ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ ПРИ ГІБРИДНІЙ РОБОТІ КОРИСТУВАЧІВ У MICROSOFT 365»

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

КИЇВ – 2023

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп’ютер

ЦОД – центр обробки даних

ACL – Access Control List

API – Application Programming Interface

APT – Advanced Persistent Threat

AWS – Amazon Web Services

CDN – Content Delivery Network

DDoS – Distributed Denial of Service

DNS – Domain Name System

IaaS – Infrastructure as a Service

ICMP – Internet Control Message Protocol

MFA – Multi-Factor Authentication

NTP – Network Time Protocol

OSI – Open Systems Interconnection model

OWASP – Open Web Application Security Project

RDP – Remote Desktop Protocol

SASE – Secure Access Service Edge

TCP – Transmission Control Protocol

VPS – Virtual Private Server

UDP – User Datagram Protocol

WAF – Web Application Firewall

ВСТУП

Актуальність дослідження. Збройне вторгнення рф в нашу державу та поширення COVID-19 у світі зумовлюють застосування віддаленого режиму роботи співробітників організацій. Все більшої популярності набирає модель гібридного робочого місця, в рамках якої співробітники поєднують роботу з дому та в офісі. Такий варіант роботи має багато переваг як для співробітників, так і роботодавців, однак також створює ідеальні умови для зловмисників.

За даними дослідження ESET, 80 % великих компаній впевнені в обізнаності своїх віддалених співробітників щодо протидії кіберзагрозам. При цьому 73 % підприємств визнали ймовірний вплив інциденту безпеки на них, а половина заявила про злам у минулому. Сьогодні перед організаціями стоять численні виклики, серед основних виокремлюють людський та технологічний фактори. Забезпечення захисту нового гібридного робочого місця – складне завдання. Однак існують методи, які можуть допомогти мінімізувати ризики збоїв у роботі та захистити конфіденційні дані.

Вищесказане визначає актуальність теми даної магістерської роботи, основний зміст якої становлять дослідження технології захисту інформаційних ресурсів організації при гібридній роботі користувачів на прикладі Microsoft 365.

Об'єкт дослідження – захист інформаційних ресурсів організації при гібридній роботі користувачів.

Предмет дослідження – технологія захисту інформаційних ресурсів організації при гібридній роботі користувачів на прикладі Microsoft 365.

Мета роботи – розробити порядок застосування технології захисту інформаційних ресурсів організації при гібридній роботі користувачів та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми захисту інформаційних ресурсів організації при гібридній роботі користувачів;

проаналізувати підходи до захисту інформаційних ресурсів організації при

гібридній роботі користувачів;

проаналізувати існуючі рішення із захисту інформаційних ресурсів організації при гібридній роботі користувачів;

проаналізувати методи та засоби захисту інформаційних ресурсів організації при гібридній роботі користувачів на прикладі Microsoft 365;

розкрити порядок реалізації технології захисту інформаційних ресурсів організації при гібридній роботі користувачів.

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

Практичне значення одержаних результатів: запропоновано порядок застосування технології захисту інформаційних ресурсів організації при гібридній роботі користувачів на прикладі Microsoft 365, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати магістерської роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ [18].

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ ПРИ ГІБРИДНІЙ РОБОТІ КОРИСТУВАЧІВ

1.1. Дослідження проблеми захисту інформаційних ресурсів організації при гібридній роботі користувачів

Eset зазначає, що нещодавній перехід до дистанційної роботи спонукав людство переосмислити, як працюють компанії та команди, коли особисті зустрічі неможливі. Зараз організації вивчають, як рухатися вперед – від встановлення гнучкої схеми роботи до забезпечення безпечного повернення в офіс. Незважаючи на труднощі, тепер у нас є унікальна можливість фундаментально покращити роботу людей, де б вони не були. Шлях вперед – це *гібридне робоче місце* [3].

Гібридне робоче місце забезпечує гнучку та безперебійну співпрацю з будь-якого місця. Хоча переваги очевидні, ця зміна вимагає зміни досвіду, який люди мають під час роботи вдома чи в офісі. Основна вимога до гібридного робочого місця – надати співробітникам багатофункціональні інтуїтивно зрозумілі інструменти для співпраці, щоб надсилати повідомлення, зустрічатися, телефонувати, ділитися вмістом і співпрацювати з будь-якого місця. Переваги гібридного робочого місця показано на рис. 1.1.

Рис. 1.1. Переваги гібридного робочого місця [4]

Гібридна робота дає людям можливість працювати на місці, за його межами

та переміщатися між місцями. Гібридна робота також сприяє інклюзивності, залученості та добробуту для всіх працівників [4].

Змішана модель роботи підтримує поєднання офісних і віддалених працівників, які можуть працювати на всіх рівнях організації. Вони можуть працювати на місці або за його межами, причому багато співробітників регулярно перемикаються між цими середовищами залежно від своїх потреб. Гнучкість роботи за межами підприємства чи на місці та як часто залежить від організації та характеру роботи працівника та його посадових обов'язків [4].

У глобальному дослідженні робочої сили за підтримки компанії Cisco зазначено, що лише 9 відсотків працівників сказали, що вони сподіваються повернутися в офіс на повний робочий день після відновлення роботи офісу. Відсутність підтримки гібридної моделі роботи може перешкодити компаніям залучати й утримувати таланти, необхідні для успіху в майбутньому [4].

Розглянемо ключові відмінності застосування гібрідної моделі роботи співробітників.

Гібридний робочий простір і гібридне робоче місце означають різні речі. Модель гібридної роботи спонукає еволюцію від уявлення про те, де виконується робота (робоче місце), орієнтованого на місцезнаходження, до більш орієнтованого на людину уявлення про те, де виконується робота (робоче місце).

Гібридне робоче місце. Історично робоче місце було фізичним офісом компанії, де працівники могли працювати на місці весь або частину робочого часу. Гібридний робочий простір: робочий простір – це будь-яке місце, де працівник працює в будь-який час. Гібридний робочий простір може бути робочою станцією у фізичному офісі компанії або домашнім офісом співробітника. Це може навіть описати стіл у готельному номері, за яким працює співробітник і підключається до мережі компанії під час подорожі [4].

Технології, включаючи як програмне, так і апаратне забезпечення, підтримують безпечну співпрацю та спілкування незалежно від того, де розташовано гібридний робочий простір. При цьому іноді застосовується архітектура SASE (Secure Access Services Edge), щоб підтримувати безпечний і

плавний доступ з будь-якого місця [4].

Прийняття гібридної робочої моделі передбачає, що всі працівники можуть безпроблемно користуватися безпечним підключенням і працювати з додатками. Це дозволяє організації легко підтримувати мережеве підключення та послідовно застосовувати свої політики безпеки на всіх робочих просторах, включаючи кампус, філію, домашнє середовище та мікроофіс.

Розглянемо технологічні основи гібридної роботи [4]. Технології відіграють важливу роль у просуванні різних атрибутів гібридної роботи.

Організації та їхні працівники можуть використовувати статистичні дані, щоб зрозуміти, як покращити інтеграцію роботи та особистого життя та допомогти побудувати якісніші зв'язки між окремими людьми та командами. Компанії також можуть використовувати інтелектуальні програми, щоб зменшити будь-яке занепокоєння в офісі, яке можуть відчувати деякі працівники, коли вони повертаються в офіс у зв'язку з глобальною кризою охорони здоров'я.

Потрібна інтелектуальна, інтуїтивно зрозуміла технологія робочого місця. Коли співробітники перебувають у робочому середовищі на місці, організації зосереджуються на забезпеченні безпечного повернення шляхом моніторингу соціальної щільності, безпечної реєстрації користувачів і пристроїв і допомоги в забезпеченні захисту співробітників у їхньому середовищі [4].

Організації можуть відстежувати порогові значення соціальної щільності, використовуючи служби на основі місцезнаходження в поєднанні з розширеною мережевою телеметрією та пристроями Інтернету речей (IoT) у будівлях. Вони можуть отримувати сповіщення в реальному часі та реагувати на інциденти за допомогою звітів про близькість [4].

Успіх застосування гібридної моделі роботи користувачів залежить від безпеки. Більш конкретно, підхід нульової довіри повинен бути прийнятий і практикуватися в усій організації.

Нульова довіра – це комплексний підхід до забезпечення повного доступу до корпоративних мереж, додатків і середовищ від будь-якого користувача, пристрою та місця. Підхід нульової довіри до безпеки дозволяє організаціям [4]:

послідовно запроваджувати контроль на основі політики;

отримати видимість користувачів, пристроїв, компонентів тощо в усьому робочому середовищі;

отримувати докладні журнали, звіти та сповіщення для покращення виявлення загроз і реагування на них;

розгорнути наскрізне шифрування та автентифікацію для користувачів і пристроїв.

Організаціям, які використовують нову гібридну модель роботи, необхідно інвестувати в програмне забезпечення для співпраці та спеціальні пристрої, які можуть надійно, безпечно та оптимально підтримувати співпрацю в реальному часі між усіма працівниками.

Усі співробітники повинні мати доступ до високоякісних інструментів для спільної роботи зі свого гібридного робочого простору – будь то робочий стіл в офісі, вдома чи в іншому місці – щоб покращити безперебійну співпрацю. Приклади цих інструментів для співпраці в реальному часі [4]:

універсальний продуктивний пристрій для робочого столу, який пропонує досвід спільної роботи на основі штучного інтелекту з придушенням шуму, віртуальним фоном і розширеними можливостями спільного створення. Ці пристрої дозволяють їм спілкуватися, зустрічатися, телефонувати та ділитися вмістом з будь-якого місця;

гарнітури, які забезпечують шумозаглушення та зменшення фонового шуму, щоб допомогти людям залишатися зосередженими та продуктивними, де б вони не працювали;

інструменти для співпраці в режимі реального часу, наприклад для відеоконференцій, також повинні дозволити компанії надавати клієнтам високоякісні умови роботи.

У розподілених робочих середовищах і середовищах додатків увага приділяється тому, щоб допомогти забезпечити постійну оптимізацію роботи користувачів і додатків. Щоб йти в ногу з потребами робочої сили, фахівцям потрібні видимість, розуміння та дії, що забезпечуються повною

спостережливістю [4].

Спостереженість повного стеку виходить за рамки моніторингу, поєднуючи дані з додатків, інфраструктури та транзакцій для створення спільного контекстного глобального уявлення про операції. Це дозволяє фахівцям працювати разом, щоб забезпечити виняткову взаємодію з користувачами, оптимізувати витрати та продуктивність і допомогти компаніям планувати майбутнє [4].

Оскільки організації продовжують перехід до хмари, їм потрібна краща продуктивність і захист для їх гібридної робочої сили та віддалених офісів. Існуючі архітектури не підтримують гнучкість, необхідну для підключення користувачів і додатків з будь-якого місця, зберігаючи та покращуючи безпеку та продуктивність.

SASE (Secure Access Service Edge) – це архітектурний підхід, який пропонує альтернативу традиційній безпеці, орієнтованій на центр обробки даних. SASE поєднує мережеві можливості з вбудованими в хмару функціями безпеки, щоб спростити розгортання та оптимізувати керування в хмарі.

Ось чотири найпоширеніші моделі гібридної роботи [3]:

1. Гнучка гібридна модель роботи.

Співробітники обирають своє місце розташування та робочий час, виходячи зі своїх пріоритетів на день. Наприклад, якщо їм потрібно зосередитися на проекті, вони можуть вибрати роботу вдома або в кафе. Якщо вони хочуть відчути спільноту, їм потрібно зустрітися зі своєю командою, відвідати тренінг або приєднатися до ратуші, вони можуть зайти в офіс. Cisco використовує цю модель і пропонує своїм співробітникам можливість вибирати, де їм працювати в будь-який день.

Переваги даної моделі:

пропонує людям свободу та гнучкість у виборі місця та часу роботи;

будує довірчі стосунки з працівниками, що підвищує лояльність і задоволеність роботою;

розширює коло талантів, сприяючи більш різноманітному мисленню;

покращує кінцевий результат за рахунок економії на офісних приміщеннях і поїздках.

Виклики даної моделі:

співробітникам важко знайти відповідний день або час для особистої командної роботи;

відсутність видимості того, скільки людей йдуть до офісу в будь-який день і чи є в будівлі потенціал для їх підтримки.

2. Фіксована гібридна модель роботи.

Організація встановлює дні та час, коли працівникам дозволяється працювати віддалено або відвідувати офіс. Наприклад, може статися так, що певні команди заходять в офіс у понеділок і середу, а інші – у вівторок і четвер. Або організація може дозволити кожному працювати з дому в заздалегідь визначені дні кожного тижня. American Express є прикладом організації, яка прийняла фіксовану гібридну модель роботи.

Переваги даної моделі:

збільшує можливості для особистої співпраці та формування команди;

надає працівникам можливість призначати зустрічі або швидко виконувати доручення в певні дні тижня;

надає можливість легко прогнозувати місткість офісу.

Виклики даної моделі:

відсутність індивідуального вибору, що може призвести до втрати продуктивності, якщо працівники не в оптимальних умовах для роботи, яку потрібно виконати;

неможливість скоротити офісну площу.

3. Офісна гібридна модель роботи.

Очікується, що працівники будуть на місці, але вони мають можливість вибрати кілька днів на тиждень для віддаленої роботи. Google планує прийняти такий тип моделі, коли співробітники працюють в офісі три дні на тиждень, але мають можливість вибрати два дні для віддаленої роботи.

Переваги даної моделі:

дозволяє гнучкість і індивідуальний вибір;

допомагає підтримувати корпоративну культуру та спільноту.

Виклики даної моделі:

відсутність видимості для співробітників навколо, хто і коли буде в офісі;

неможливість точно передбачити, скільки співробітників буде в офісі в певний день

4. Дистанційна гібридна модель роботи.

Співробітники більшу частину часу працюють віддалено, час від часу відвідуючи коворкінг або офіс для командоутворення, співпраці та навчання. У цій моделі компанія може не мати офісних приміщень і натомість покладається на членів команди в одній зоні, щоб збиратися разом, коли вони вважають за потрібне. Twitter прийняв цю модель дистанційного керування та дозволить усім співробітникам працювати з дому.

Переваги даної моделі:

підвищує продуктивність і задоволеність роботою для співробітників, які хочуть працювати віддалено більшу частину часу;

надає можливість скоротити витрати за рахунок скорочення або ліквідації офісних площ.

Виклики даної моделі:

потенціал для співробітників відчувати себе ізольованими;

збільшення проблем із підтриманням культури компанії та спільноти.

1.2. Аналіз підходів до захисту інформаційних ресурсів організації при гібридній роботі користувачів

Відмічається, що віддалена робоча сила здебільшого була потребою, спричиненою пандемією, яка недовго довела свою зручність. Гібридна робоча модель привнесла динаміку в офіс, надаючи гібридним робочим середовищам більше гнучкості для управління робочою силою компанії та розширюючи можливості людських ресурсів і кваліфікованих талантів з усього світу [5].

Віддалена робота стала піонером створення гібридної політики роботи від малих до великих підприємств, дозволяючи працівникам працювати звідки завгодно, дозволяючи роботодавцям зменшувати кількість статичних робочих місць в офісі, заощаджуючи всім сторонам значну частину часу та фінансових ресурсів [5].

Незважаючи на те, що віддалена робота набуває позитивного значення та є сучасним підходом для віртуального офісу, вона все ще несе вагу проблем, пов'язаних із питаннями безпеки, конфіденційності та захисту бізнесу. Відповідно до звіту Microsoft Digital Defense Report, кіберзлочинці здійснюють значну кількість програм-вимагачів, шкідливих програм або фішингових атак. Останній охоплює до 70% пов'язаних з підприємством порушень безпеки , що демонструє лише невелику частину вразливості інфраструктури [5].

Розглянемо проблеми гібридного робочого середовища.

До того, як гібридна модель роботи стала новим звичаєм у більшості корпоративних процедур, компанії працювали виключно в межах власної створеної локальної інфраструктури. Однак дистанційна робота розширила визначення периметра компанії, а заходи безпеки природним чином порушилися через більший вплив внутрішніх і зовнішніх загроз [5].

Так само, як і офісні співробітники, віддалені працівники допомагають убезпечити повсякденні бізнес-операції та є незамінними активами компанії, але адаптація середовища домашнього офісу має обмеження. Організації не можуть самостійно забезпечити безпеку мережі та кінцевих точок за допомогою гібридної робочої сили. Компанія також набагато надійніше довіряє кінцевим точкам, які намагаються отримати доступ до ресурсів компанії, оскільки ідентифікаційні дані або пристрої можуть бути скомпрометовані [5].

Крім того, більшість периметрів компанії базується на застарілій IT-інфраструктурі, яка не в змозі відповідати зростаючим потребам у безпеці та підтримувати спеціальні вимоги підприємств, що розвиваються. Відсутність підготовки відкриває двері для ворожих акторів, що часто призводить до витоку даних або навіть фінансових і репутаційних втрат, що збільшуються з кожним

роком [5].

Проблема витоку даних є однією з найбільш серйозних загроз безпеці, незважаючи на розмір і ринок організації, оскільки вона може вплинути на бізнес, співробітників і, що найважливіше, на користувачів і клієнтів компанії.

Вражаючі цифри, зібрані Acronis, постачальником засобів захисту даних, підтверджують, що зловмисники завжди шукають прогалину, щоб проникнути туди. Майже третина респондентів підтвердили принаймні одну атаку на свою організацію щомісяця, тоді як близько 20% компанії атакували щотижня та щодня [5].

Відповідно до звіту Verizon про розслідування витоку даних (2021), 85% порушень пов'язані з «людським фактором». Компанії несуть відповідальність за впровадження практичних рішень щодо посилення організаційної кібербезпеки, щоб подолати це.

Модель гібридної роботи ставить перед організаціями ще один виклик – як усі віддалені працівники отримають доступ до корпоративної мережі для виконання своїх щоденних завдань, не ставлячи під загрозу безпеку даних компанії?

Повсякденні операції вимагають від співробітників доступу до даних і обміну файлами, підключення до локальних пристроїв IoT і доступу до іншого пристрою користувача в разі потреби технічної підтримки. Однак без ефективного оновлення продуктивність і потужність застарілої інфраструктури не можуть гарантувати достатню безперервність бізнес-операцій. Це також створює більше навантаження на адміністраторів, відповідальних за те, щоб користувачам у мережі компанії можна було довіряти, щоб уникнути будь-яких потенційних загроз, тому заходи безпеки також повинні бути посилені [5].

Явна довіра до кінцевих точок, які отримують доступ до корпоративної мережі за одноразово дозволеним входом, є однією з найбільш значних вразливостей безпеки. Віддалений означає, що немає впевненості в тому, як і ким хтось працює в мережі. Відстеження дій користувачів вручну забирає багато часу, особливо коли для цього потрібно багато користувачів, що призводить до ще

однієї помилки людини [5].

Згідно зі звітом CIRA Cybersecurity Report 2020, дві третини співробітників компанії використовують пристрої, випущені компанією, але 50% гібридної робочої сили стверджують, що періодично використовують персональні пристрої для робочих цілей – це підкреслює масштаби неконтрольованого та некерованого доступу до корпоративної мережі.

Порушення даних швидко зростає, тому *компанія повинна впровадити найважливіші заходи безпеки для захисту цінної інформації.* Незахищені пристрої з непідтвердженими користувачами сигналізують про важливість керування ідентифікацією. Недостатня політика безпеки та обмеження застарілої периметральної інфраструктури на місці не можуть забезпечити якість продуктивності гібридної робочої сили бізнесу, створюючи контрпродуктивне середовище для IT-адміністраторів [5].

Гібридна робота полягає в тому, щоб залишити виділену мережу компанії та отримати доступ до ресурсів через загальнодоступні та домашні мережі, які несуть серйозні загрози безпеці. Встановлення підключення через бізнес-VPN допомагає створити безпечну та приховану мережу для кожного співробітника.

Відсутність людей в офісі потребує альтернативних підходів до перевірки їх особи та автентифікації доступу до мережі компанії. «Не довіряй нікому, перевіряй усе» – це спосіб мислення, заснований на моделі нульової довіри, реалізований за допомогою автентифікації особи для доступу до робочих пристроїв і ресурсів, сегментації мережі та керування контролем доступу.

Фізична інфраструктура обмежена дорогим апаратним забезпеченням і обслуговуванням на місці – це повна протилежність гнучкості, простоті в розгортанні й оновленні. Тому перехід до хмарних середовищ є основним рішенням для підвищення ефективності та стійкості. Сучасна архітектура кібербезпеки Secure Access Service Edge (SASE) вирівнює все до віртуального рівня, яким легше керувати та масштабувати за запитом [5].

Гібридні робочі середовища призводять до багатьох запитів, кінцевих точок та інцидентів, якими з часом стає важко керувати, і вони вимагають більше часу

та робочих ресурсів від IT-адміністраторів. Підвищення тиску залишає більше місця для людських помилок, тому автоматизація є одним із ключових факторів для спрощення операцій моніторингу та виявлення відхилень у режимі реального часу.

Зростаюче усвідомлення співробітниками важливості безпеки є таким же необхідним, як і будь-який інструмент або програмне забезпечення, яке допомагає забезпечити безпеку в компанії. Співробітники можуть не знати про потенційні загрози безпеці, які ховаються за стінами офісу. Тому навчання та формування знань щодо особистої відповідальності та актуальності застосовуваних заходів безпеки є вирішальними для кожного бізнесу.

Оскільки світ переходить до більш постійної гібридної робочої сили, гнучкість приносить як нові переваги, так і проблеми для роботодавців і працівників. Незалежно від того, чи працює ваша команда в офісі, віддалено чи щось посередині, вам не потрібно поступатися безпекою для більшої гнучкості. Ось список із п’яти простих порад, як підтримувати культуру гібридної робочої сили, одночасно захищаючи працівників і активи компанії [6].

Працівники очікують, що технологія супроводжуватиме їх, куди б вони не пішли, але гнучкі місця розташування піддають їх (і вашу організацію) новим загрозам. Ось чому IT-команди та команди безпеки повинні забезпечити безпеку гібридного досвіду на кожній кінцевій точці, навчаючи користувачів безпечним методам і потенційним ризикам [6].

Багатофакторна автентифікація (MFA) – це простий перший рівень безпеки, необхідний усім компаніям, перш ніж вони зможуть надати доступ до активів компанії.

VPN забезпечує безпечний тунель між користувачами та додатками, щоб працівники могли залишатися продуктивними та на зв’язку, коли вони в дорозі або працюють з дому. Це допомагає забезпечити доступ лише схвалених користувачів, забезпечуючи належний рівень безпеки без шкоди для взаємодії з користувачем.

Більшість порушень безпеки спрямовані на кінцевих користувачів,

вимагаючи першої лінії захисту на рівні DNS і останньої лінії для загроз, які прослизають. Перший рівень блокує домени, пов’язані зі зловмисною поведінкою, перш ніж вони потраплять у вашу мережу або містять зловмисне програмне забезпечення, якщо воно вже є всередині, а останній рівень захищає від більш складних загроз.

За даними [7] зазначається, що безпека є спільною відповідальністю:

76% осіб, які приймають рішення з питань безпеки, погоджуються, що інформаційна безпека стає все більш консультативною за своєю природою, що спонукає до більшого розуміння того, що загрози безпеці є загрозою для бізнесу, а не лише загрозою для технологій;

90% працівників інформаційних технологій погоджуються з тим, що безпека є спільною відповідальністю;

85% осіб, які приймають рішення у сфері безпеки, поділяють цю думку;

73% осіб, які приймають рішення у сфері безпеки, вважають, що їхні працівники добре обізнані про потенційні ризики безпеці, а 64% працівників інтелектуальної сфери стверджують, що вони усвідомлюють це.

Протоколи інформаційної безпеки, які були пріоритетними для підтримки гібридної та віддаленої роботи, включають багатофакторну автентифікацію (MFA) (28%), додаткову освіту співробітників (28%) і Cloud/SaaS для покращеної видимості та контролю (28%). Незважаючи на те, що ці зміни могли зашкодити, важливий висновок опитування [7] полягає в тому, що 91% працівників інформаційних технологій стверджують, що нові протоколи безпеки покращили або не вплинули на роботу їхніх співробітників, а 90% стверджують, що вони не вплинули на продуктивність.

Справді, схоже, що CISO надають пріоритет досвіду співробітників у своїх планах трансформації IT, і 78% осіб, які приймають рішення з питань безпеки, погоджуються, що протягом останніх 12 місяців команди безпеки досліджували способи спрощення стратегій безпеки [7].

Доказ є простим – лише чверть (27%) працівників інформаційних технологій визнають, що вважають їхні протоколи безпеки складними для

розуміння, і лише 30% важко запам’ятати складні процедури безпеки. Це важливо, оскільки тертя користувачів можуть значно перешкодити зусиллям безпеки.

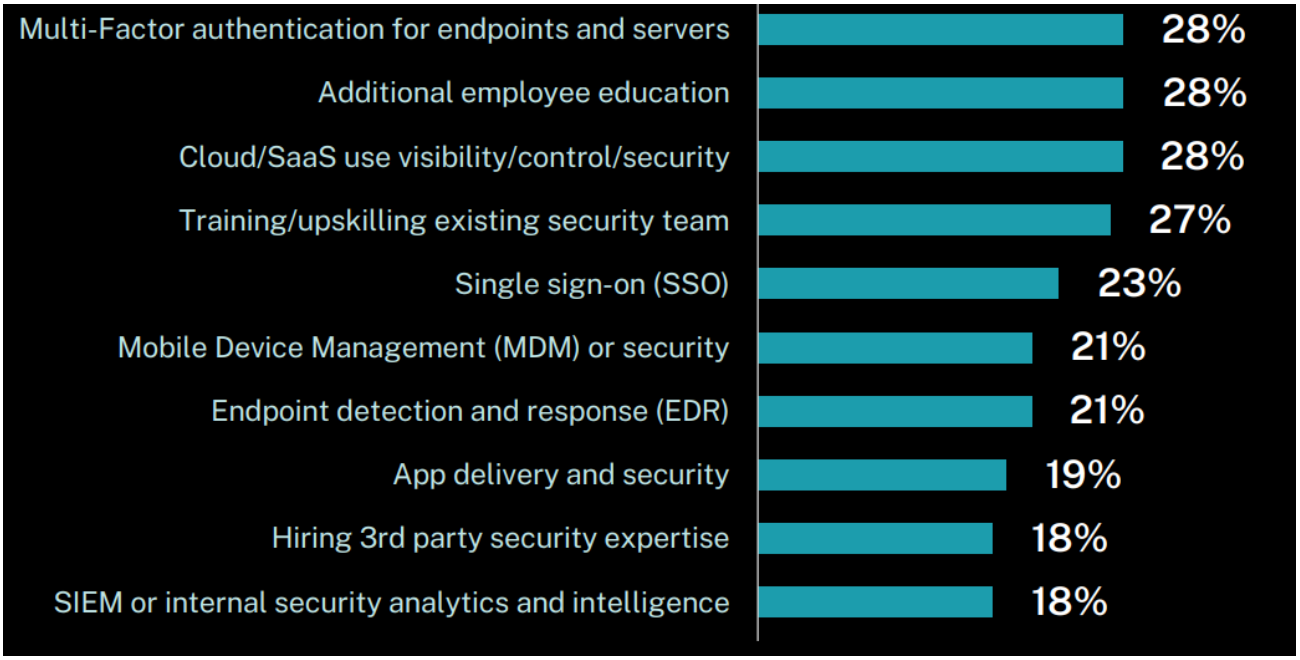

Рис. 1.2. Найкращі протоколи інформаційної безпеки, яким компанії віддають перевагу для кращого захисту віддаленої та гібридної робочої сили [7]

Нульова довіра та єдиний вхід (SSO) були найпопулярнішими технологіями, які відстоювали CISO, опитані для дослідження, а також технології без пароля, такі як MFA, усі з наміром спростити роботу користувача.

Орієнтований на людей підхід до безпеки – це, зрештою, майбутнє, яке поєднує в собі адаптивний доступ із надійною мережевою безпекою, щоб працівники могли адаптуватися до життя після пандемії та гібридного майбутнього роботи. IT відіграватимуть вирішальну роль у досягненні цього. Завдяки правильній технології, служби безпеки зможуть забезпечити послідовний, безпечний і надійний доступ до ресурсів, необхідних співробітникам для виконання роботи, де б вона не була виконана, і дадуть їм змогу працювати якнайкраще [7].

1.3. Аналіз існуючих рішень щодо захисту інформаційних ресурсів організації при гібридній роботі користувачів

Розглянемо основні рішення для забезпечення безпеки віддаленої роботи користувачів організації.

Рішення для безпеки BYOD

Політики Bring Your Own Device (BYOD) дозволяють співробітникам працювати зі своїми особистими пристроями в корпоративних організаціях – виконувати такі завдання, як листування електронною поштою, підключення до корпоративної глобальної мережі та використання корпоративних додатків і даних.

BYOD дає можливість співробітникам використовувати свої особисті смартфони, планшети, ноутбуки та носяться пристрої для доступу до корпоративних даних з будь-якого місця. Щоб підтримувати безпеку, організації повинні збалансувати обмеження конфіденційних даних компанії з продуктивністю користувачів. Необхідно втілювати рішення BYOD, яке дозволяє IT, корпоративній персоні чи контейнеру контролювати, хто має доступ до BYOD і до яких даних. З більшою кількістю віддалених працівників, ніж будь-коли, необхідні технології та добре продумана політика BYOD стали обов’язковими [10].

Щоб підтримувати належний рівень безпеки для політик BYOD, організації потрібно буде керувати пристроями, поєднуючи сучасне й традиційне керування, одночасно підтримуючи нестандартні пристрої на тому ж рівні, що й стандартні. Вони також повинні подолати ризик скомпрометованих облікових даних і мати можливість виявляти заражені пристрої, які намагаються підключитися до корпоративних додатків і даних [10].

MaaS360 Mobile Device Management (SaaS) – це платформа мобільного управління на рівні підприємства (enterprise mobility management, EMM), яка забезпечує можливість бачити смартфони та планшети на підприємстві та керувати ними. Рішення MaaS360 підтримує такі пристрої, як iPhone, iPad та

Android. MaaS360 інтегрується з IBM Security Verify, заснованим на хмарі рішенням з управління ідентифікацією та доступом, щоб забезпечити можливості єдиної реєстрації (single sign-on, SSO), що гарантують, що тільки довірені пристрої та додатки зможуть отримати доступ до ресурсів підприємства або корпоративних ресурсів [10].

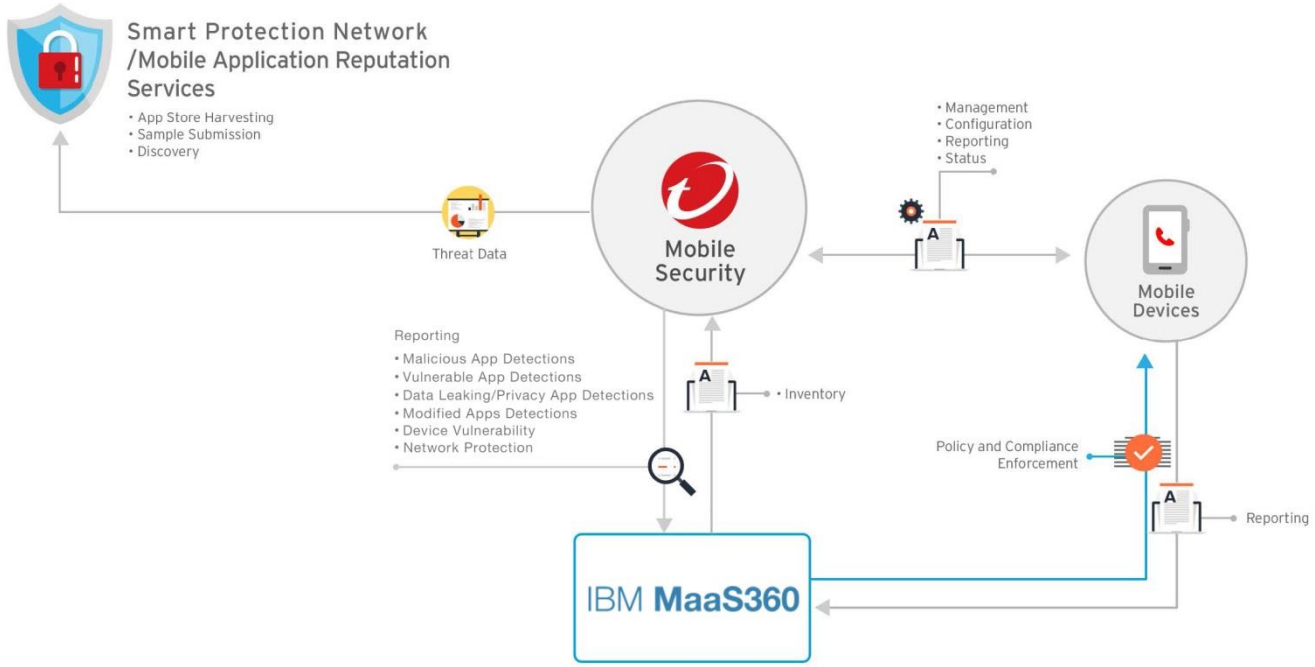

Рис. 1.3. Архітектура інтегрування IBM MaaS360 [10]

VPN віддаленого доступу

VPN віддаленого доступу створює зашифрований тунель між ресурсами вашої організації, кінцевими точками та співробітниками, які їх використовують, захищаючи всю онлайн-активність від зовнішніх користувачів і захищаючи конфіденційні зони мережі.

Хмарна віртуальна приватна мережа (хмарна VPN) – це рішення, яке створює зашифровані тунелі між віддаленими користувачами та корпоративними мережами в хмарі або локально. Шлюзи VPN захищають дані та активи шляхом шифрування та дешифрування трафіку, що передається через Інтернет [11].

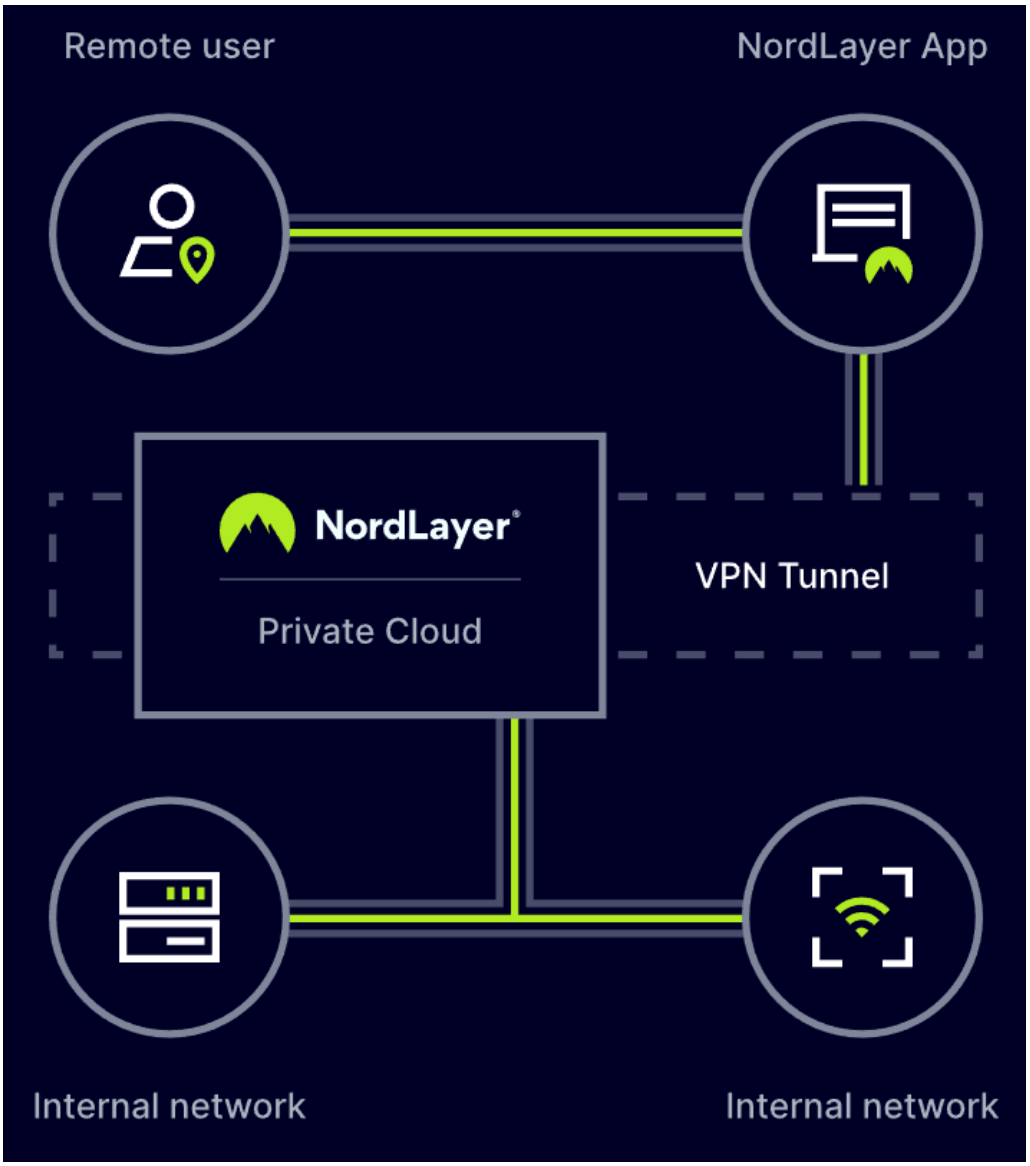

Рис. 1.4. Схема корпоративного VPN [11]

VPN NordLayer від сайту до сайту використовує протоколи IPsec для створення безпечних з'єднань між вашими віддаленими сайтами та хмарними ресурсами AWS [11].

Нульова довіра

Використовуйте рішення для кібербезпеки, спрямоване на усунення неявної довіри будь-якого користувача чи пристрою, які намагаються отримати доступ до мережі компанії. Завдяки принципу «нікому не довіряти, перевіряти все» можна досягти сегментації бізнес-мережі.

ZTNA – це функція Zero Trust Access (ZTA), яка контролює доступ до додатків. Він розширює принципи ZTA для перевірки користувачів і пристроїв

перед кожним сеансом додатку. ZTNA підтверджує, що вони відповідають політиці організації щодо доступу до цього додатку [9].

Fortinet додає Universal ZTNA до Fortinet Security Fabric. Унікальний підхід, завдяки якому Universal ZTNA є частиною брандмауера нового покоління FortiGate (NGFW), робить його надзвичайно гнучким, охоплюючи користувачів, коли вони віддалені або в офісі. Універсальні можливості ZTNA автоматично вмикаються на будь-якому пристрої чи службі під керуванням FortiOS 7.0 і вище. Це включає апаратне забезпечення, віртуальні машини в хмарах і службу FortiSASE.

FortiGate і агент FortiClient ZTNA – технології, які потрібно для більш безпечного доступу та кращого досвіду для віддалених користувачів, як у мережі, так і поза нею.

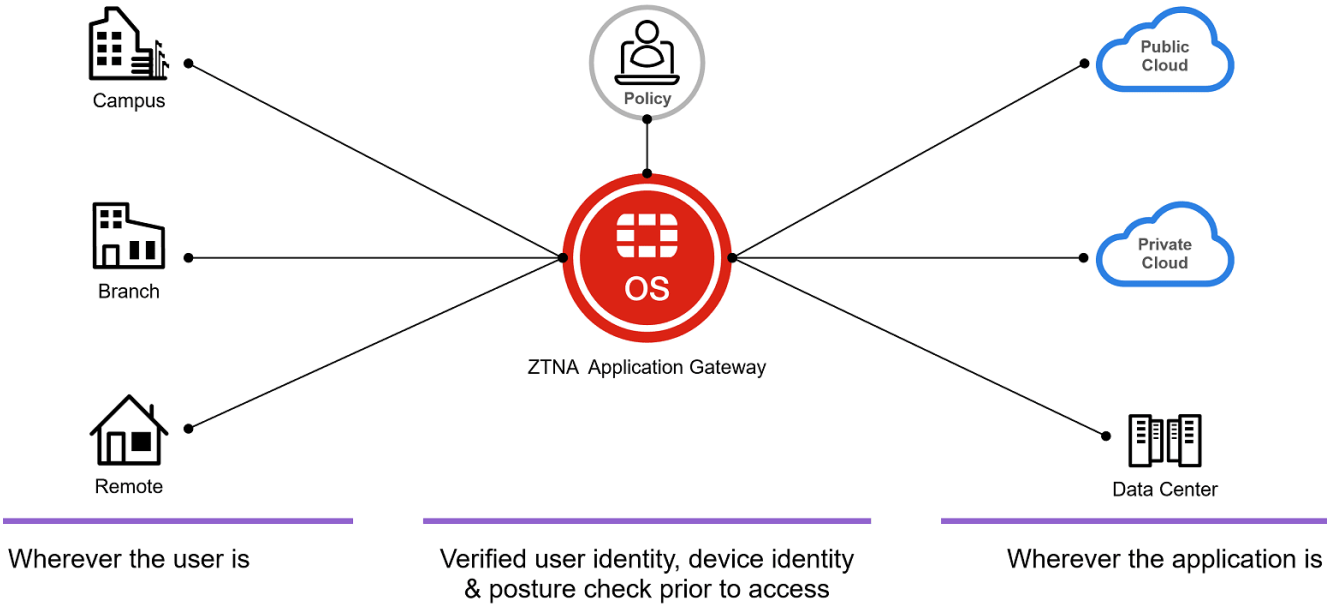

Рис. 1.5. Приклад архітектури ZTNA [8]

Технологія SASE

SASE – це багаторівнева структура, яка об’єднує програмно визначені мережі та сучасні можливості безпеки. З урахуванням постійно мінливого ландшафту рішення SASE має забезпечити захист від внутрішніх і зовнішніх загроз.

Secure Access Service Edge (SASE) – це модель хмарної архітектури, яка поєднує функції мережі та безпеки як послуги разом і надає їх як єдину хмарну службу. Концептуально SASE розширює мережеві можливості та можливості безпеки за межі, де вони зазвичай доступні. Це дозволяє працювати будь-де та віддаленим працівникам, користуватися перевагами брандмауера як послуги (FWaaS), захищеного веб-шлюзу (SWG), доступу до мережі з нульовою довірою (ZTNA) і набором функцій виявлення загроз. SASE складається з Security Service Edge (SSE) і SD-WAN [8].

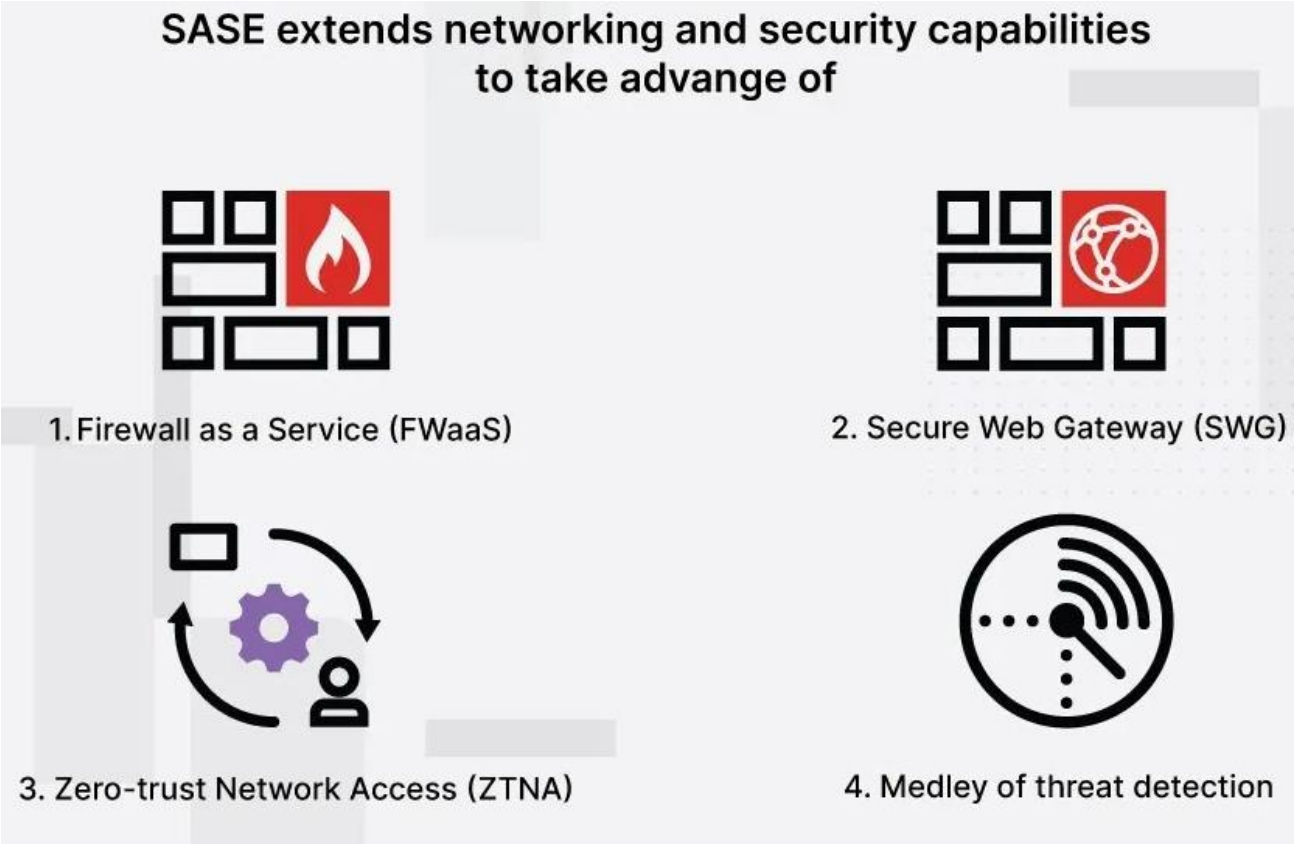

Рис. 1.6. Основні компоненти технології SASE [8]

Корпоративні мережі все більше покладаються на хмарні додатки для ведення бізнесу та підтримки розподілених робочих процесів для підтримки віддалених і мобільних користувачів. Це призвело до того, що звичайна корпоративна мережа швидко виросла за межі звичайної мережі, ставши перед лідерами інфраструктури завдання захистити та керувати поверхнею атак , що постійно розширюється. Хоча мережі досить швидко розвиваються, щоб

підтримувати робочі процеси цих віддалених кінцевих точок, більшість інструментів безпеки не встигають за ними, що робить рішення лише для VPN застарілими. Щоб організації залишалися конкурентоспроможними, усі кінцеві точки мають бути захищені та керовані за допомогою тих самих політик безпеки та мережевої політики, що й їх локальна інфраструктура, незалежно від їх розташування [8].

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ ПРИ ГІБРИДНІЙ РОБОТІ КОРИСТУВАЧІВ НА ПРИКЛАДІ MICROSOFT 365

2.1. Призначення комплексного програмного пакета Microsoft 365 та реалізація підходу «нульової довіри»

Офіс залишається серцем повсякденної роботи компанії – його відповідне функціонування є абсолютно необхідним. Сьогодні більшість офісних процесів оцифровані, тож програмне забезпечення має працювати на найвищому рівні. Працівники часто використовують різноманітне програмне забезпечення, що призводить до проблем з ефективністю та безпекою. Пов'язаний, цілісний програмний пакет необхідний компаніям для того, щоби відповідати потребам сучасних офісів та справлятися з будь-якими викликами та задачам, які постають перед працівниками у щоденній роботі [12].

Для впровадження офісних рішень організації використовують розумний та комплексний програмний пакет Microsoft 365. Рішення Microsoft добре відомі на ринку та зарекомендували себе у сегменті програмного забезпечення для бізнесу – вони щоденно використовуються компаніями у всьому світі. Microsoft 365 дозволяє працівникам підключатися до хмарної платформи та ефективно працювати будь-де, як в офісі [12].

Microsoft 365 задовольняє всі потреби, пов'язані з виконанням офісних задач впродовж робочого дня: від підготовки документів, створення презентацій, роботи з таблицями та розрахунками до керування календарем, комунікації у команді тощо. ПЗ також забезпечує прямий доступ до даних, електронної пошти та зустрічей у віддаленому режимі. Microsoft 365 дозволяє користувачам одночасно працювати з документами в режимі реального часу та безпечно комунікувати з колегами та клієнтами за допомогою текстових чатів та дзвінків. Всі ці рішення пов'язані одне з одним [12].

Microsoft 365 легко інтегрує всі додатки для синергії в роботі. Користувачі можуть обмінюватися документами, створеними у Word, Excel чи PowerPoint, під час онлайн-зустрічі у Skype чи співпрацювати між департаментами у Teams та OneDrive – з рішеннями Microsoft 365 можливо все. Рішення повністю сумісні з операційними системами Windows та MacOS. Надійний та зрозумілий інтерфейс Microsoft також оптимізований для використання на мобільних пристроях – сумісний з iOS й Android, що сприяє універсальності доступу [12].

Будь-які офісні процеси мають бути захищеними. Microsoft 365 надає безпечний спосіб керування даними та процесами, що відповідає вимогам до захисту даних.

Розглянемо план розгортання для створення безпеки Zero Trust із Microsoft 365. Zero Trust – це нова модель безпеки, яка передбачає порушення та перевіряє кожен запит так, ніби він походить із неконтрольованої мережі. Незалежно від того, звідки надходить запит або до якого ресурсу він отримує доступ, модель Zero Trust вчить нас «ніколи не довіряти, завжди перевіряти».

Архітектура безпеки Zero Trust

Підхід «нульової довіри» поширюється на всю цифрову нерухомість і служить інтегрованою філософією безпеки та наскрізною стратегією [13].

Рисунок 2.1 демонструє основні елементи, які сприяють нульовій довірі. На рисунку 2.1 показано [13]:

застосування політики безпеки є центром архітектури Zero Trust. Це включає в себе багатофакторну автентифікацію з умовним доступом, який враховує ризик облікового запису користувача, стан пристрою та інші критерії та політики, які встановлюються;

ідентифікатори, пристрої, дані, додатки, мережа та інші компоненти інфраструктури налаштовано з відповідним захистом. Політики, налаштовані для кожного з цих компонентів, узгоджуються з загальною стратегією Zero Trust. Наприклад, політики пристроїв визначають критерії працездатності пристроїв, а політики умовного доступу вимагають справних пристроїв для доступу до певних додатків і даних;

захист від загроз і розвідка контролюють середовище, виявляють поточні ризики та вживають автоматизованих заходів для усунення атак.

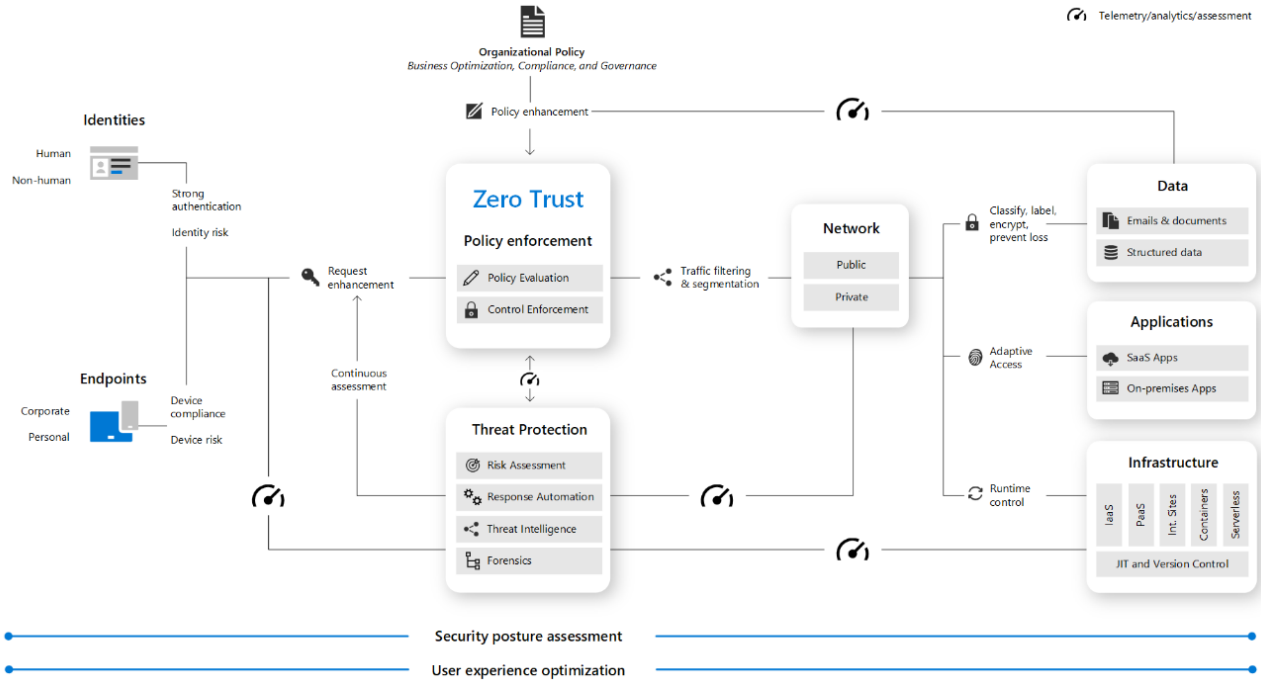

Рис. 2.1. Архітектура безпеки Zero Trust [13]

Порядок розгортання Zero Trust для Microsoft 365.

Microsoft 365 навмисно створено з багатьма можливостями безпеки та захисту інформації, щоб допомогти організаціям створити Zero Trust у своєму середовищі. Багато можливостей можна розширити, щоб захистити доступ до інших додатків SaaS, які використовує організація, і даних у цих додатках.

Рисунок 2.2 представляє роботу з розгортання можливостей Zero Trust. Ця робота розбита на одиниці роботи, які можна конфігурувати разом, починаючи знизу й продовжуючи до верху, щоб гарантувати виконання передумов.

На рисунку 2.2 показано [13]:

нульова довіра починається з фундаменту ідентифікації та захисту пристрою;

можливості захисту від загроз побудовані на цій основі, щоб забезпечити моніторинг у реальному часі та усунення загроз безпеці;

захист інформації та управління забезпечують складні засоби контролю,

націлені на певні типи даних, щоб захистити найціннішу інформацію та допомогти організаціям дотримуватися стандартів відповідності, зокрема захисту особистої інформації.

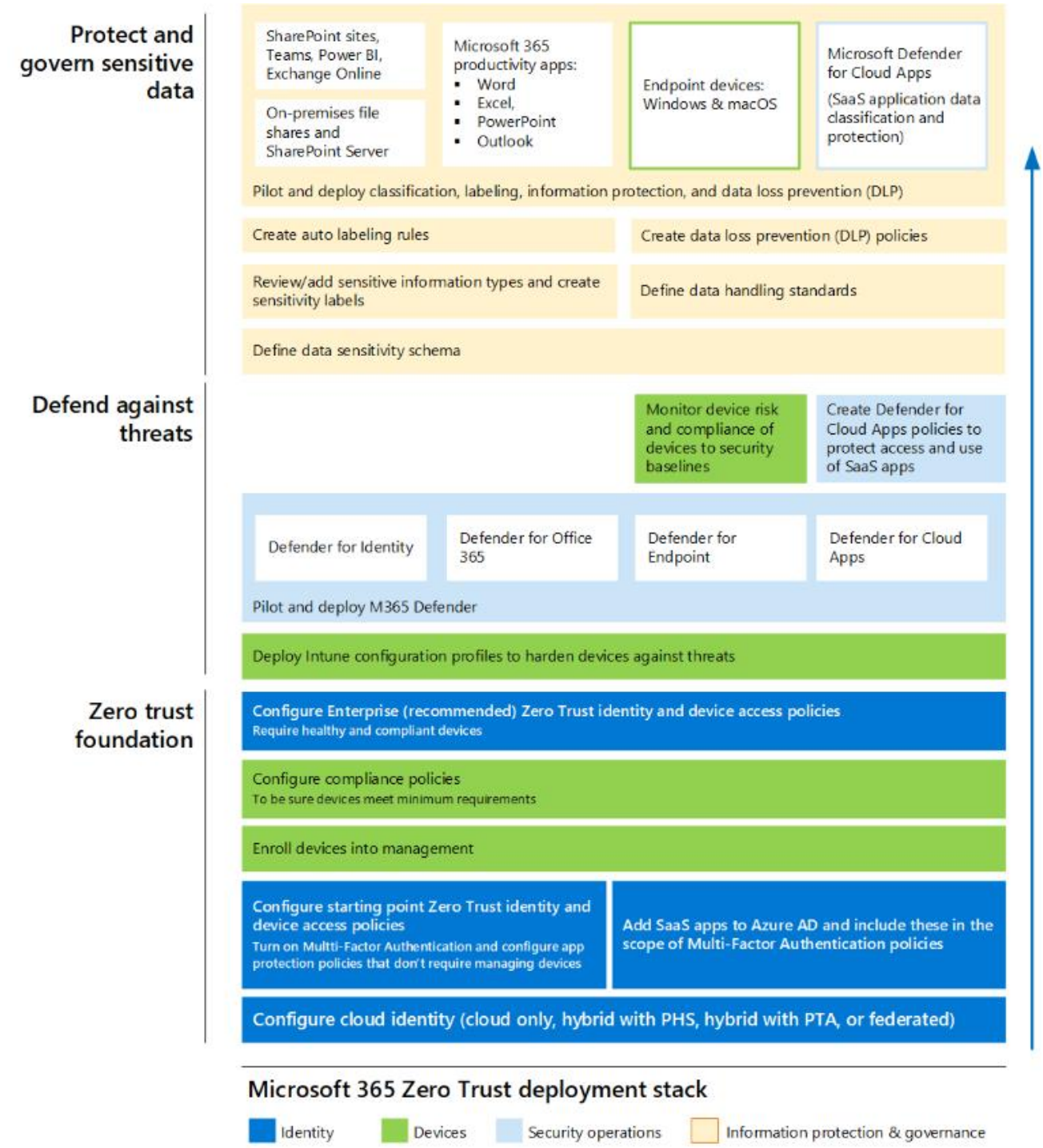

Рис. 2.2. Порядок розгортання можливостей Zero Trust [13]

Крок 1. Налаштуйте ідентифікацію Zero Trust і захист доступу до пристрою – початкові політики.

Перший крок – створити основу Zero Trust, налаштувавши ідентифікацію та захист доступу до пристрою.

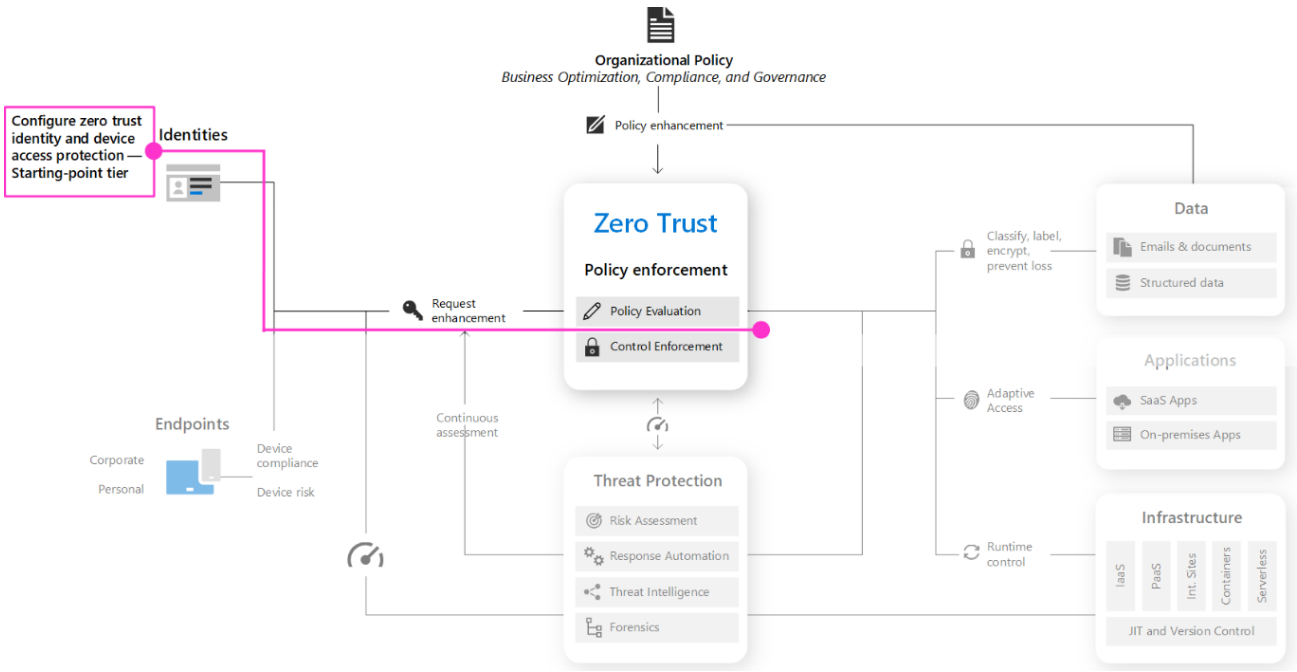

Рис. 2.3. Віртуальна глобальна мережа Azure [13]

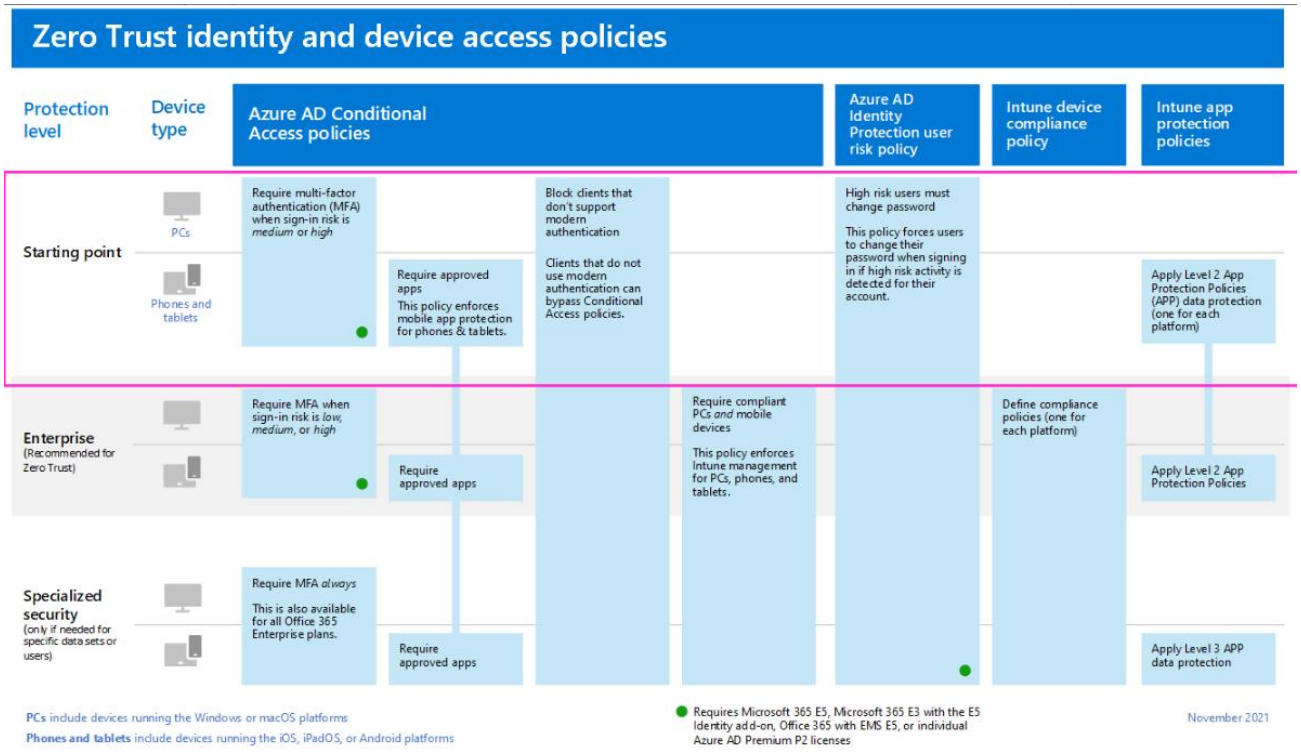

Рис. 2.4. Набір обов’язкових конфігурацій ідентифікації та доступу до пристрою

Для цього необхідно створити набір обов'язкових конфігурацій ідентифікації та доступу до пристрою, а також набір умовного доступу Azure Active Directory (Azure AD), Microsoft Intune та інших політик для безпечного доступу до Microsoft 365 для корпоративних хмарних додатків і служб, інших сервісів SaaS, а також локальні додатки, опубліковані за допомогою Azure AD Application Proxy. Необхідно починати із впровадження рівня початкової точки (рис. 2.4). Ці політики не вимагають реєстрації пристроїв для керування.

Крок 2. Керування кінцевими точками за допомогою Intune.

Далі необхідно зареєструвати пристрої в системі керування та почати захищати їх за допомогою більш складних засобів керування.

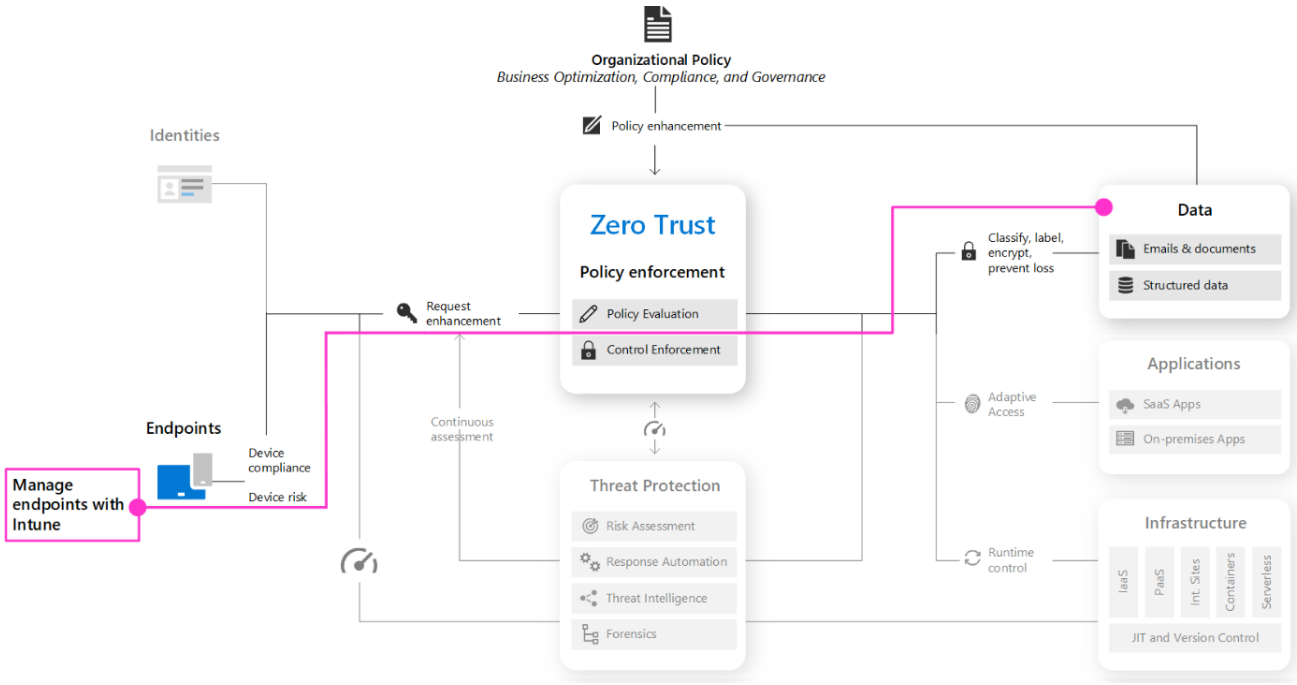

Рис. 2.5. Схема керування кінцевими точками за допомогою Intune [13]

Крок 3. Додавання ідентифікації Zero Trust і захисту доступу до пристрою – корпоративні політики.

З пристроями, зареєстрованими в системі керування, тепер можна запровадити повний набір рекомендованих політик ідентифікації та доступу до пристроїв Zero Trust, для яких потрібні сумісні пристрої.

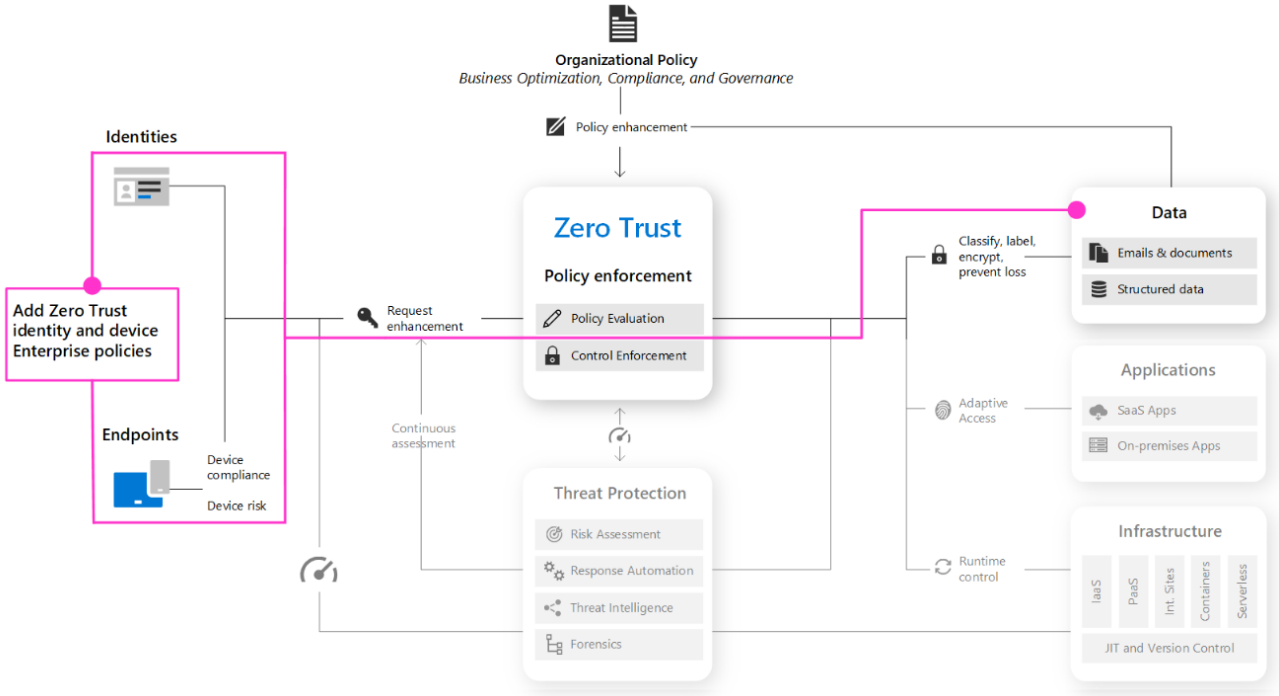

Рис. 2.6. Схема ідентифікації Zero Trust і захисту доступу до пристрою [13]

Необхідно додати політики на рівні підприємства див. рис. 2.7.

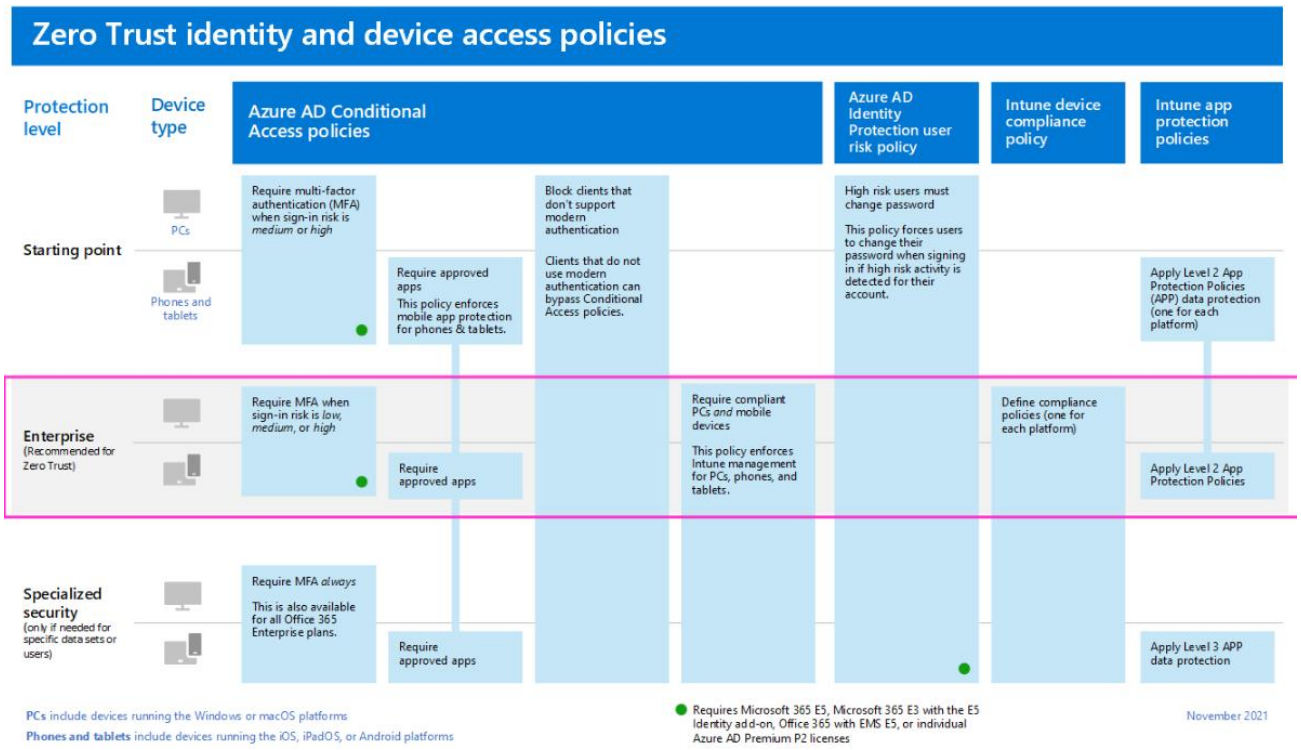

Рис. 2.7. Додавання політики на рівні підприємства [13]

Крок 4. Оцінювання, керування та розгортання Microsoft 365 Defender.

Microsoft 365 Defender – це розширене рішення для виявлення та реагування (XDR), яке автоматично збирає, співвідносить та аналізує дані про сигнали, загрози та сповіщення з усього середовища Microsoft 365, включаючи кінцеву точку, електронну пошту, додатки та ідентифікаційні дані.

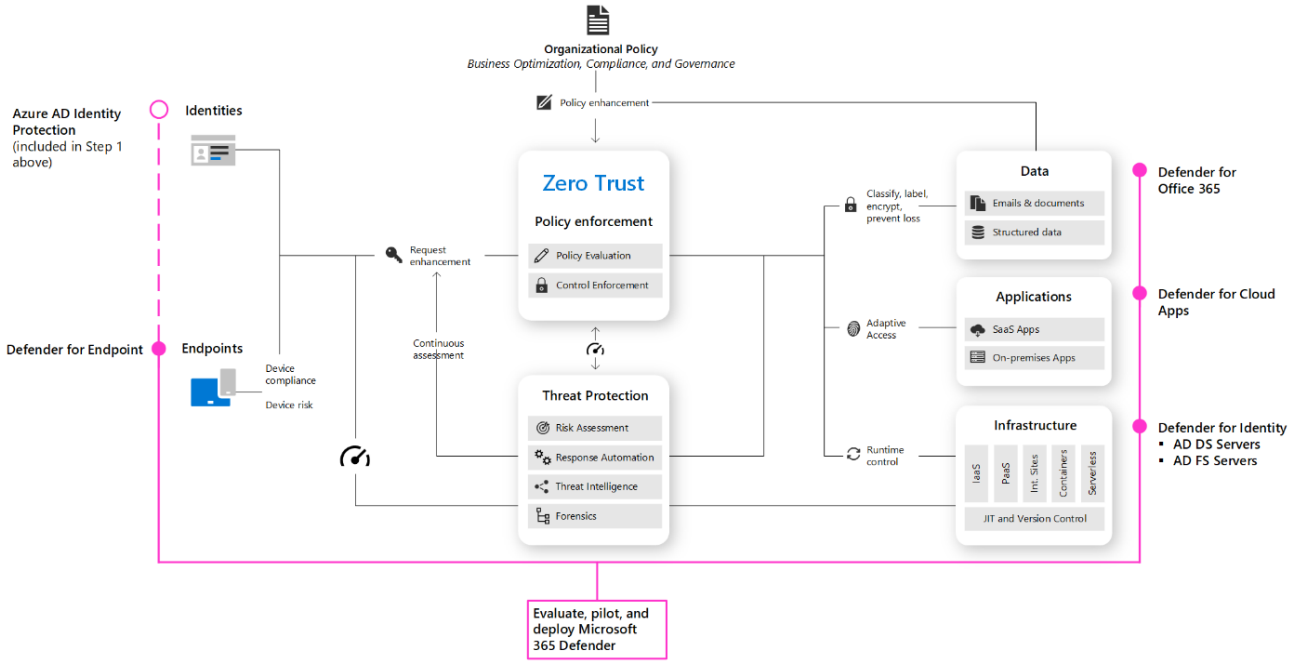

Рис. 2.8. Схема розгортання Microsoft 365 Defender [13]

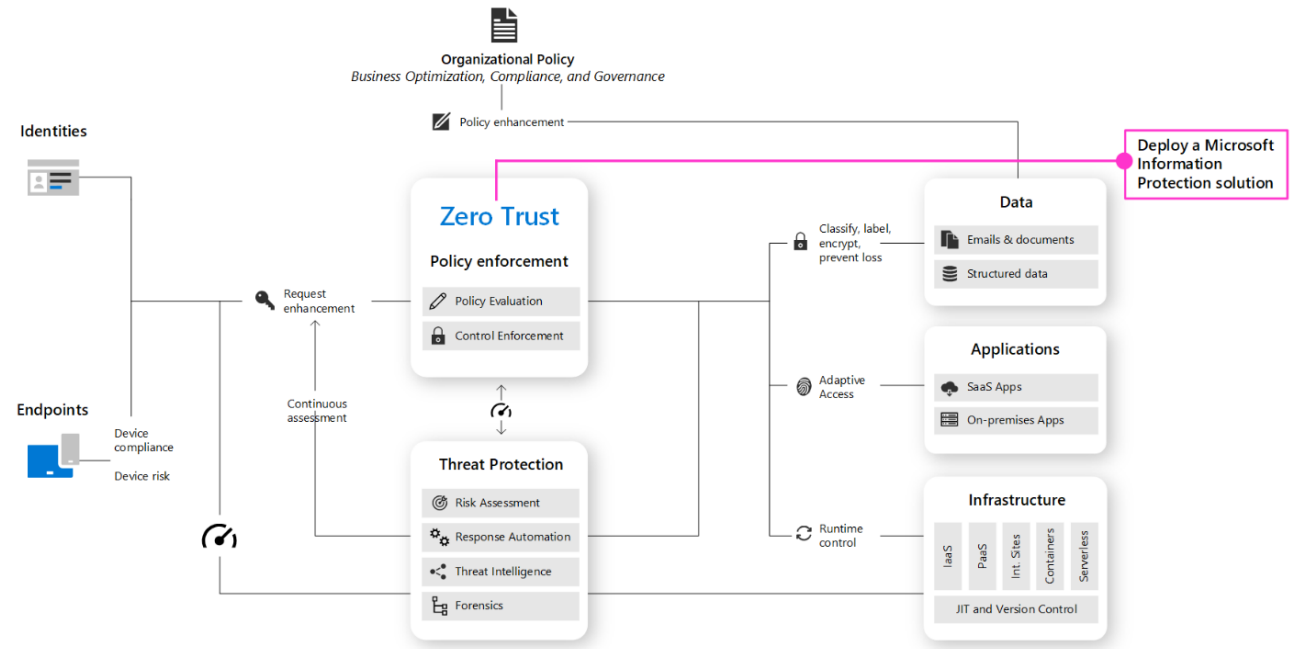

Рис. 2.9. Схема розгортання Microsoft Purview Information Protection [13]

Крок 5. Захист конфіденційних даних і керування ними.

Застосуйте Microsoft Purview Information Protection, щоб виявляти, класифікувати та захищати конфіденційну інформацію, де б вона не була.

Можливості Microsoft Purview Information Protection включені в Microsoft Purview і дають інструменти для ознайомлення з даними, захисту даних і запобігання втраті даних.

Microsoft Purview Information Protection надає структуру, процес і можливості, які можна використовувати для досягнення конкретних бізнес-цілей.

2.2. Призначення та основні функції інфраструктури для гібридної роботи користувачів з Microsoft 365

Щоб забезпечити й оптимізувати продуктивність і співпрацю співробітників, потрібно дозволити співробітникам на місці та віддаленим працівникам легко й безпечно отримувати доступ до локальної та хмарної інформації, інструментів і ресурсів організації. Це рішення передбачає розгортання ключових рівнів інфраструктури, які дають змогу працівникам виконувати роботу якнайкраще, де б вони не були [14].

Гібридні працівники можуть працювати на місці або віддалено в різних місцях. Дозвіл працівникам працювати поза традиційним офісом є важливим для багатьох організацій, щоб [14]:

наймати й утримувати працівників, які не бажають переїжджати або потребують гнучкого робочого середовища;

зменшити поїздки працівників на роботу, залишаючи їм більше часу для продуктивної діяльності та позаробочих заходів, що зменшують стрес;

економити офісний простір.

Microsoft 365 має можливості, щоб надати гібридним працівникам можливість працювати як на місці, так і віддалено (рис. 2.10).

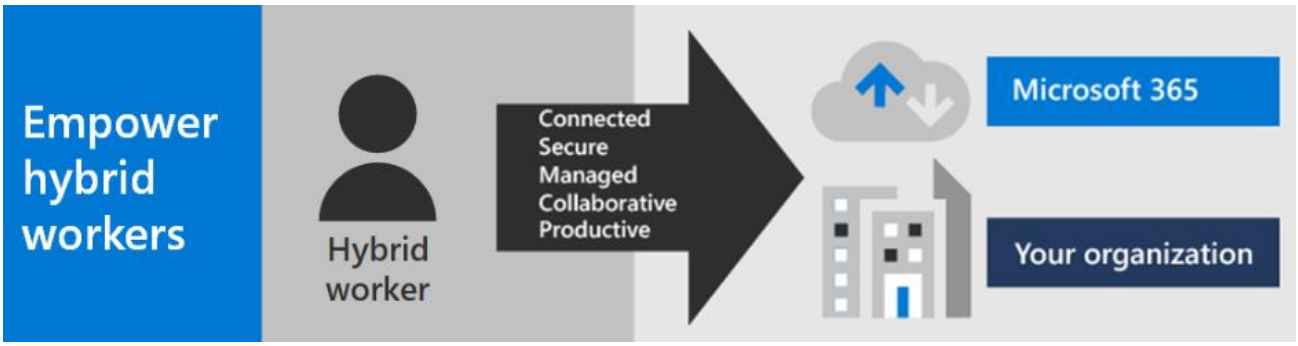

Рис. 2.10. Схема забезпечення гібридної роботи працівників [14]

Для фахівців, які керують локальною та хмарною інфраструктурою для забезпечення гібридної продуктивності працівників, це рішення надає такі ключові можливості [14]:

підключення. З будь-якої точки світу та в будь-який час працівники мають доступ до хмарних служб та даних у Microsoft 365, а також організаційних ресурсів, такі як ті, що пропонуються локальними центрами обробки даних додатків.

безпека. Вхід захищено за допомогою багатофакторної автентифікації (MFA), а вбудовані функції безпеки Microsoft 365 і Windows 11 або 10 захищають від шкідливих програм, зловмисних атак і втрати даних;

керування. Пристроями гібридного працівника можна керувати з хмари за допомогою налаштувань безпеки, дозволених додатків і вимагати відповідності справності системи.

співпраця та продуктивність. Гібридні працівники можуть бути такими ж продуктивними, як і локальні, завдяки тісній співпраці:

онлайн-зустрічі та сеанси чату з Teams;

спільні робочі області для зберігання файлів у хмарі з глобальною доступністю та співпрацею в реальному часі за допомогою SharePoint і OneDrive;

спільні завдання та робочі процеси для розподілу роботи та виконання завдань.

Для безпроблемного входу локальні облікові записи користувачів доменних служб Active Directory (AD DS) мають бути синхронізовані з Azure Active

Directory (Azure AD). Щоб захистити свої пристрої з Windows 11 або 10, їх потрібно зареєструвати в Intune. Схема інфраструктури високого рівня показано на рисунку 2.11.

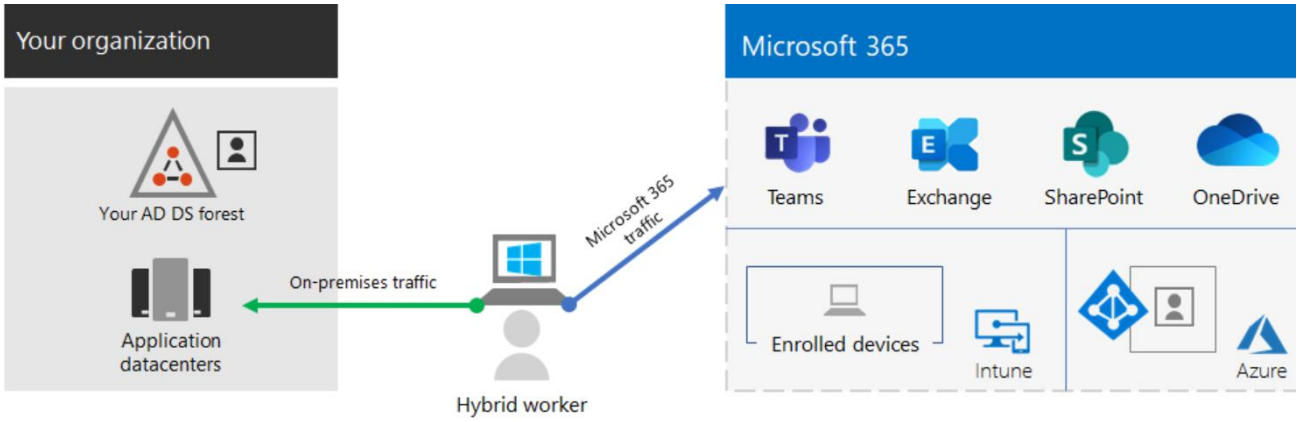

Рис. 2.11. Схема інфраструктури високого рівня [14]

Щоб увімкнути можливості Microsoft 365 для своїх гібридних працівників, необхідно скористатися функціями Microsoft 365, які наведені у таблиці 2.1.

Забезпечення гібридної роботи для всіх працівників може бути здійснено за допомогою цих пристроїв [14]:

сучасний пристрій, наприклад ноутбук Surface і Windows 11 або 10, який має функції, безпеку та продуктивність для доступу до хмарних додатків і служб Microsoft 365 безпосередньо через Інтернет;

будь-який пристрій, включаючи старіші ноутбуки або настільні комп’ютери, які використовуються вдома, і які можуть отримати доступ до хмарних додатків і служб Microsoft 365 опосередковано через Windows 365 Cloud PC. Ця опція забезпечує високу продуктивність, міцну безпеку та спрощене керування IT.

Таблиція 2.1

Функції Microsoft 365 для забезпечення гібридної роботи працівників

Можливість або функція	**опис**	**Ліцензування**
MFA застосовується примусово з параметрами безпеки за замовчуванням	Захистіть себе від скомпрометованих ідентифікаторів і пристроїв, вимагаючи другу форму автентифікації для входу. Стандартні параметри безпеки вимагають MFA для всіх облікових записів користувачів.	Microsoft 365 E3 або E5
MFA запроваджено за допомогою умовного доступу	Вимагати MFA на основі властивостей входу з політиками умовного доступу.	Microsoft 365 E3 або E5
MFA забезпечено умовним доступом на основі ризиків	Вимагати MFA на основі ризику входу користувача за допомогою Azure AD Identity Protection.	Microsoft 365 E5 або E3 з ліцензіями Azure AD Premium P2
Скидання пароля самостійного обслуговування (SSPR)	Дозвольте користувачам скидати або розблоковувати свої паролі чи облікові записи.	Microsoft 365 E3 або E5
Проксі-сервер програми Azure AD	Забезпечте безпечний віддалений доступ для веб-додатків, розміщених на серверах внутрішньої мережі.	Потрібна окрема платна підписка Azure
Azure Point-to-Site VPN	Створіть безпечне з'єднання від пристрою віддаленого працівника до вашої внутрішньої мережі через віртуальну мережу Azure.	Потрібна окрема платна підписка Azure
Windows 365	Підтримуйте віддалених співробітників, які можуть використовувати лише свої особисті та некеровані пристрої з Windows 365 Cloud PC.	Потрібна окрема платна підписка Azure
Віддалений робочий стіл	Дозвольте співробітникам підключатися до комп'ютерів на базі Windows у вашій інтрамережі.	Microsoft 365 E3 або E5
Шлюз служб віддаленого робочого стола	Шифруйте зв'язок і запобігайте прямому доступу до Інтернету для хостів RDS.	Потрібні окремі ліцензії Windows Server
Microsoft Intune	Керуйте пристроями та програмами.	Microsoft 365 E3 або E5
Менеджер конфігурації	Керуйте встановленням програмного забезпечення, оновленнями та налаштуваннями на своїх пристроях	Потрібні окремі ліцензії Configuration Manager
Аналітика кінцевих точок	Визначте готовність до оновлення ваших клієнтів Windows.	Потрібні окремі ліцензії Configuration Manager
Автопілот Windows	Налаштуйте та попередньо налаштуйте нові пристрої з Windows 11 або 10 для продуктивного використання.	Microsoft 365 E3 або E5
Microsoft Teams, Exchange Online, SharePoint Online і OneDrive, програми Microsoft 365, Microsoft Power Platform і Yammer	Створюйте, спілкуйтеся та співпрацюйте.	Microsoft 365 E3 або E5

2.3. Порядок забезпечення безпеки інформаційних ресурсів організації при гібридній роботі користувачів

Для того, щоб захистити й оптимізувати доступ до серверів і хмарних сервісів організації та максимально підвищити продуктивність гібридної роботи працівників, необхідно дотримуватися наступного порядку (рис. 2.12) [14]:

необхідно підвищити безпеку входу за допомогою MFA;

необхідно надати віддалений доступ до локальних додатків і служб;

необхідно розгорнути служби безпеки та відповідності;

необхідно розгорнути керування кінцевими точками для своїх пристроїв, ПК та інших кінцевих точок;

необхідно розгорнути гібридні додатки та служби для підвищення продуктивності працівників;

необхідно навчити своїх працівників і розглядати відгуки про використання.

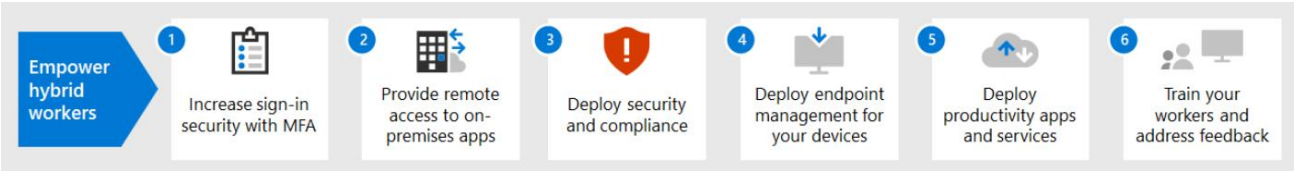

Рис. 2.12. Загальний порядок захисту й оптимізації доступ до серверів і хмарних сервісів організації [14]

Розглянемо більш детально кожен крок даного порядку.

Крок 1. Підвищення безпеки входу для гібридних працівників за допомогою MFA.

Щоб підвищити безпеку входу гібридних працівників, використовується багатофакторна автентифікація (MFA). MFA вимагає, щоб під час входу користувачів проходила додаткова перевірка, крім пароля облікового запису користувача. Навіть якщо зловмисник визначає пароль облікового запису користувача, він також повинен мати можливість відповісти на додаткову перевірку, наприклад текстове повідомлення, надіслане на смартфон, перш ніж

отримати доступ.

Усім користувачам, у тому числі гібридним працівникам і особливо адміністраторам, Microsoft наполегливо рекомендується MFA.

Політики умовного доступу – це набір правил, які визначають умови, за яких вхід оцінюється та дозволяється. Наприклад, ви можете створити політику умовного доступу, у якій зазначено:

якщо ім’я облікового запису користувача є членом групи для користувачів, яким призначено ролі Exchange, користувача, пароля, безпеки, SharePoint або глобального адміністратора, вимагайте MFA, перш ніж дозволити доступ.

Ця політика дозволяє вимагати MFA на основі членства в групі, замість того, щоб намагатися налаштувати окремі облікові записи користувачів для MFA, коли їм призначено або скасовано ці ролі адміністратора.

Ви також можете використовувати політики умовного доступу для більш розширених можливостей, наприклад, вимагати, щоб вхід здійснювався із сумісного пристрою, наприклад ноутбука з Windows 11 або 10.

На додаток до хмарної автентифікації для користувачів, Azure AD також може стати центральним засобом захисту всіх додатків організації, незалежно від того, чи є вони локальними, у хмарі Microsoft або в іншій хмарі. Інтегрувавши додатки в Azure AD, можна полегшити гібридним працівникам пошук потрібних їм додатків і безпечний вхід у них.

Крок 2. Надання віддаленого доступу до локальних додатків і служб.

Якщо організація використовує рішення VPN віддаленого доступу, зазвичай із серверами VPN на межі корпоративної мережі та клієнтами VPN, встановленими на пристроях користувачів, користувачі можуть використовувати підключення VPN віддаленого доступу для доступу до локальних додатків і серверів. Але вам може знадобитися оптимізувати трафік до хмарних служб Microsoft 365.

Якщо користувачі не використовують рішення VPN, можна використовувати Azure Active Directory (Azure AD) Application Proxy і Azure Point-to-Site (P2S) VPN, щоб надати доступ, залежно від того, чи всі додатки є

веб-орієнтованими.

Ось основні конфігурації для віддаленого доступу:

використовується рішення VPN віддаленого доступу;

не використовується рішення VPN віддаленого доступу та передбачається, що віддалені працівники використовують свої персональні комп'ютери;

не використовується рішення VPN віддаленого доступу, є гібридна ідентифікація, і потрібен віддалений доступ лише до локальних веб-додатків;

не використовується рішення VPN віддаленого доступу, і потрібен доступ до локальних додатків, деякі з яких не є веб-інтерфейсом.

На рисунку 2.13 зображено блок-схему для параметрів конфігурації віддаленого доступу, розглянутих вище.

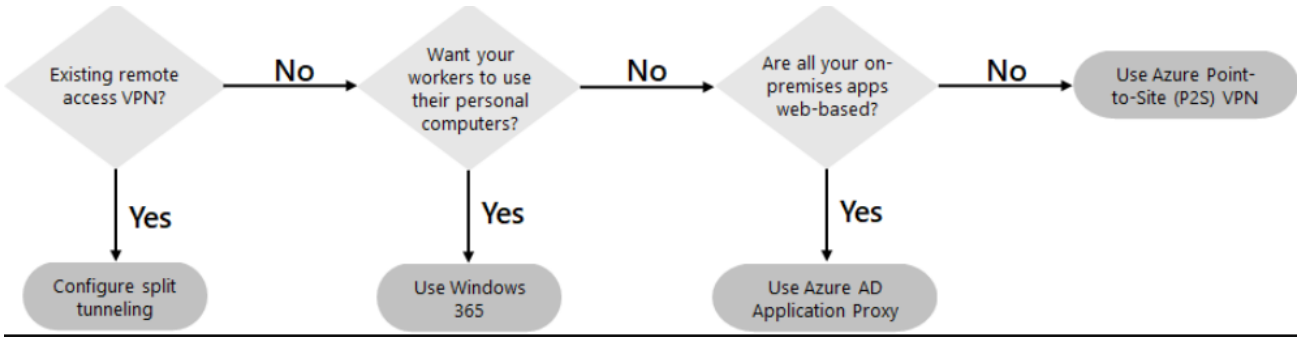

Рис. 2.13. Блок-схема для параметрів конфігурації віддаленого доступу [14]

Якщо віддалені працівники використовують традиційний клієнт VPN для отримання віддаленого доступу до мережі організації, необхідно переконатися, що клієнт VPN підтримує розділене тунелювання.

Без розділеного тунелювання весь віддалений робочий трафік надсилається через VPN-з'єднання, звідки його потрібно перенаправляти на периферійні пристрої організації, обробляти, а потім надсилати в Інтернет.

Трафік Microsoft 365 має проходити непрямим маршрутом через організацію, який може бути перенаправлений до точки входу в мережу Microsoft, розташованої далеко від фізичного розташування клієнта VPN. Цей непрямий шлях додає затримку мережевого трафіку та знижує загальну продуктивність.

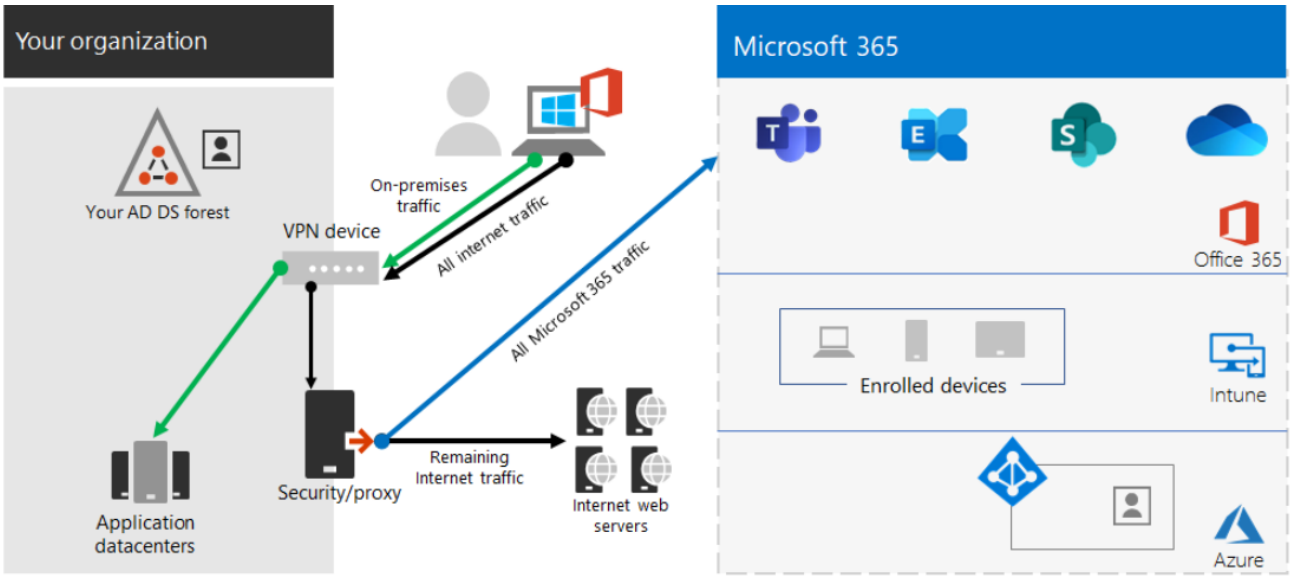

Рис. 2.14. Схема використання традиційного клієнта VPN

За допомогою розділеного тунелювання можна налаштувати свій VPN-клієнт, щоб виключити певні типи трафіку від надсилання через VPN-з'єднання до мережі організації.

Щоб оптимізувати доступ до хмарних ресурсів Microsoft 365, необхідно налаштувати свої VPN-клієнти розділеного тунелювання, щоб виключити трафік до кінцевих точок Microsoft 365 категорії «Оптимізація » через VPN-з'єднання.

Якщо віддалені працівники не використовують традиційний клієнт VPN, а локальні облікові записи та групи користувачів синхронізовано з Azure AD, то можна використовувати Azure AD Application Proxy для забезпечення безпечного віддаленого доступу для веб-додатків, розміщених на локальних серверах. До веб-додатків належать сайти SharePoint Server, сервери Outlook Web Access або будь-які інші веб-додатки для бізнесу.

Компоненти Azure AD Application Proxy показано на рисунку 2.15.

Крок 3. Розгортання безпеки та відповідності вимогам для гібридних працівників.

Для гібридних працівників, деякі з яких ніколи не ходять в офіс або ходять рідко, безпека та відповідність є важливою частиною загального рішення. Усі їхні комунікації відбуваються через Інтернет, а не обмежуються внутрішньою мережею організації.

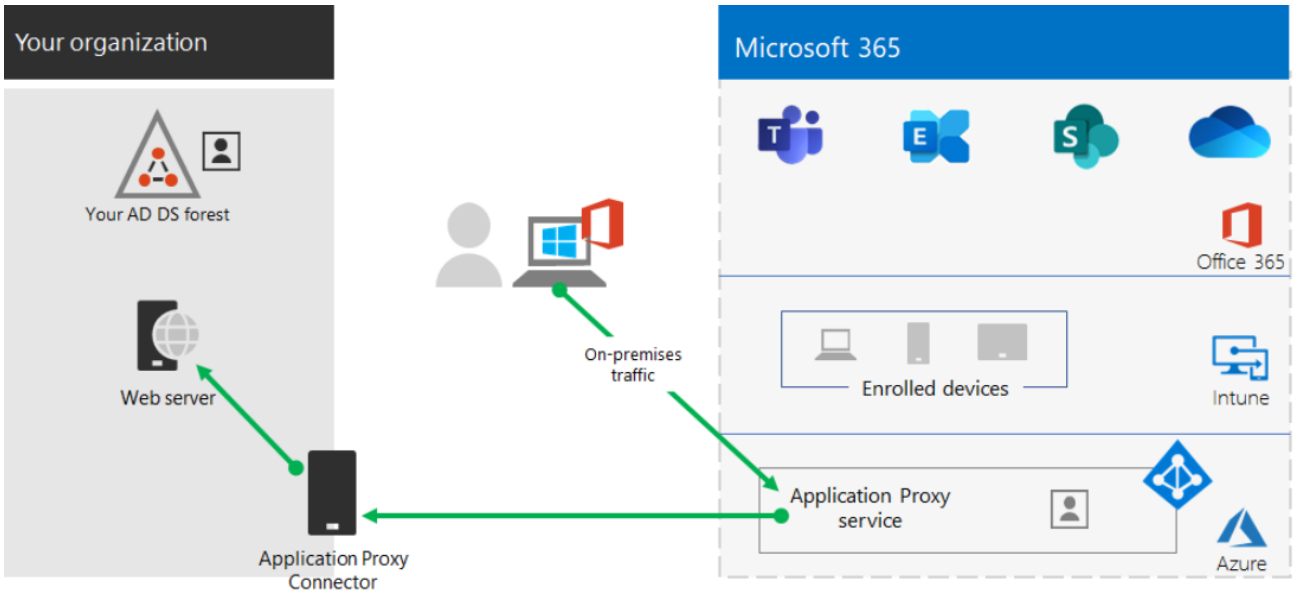

Рис. 2.15. Схема компонентів Azure AD Application Proxy

Є речі, які працівники можуть зробити, щоб залишатися продуктивними, одночасно зменшуючи ризики кібербезпеки та дотримуючись внутрішніх політик і правил щодо даних.

Віддалена робота потребує таких елементів безпеки та відповідності [14]:

контрольований доступ до програм продуктивності, які використовують гібридні працівники, наприклад Microsoft Teams;

контрольований доступ і захист даних, які створюють і використовують гібридні працівники, як-от бесіди в чаті або спільні файли;

захист пристроїв Windows 11 або 10 від шкідливих програм та інших видів кібератак;

захист електронної пошти, файлів і сайту за допомогою узгодженого маркування рівнів конфіденційності та захисту;

запобігання витоку інформації;

дотримання регіональних правил даних.

Нижче наведено функції Microsoft 365, які надають послуги безпеки та відповідності для гібридних працівників (рис. 2.16).

Рис. 2.16. Функції Microsoft 365, які надають послуги безпеки та відповідності для гібридних працівників [14]

Результатами кроку 3 для гібридних працівників є запровадження [14]:

точки зору безпеки:

контрольований доступ до додатків і даних, які гібридні працівники використовують для спілкування та співпраці;

захист від шкідливих програм для даних хмарних служб, електронної пошти та пристроїв з Windows 11 або 10;

точки зору відповідності:

послідовне маркування рівнів чутливості та захисту;

політики запобігання витоку інформації;

дотримання регіональних правил даних.

Крок 4. Розгортання керування кінцевими точками для корпоративних пристроїв, ПК та інших кінцевих точок.

Завдяки гібридним працівникам потрібно підтримувати все більшу кількість персональних пристроїв. Керування кінцевими точками – це підхід до безпеки на основі політики, який вимагає, щоб пристрої відповідали певним критеріям, перш ніж їм буде надано доступ до ресурсів. Microsoft Endpoint Manager надає сучасні можливості керування для захисту даних у хмарі та локально.

Microsoft Endpoint Manager надає служби та інструменти для керування

мобільними пристроями, настільними комп'ютерами, віртуальними машинами, вбудованими пристроями та серверами, поєднуючи наведені на рисунку 2.17 служби.

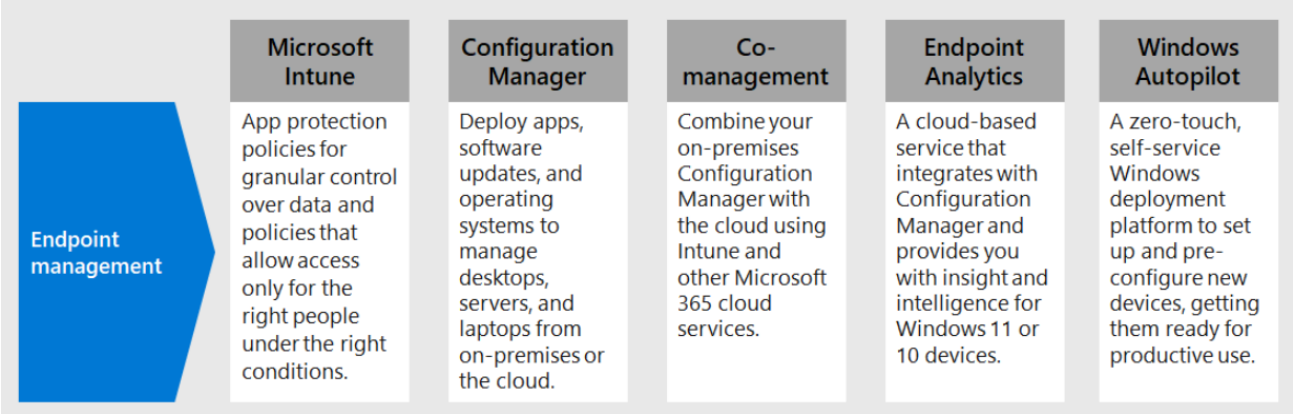

Рис. 2.17. Сервіси керування кінцевими точками [14]

Microsoft Intune – це хмарна служба, яка зосереджена на керуванні мобільними пристроями (MDM) і мобільними програмами (MAM), що входить до складу Microsoft 365.

MDM: для пристроїв, що належать організації, можна здійснювати повний контроль, включаючи налаштування, функції та безпеку. Пристрої «реєструються» в Intune, де вони отримують політики Intune із правилами та налаштуваннями. Наприклад, можна встановити вимоги до пароля та PIN-коду, створити з'єднання VPN, налаштувати захист від загроз тощо.

MAM: віддалені працівники можуть не захотіти, щоб ви мали повний контроль над їхніми особистими пристроями, також відомими як пристрої, які приносять із собою (BYOD). Можна надати своїм гібридним працівникам варіанти і все одно захистити організацію. Наприклад, гібридні працівники можуть зареєструвати свої пристрої, якщо їм потрібен повний доступ до ресурсів організації. Або, якщо цим користувачам потрібен лише доступ до електронної пошти чи Microsoft Teams, скористайтеся політиками захисту додатків, які потребують багатофакторної автентифікації (MFA) для використання цих додатків.

Крок 5. Розгортання гібридних додатків та сервісів для підвищення продуктивності працівників.

Щоб бути продуктивними, люди повинні спілкуватися та співпрацювати один з одним. Їм потрібно зустрічатися, спілкуватися голосом і текстовими повідомленнями, створювати новий вміст і ділитися інформацією та файлами, обмінюватися електронною поштою та керувати календарями та завданнями. Microsoft 365 надає хмарні служби для всіх цих ключових функцій (рис. 2.18).

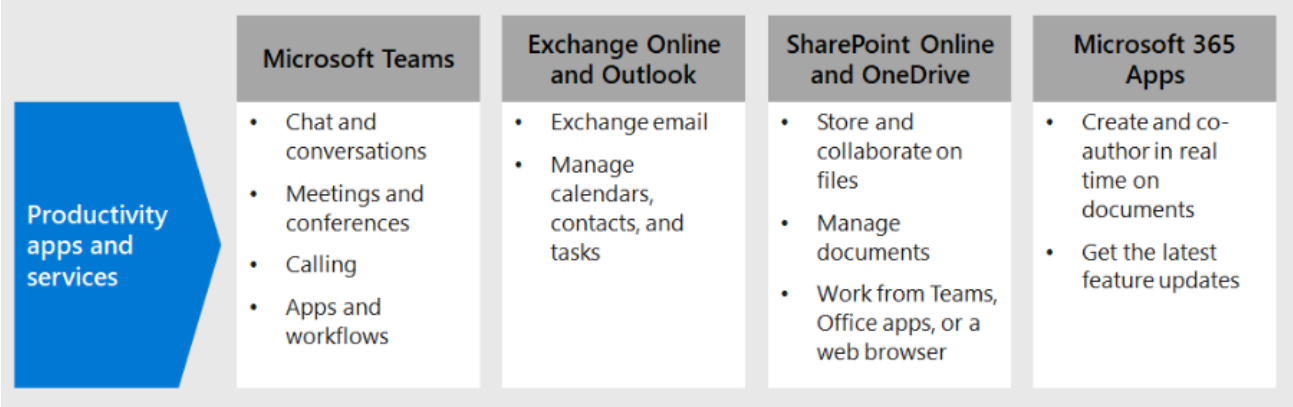

Рис. 2.18. Гібридні додатки та сервіси для підвищення продуктивності працівників [14]

Крок 6. Навчання працівників і розгляд відгуків про використання.

Необхідно навчати своїх гібридних працівників такому [14]:

належним процедурам входу за допомогою MFA, включаючи реєстрацію додаткового методу перевірки;

використанню пристроїв і те, як політики керування кінцевими точками можна використовувати для блокування доступу для невідповідних або некерованих пристроїв;

використанню дозволених додатків і те, як політики додатків керування кінцевими точками можна використовувати для блокування використання деяких програм;

функціям безпеки Windows 11 або 10 Enterprise;

як використовувати Teams для чату, відеоконференцій, обміну документами

та ланцюжкових розмов;

як використовувати Outlook для електронної пошти та планування;

як використовувати команду SharePoint або сайти спілкування та папки OneDrive для перегляду та спільної роботи над файлами в бібліотеці користувача та файлами, що належать до групи.

Це навчання має включати практичні вправи, щоб працівники могли відчути ці можливості та їхні результати.

Необхідно створити форум для своїх співробітників, щоб ставити запитання або отримувати вирішення проблем, як-от команда або група Yammer.

Протягом тижнів після тренування:

швидко розглядайте відгуки працівників на своєму форумі та змінюйте свої політики та конфігурації за потреби;

проаналізуйте використання для команд, електронної пошти, сайтів SharePoint і папок OneDrive і порівняйте це зі своїми очікуваннями щодо прийняття користувачами.

Потім за потреби перенавчіть користувачів.

У результаті, гібридні працівники пройшли навчання, і для них є оперативний і відкритий форум, де вони можуть надавати відгуки та публікувати проблеми з безпекою, відповідністю, віддаленим доступом і додатками для продуктивності.

3 ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ ПРИ ГІБРИДНІЙ РОБОТІ КОРИСТУВАЧІВ НА ПРИКЛАДІ MICROSOFT 365

3.1. Порядок підтримки гібридної роботи користувачів

Розглянемо пріоритети завдань (рис. 3.1), щоб допомогти групам безпеки якнайшвидше реалізувати найважливіші можливості безпеки для підтримки гібридної роботи користувачів.

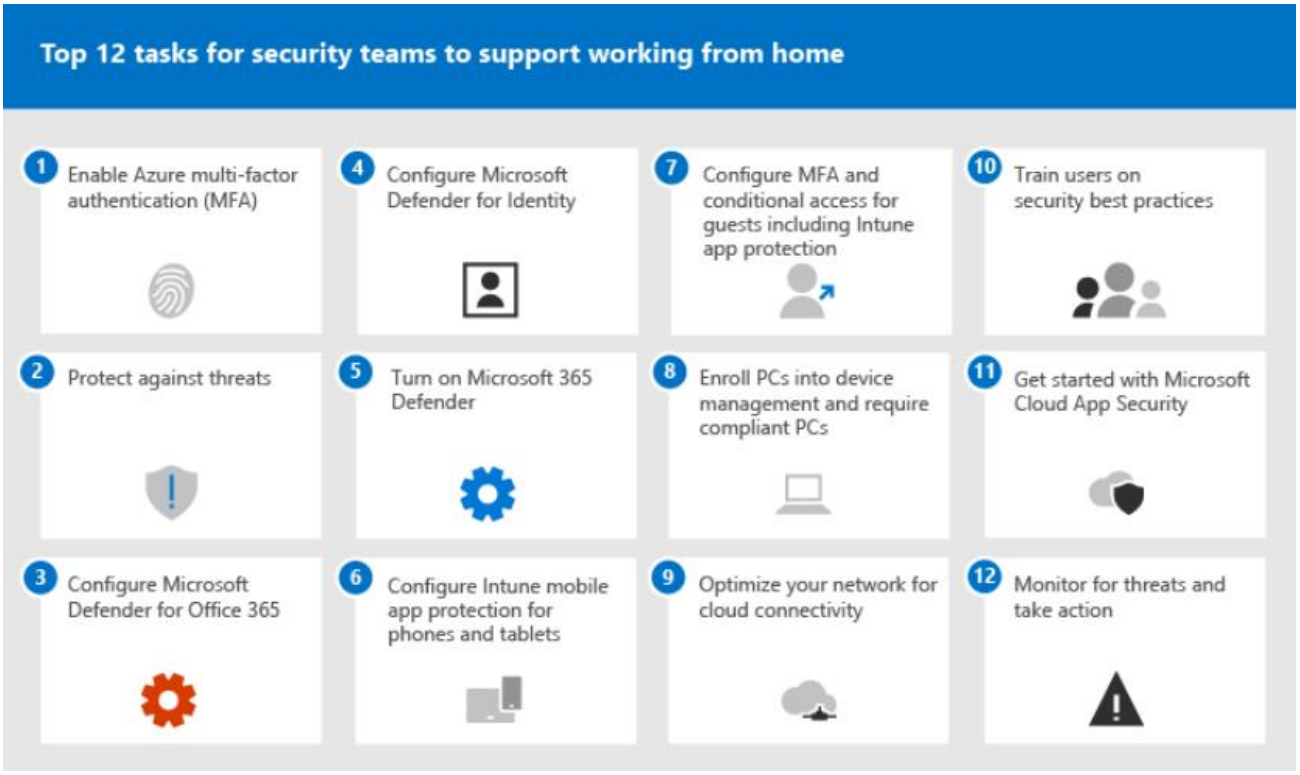

Рис. 3.1. Основні завдання з підтримки гібридної роботи користувачів [15]

Перш ніж почати, необхідно перевірити свій рейтинг безпеки Microsoft 365 на порталі Microsoft 365 Defender. За допомогою централізованої інформаційної панелі ви можете контролювати та покращувати безпеку своїх ідентифікаційних даних, даних, додатків, пристроїв та інфраструктури Microsoft 365.

Таблиця 3.1

Завдання, які необхідно виконати відповідно до корпоративних планів

Крок	завдання	Усі плани Office 365 Enterprise	Microsoft 365 E3	Microsoft 365 E5
1	Увімкнути багатофакторну автентифікацію (MFA) Azure AD	✓	✓	✓
2	Захист від загроз	✓	✓	✓
3	Налаштуйте Microsoft Defender для Office 365			✓
4	Налаштуйте Microsoft Defender для Identity			✓
5	Увімкніть Microsoft 365 Defender			✓
6	Налаштуйте захист мобільних програм Intune для телефонів і планшетів		✓	✓
7	Налаштуйте MFA та умовний доступ для гостей, включаючи захист програми Intune		✓	✓
8	Зареєструйте ПК у програмі керування пристроями та вимагайте сумісних ПК		✓	✓
9	Оптимізуйте свою мережу для підключення до хмари	✓	✓	✓
10	Навчати користувачів	✓	✓	✓
11	Почніть роботу з Microsoft Defender для хмарних програм			✓
12	Слідкуйте за загрозами та вживайте заходів	✓	✓	✓

При цьому нараховуються бали за налаштування рекомендованих функцій безпеки, виконання завдань, пов’язаних із безпекою (наприклад, перегляд звітів), або виконання рекомендацій за допомогою програми чи програмного забезпечення третьої сторони [15].

1. Необхідно ввімкнути багатофакторну автентифікацію Azure AD (MFA).

Найкраще, що ви можете зробити, щоб покращити безпеку для співробітників, які працюють вдома, – увімкнути MFA. Якщо у вас ще немає процесів, сприймайте це як екстрений пілот і переконайтеся, що у вас є спеціалісти з підтримки, готові допомогти співробітникам, які опинилися в

глухому куті. Оскільки ви, ймовірно, не можете розповсюджувати апаратні пристрої безпеки, використовуйте біометричні дані Windows Hello та програми автентифікації смартфонів, такі як Microsoft Authenticator.

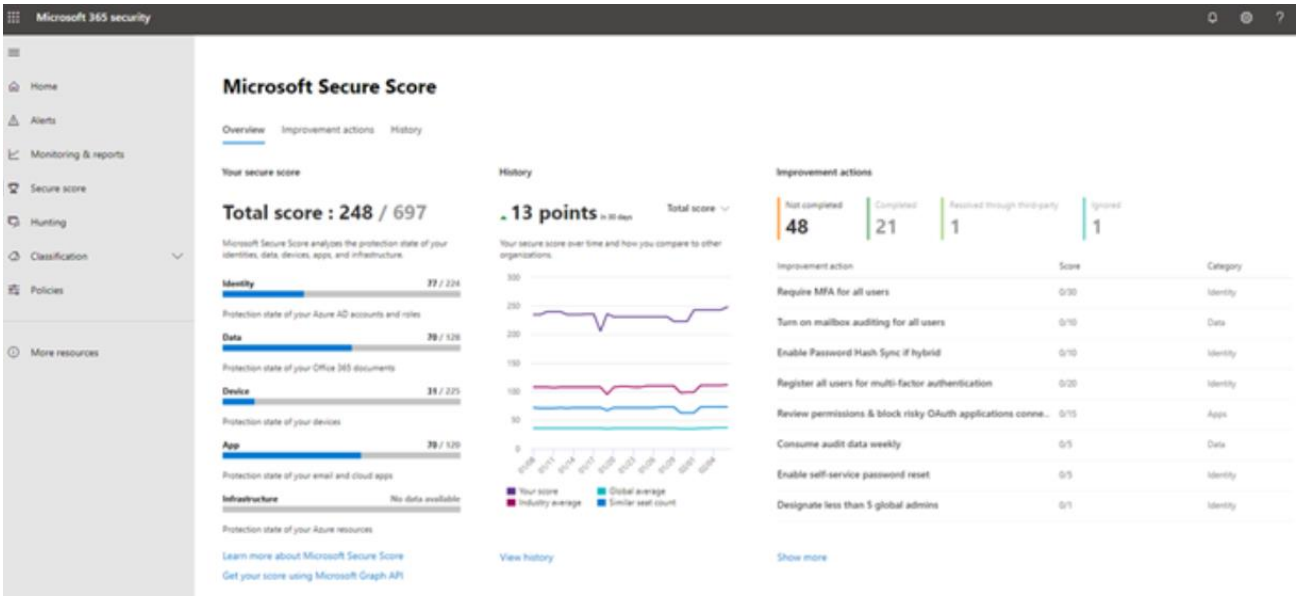

Рис. 3.2. Панель Microsoft 365 security [15]

2. Необхідно налаштувати захист від загроз.

Усі плани Microsoft 365 включають різноманітні функції захисту від загроз:

захист від шкідливих програм;

захист від шкідливих URL і файлів;

захист від фішингу;

захист від спаму.

3. Необхідно налаштувати Microsoft Defender для Office 365

Microsoft Defender для Office 365, що входить до складу Microsoft 365 E5 та Office 365 E5, захищає організацію від зловмисних загроз, створених електронними повідомленнями, посиланнями (URL-адресами) та інструментами для співпраці.

Microsoft Defender для Office 365 [15]:

захищає організацію від невідомих загроз електронною поштою в режимі реального часу за допомогою інтелектуальних систем, які перевіряють вкладення

та посилання на наявність шкідливого вмісту. Ці автоматизовані системи включають надійну платформу детонації, евристичні моделі та моделі машинного навчання;

захищає організацію, коли користувачі співпрацюють і обмінюються файлами, виявляючи та блокуючи шкідливі файли на сайтах груп і в бібліотеках документів;

застосовує моделі машинного навчання та розширені алгоритми виявлення імітації для запобігання фішинговим атакам.

Глобальний адміністратор може налаштувати ці засоби захисту:

налаштувати політику безпечних посилань;

налаштувати глобальні параметри для безпечних посилань;

налаштувати політику безпечних вкладень.

Щоб налаштувати Defender для Office 365 для таких робочих навантажень, потрібно буде попрацювати з адміністратором Exchange Online і SharePoint Online.

4. Необхідно налаштувати Microsoft Defender для Identity

Microsoft Defender for Identity – це хмарне рішення безпеки, яке використовує ваші локальні сигнали Active Directory для ідентифікації, виявлення та дослідження складних загроз, скомпрометованих ідентифікаційних даних і зловмисних інсайдерських дій, спрямованих на організацію. Далі зосередьтеся на цьому, оскільки він захищає локальну та хмарну інфраструктуру, не має залежностей чи передумов і може забезпечити негайну вигоду.

5. Необхідно ввімкнути Microsoft 365 Defender.

Тепер, коли налаштовано Microsoft Defender для Office 365 і Microsoft Defender for Identity, можна переглядати об’єднані сигнали від цих можливостей на одній інформаційній панелі. Microsoft 365 Defender об’єднує сповіщення, інциденти, автоматизоване розслідування та реагування, а також розширений пошук різних робочих навантажень (Microsoft Defender для Identity, Defender для Office 365, Microsoft Defender для Endpoint і Microsoft Defender для хмарних програм) на одній панелі в Microsoft 365 Defender.

6. Налаштуйте захист мобільних програм Intune для телефонів і планшетів

Керування мобільними додатками Microsoft Intune (MAM) дозволяє керувати та захищати дані організації на телефонах і планшетах, не керуючи цими пристроями. Ось як це працює:

створюється політика захисту додатків (APP), яка визначає, які додатки на пристрої є керованими та які дії дозволені (наприклад, запобігання копіюванню даних із керованої програми в некеровану програму). Ви створюєте одну політику для кожної платформи (iOS, Android);

після створення політик захисту додатків забезпечується їх виконання, створюючи правило умовного доступу в Azure AD, щоб вимагати схвалених додатків і захисту даних APP.

Політики захисту APP містять багато налаштувань. На щастя, вам не потрібно вивчати кожне налаштування та зважувати варіанти. Корпорація Microsoft спрощує застосування конфігурації параметрів, рекомендуючи початкові точки. Структура захисту даних із використанням політик захисту програм включає три рівні, які ви можете вибрати.

7. Необхідно налаштувати MFA та умовний доступ для гостей, включаючи захист мобільних додатків Intune.

Далі необхідно переконатися, що ви можете продовжувати співпрацювати та працювати з гостями. Якщо ви використовуєте план Microsoft 365 E3 і впровадили MFA для всіх користувачів, усе готово.

Якщо ви використовуєте план Microsoft 365 E5 і користуєтеся перевагами Azure Identity Protection для MFA на основі ризиків, вам потрібно внести кілька змін (оскільки захист Azure AD Identity не поширюється на гостей):

створіть нове правило умовного доступу, щоб завжди вимагати MFA для гостей і зовнішніх користувачів;

оновіть правило умовного доступу MFA на основі ризиків, щоб виключити гостей і зовнішніх користувачів;

скористайтеся вказівками, щоб дозволити та захистити гостьовий і зовнішній доступ, щоб зрозуміти, як гостьовий доступ працює з Azure AD, і

оновити відповідні політики.

Політики захисту мобільних програм Intune, які були створені, разом із правилом умовного доступу, що вимагає схвалених додатків і захисту APP, застосовуються до облікових записів гостей і допоможуть захистити дані організації.

Якщо ви вже зареєстрували ПК у системі керування пристроями, щоб вимагати сумісних ПК, вам також потрібно буде виключити гостьові облікові записи з правила умовного доступу, яке забезпечує відповідність пристрою.

8. Необхідно зареєструвати ПК у програмі керування пристроями та вимагайте сумісних ПК.

Є кілька способів зареєструвати пристрої ваших співробітників. Кожен метод залежить від власника пристрою (особистого чи корпоративного), типу пристрою (iOS, Windows, Android) і вимог до керування (скидання, зв'язок, блокування). Найшвидший спосіб розпочати – налаштувати автоматичну реєстрацію для пристроїв Windows 10 .

Необхідно визначити політику відповідності пристрою – рекомендовані параметри для Windows 10 включають обов'язковий антивірусний захист. Якщо у вас є Microsoft 365 E5, використовуйте Microsoft Defender for Endpoint, щоб контролювати справність пристроїв співробітників. Переконайтеся, що політики відповідності для інших операційних систем включають антивірусний захист і програмне забезпечення для захисту кінцевих точок.

Вимагати сумісних ПК – це правило умовного доступу в Azure AD, яке забезпечує виконання політик відповідності пристроїв.

Тільки одна організація може керувати пристроєм, тому обов'язково виключіть гостьові облікові записи з правила умовного доступу в Azure AD. Якщо ви не виключаєте гостьових і зовнішніх користувачів із політик, які вимагають відповідності пристрою, ці політики блокуватимуть цих користувачів.

9. Необхідно оптимізувати мережу для підключення до хмари.

Якщо ви швидко дозволяєте більшості своїх співробітників працювати з дому, це раптове перемикання моделей підключення може мати значний вплив на

інфраструктуру корпоративної мережі. Багато мереж було масштабовано та розроблено до впровадження хмарних служб. У багатьох випадках мережі толерантні до віддалених працівників, але не розроблені для віддаленого використання всіма користувачами одночасно.

Мережеві елементи, такі як концентратори VPN, центральне мережеве вихідне обладнання (таке як проксі-сервери та пристрої запобігання втраті даних), центральна пропускна здатність Інтернету, зворотні канали MPLS, можливості NAT тощо раптово зазнають величезного навантаження через навантаження всього бізнесу, що використовує їх. Кінцевим результатом є низька продуктивність і продуктивність у поєднанні з поганим користуванням для користувачів, які адаптуються до роботи вдома.

Деякі засоби захисту, які традиційно забезпечуються маршрутизацією трафіку через корпоративну мережу, забезпечуються хмарними додатками, до яких мають доступ користувачі.

10. Необхідно навчити користувачів.

Навчання користувачів може заощадити вашим користувачам і групі безпеки багато часу та розчарування. Кмітливі користувачі рідше відкривають вкладення або клацають посилання в сумнівних повідомленнях електронної пошти, а також уникають підозрілих веб-сайтів.

11: Почніть роботу з Microsoft Defender для хмарних додатків.

Microsoft Defender для хмарних додатків забезпечує широку видимість, контроль над переміщенням даних і складну аналітику для виявлення та боротьби з кіберзагрозами в усіх хмарних службах організації. Коли ви починаєте працювати з Defender for Cloud Apps, політики виявлення аномалій вмикаються автоматично, але Defender for Cloud Apps має початковий період навчання тривалістю сім днів, протягом якого надсилаються не всі сповіщення про виявлення аномалій.

12. Необхідно відстежувати загрози та вживайте заходів.

Microsoft 365 містить кілька способів відстеження стану та виконання відповідних дій. Вашою найкращою відправною точкою є портал Microsoft 365

Defender, де ви можете переглядати рейтинг Microsoft Secure Score організації та будь-які сповіщення чи сутності, які потребують вашої уваги.

3.2. Порядок втілення політики ідентифікації нульової довіри та доступу до пристрою в Microsoft 365

Розглянемо загальну рекомендовану політику ідентифікації нульової довіри та доступу до пристрою для захисту доступу до хмарних служб Microsoft 365, включаючи локальні програми, опубліковані за допомогою проксі-сервера додатків Azure AD.

Налаштування цих політик в окремому лабораторному середовищі дає змогу зрозуміти й оцінити рекомендовані політики перед початком розгортання у попередньому та робочому середовищах. Створене середовище може бути лише хмарним або гібридним відповідно до потреб.

На рисунку 3.3. показано рекомендований набір політик. Він показує, до якого рівня захисту застосовується кожна політика та чи застосовуються політики до ПК, телефонів і планшетів чи обох категорій пристроїв. Він також вказує, де налаштовуються ці політики.

Перед реєстрацією пристроїв в Intune рекомендується вимагати використання багатофакторної автентифікації (MFA), щоб переконатися, що пристрій перебуває у володінні призначеного користувача. Адміністратор повинен зареєструвати пристрої в Intune, перш ніж застосовувати політики відповідності пристроїв.

Рекомендується реалізувати нижченаведені початкові політики в указаному порядку. Однак політики MFA для корпоративних і спеціалізованих рівнів безпеки можна запровадити в будь-який час.

Політика: вимагати MFA на основі ризику входу.

Ви повинні зареєструвати своїх користувачів у MFA, перш ніж вимагати його використання. Якщо у вас є Microsoft 365 E5, Microsoft 365 E3 з надбудовою безпеки E5, Office 365 з EMS E5 або окремі ліцензії Azure AD Premium P2, ви

можете використовувати політику реєстрації MFA з Azure AD Identity Protection, щоб вимагати від користувачів реєстрації для МЗС. Попередня робота включає реєстрацію всіх користувачів у MFA.

Після реєстрації користувачів ви можете вимагати MFA для входу за допомогою нової політики умовного доступу.

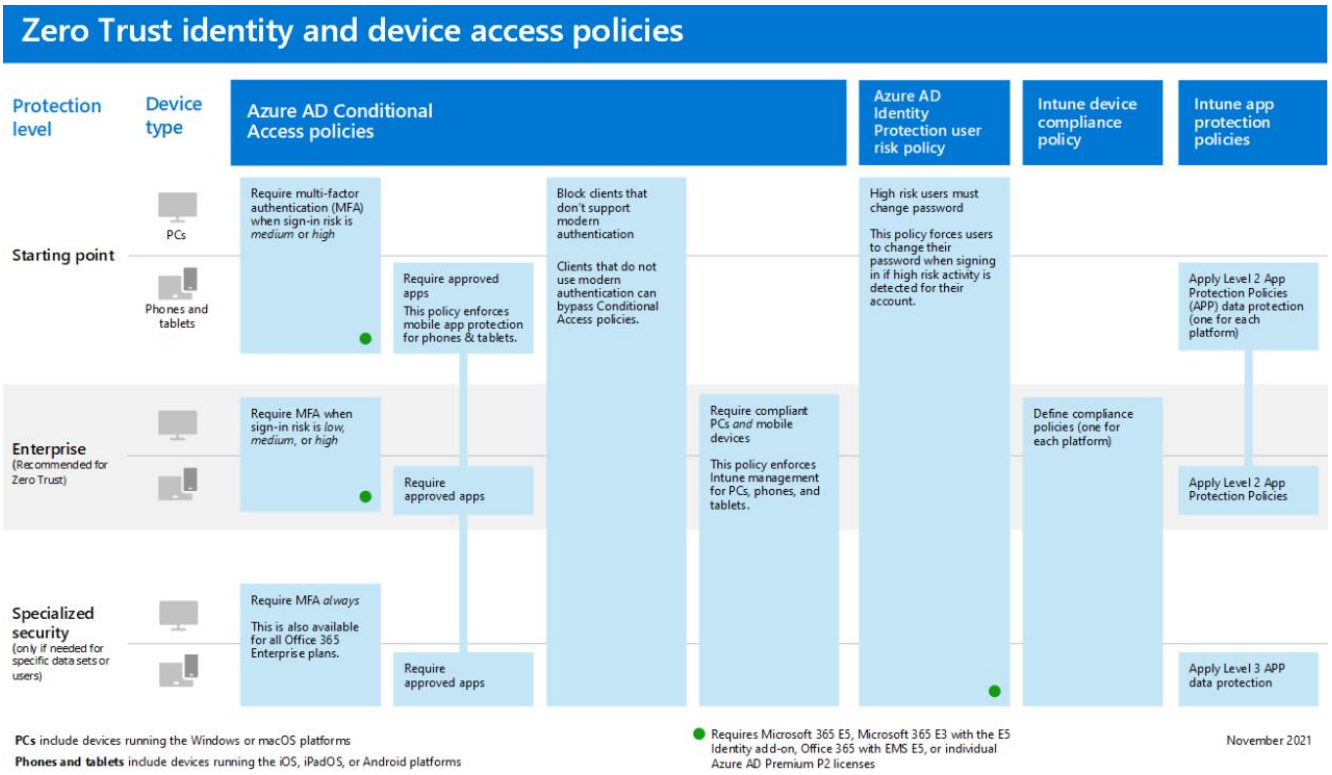

Рис. 3.3. Перелік політик захисту та місця їх налаштування [16]

Політика: блокувати клієнтів, які не підтримують MFA.

Клієнти, які не використовують сучасну автентифікацію, можуть обійти політики умовного доступу, тому їх важливо заблокувати. Використовуйте налаштування для політики умовного доступу, щоб блокувати клієнтів, які не підтримують багатофакторну автентифікацію.

Політика: користувачі з високим ризиком повинні змінити пароль.

Щоб гарантувати, що всі скомпрометовані облікові записи користувачів із високим ризиком змушені будуть змінювати пароль під час входу, ви повинні застосувати дану політику. Змушує користувачів змінювати пароль під час входу, якщо для їх облікового запису виявлено активність із високим рівнем ризику.

Політика: застосування політики захисту даних Application Protection Policies (APP).

APP визначає, які додатки дозволені та дії, які вони можуть виконувати з даними організації. Варіанти, доступні в APP, дозволяють організаціям адаптувати захист до своїх конкретних потреб. Для деяких може бути неочевидним, які параметри політики потрібні для реалізації повного сценарію. Щоб допомогти організаціям визначити пріоритетність захисту кінцевих точок мобільних клієнтів, Microsoft запровадила таксономію для своєї системи захисту даних APP для керування мобільними додатками iOS та Android.

Структура захисту даних APP організована в три окремі рівні конфігурації, причому кожен рівень будується на основі попереднього рівня [16]:

рівень 1: корпоративний базовий захист даних гарантує, що додатки захищені PIN-кодом і зашифровані, а також виконує вибіркові операції стирання. Для пристроїв Android цей рівень підтверджує атестацію пристрою Android. Це конфігурація початкового рівня, яка забезпечує аналогічний контроль захисту даних у політиках поштових скриньок Exchange Online і представляє IT-спеціалістів і користувачів APP;

рівень 2: розширений захист корпоративних даних включає механізми запобігання витоку даних APP і мінімальні вимоги до ОС. Це конфігурація, яка застосовна до більшості мобільних користувачів, які мають доступ до робочих або навчальних даних;

рівень 3: Високий рівень захисту корпоративних даних включає розширені механізми захисту даних, розширену конфігурацію PIN-коду та захист від загроз APP Mobile. Ця конфігурація бажана для користувачів, які мають доступ до даних високого ризику.

Політика: вимагати схвалених додатків і захисту APP.

Щоб застосувати політики захисту додатків, які ви застосували в Intune, ви повинні створити політику умовного доступу, щоб вимагати схвалених клієнтських додатків і умов, установлених у політиках захисту APP.

Політика: визначати політику відповідності кожному пристрою.

Політика відповідності пристроїв визначає вимоги, яким мають відповідати пристрої, щоб вважатися сумісними. Ви створюєте політики відповідності пристрою Intune у центрі адміністрування Microsoft Endpoint Manager.

Ви повинні створити політику для кожної платформи ПК, телефону чи планшета.

Політика: вимагати MFA на основі ризику входу.

Ви повинні зареєструвати своїх користувачів у MFA, перш ніж вимагати його використання. Якщо у вас є Microsoft 365 E5, Microsoft 365 E3 з надбудовою безпеки E5, Office 365 з EMS E5 або окремі ліцензії Azure AD Premium P2, ви можете використовувати політику реєстрації MFA з Azure AD Identity Protection, щоб вимагати від користувачів реєстрації для МЗС. Попередня робота включає реєстрацію всіх користувачів у MFA.

Політика: призначення політик групам і користувачам.

Перш ніж налаштовувати політики, визначте групи Azure AD, які ви використовуєте для кожного рівня захисту. Як правило, захист початкової точки стосується всіх в організації. До користувача, який включено як для початкової точки, так і для захисту підприємства, застосовуватимуться всі політики початкової точки, а також корпоративні політики. Захист є накопичувальним, і застосовується найсуворіша політика.

3.3. Рекомендації щодо застосування технології захисту інформаційних ресурсів організації при гібридній роботі користувачів

За результатами дослідження Accenture [17] повідомляється, що 83% із 9326 опитаних працівників сказали, що віддають перевагу гібридній моделі та гібридна робота має стати новим способом життя для мільйонів працівників по всій країні.

Незважаючи на те, що гібридна робота створює різноманітні можливості та переваги як для працівників, так і для роботодавців, *гібридна модель роботи викликає питання щодо вразливості безпеки даних*. Постійна передача конфіденційних даних між домом і офісом може поставити компанії під загрозу

через постійні проблеми, такі як незахищені приватні мережі або людські помилки.

Пропонуємо рекомендації щодо покращення захисту інформаційних ресурсів організації при гібридній роботі користувачів, щоб мінімізувати ризик витоку даних.

Зберігайте надійну резервну копію конфіденційної інформації.

Необхідно регулярно створювати надійні резервні копії всіх важливих файлів. Резервне копіювання цінних даних на зашифрований USB-накопичувач із автентифікацією PIN-кодом або жорсткий диск/SSD може позбавити підприємства від проблем із втратою доступу до важливої інформації під час атаки програм-вимагачів. Варто відзначити важливість того, щоб увесь персонал, особливо той, хто працює віддалено, мав безпечне з'єднання Wi-Fi і перевіряв, чи все програмне забезпечення безпеки оновлено, щоб уникнути такої атаки.

Важливо використовувати зашифрований диск для резервного копіювання даних. Для максимального захисту вибраний диск бажано мати на пристрої крипточіп, який пропонує найвищий стандарт шифрування, відомий як 256-бітне апаратне шифрування AES-XTS. У результаті, якщо зашифрований пристрій, наприклад флеш-накопичувач USB або жорсткий диск, буде втрачено або викрадено, це не призведе до порушення даних для розкриття даних клієнта або компанії.

Зашифрований флеш-накопичувач USB або жорсткий диск/SSD має додатково включати додатковий рівень безпеки, такий як Common Criteria EAL 5+ (Hardware Certified), який використовує вбудовані механізми фізичного захисту, призначені для запобігання низці кібератак, такі як атаки по бічному каналу.

Безпечно транспортуйте файли.

Безпечно носіть роботу з собою додому, використовуючи захищений PIN-кодом, зашифрований флеш-накопичувач USB або жорсткий диск/SSD. У найгіршому випадку, коли диск буде втрачено або викрадено, коли співробітники транспортують файли або працюють поза офісом, зашифрований диск, як описано вище, дозволить організаціям уникнути ризику доступу або перегляду їхніх

даних.

Крім того, якщо доступ до дисків доступний лише за допомогою введення унікального 7-15-значного PIN-коду, це запобігає несанкціонованому доступу до даних, що зберігаються на диску. Ще одна особливість, яку варто враховувати, це обмеження атак грубої сили. Якщо PIN-код введено неправильно визначену кількість разів, усі дані, які раніше зберігалися на накопичувачі, буде видалено, а накопичувач буде скинуто.

Коли живлення USB-порту вимикається, або якщо накопичувач від'єднано від головного пристрою, або після попередньо визначеного періоду бездіяльності, накопичувач має автоматично заблокуватися, щоб запобігти несанкціонованому доступу. Використання диска, який також можна налаштувати лише для читання (захист від запису), забезпечить відсутність незаконної зміни даних.

Шифруйте дані, що зберігаються в хмарі.

Хмара часто є кращим варіантом для гібридної роботи. Однак безпека в хмарі є загальною проблемою, тобто більшість компаній не будуть зберігати будь-яку конфіденційну інформацію в хмарі.

Щоб забезпечити конфіденційність даних під час зіткнення зі звичайними загрозами, такими як DDoS-атаки та атаки зловмисного програмного забезпечення, дані мають бути зашифровані під час передавання та зберігання. Шифрування даних робить збережені та передані дані нечитабельними та непридатними для використання у разі крадіжки або ненавмисного витоку даних.

Шифрування не може залежати від постачальника хмарних послуг (CSP). За допомогою шифрування на стороні сервера ключ шифрування зберігається в хмарі, тому він доступний для хакерів і персоналу хмари. Тому для організацій найкраще індивідуально шифрувати дані, що зберігаються в загальнодоступній хмарі. Користувачеві потрібен повний і безпечний контроль над ключем шифрування, щоб гарантувати конфіденційність даних, навіть якщо хмарний обліковий запис зламано. Наявність власної системи керування ключами не тільки дасть вам більше контролю над ключами шифрування, але й стане зручнішим для тих, хто використовує багатохмарне рішення.

Ідеальним рішенням для контролю ключа шифрування є буквальне видалення його з хмари та фізичне збереження зашифрованого ключа шифрування в USB-модулі з PIN-кодом. Модуль не зберігатиме жодних даних. Швидше, він діятиме як ключ для шифрування даних і доступу до будь-яких даних у хмарі. Таким чином, його можна використовувати для надійного шифрування конфіденційної інформації, що зберігається на локальному комп'ютері чи мережевому диску, надсилається електронною поштою чи за допомогою служби обміну файлами.

Необхідно забезпечити авторизований доступ до даних.

За допомогою спеціального програмного забезпечення, можна скопіювати всі критичні параметри безпеки між основним модулем шифрування та будь-якою кількістю вторинних модулів шифрування, у тому числі випадково згенерований ключ шифрування та всі PIN-коди. Лише ті, у кого є копія ключа шифрування, зможуть розшифрувати спільні дані. Це забезпечує безпечну та миттєву співпрацю в хмарі між авторизованими користувачами, незалежно від місця розташування.

Компанії потребують чіткої процедури, якої дотримується весь персонал, щоб підтримувати дотримання правил захисту даних, тим більше це стосується зростання кількості віддалених працівників. Багатофакторна автентифікація є настійно рекомендованою найкращою практикою для відповідності захисту даних. Якщо хакер отримає облікові дані користувача хмари, злам залишиться непоміченим для CSP, оскільки він не зможе розшифрувати між законним користувачем і зловмисником. З іншого боку, модуль шифрування посилює заходи безпеки до безпрецедентної п'ятифакторної автентифікації, оскільки ключ шифрування зберігається подалі від хмари.

Необхідно віддалено керувати доступом до даних.

Передача уповноваженому персоналу модуля шифрування сприятиме зниженню ризику втрати даних через людську помилку. Однак це не виключає повністю можливість такого явища. Наприклад, особа може втратити модуль шифрування або бути звільненою та зберегти пристрій. Тут потрібне

централізоване управління.

Ті, хто відповідає за безпеку хмари та даних в організації, повинні мати можливість відстежувати активність файлів, встановлювати обмеження на геозонування та час, шифрувати імена файлів і віддалено вимикати доступ користувачів до даних. Це значною мірою допоможе усунути ризики безпеки в хмарі та допоможе менеджерам мати повну видимість та адміністрування конфіденційних даних і доступу користувачів

Ці заходи будуть сприяти підтримці безперервності бізнесу, дотриманню правил захисту даних і усуненню будь-якої складності віддаленої роботи.

ВИСНОВКИ

В роботі досліджено проблему управління доступом користувачів до віртуальних машин організації при застосуванні хмарних платформ, визначено його мету та завдання.

Досліджено проблему захисту інформаційних ресурсів організації при гібридній роботі користувачів. Гібридне робоче місце забезпечує гнучку та безперебійну співпрацю з будь-якого місця. Успіх застосування гібридної моделі роботи користувачів залежить від безпеки.

Нульова довіра – це комплексний підхід до забезпечення повного доступу до корпоративних мереж, додатків і середовищ від будь-якого користувача, пристрою та місця.

Проаналізовано підходи до захисту інформаційних ресурсів організації при гібридній роботі користувачів. Гібридна робота полягає в тому, щоб залишити виділену мережу компанії та отримати доступ до ресурсів через загальнодоступні та домашні мережі, які несуть серйозні загрози безпеці. Тому, потрібно забезпечити безпеку гібридної моделі роботи на кожній кінцевій точці, навчаючи користувачів безпечним методам і потенційним ризикам.

Проаналізовано існуючі рішення щодо захисту інформаційних ресурсів організації при гібридній роботі користувачів. SASE – це модель хмарної архітектури, яка поєднує функції мережі та безпеки як послуги разом і надає їх як єдину хмарну службу SASE дозволяє працювати будь-де та віддаленим працівникам, користуватися перевагами брандмауера як послуги (FWaaS), захищеного веб-шлюзу (SWG), доступу до мережі з нульовою довірою (ZTNA) і набором функцій виявлення загроз.

Рішення Microsoft 365 створено з багатьма можливостями безпеки та захисту інформації, щоб допомогти організаціям створити Zero Trust у своєму середовищі. Багато можливостей можна розширити, щоб захистити доступ до інших додатків SaaS, які використовує організація, і даних у цих додатках.

Розглянуто призначення та основні функції інфраструктури для гібридної роботи користувачів з Microsoft 365, а також порядок забезпечення безпеки інформаційних ресурсів організації при гібридній роботі користувачів.

Розглянуто порядок підтримки гібридної роботи користувачів. Для того, щоб захистити й оптимізувати доступ до серверів і хмарних сервісів організації та максимально підвищити продуктивність гібридної роботи працівників, необхідно дотримуватися даного порядку.

Визначено пріоритети завдань, щоб допомогти фахівцям з безпеки якнайшвидше реалізувати найважливіші можливості безпеки для підтримки гібридної роботи користувачів.

Розглянуто порядок втілення політики ідентифікації нульової довіри та доступу до пристрою в Microsoft 365. Втілення даних політик забезпечить захист доступу до хмарних служб Microsoft 365, включаючи локальні додатки, опубліковані за допомогою проксі-сервера додатків Azure AD.

Запропоновано рекомендації фахівцям з кібербезпеки щодо застосування технології захисту інформаційних ресурсів організації при гібридній роботі користувачів.

Таким чином, правильна реалізація захисту інформаційних ресурсів організації при гібридній роботі користувачів має забезпечити конфіденційність, цілісність та доступність корпоративних даних та кібербезпеку інформаційної системи організації в цілому.

ПЕРЕЛІК ПОСИЛАНЬ

1. Нова модель роботи: як захистити гібридне робоче місце. ESET, 13.08.2021. [Електронний ресурс] – Режим доступу: https://eset.ua/ua/blog/view/121/novaya-model-raboty-kak-zashchitit-gibridnoye-rabocheye-mesto.

2. Set up your infrastructure for hybrid work with Microsoft 365. Article 23/09/2022. Microsoft. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-gb/microsoft-365/solutions/empower-people-to-work-remotely?view=o365-worldwide.

3. Embracing the hybrid workplace. Your guide to the new era of work. Webex by Cisco. May 2021. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/dam/en/us/solutions/collateral/collaboration/embracing-the-hybrid-workplace.pdf.

4. What Is Hybrid Work? Cisco. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-hybrid-work.html.

5. Hybrid work security: challenges & best practices. NordLayer, 18 Jan 2022. [Електронний ресурс] – Режим доступу: https://nordlayer.com/blog/hybrid-work-security-challenges-and-best-practices/.

6. Five tips to keep your hybrid workforce secure. Cisco. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/m/en_us/solutions/security/secure-hybrid-work-solution/five-tips.html.

7. The State of Security in a Hybrid Work Environment. [Електронний ресурс] – Режим доступу: https://www.citrix.com/content/dam/citrix/en_us/documents/analyst-report/the-state-of-security-in-a-hybrid-work-environment.pdf.

8. Secure Access Service Edge (SASE). Fortinet. [Електронний ресурс] – Режим доступу: https://www.fortinet.com/resources/cyberglossary/sase.

9. Universal Zero Trust Network Access (ZTNA). Fortinet. [Електронний ресурс] – Режим доступу: https://www.fortinet.com/solutions/enterprise-midsize-

business/network-access/application-access.

10. BYOD platform overview. IBM. [Електронний ресурс] – Режим доступу: https://www.ibm.com/products/maas360/byod.

11. Cloud VPN. NordLayer. [Електронний ресурс] – Режим доступу: https://nordlayer.com/cloud-vpn.

12. Задоволення основних потреб офісу на найвищому рівні. Konica Minolta. [Електронний ресурс] – Режим доступу: https://www.konicaminolta.ua/uk-ua/software/it-services/microsoft-365.

13. Zero Trust deployment plan with Microsoft 365. Article 11/02/2022. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/microsoft-365/security/microsoft-365-zero-trust?view=o365-worldwide.

14. Set up your infrastructure for hybrid work with Microsoft 365. Article 09/23/2022. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/microsoft-365/solutions/empower-people-to-work-remotely?view=o365-worldwide.

15. Top 12 tasks for security teams to support working from home. Article 09/28/2022. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/microsoft-365/security/top-security-tasks-for-remote-work?view=o365-worldwide.

16. Common Zero Trust identity and device access policies. Article 10/20/2022. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/identity-access-policies?view=o365-worldwide.

17. 5 Tips for protecting your data when hybrid working. [Електронний ресурс] – Режим доступу: https://istorage-uk.com/hyrbid-working-5-tips-to-protect-your-data/

18. Татаренко В. О. Технологія захисту інформаційних ресурсів організації при гібридній роботі користувачів у Microsoft 365. Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». Державний Університет Телекомунікацій. 27 жовтня 2022. Тези доповідей. С. 29-31. [Електронний ресурс] – Режим доступу: https://dut.edu.ua/uploads/p_2121_20358827.pdf

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)