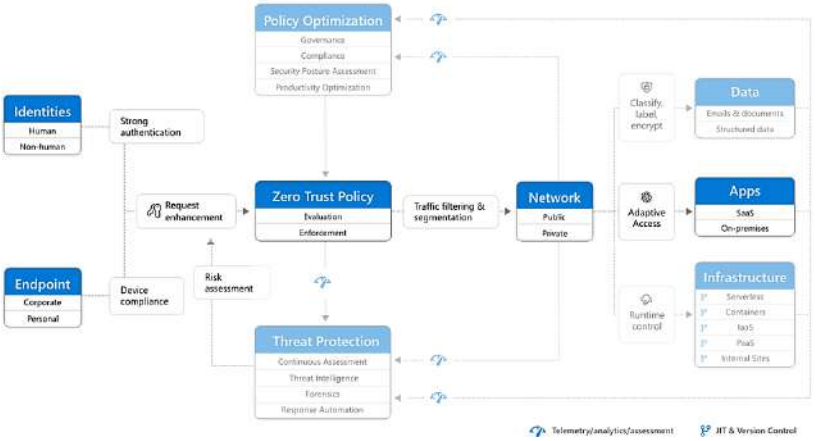


Рисунок 67 – Досліджувана архітектура Zero Trust на базі Microsoft Intune

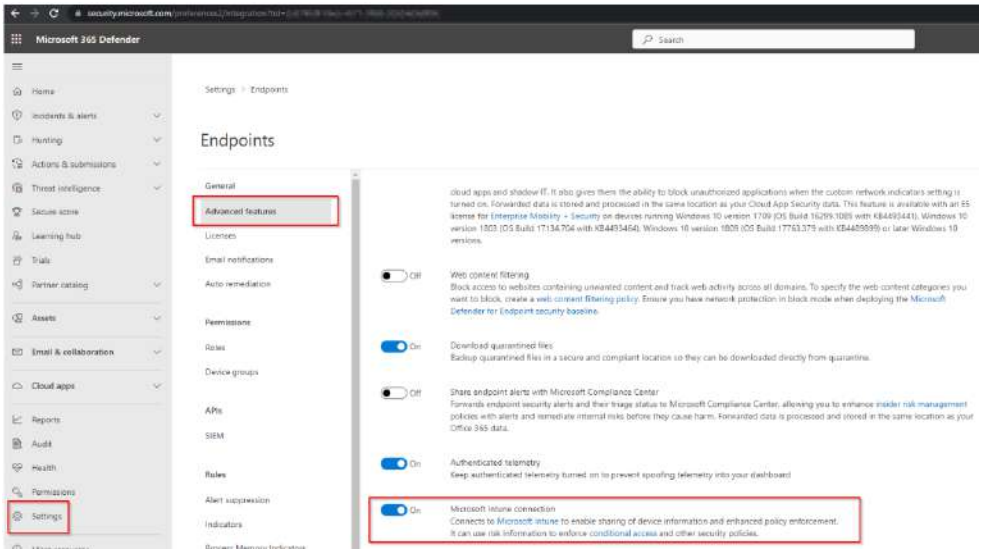


Рисунок 68 – Активація Microsoft Defender XDR в Microsoft Intune

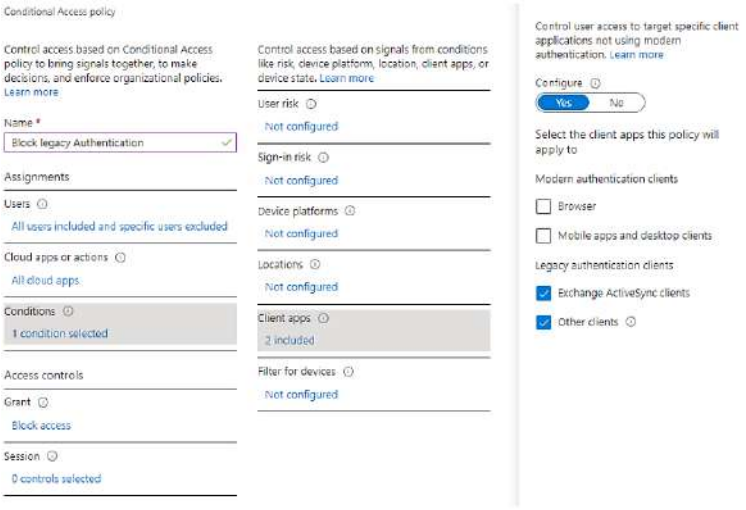


Рисунок 69 – Налаштування політики блокування користувачів, які не підтримують сучасну автентифікацію

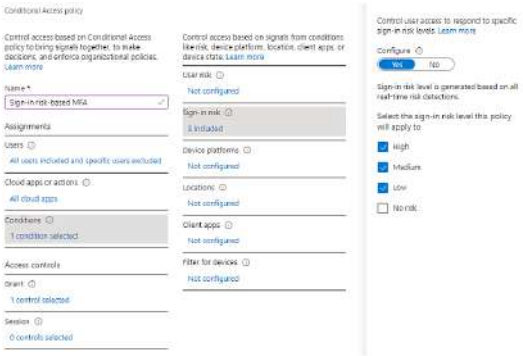


Рисунок 70 – Налаштування політики вимагання багатофакторної автентифікації

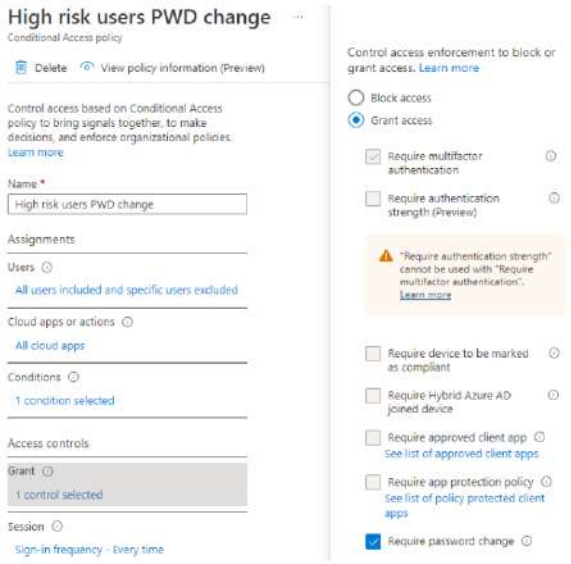


Рисунок 71 – Налаштування політики примусової зміни паролю у разі виявлення ризику безпеці корпоративної мережі

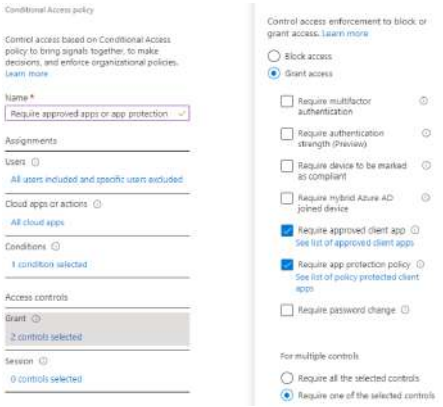


Рисунок 72 – Налаштування політики використання лише схвалених програм та застосунків

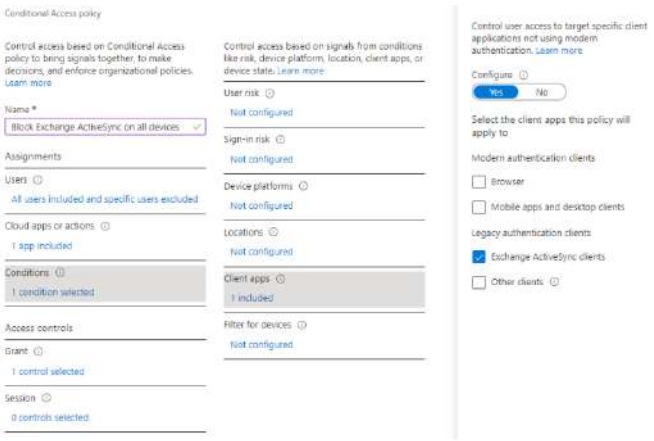


Рисунок 73 – Налаштування політики блокування Exchange ActiveSync на всіх пристроях

Basics Edit

Name	Windows 10 and later Compliance policy
Description	--
Platform	Windows 10 and later
Profile type	Windows 10/11 compliance policy

Compliance settings Edit

Device Health	
Require BitLocker	Require
Require Secure Boot to be enabled on the device	Require
Require code integrity	Require
Device Properties	
Minimum OS version	10.0.19045.2486
System Security	
Require a password to unlock mobile devices	Require
Simple passwords	Block
Minimum password length	6
Maximum minutes of inactivity before password is required	15 minutes
Require password when device returns from idle state (Mobile and Holographic)	Require
Require encryption of data storage on device.	Require
Firewall	Require
Trusted Platform Module (TPM)	Require
Antivirus	Require
Antispyware	Require
Microsoft Defender Antimalware	Require
Microsoft Defender Antimalware minimum version	4.18.2301.6
Microsoft Defender Antimalware security intelligence up-to-date	Require
Real-time protection	Require
Microsoft Defender for Endpoint	
Require the device to be at or under the machine risk score:	Medium

Рисунок 74 – Політика відповідності Windows 10 і новіших версій

Рисунок 75 – Політика відповідності Android

Рисунок 76 – Політика відповідності iOS

Надалі проводимо тестування налаштованої архітектури Zero Trust для ідентифікаторів і кінцевих точок за допомогою інструментів Microsoft Intune – Рисунок 77

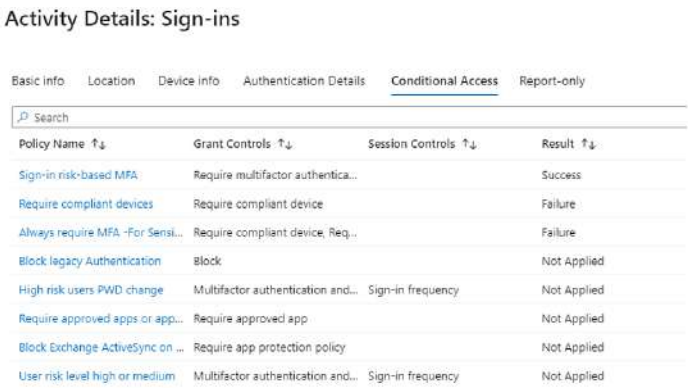


Рисунок 77 – Застосування політики умовного доступу

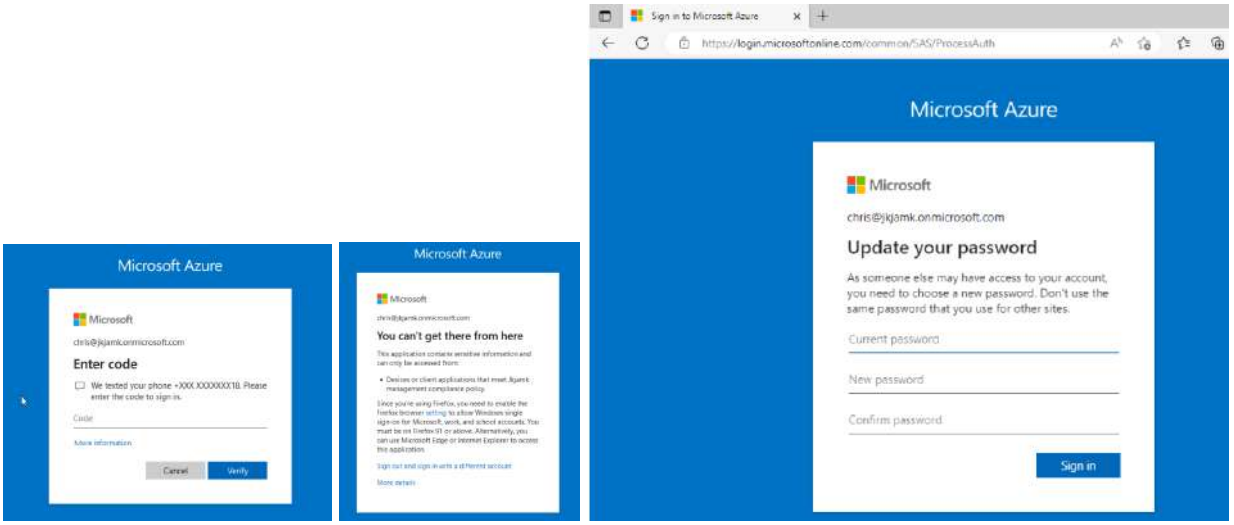


Рисунок 78 – Приклади взаємодії користувача та системи під час автентифікації з політикою примусової зміни паролю у разі виявлення ризиків порушення контуру безпеки

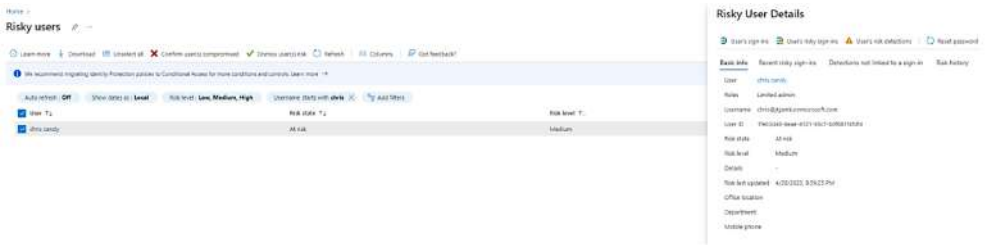


Рисунок 79 – Виявлення користувача з ризиками для безпеки корпоративної системи

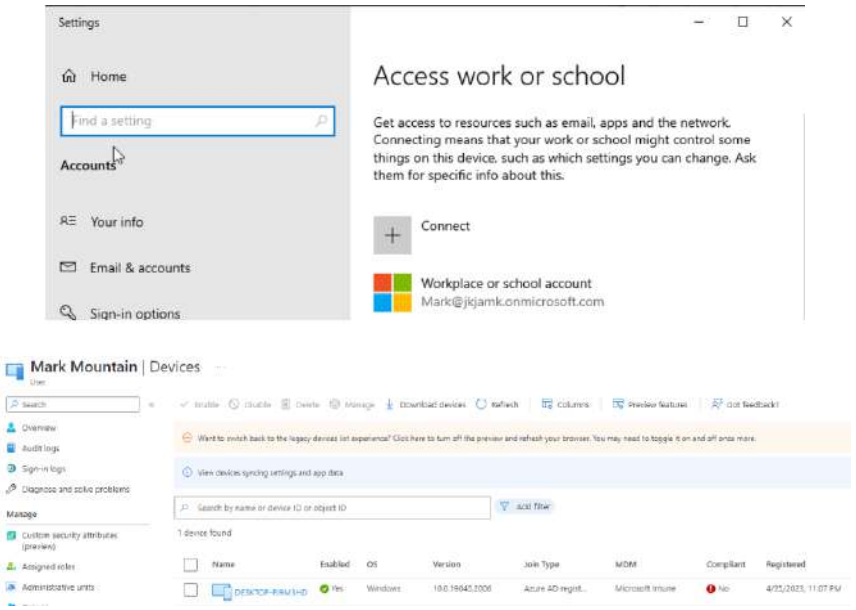


Рисунок 80 – Ілюстрація використання вразливості системи у разі викрадення облікових даних користувача: система блокує новий пристрій, у зв’язку невідповідності політикам безпеки

Рисунок 81 – Ілюстрація блокування зловмисника за схемою додавання до корпоративної мережі нового пристрою: блокування здійснено через невідповідність налаштованим політикам безпеки

Послуговуючись інструментами Microsoft 365 Defender [86] визначимо рівень безпеки досліджуваної корпоративної мережі до та після імплементації політики Zero Trust для ідентифікаторів і кінцевих точок за допомогою інструментів Microsoft Intune – Рисунок 82.

(a) до імплементації Zero Trust (b) після імплементації Zero Trust

Рисунок 82 – Тестування досліджуваної корпоративної мережі до та після імплементації безпекової політики Zero Trust на базі Microsoft Intune з використанням інструментів Microsoft 365 Defender [86]

Відповідно до наведеного аналізу результатів тестування досліджуваної корпоративної мережі з використанням інструментів Microsoft 365 Defender [86], встановлено що застосування політики Zero Trust на базі Microsoft Intune підвищило рівень контуру безпеки на 76% (з 24,90% до 43,83%).

При цьому вдалось досягнути покращення показників ідентифікації (Рисунок 83) та безпеки пристрою (Рисунок 84).

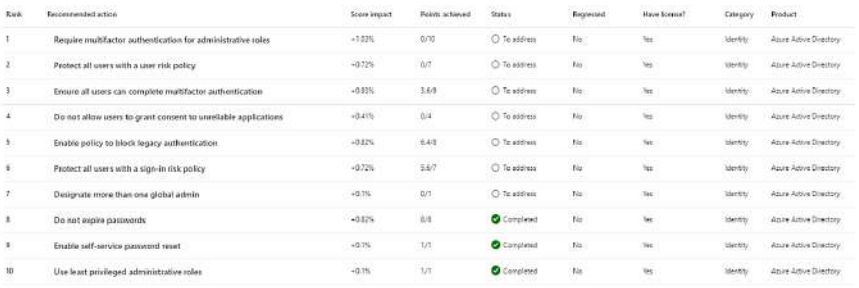
Activity	Resulting points
0.40 points gained for Enable policy to block legacy authentication because 1 fewer users are affected	6.4/8
0.90 points regressed for Ensure all users can complete multifactor authentication because 3 more users are affected	3.6/9
1.00 points gained by completing Enable self-service password reset. Great work!	1/1
0.35 points gained for Protect all users with a sign-in risk policy because 1 fewer users are affected	5.6/7
6.00 points gained for Enable policy to block legacy authentication because 1 fewer users are affected	6/8
4.50 points gained for Ensure all users can complete multifactor authentication because 2 fewer users are affected	4.5/9
5.25 points gained for Protect all users with a sign-in risk policy because 1 fewer users are affected	5.25/7

Рисунок 83 – Покращення показників ідентифікації

+10.00 points score change because Turn on real-time protection has become relevant	10/10	Device
+10.00 points score change because Turn on Microsoft Defender for Endpoint sensor has beco...	10/10	Device
+10.00 points score change because Turn on Microsoft Defender Firewall has become relevant	10/10	Device
+10.00 points score change because Turn on Microsoft Defender Antivirus has become relevant	10/10	Device
+10.00 points score change because Fix Microsoft Defender for Endpoint sensor data collectio...	10/10	Device
+10.00 points score change because Fix Microsoft Defender for Endpoint impaired communica...	10/10	Device
+10.00 points score change because Enable Microsoft Defender Antivirus scanning of downloa...	10/10	Device

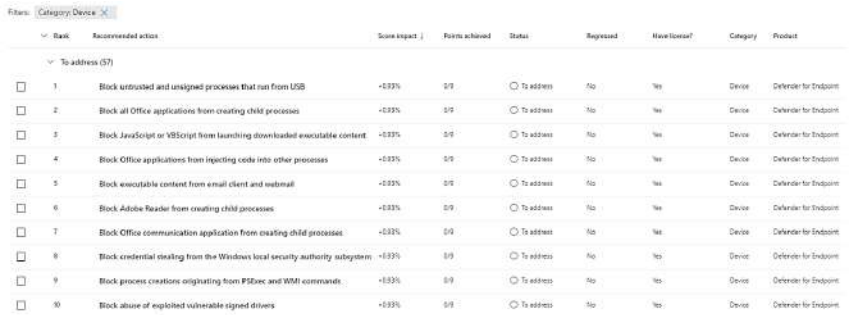
Рисунок 84 – Покращення показників безпеки пристрою

Разом з цим, інструменти Microsoft 365 Defender [86] сформували відповідні оптимізаційні рекомендації, впровадження яких дозволить підвищити безпеку процесів автентифікації користувачів (Рисунок 85) та керування кінцевими точками (Рисунок 86).



Rank	Recommended action	Score impact	Points achieved	Status	Regressed	Have license?	Category	Product
1	Require multifactor authentication for administrative roles	+1.03%	0/10	To address	No	Yes	Identity	Azure Active Directory
2	Protect all users with a user risk policy	+0.72%	0/7	To address	No	Yes	Identity	Azure Active Directory
3	Ensure all users can complete multifactor authentication	+0.93%	3.6/8	To address	No	Yes	Identity	Azure Active Directory
4	Do not allow users to grant consent to unreliable applications	+0.41%	0/4	To address	No	Yes	Identity	Azure Active Directory
5	Enable policy to block legacy authentication	+0.82%	6.4/8	To address	No	Yes	Identity	Azure Active Directory
6	Protect all users with a sign-in risk policy	+0.72%	5.6/7	To address	No	Yes	Identity	Azure Active Directory
7	Designate more than one global admin	+0.1%	0/1	To address	No	Yes	Identity	Azure Active Directory
8	Do not expire passwords	+0.82%	8/8	Completed	No	Yes	Identity	Azure Active Directory
9	Enable self-service password reset	+0.1%	1/1	Completed	No	Yes	Identity	Azure Active Directory
10	Use least privileged administrative roles	+0.1%	1/1	Completed	No	Yes	Identity	Azure Active Directory

Рисунок 85 – Рекомендації Microsoft 365 Defender [86] для підвищення безпеки процесів автентифікації користувачів



Filters: Category: Device

	Rank	Recommended action	Score impact	Points achieved	Status	Regressed	Have license?	Category	Product
		To address (57)							
☐	1	Block untrusted and unsigned processes that run from USB	+0.93%	0/9	To address	No	Yes	Device	Defender for Endpoint
☐	2	Block all Office applications from creating child processes	+0.93%	0/9	To address	No	Yes	Device	Defender for Endpoint
☐	3	Block JavaScript or VBScript from launching downloaded executable content	+0.93%	0/9	To address	No	Yes	Device	Defender for Endpoint
☐	4	Block Office applications from injecting code into other processes	+0.93%	0/9	To address	No	Yes	Device	Defender for Endpoint
☐	5	Block executable content from email client and webmail	+0.93%	0/9	To address	No	Yes	Device	Defender for Endpoint
☐	6	Block Adobe Reader from creating child processes	+0.93%	0/9	To address	No	Yes	Device	Defender for Endpoint
☐	7	Block Office communication application from creating child processes	+0.93%	0/9	To address	No	Yes	Device	Defender for Endpoint
☐	8	Block credential stealing from the Windows local security authority subsystem	+0.93%	0/9	To address	No	Yes	Device	Defender for Endpoint
☐	9	Block process creations originating from PSExec and WMI commands	+0.93%	0/9	To address	No	Yes	Device	Defender for Endpoint
☐	10	Block abuse of exploited vulnerable signed drivers	+0.93%	0/9	To address	No	Yes	Device	Defender for Endpoint

Рисунок 86 – Рекомендації Microsoft 365 Defender [86] для підвищення безпеки процесів керування кінцевими точками

Таким чином, доведено, що застосування системи політики Zero Trust для ідентифікаторів і кінцевих точок за допомогою інструментів Microsoft

Intune дозволяє значним чином підвищити безпековий рівень IT-інфраструктури організацій та підприємств.

Висновок до 3 розділу

Концепція Zero Trust визначає новий стандарт у сфері кібербезпеки, де перевірка та автентифікація користувачів та пристроїв є обов'язковими, незалежно від їхнього місцезнаходження у мережі. Основні принципи включають мінімізацію дозволів, застосування багатофакторної аутентифікації та активний моніторинг безпеки. В контексті Microsoft Intune впровадження Zero Trust створює надійне середовище для управління мобільними пристроями та захисту корпоративних ресурсів. Ця концепція ефективно забезпечує кібербезпеку та є ключовим етапом у відповіді на постійно зростаючі цифрові загрози, демонструючи передовий підхід до захисту інформації та інфраструктури.

Згідно з проведеним аналізом результатів тестування корпоративної мережі з використанням інструментів Microsoft 365 Defender, встановлено, що впровадження політики Zero Trust на основі Microsoft Intune призвело до підвищення рівня безпеки контуру на 76% (з 24,90% до 43,83%). Одночасно було досягнуте удосконалення показників ідентифікації та безпеки пристроїв. Також інструменти Microsoft 365 Defender надали конкретні оптимізаційні рекомендації, їх впровадження обіцяє підвищити безпеку процесів автентифікації користувачів та управління кінцевими точками. Таким чином, ефективність впровадження системи політики Zero Trust для ідентифікаторів і кінцевих точок з використанням Microsoft Intune переконливо підтверджена, в значній мірі підвищуючи рівень безпеки IT-інфраструктури організацій та підприємств.

ВИСНОВОК

У відповідності до поставлено мети та завдань проведено дослідження хмарних рішень з управління та захисту кінцевими точками корпоративних мереж. За результатами дослідження встановлено ряд ключових аспектів.

Microsoft Intune – інтегрована платформа для керування кінцевими точками та забезпечення цифрової безпеки в організаціях, яка включає Mobile Device Management (MDM), Mobile Application Management (MAM), Conditional Access, Azure Information Protection, Microsoft Defender for Endpoint та Intune App Protection Policies. Архітектура Microsoft Intune включає Intune Service, Azure Active Directory (Azure AD), MDM, MAM, Conditional Access, Azure Information Protection, Microsoft Defender for Endpoint та Intune App Protection Policies, створюючи цілісне рішення для цифрової безпеки та управління кінцевими точками. Процедура розгортання включає реєстрацію, налаштування параметрів, реєстрацію кінцевих точок, створення політик безпеки та оптимізацію, сприяючи зменшенню ризиків і підвищенню продуктивності користувачів.

Результати тестування корпоративної мережі з використанням Microsoft 365 Defender підтверджують, що впровадження політики Zero Trust на базі Microsoft Intune призвело до значного підвищення рівня безпеки контуру (на 76%). Оптимізація ідентифікації та безпеки пристроїв також відзначилася позитивними змінами. Інструменти Microsoft 365 Defender надали конкретні рекомендації для оптимізації, що сприятиме підвищенню безпеки процесів автентифікації та управління кінцевими точками. Таким чином, використання системи політики Zero Trust за допомогою Microsoft Intune ефективно підвищує безпеку IT-інфраструктури організацій та підприємств.

ПЕРЕЛІК ПОСИЛАНЬ

Наукові статті у періодичних виданнях, матеріали конференцій, семінарів

[1] Remote work and the COVID-19 pandemic: an artificial intelligence-based topic modeling and a future agenda / M. Aleem et al. *Journal of business research*. 2022. P. 113303. URL: https://doi.org/10.1016/j.jbusres.2022.113303 (date of access: 26.10.2023).

[2] Beland L.-P., Brodeur A., Wright T. The short-term economic consequences of COVID-19: exposure to disease, remote work and government response. *Plos one*. 2023. Vol. 18, no. 3. P. e0270341. URL: https://doi.org/10.1371/journal.pone.0270341 (date of access: 26.10.2023).

[3] Lissillour R., Michel Sahut J. The adoption of remote work platforms after the Covid-19 lockdown: new approach, new evidence. *Journal of business research*. 2022. P. 113345. URL: https://doi.org/10.1016/j.jbusres.2022.113345 (date of access: 26.10.2023).

[4] de Aragao, M. *An exploratory research into the situation of Serbian freelancers working on digital labour platforms in the context of the war in Ukraine*. Memoir. Universit´e de Lausanne. 2022. URL: https://serval.unil.ch/resource/serval:BIB_S_35983.P001/REF.pdf (date of access: 26.10.2023).

[5] Zhenchenko M., Izarova I., Baklazhenko Y. Impact of war on editors of science journals from Ukraine: Results of a survey. *European Science Editing*. 2019. Vol. 49. P. e97925. URL: https://ese.arphahub.com/article/97925/download/pdf/ (date of access: 26.10.2023).

[6] Atzeni M., Cini L. New theories and politics for working class organizing in the gig and precarious world of work. *Economic and industrial democracy*. 2023. URL: https://doi.org/10.1177/0143831x231201009 (date of access: 26.10.2023).

[7] Sánchez-Vergara J. I., Orel M., Capdevila I. “Home office is the here and now.” Digital nomad visa systems and remote work-focused leisure policies. *World leisure journal*. 2023. P. 1–20. URL: https://doi.org/10.1080/16078055.2023.2165142 (date of access: 26.10.2023).

[8] Pianese T., Errichiello L., Cunha J. V. Organizational control in the context of remote working: a synthesis of empirical findings and a research agenda. *European management review*. 2022. URL: https://doi.org/10.1111/emre.12515 (date of access: 26.10.2023).

[9] Van Nieuwerburgh S. The remote work revolution: impact on real estate values and the urban environment. *Real estate economics*. 2022. URL: https://doi.org/10.1111/1540-6229.12422 (date of access: 26.10.2023).

Електронні ресурси

[10] WFH Research | Survey of Working Arrangements and Attitudes. *WFH Research | Survey of Working Arrangements and Attitudes*. URL: https://wfhresearch.com/ (date of access: 26.10.2023).

[11] Upwork Study Finds 22% of American Workforce Will Be Remote by 2025. *Upwork*. URL: https://www.upwork.com/press/releases/upwork-study-finds-22-of-american-workforce-will-be-remote-by-2025 (date of access: 26.10.2023).

[12] State Of Remote Work 2023. *Buffer*. URL: https://buffer.com/state-of-remote-work/2023 (date of access: 26.10.2023).

[13] 2021 Hiring Trends Report. *Indeed*. URL: https://www.indeed.com/lead/2021-hiring-trends-report (date of access: 26.10.2023).

[14] Statistics On Remote Workers That Will Surprise You - Apollo Technical LLC. *Apollo Technical LLC*. URL: https://www.apollotechnical.com/statistics-on-remote-workers/ (date of access: 26.10.2023).

[15] Haan K. Remote Work Statistics And Trends In 2023. *Forbes Advisor*. URL: https://www.forbes.com/advisor/business/remote-work-statistics/ (date of access: 26.10.2023).

[16] Remote Workforce Cybersecurity Survey | OpenVPN. *OpenVPN*. URL: https://openvpn.net/blog/remote-workforce-cybersecurity-quick-poll/ (date of access: 26.10.2023).

[17] The Latest Remote Work Cybersecurity Statistics. *GITNUX*. URL: https://blog.gitnux.com/remote-work-cybersecurity-statistics/ (date of access: 26.10.2023).

[18] J700 Group Limited. Seven cybersecurity risks of remote work and how to address them | LBV Hub. *Lancashire Business View*. URL: https://www.lancashirebusinessview.co.uk/latest-news-and-features/seven-cybersecurity-risks-of-remote-work-and-how-to-address-them-6748 (date of access: 26.10.2023).

[19] Digital.com Staff. 6 in 10 employers require monitoring software for remote workers. *Digital.com*. URL: https://digital.com/6-in-10-employers-require-monitoring-software-for-remote-workers/ (date of access: 26.10.2023).

[20] What is Microsoft Intune . *Microsoft Learn: Build skills that open doors in your career*. URL: https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune (date of access: 26.10.2023).

[21] Microsoft Intune – керування кінцевими точками | Захисний комплекс Microsoft. *Microsoft*. URL: https://www.microsoft.com/uk-ua/security/business/microsoft-intune (дата звернення: 26.10.2023).

[22] Основні можливості microsoft intune | захисний комплекс microsoft. *Microsoft*.
URL: https://www.microsoft.com/uk-ua/security/business/endpoint-management/microsoft-intune (дата звернення: 26.10.2023).

Наукові статті у періодичних виданнях, матеріали конференцій, семінарів

[23] Wedha B. Y., Vasandani M. S., Wedha A. E. P. B. Enterprise architecture design for the transformation of online financial services. *Sinkron*. 2023. Vol. 8, no. 4. P. 2670–2678.
URL: https://doi.org/10.33395/sinkron.v8i4.13042 (date of access: 20.11.2023).

[24] Manolache F. B., Rusu O. Enterprise data collection and cross-referencing system. *2023 22nd roedunet conference: networking in education and research (roedunet)*, Craiova, Romania, 21–22 September 2023. 2023.
URL: https://doi.org/10.1109/roedunet60162.2023.10274910 (date of access: 20.11.2023).

[25] Gao Q., Wang Q., Wu C. Construction of enterprise digital service and operation platform based on internet of things technology. *Journal of innovation & knowledge*. 2023. Vol. 8, no. 4. P. 100433.
URL: https://doi.org/10.1016/j.jik.2023.100433 (date of access: 20.11.2023).

[26] Enterprise architecture trends in the digital transformation era / I. Mahendra et al. *2023 international seminar on application for technology of information and communication (isemantic)*, Semarang, Indonesia, 16–17 September 2023. 2023.
URL: https://doi.org/10.1109/isemantic59612.2023.10295330 (date of access: 20.11.2023).

[27] Nour B., Pourzandi M., Debbabi M. A survey on threat hunting in enterprise networks. *IEEE communications surveys & tutorials*. 2023. P. 1.
URL: https://doi.org/10.1109/comst.2023.3299519 (date of access: 20.11.2023).

[28] Zheng X., Leivadeas A., Falkner M. Intent Based Networking management with conflict detection and policy resolution in an enterprise network. *Computer networks*. 2022. P. 109457.
URL: https://doi.org/10.1016/j.comnet.2022.109457 (date of access: 20.11.2023).

[29] HE-SNA: an efficient cross-platform network alignment scheme from privacy-aware perspective / L. Zhou et al. *Complex & intelligent systems*. 2023.
URL: https://doi.org/10.1007/s40747-023-01052-0 (date of access: 20.11.2023).

[30] Henge S. K., Dhiman P. Integrating of rule based secure parameters for analyzing third-party applications and libraries in cross platform development. *The fourth scientific conference for electrical engineering techniques research (eetr2022)*, Baghdad, Iraq. 2023.
URL: https://doi.org/10.1063/5.0167752 (date of access: 20.11.2023).

[31] Cross-Platform file system activity monitoring and forensics – A semantic approach / K. Kurniawan et al. *ICT systems security and privacy*

protection. Cham, 2020. P. 384–397. URL: https://doi.org/10.1007/978-3-030-58201-2_26 (date of access: 20.11.2023).

[32] A novel architecture for an integrated enterprise network security system / B. Thanudas et al. *International journal of security and networks*. 2019. Vol. 14, no. 1. P. 47. URL: https://doi.org/10.1504/ijsn.2019.098919 (date of access: 20.11.2023).

[33] MSNetViews: geographically distributed management of enterprise network security policy / I. Anjum et al. *SACMAT '23: the 28th ACM symposium on access control models and technologies*, Trento Italy. New York, NY, USA, 2023. URL: https://doi.org/10.1145/3589608.3593836 (date of access: 20.11.2023).

[34] Li K., Zhang D., Dong X. Simulation of network traffic risk of enterprise cloud financial system by using deep learning. *Computers and electrical engineering*. 2023. Vol. 112. P. 109027. URL: https://doi.org/10.1016/j.compeleceng.2023.109027 (date of access: 20.11.2023).

[35] Khan H. U., Samad H. S. I. A. Enterprise strategic shift of technology: cloud-based systems verses traditional distributed system. *International journal of enterprise network management*. 2020. Vol. 11, no. 4. P. 320. URL: https://doi.org/10.1504/ijenm.2020.111775 (date of access: 20.11.2023).

[36] Security-aware dynamic scheduling for real-time optimization in cloud-based industrial applications / S. Meng et al. *IEEE transactions on industrial informatics*. 2020. P. 1. URL: https://doi.org/10.1109/tii.2020.2995348 (date of access: 20.11.2023).

[37] Bakić B. (2023). An Approach for Efficient Identification and Treatment of Common Risks in CI/CD and Cloud-Based Enterprise Solution Ecosystem. URL: http://urn.fi/URN:NBN:fi:aalto-202308275264 (date of access: 20.11.2023).

[38] Di Z., Liu Y., Li S. Networked organizational structure of enterprise information security management based on digital transformation and genetic algorithm. *Frontiers in public health*. 2022. Vol. 10. URL: https://doi.org/10.3389/fpubh.2022.921632 (date of access: 20.11.2023).

[39] Tupkalo V., Cherepkov S. Information security system structural modelling concept of digital process-oriented enterprise. *Measurements infrastructure*. 2022. No. 4. URL: https://doi.org/10.33955/v4(2022)-019 (date of access: 20.11.2023).

[40] Singh N., Krishnaswamy V., Zhang J. Z. Intellectual structure of cybersecurity research in enterprise information systems. *Enterprise information systems*. 2022. P. 1–25. URL: https://doi.org/10.1080/17517575.2022.2025545 (date of access: 20.11.2023).

[41] Barbosa I., Ribeiro S. Brazilian integrated cross-platform security assessment framework: context of cybersecurity methodology. *Proceedings of eighth international congress on information and communication technology*.

Singapore, 2023. P. 1015–1026. URL: https://doi.org/10.1007/978-981-99-3043-2_84 (date of access: 20.11.2023).

[42] Prototype cross platform oriented on cybersecurity, virtual connectivity, big data and artificial intelligence control / A. Massaro et al. *IEEE access*. 2020. Vol. 8. P. 197939–197954. URL: https://doi.org/10.1109/access.2020.3034399 (date of access: 20.11.2023).

[43] Construction of a scientific research integrated management information service platform integration in a form of cross-platform and multi-disciplinary organization / B. Qiang et al. *China's e-science blue book 2020*. Singapore, 2021. P. 503–522. URL: https://doi.org/10.1007/978-981-15-8342-1_29 (date of access: 20.11.2023).

[44] Malatji M. Management of enterprise cyber security: A review of ISO/IEC 27001:2022. *2023 international conference on cyber management and engineering (cymaen)*, Bangkok, Thailand, 26–27 January 2023. 2023. URL: https://doi.org/10.1109/cymaen57228.2023.10051114 (date of access: 20.11.2023).

[45] Shepita P., Tupychak L., Shepita J. Analysis of cyber security threats of the printing enterprise. *Journal of cyber security and mobility*. 2023. URL: https://doi.org/10.13052/jcsm2245-1439.123.8 (date of access: 20.11.2023).

[46] Pawar S. A., Palivela H. Importance of least cybersecurity controls for small and medium enterprises (smes) for better global digitalised economy. *Smart analytics, artificial intelligence and sustainable performance management in a global digitalised economy*. 2023. P. 21–53. URL: https://doi.org/10.1108/s1569-375920230001l0b002 (date of access: 20.11.2023).

[47] He W., Zhang Z. (. Enterprise cybersecurity training and awareness programs: recommendations for success. *Journal of organizational computing and electronic commerce*. 2019. Vol. 29, no. 4. P. 249–257. URL: https://doi.org/10.1080/10919392.2019.1611528 (date of access: 20.11.2023).

[48] Reagin M. J., Gentry M. V. Enterprise cybersecurity. *Frontiers of health services management*. 2018. Vol. 35, no. 1. P. 13–22. URL: https://doi.org/10.1097/hap.0000000000000037 (date of access: 20.11.2023).

[49] Enterprise cybersecurity study guide / S. E. Donaldson et al. Berkeley, CA : Apress, 2018. URL: https://doi.org/10.1007/978-1-4842-3258-3 (date of access: 20.11.2023).

[50] Data security issues in cloud-based Software-as-a-Service ERP / P. Saa et al. *2017 12th iberian conference on information systems and technologies (CISTI)*, Lisbon, Portugal, 21–24 June 2017. 2017. URL: https://doi.org/10.23919/cisti.2017.7975779 (date of access: 20.11.2023).

[51] A Cloud-based platform for the emulation of complex cybersecurity scenarios / A. Furfaro et al. *Future generation computer systems*. 2018. Vol. 89.

P. 791–803. URL: https://doi.org/10.1016/j.future.2018.07.025 (date of access: 20.11.2023).

[52] Digital transformation and cybersecurity challenges for businesses resilience: issues and recommendations / S. Saeed et al. *Sensors*. 2023. Vol. 23, no. 15. P. 6666. URL: https://doi.org/10.3390/s23156666 (date of access: 20.11.2023).

Електронні ресурси

[53] *Azure Active Directory is now Microsoft Entra ID*. Microsoft. URL: https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id (date of access: 20.11.2023).

[54] *AWS Key Management Service - AWS Key Management Service*. URL: https://docs.aws.amazon.com/kms/latest/developerguide/overview.html (date of access: 20.11.2023).

[55] What is Azure Information Protection (AIP)?. *Microsoft Learn: Build skills that open doors in your career*. URL: https://learn.microsoft.com/en-us/azure/information-protection/what-is-information-protection (date of access: 20.11.2023).

[56] What Is AWS CloudTrail? - AWS CloudTrail. URL: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html (date of access: 20.11.2023).

[57] Azure Monitor overview - Azure Monitor. *Microsoft Learn: Build skills that open doors in your career*. URL: https://learn.microsoft.com/en-us/azure/azure-monitor/overview (date of access: 20.11.2023).

[58] What is Amazon GuardDuty? - Amazon GuardDuty. URL: https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html (date of access: 20.11.2023).

[59] What is Microsoft Defender for Cloud? - Microsoft Defender for Cloud. *Microsoft Learn: Build skills that open doors in your career*. URL: https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction (date of access: 20.11.2023).

[60] What is VMware Workspace ONE? | VMware. *Digital Workspace Tech Zone*. URL: https://techzone.vmware.com/resource/what-workspace-one (date of access: 20.11.2023).

[61] What is AWS Backup? - AWS Backup. URL: https://docs.aws.amazon.com/aws-backup/latest/devguide/whatisbackup.html (date of access: 20.11.2023).

[62] Cloud Storage. *Google Cloud*. URL: https://cloud.google.com/storage (date of access: 20.11.2023).

[63] Cloudflare Application Services | Security and Performance. *Cloudflare*.

URL: https://www.cloudflare.com/application-services/ (date of access: 20.11.2023).

[64] Cisco Umbrella products | Integrated security from the cloud. *Cisco Umbrella*. URL: https://umbrella.cisco.com/products (date of access: 20.11.2023).

[65] Citrix Endpoint Management. *Citrix Product Documentation*. URL: https://docs.citrix.com/en-us/citrix-endpoint-management/endpoint-management.html (date of access: 20.11.2023).

[66] MobileIron Core overview. *Software & Technical Documentation | Ivanti*.
URL: https://help.ivanti.com/mi/help/en_US/core/10.7.0.0/gsg/Content/CoreGettingStarted/MobileIron_Core_overview.htm (date of access: 20.11.2023).

Наукові статті у періодичних виданнях, матеріали конференцій, семінарів

[67] Ghasemshirazi S., Shirvani G., Alipour M. A. Zero Trust: Applications, Challenges, and Opportunities. *arXiv preprint arXiv:2309.03582*. 2023. URL: https://doi.org/10.48550/arXiv.2309.03582 (date of access: 21.11.2023).

[68] Phiayura P., Teerakanok S. A comprehensive framework for migrating to zero trust architecture. *IEEE access*. 2023. P. 1. URL: https://doi.org/10.1109/access.2023.3248622 (date of access: 21.11.2023).

[69] Saleem M., Warsi M. R., Islam S. Secure information processing for multimedia forensics using zero-trust security model for large scale data analytics in SaaS cloud computing environment. *Journal of information security and applications*. 2023. Vol. 72. P. 103389. URL: https://doi.org/10.1016/j.jisa.2022.103389 (date of access: 21.11.2023).

[70] Cheng R., Chen S., Han B. Towards zero-trust security for the metaverse. *IEEE communications magazine*. 2023. P. 1–7. URL: https://doi.org/10.1109/mcom.018.2300095 (date of access: 21.11.2023).

[71] ZTWeb: cross site scripting detection based on zero trust / A. Wu et al. *Computers & security*. 2023. Vol. 134. P. 103434. URL: https://doi.org/10.1016/j.cose.2023.103434 (date of access: 21.11.2023).

[72] Vukotich G. Healthcare and cybersecurity: taking a zero trust approach. *Health services insights*. 2023. Vol. 16. URL: https://doi.org/10.1177/11786329231187826 (date of access: 21.11.2023).

[73] Seaman J. Zero trust security strategies and guideline. *Digital transformation in policing: the promise, perils and solutions*. Cham, 2023. P. 149–168. URL: https://doi.org/10.1007/978-3-031-09691-4_9 (date of access: 21.11.2023).

[74] Multi-secret sharing scheme for zero trust environment / Q. Zhou et al. *2023 IEEE 14th international conference on software engineering and service science (ICSESS)*, Beijing, China, 17–18 October 2023. 2023.

URL: https://doi.org/10.1109/icsess58500.2023.10292945 (date of access: 21.11.2023).

[75] Kumar N., Kasbekar G. S., Manjunath D. Application of data collected by endpoint detection and response systems for implementation of a network security system based on zero trust principles and the eigentrust algorithm. *ACM SIGMETRICS performance evaluation review*. 2023. Vol. 50, no. 4. P. 5–7. URL: https://doi.org/10.1145/3595244.3595247 (date of access: 21.11.2023).

Електронні ресурси

[76] Zero Trust with Microsoft Intune. *Microsoft Learn: Build skills that open doors in your career*. URL: https://learn.microsoft.com/en-us/mem/intune/fundamentals/zero-trust-with-microsoft-intune (date of access: 21.11.2023).

[77] Проактивний захист завдяки моделі нульової довіри. *Microsoft*. URL: https://www.microsoft.com/uk-ua/security/business/zero-trust (date of access: 21.11.2023).

[78] Secure endpoints with Zero Trust. *Microsoft Learn: Build skills that open doors in your career*. URL: https://learn.microsoft.com/en-us/security/zero-trust/deploy/endpoints (date of access: 21.11.2023).

[79] What is Zero Trust?. *Microsoft Learn: Build skills that open doors in your career*. URL: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview (dat e of access: 21.11.2023).

[80] SP 800-207, Zero Trust Architecture | CSRC. *NIST Computer Security Resource Center | CSRC*. URL: https://csrc.nist.gov/pubs/sp/800/207/final (date of access: 21.11.2023).

Наукові статті у періодичних виданнях, матеріали конференцій, семінарів

[81] Levine A., Tucker B. A. Zero trust architecture: risk discussion. *Digital threats: research and practice*. 2023. Vol. 4, no. 1. P. 1–6. URL: https://doi.org/10.1145/3573892 (date of access: 21.11.2023).

[82] Hardin D. Hardware/Software co-assurance for the rust programming language applied to zero trust architecture development. *ACM SIGAda Ada Letters*. 2023. Vol. 42, no. 2. P. 55–61. URL: https://doi.org/10.1145/3591335.3591340 (date of access: 21.11.2023).

[83] Study on zero-trust architecture, application areas & challenges of 6G technology in future / R. Singh et al. *2023 international conference on disruptive technologies (ICDT)*, Greater Noida, India, 11–12 May 2023. 2023. URL: https://doi.org/10.1109/icdt57929.2023.10150745 (date of access: 21.11.2023).

[84] Che K., Sheng S. Cloud native network security architecture strategy under zero trust scenario. *2023 IEEE 7th information technology and mechatronics engineering conference (ITOEC)*, Chongqing, China, 15–17 September 2023. 2023. URL: https://doi.org/10.1109/itoec57671.2023.10291357 (date of access: 21.11.2023).

[85] A survey on zero trust architecture: challenges and future trends / Y. He et al. *Wireless communications and mobile computing*. 2022. Vol. 2022. P. 1–13. URL: https://doi.org/10.1155/2022/6476274 (date of access: 21.11.2023).

Електронні ресурси

[86] Microsoft Defender для Office 365. *Microsoft*. URL: https://www.microsoft.com/uk-ua/security/business/siem-and-xdr/microsoft-defender-office-365 (date of access: 21.11.2023).