ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«Технологія забезпечення захищеного доступу до хмарних сервісів на базі рішення Microsoft Cloud App Security»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Осьмак Д.П.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2020

РЕФЕРАТ

Текстова частина магістерської роботи: 61 сторінка, 15рисунків, 12 джерел.

Об'єкт дослідження – процес забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи.

Предмет дослідження – технологія забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи.

Мета роботи – розробити варіант технології забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи та рекомендації щодо застосування технології на підприємстві.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи.

В роботі проведено аналіз для забезпечення кібербезпеки корпоративної інформаційної системи при використанні доступу до хмарних сервісів та визначено мета та завдання. Визначено основні проблеми щодо забезпечення доступу до хмарних сервісів.

Досліджено методи та засоби забезпечення доступу до хмарних сервісів на прикладі рішення Microsoft Cloud App Security. Визначено призначення, основні функції та принципи роботи рішення Microsoft Cloud App Security.

На основі досліджень проведених в роботі розроблено варіант технології забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи та рекомендації щодо застосування даної технології на підприємстві.

Галузь використання – кібербезпека корпоративної інформаційної системи.

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, ЗАХИСТ ДОСТУПУ, ХМАРНИЙ СЕРВІС, МЕТОДИ ТА ЗАСОБИ CASB, ТЕХНОЛОГІЯ ЗАХИЩЕНОГО ДОСТУПУ

ЗМІСТ

ВСТУП

Актуальність дослідження. Брокер безпеки хмарного доступу (CASB) - це локальне або хмарне програмне забезпечення, яке знаходиться між споживачем хмарних послуг і постачальником хмарних послуг. Він служить інструментом для забезпечення дотримання політик безпеки організації за допомогою виявлення ризиків і дотримання нормативних вимог при кожному доступі до хмарних даних.

Додатки «Інфраструктура як послуга» (IaaS) і «Безпека як послуга» (SaaS) дуже гнучкі і економічні, що робить їх особливо привабливими для організацій, проте в процесі відстеження та адміністрування таких програм можуть виникнути труднощі. CASB - це посередницька служба хмарної безпеки (CASB), розроблена з метою відстеження, забезпечення відповідності вимогам, захисту даних і протидії загрозам для хмарних служб корпоративних інформаційних систем.

Перехід в хмару збільшує гнучкість як для співробітників, так і для IT-відділу. Однак це також створює нові проблеми і складнощі для забезпечення безпеки корпоративної інформаційної системи. Щоб отримати всі переваги хмарних додатків і послуг, IT-команда повинна знайти правильний баланс підтримки доступу при збереженні контролю для захисту критично важливих даних.

Microsoft Cloud App Security - це брокер безпеки хмарного доступу (CASB), який підтримує різні режими розгортання, включаючи збір журналів, з'єднувачі API і зворотний проксі. Він забезпечує широку видимість, контроль над переміщенням даних і складну аналітику для виявлення і боротьби з кіберзагрозами у всіх хмарних сервісах різних виробників.

Вищенаведені аргументи актуалізують дослідження щодо забезпечення кібербезпеки корпоративної інформаційної системи при використанні доступу до хмарних сервісів Microsoft Cloud App Security.

Об’єкт дослідження – процес забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи.

Предмет дослідження – технологія забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи.

Мета роботи – розробити варіант забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи та рекомендації щодо застосування технології на підприємстві.

Наукові завдання:

дослідити сутність проблеми забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи;

встановити основні вимоги щодо забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи;

проаналізувати забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи;

проаналізувати методи та засоби забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи;

Розробити технологію забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи.

Методи дослідження –опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи.

Практичне значення одержаних результатів полягає в розробці технології забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи на базі рішення Microsoft Cloud App Security, а також у розробці рекомендацій щодо застосування технології забезпечення захисту хмарних сервісів корпоративної інформаційної системи.

Апробація результатів

Осьмак Д.П. Технологія забезпечення захисту хмарних сервісів на базі рішення Microsoft Cloud App security [Електронний ресурс]. - Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки».- Київ, ДУТ.- с. 129-132[режим доступу:http://www.dut.edu.ua/uploads/p_1739_27992763.pdf]

1 АНАЛІЗ ЗАБЕЗПЕЧЕННЯ ХМАРНИХ СЕРВІСІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ПІДПРИЄМСТВА

1.1. Аналіз хмарних сервісів, які використовують підприємства

1.1.1. Хмарні сервіси та переваги їх використання

Хмарні сервіси - це IT-сервіси, які компанія надає користувачам ззовні. Найяскравішим прикладом хмарного сервісу, існуючим вже більше 10 років, є хостинг web-сайтів або електронної пошти. Поняття хмарні обчислення з'явилося відносно недавно і розширило поняття хостингу. Зараз під хмарними обчисленнями мається на увазі використання обчислювальних ресурсів віддаленого програмно-апаратного майданчика постачальника хмарних сервісів. Такими сервісами можуть бути віртуальні сервери, сервери електронної пошти, IP-телефонія, вилучені сервери терміналів і т.д. [12]

Використання хмарних сервісів надає ряд переваг власникам компаній.

Мінімальні початкові витрати. При використанні власної IT-інфраструктури, компанії для побудови власної інформаційної системи або для впровадження нового сервісу, необхідно придбати дороге устаткування і програмне забезпечення з урахуванням майбутнього зростання компанії, підготувати місце для цього обладнання, забезпечити його електроживленням і системами охолодження, потім провести розгортання програмного забезпечення , налагодити його працездатність, тощо. Для введення нових сервісів для всього комплексу необхідно залучити висококваліфікованих фахівців. Таким чином, все це вимагає не тільки великі фінансові витрати, але і багато часу для побудови нової інфраструктури. [1]

Таким чином для того, щоб почати користуватися хмарними сервісами або впроваджувати додаткові достатньо укласти контракт з постачальником хмарних

сервісів і дуже швидко почати використовувати сервіси, необхідні для розвитку бізнесу компанії, за відповідну платню.

Висока доступність і надійність. Надійність і доступність інформаційної системи є одним з найбільш важливих факторів, що безпосередньо впливають на стійкість бізнесу компанії. При використанні своєї інфраструктури, компанії необхідно постійно підтримувати її надійність і збереження даних, які там зберігаються. Але високонадійна інфраструктура і кластерні технології дорого коштують для компанії. Але якщо навіть вкласти великі кошти в відмовостійкість інформаційної системи, компанія не буде застрахована від таких випадків, як пожежі, вилучення серверів з офісу компанії, перебоїв з електроживленням та інше. [1]

Інфраструктура для надання хмарних сервісів, яку буде використовувати компанія створена для забезпечення найвищого ступеня надійності та відмовостійкості. Все обладнання буде розміщуватися в захищених центрах обробки даних, де забезпечується безперебійне електроживлення, відмовостійкі системи кондиціонування та пожежогасіння. Всі сервери об'єднані в кластери і захищені від відмови обладнання. Центр обробки даних також буде забезпечено резервними Інтернет-каналами. Таким чином, використання хмарних сервісів, компанія отримує у користування високонадійну і захищену інформаційну систему з доступністю 24/7.

Відсутність експлуатаційних витрат. Власна інформаційна система компанії вимагає великих витрат на обслуговування і підтримку. Для обслуговування парку серверів потрібно штат кваліфікованих системних адміністраторів. Все обладнання та програмне забезпечення вимагає постійного моніторингу і вирішення різного роду проблем. Устаткування, як правило може виходити з ладу, що викликає додаткові витрати на ремонт і заміну комплектуючих. Крім того, один раз в 3-5 років потрібно оновлювати обладнання, і в свою чергу оновлення програмного забезпечення. Тобто, по суті необхідно знову поводити витрати на повторну побудову IT-інфраструктури. [1]

Купуючи хмарні технології у хмарного провайдера є можливість отримати необхідні для компанії IT-сервіси, не замислюючись про витрати на їх експлуатацію, оновлення та підтримку, тому що це проблема хмарного провайдера

Гнучкість IT-інфраструктури. Якщо у компанії виникла ситуація, коли терміново необхідно впровадити який-небудь новий сервіс, або нові обчислювальні потужності для існуючих сервісів. Як приклад, просто збільшився штат співробітників, стало недостатньо дискового простору, або обчислювальної потужності для 1С сервера бухгалтерії. Компанія буде змушена купувати нове обладнання, нові ліцензії на програмне забезпечення, потім розгортати і налаштовувати його, що може зайняти багато часу на встановлення та налаштування. Все це буде гальмувати бізнес-процеси компанії. [1]

У разі використання хмарних сервісів, ви просто купуєте додаткові потужності хмарного провайдера і через пару годин отримуєте нові обчислювальні ресурси або сервіси.

Інша ситуація може виникнути, коли компанія вирішила відкрити новий напрямок бізнесу і для цього необхідно ряд IT-сервісів, для забезпечення працездатності яких потрібно закупити обладнання та програмне забезпечення на велику суму і все це необхідно зробити в кредит. И якщо потім виникає ситуація (наприклад, фінансова криза), яка змушує компанію закрити цей напрямок бізнесу. Назад придбане обладнання і ПЗ у компанії вже ніхто не купить і гроші не повернуть, але доведеться продовжувати виплачувати кредит. У разі використання хмарних сервісів, оплата відбувається за ті сервіси, які вам необхідні, коли необхідність пропала, ви просто припиняєте контракт з постачальником хмарних послуг.

Мобільність. Звичайна серверна інфраструктура досить сильно прив'язана до місцезнаходження компанії. Особливо проблеми виникають при переїзді головного офісу. Все це вимагає перекладку кабельної комунікації, перевезенню всього обладнання, переукладання договорів з Інтернет-провайдерами, переналаштування служби в зв'язку зі зміною адресації і тощо. Здійснити таку процедуру без переривання

роботи сервісів практично неможливо. Все це викликає у роботі компанії простій не тільки у переїзді офісу, а і у всіх дочірніх філій, які використовують сервіси центрального офісу. [1].

Таким чином при використанні хмарних сервісів, компанія не залежить від свого офісу. Хмарні сервіси доступні звідусіль, де є доступ в Інтернет. Це дозволяє працювати з будь-якого офісу, з дому або з відрядження.

1.1.2. Кібербезпека використання хмарних сервісів

Перехід в хмару надає більш гнучкі можливості роботи співробітників компаній. До основних переваг на такі сервіси є велика кількість зручних інструментів, зменшення витратна IT-інфраструктуру. Більшість співробітників компаній все частіше використовують публічні хмарні сервіси для виконання своїх робочих завдань, але це відбувається без участі ІБ-департаментів і, відповідно, без проведення оцінки ризику використання цих сервісів, а також без урахування можливого їх впливу на дотримання внутрішніх політик ІБ і відповідності вимогам зовнішніх регуляторів. Така модель використання хмарних сервісів приводить до відповідних ризиків, що вимагає від ІБ департаментів знайти баланс між зручністю використання хмарних сервісів та забезпеченням кібербезпеки. Отже, незважаючи на цілий ряд переваг використання хмарних сервісів і перенесення даних в хмари створює для компаній проблему щодо забезпечення кібербезпеки в питанні керування великою кількістю пристроїв, які використовують співробітника для доступу в хмарні сервіси. [2].

До основних проблем кібербезпеки хмари можна віднести наступне:

- відсутність видимості контролю;
- тіньові IT;
- ймовірність випадкової публікації даних;
- навмисний виток даних;
- спотворення або втрата критичних даних;

- невідповідність вимогам регуляторів;
- присутність хмарних шкідливих програм;
- ймовірність розповсюдження шкідливого ПЗ на всю мережу

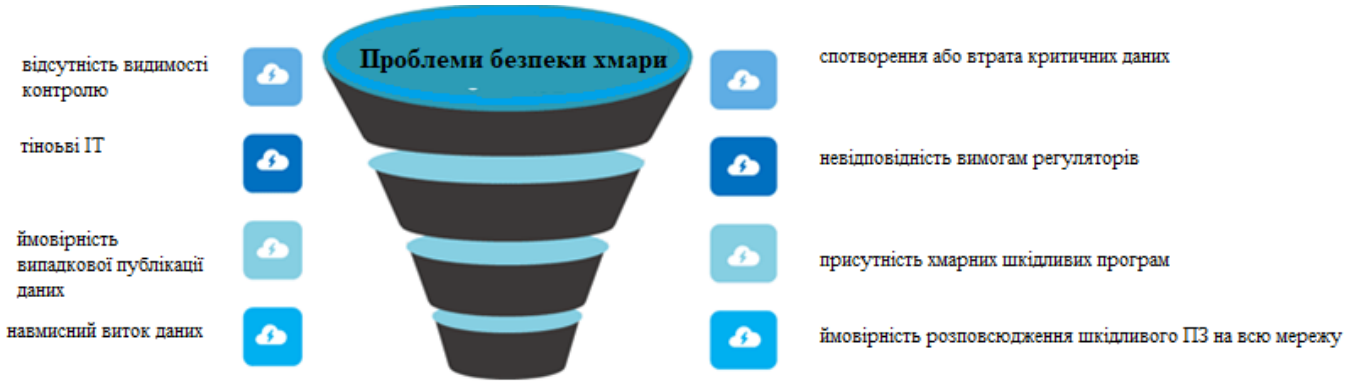

Рис 1.1. Проблеми безпеки хмари

На ринку все ще залишаються організації, які виключають ризики, які пов'язані з хмарними додатками / сервісами, і роблять це шляхом повного блокування їх використання. Але цей підхід не є ефективний і може мати негативний вплив використовувані бізнес-процеси сучасних організацій, наприклад, там, де співробітники компанії вже мали досвід використання в своїй роботі хмарних сервісів. Оскільки вже зараз, з економічною обстановкою в країні і світі більшість компаній все ж переводять свої робочі процеси в хмару і все частіше впроваджують до використання хмарні сервіси, виникає питання: які ж заходи забезпечення безпеки необхідно зробити, щоб безпечно користуватися хмарними сервісами і не боятися переносити корпоративні дані в хмари? Для вирішення питань щодо забезпечення кібербезпеки в хмарах і дотримання вимог внутрішніх служб інформаційної безпеки та зовнішніх регулюючих органів в частині роботи з хмарними даними на ринку пропонуються рішення класу Cloud Access Security Brokers (CASB) - брокер безпеки хмарного доступу. CASB є однією з нових, але швидко розвиваються технологій хмарної безпеки, які буде розглянуто в даній магістерській роботі.

1.2. Аналіз архітектури хмар

Модель хмарних обчислень - це тип сервісу, який надається користувачам. Перш ніж визначити, що спочатку пропонують користувачам хмарні обчислення, візначімо основи хмарних обчислень.

Хмарні обчислення - це доступність за запитом таких ресурсів, як обчислення, оперативна пам'ять і сховище, постачальником хмарних послуг (CSP) з централізованого центру обробки даних через підключення до Інтернету.

Існує чотири основних типи моделей розгортання, кожна зі своїми унікальними характеристиками, які пропонують різні переваги компаніям різного розміру і галузі. Залежно від моделі розгортання вони бувають (рис 1.2) [12]:

Private cloud - приватна хмара, призначене для використання однією організацією, може знаходиться як у власності цієї організаці, так і інший.

Public cloud - публічна хмара, призначена для вільного використання різними користувачами різних компаній.

Hybrid cloud - гібридне хмара представляє собою комбінацію з двох або більше різних хмарних інфраструктур (приватних, публічних або суспільних), що залишаються унікальними об'єктами, але пов'язаних між собою стандартизованими або приватними технологіями передачі даних і додатків.

Community cloud - суспільна або комунальна хмара, призначена для використання конкретною спільнотою споживачів з організацій, що мають спільні завдання (наприклад, вимог безпеки). Громадська хмара може перебувати в кооперативній (спільній) власності, управління та експлуатація однієї або більше з організацій спільноти або третьої сторони (або будь-якої їх комбінації).

Розглянемо кожний з цих типів моделей розгортання хмарних обчислень.

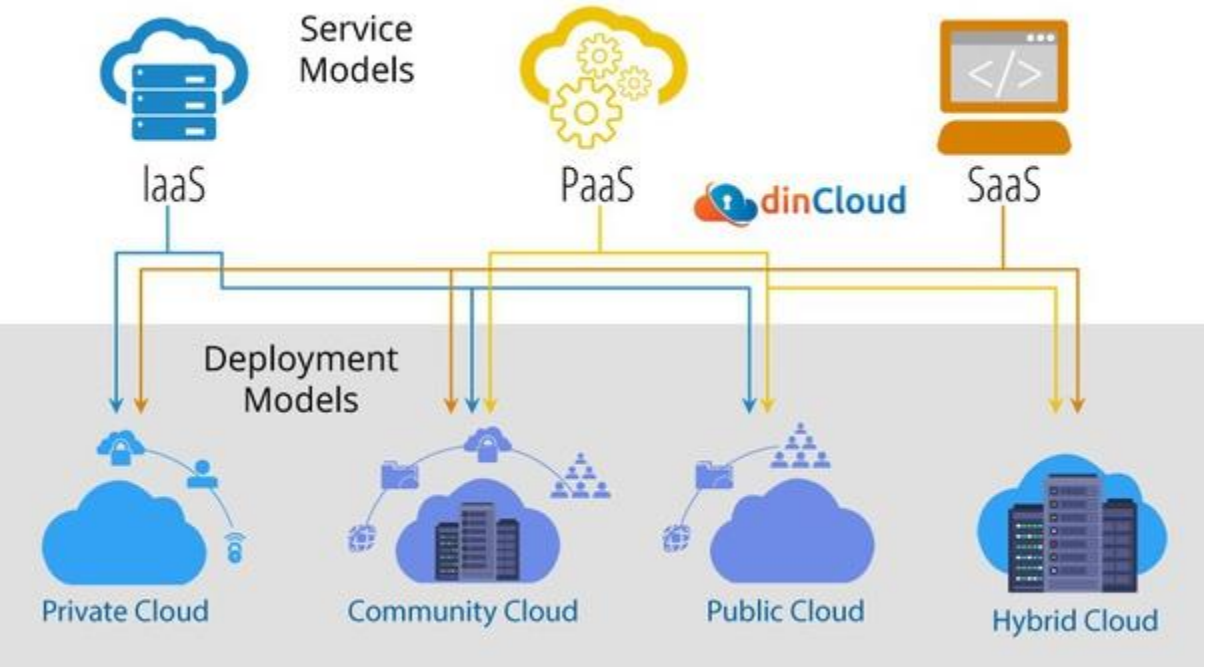

Рис. 1.2. Моделі розгортання

1.2.1 Характеристика приватної хмари

Приватна хмара обмежена окремою організацією, в якій IT-інфраструктура розміщується всередині приміщення. Виділені ресурси не використовуються спільно з іншими об'єктами, тому ми називаємо це приватним хмарою (Рис. 1.3). [3]

Характеристики приватної хмари:

1. *Безпека*: приватна хмара забезпечує кращу безпеку даних, оскільки IT-інфраструктура розгортається локально, що дає організації повний контроль над збереженням безпеки і іншими запобіжними заходами. Віна найкраще підходить для організацій, які працюють в сфері охорони здоров'я та інших галузях, де використовуються конфіденційні дані.

2. Початкові і масштабовані витрати: IT-інфраструктура, необхідна для розгортання приватної моделі, зазвичай перевищує очікувані витрати, виходить за рамки бюджету і стає дорогою. Якщо організація хоче розширити свої ресурси через зростаючі вимоги, це варіант який найбільше підходить, оскільки центр обробки даних та інше обладнання легко доступні на місці.

3. Доступність: несправність обладнання в віртуальних центрах обробки даних може бути досить складним завданням. Оскільки все IT-обладнання знаходиться в приміщенні, досвідчений IT-персонал завжди готовий вирішити цю проблему.

1.2.2 Характеристика публічної хмари

Public Cloud - це модель хмарних обчислень, яка пропонує спільне використання ресурсів, оскільки вона відображає структуру з кількома орендарями, аналогічно багатоповерховій квартирі, в якій орендарі оточені обмеженою кількістю життєвих і необхідних ресурсів (Рис. 1.3). [3]

Характеристики публічного хмари:

1. *Економія витрат*: IT-інфраструктура, що включає центри обробки даних та інше допоміжне обладнання, передається на аутсорсинг постачальнику хмарних послуг (CSP), що позбавляє організацію від авансових витрат. Навіть після розгортання тарифні плани приватного хмари є недорогими, що робить її дуже вигідною для малих і середніх організацій.

2. *Масштабованість*: Public Cloud пропонує масштабувати ваші ресурси з мінімальними витратами. При масштабуванні хмарний клієнт просто платить CSP додаткову плату за використання. Якщо ваші вимоги знижуються, ваша організація може легко зменшити масштаб ресурсів за кілька хвилин.

3. *Надійність*: публічна хмара досить надійна, тому що дані зберігаються в кількох центрах обробки даних. Це робить дані безпечними в разі стихійних лих або кібератак. Навіть якщо дані в одному місці стають недоступними, до них можна отримати доступ через альтернативний центр обробки даних CSP.3.

1.2.3 Характеристика гібридної хмари

Гібридна хмара - це модель хмарних обчислень, в якій організації одночасно використовують як публічну, так і приватну моделі. Це рішення застосовується, якщо будь-яка окрема хмара не відповідає всім вимогам. Вона найкраще підходить для

організацій, які працюють з величезною кількістю обчислювальних ресурсів, сховищ і особистої інформації, яка повинна бути у вищій мірі захищеною (Рис. 1.3). [3]

Характеристики гібридної хмари:

1. *Масштабованість*: ваша організація може вибрати тип ресурсів і масштабувати їх відповідно до необхідної специфікації. При таких організації роботи компанія будете зобов'язана платити тільки за ті ресурси, які використовує. Тут можна додати ЦП, ОЗУ і т. д. За додаткову плату.

2. *Краща безпека даних*: гібридна хмара пропонує кращу модель безпеки даних, оскільки обидві моделі вже пов'язані з основними функціями безпеки. Кожна організація приймає рішення зберігати свої дані або у власномій приватній хмарі, або в публічній хмарі.

3. *Гнучкість:* гібридна модель пропонує гнучкість у виборі типу ресурсів відповідно до унікальних потреб компанії. Вибір того, які хмарні моделі будуть використовуватис, повністю залежить від їх потреб.

1.2.4 Характеристика хмари спільноти

Хмара спільноти - це модель розгортання, в якій кілька організацій, які є частиною спільноти, спільно використовують ресурси хмарних обчислень (Рис. 1.3). Приклади включають університети, які проводять однакові дослідження, поліцейські центри в одному районі, області або регіоні.

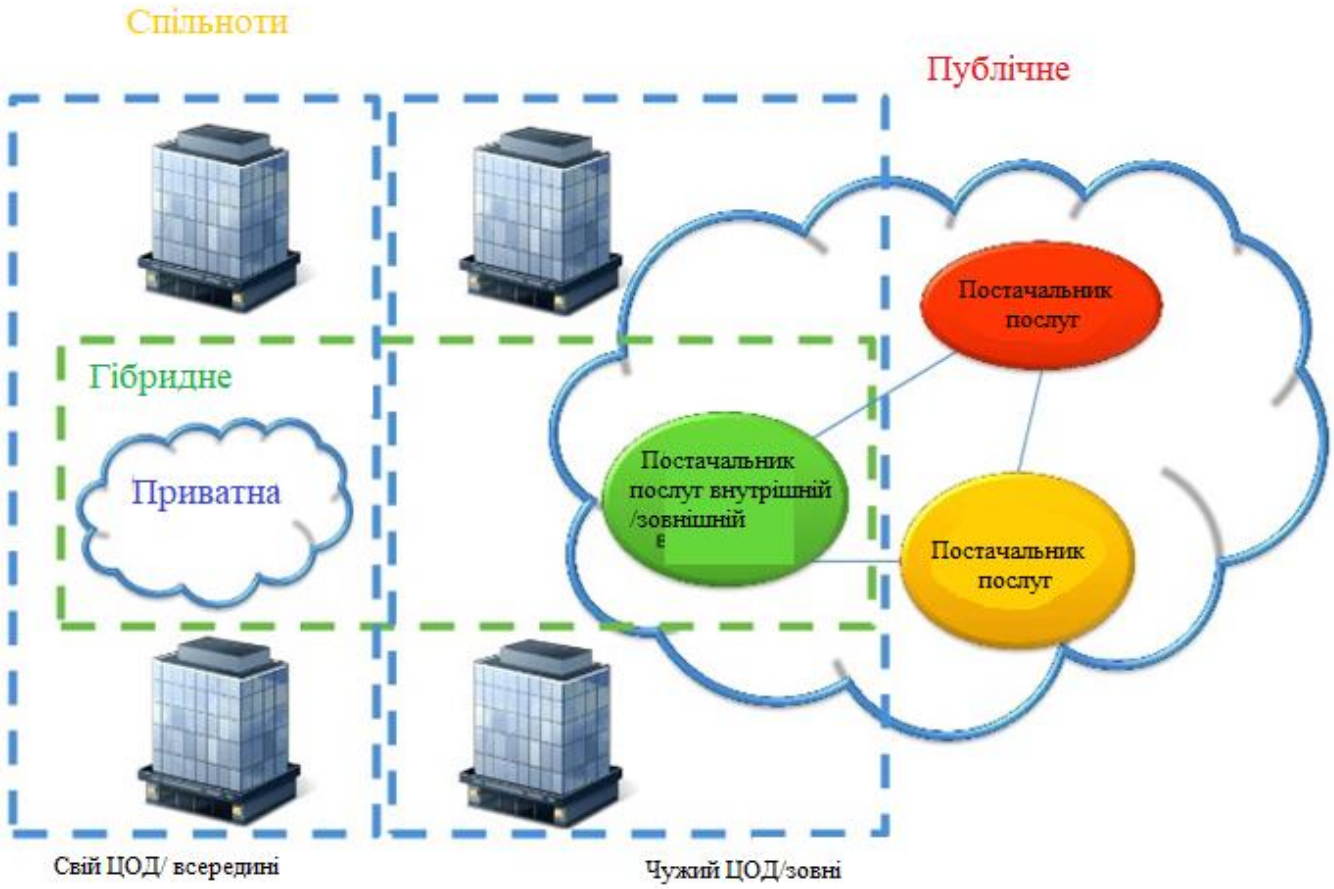

Рис. 1.3. Характеристика моделей

Залежно від моделі обслуговування хмарні обчислення поділяються на (Рис.1.4):

- SaaS - програма як послуга;
- PaaS - платформа як послуга;
- IaaS - інфраструктура як плуга

Рис.1.4. Моделі обслуговування хмар

Для кожної з моделі обслуговування хмари можна виділити рівні відповідальності клієнта та постачальника послуг, як це показано на рис.1.5.

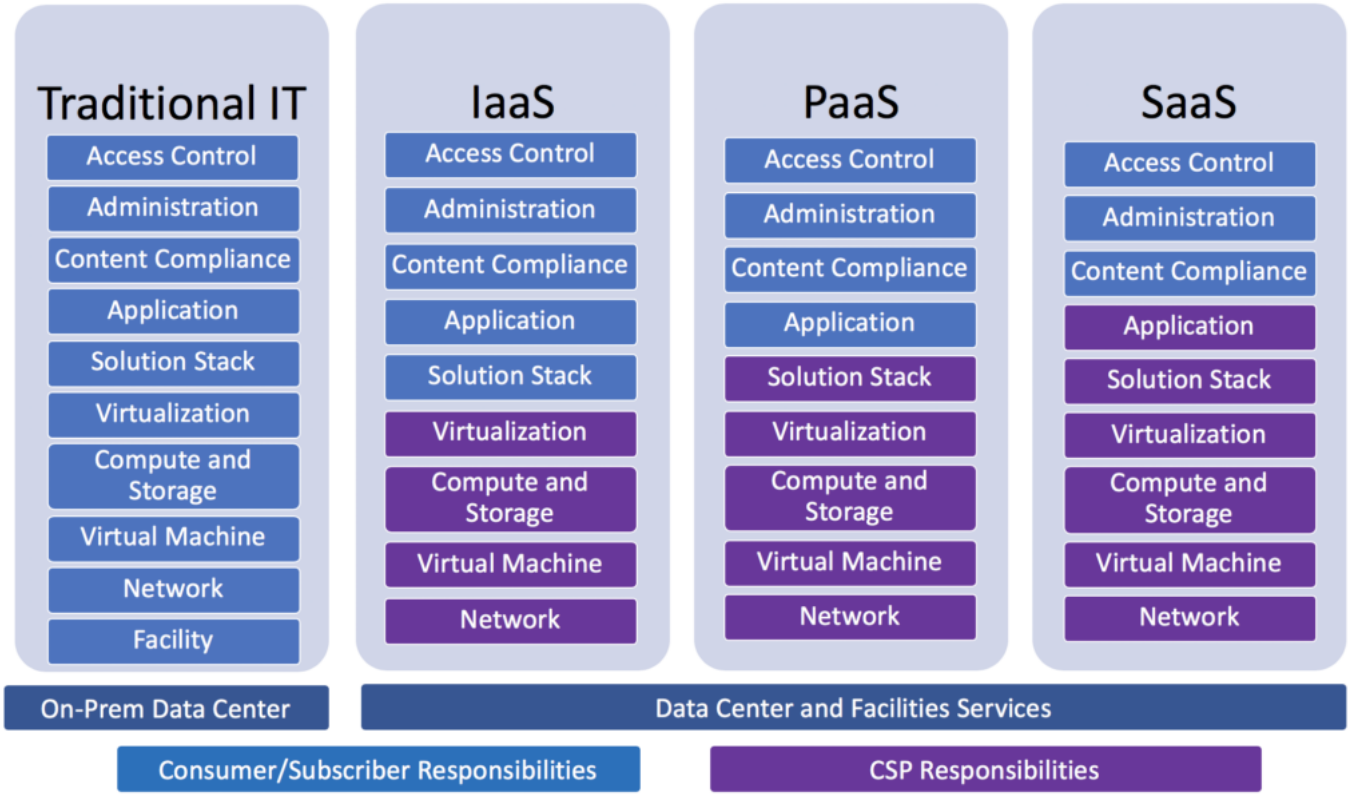

Рис. 1.5. Рівні відповідальності хмарної відповідальності

Відкритий альянс по впровадженню хмарних технологій (OACA) визнав необхідність фіксувати операційні та управлінські ролі та відповідальність хмарних

ресурсів. Вони відносяться до операцій та управління в тому, що OACA називає «моделлю загальних ресурсів хмари».

Open Alliance for Cloud Adoption - це консорціум глобальних технологічних організацій, очолюваний членами, які покликані полегшити впровадження сумісних рішень і послуг, що стосуються хмарних обчислень, для підприємств по всьому світу. [4]

У цій моделі є дві різні ролі: хмарний постачальник і хмарний передплатник. Для цілей цього обговорення використовують стандарт NIST SP 500-292 (еталонна архітектура хмарних обчислень NIST) «Хмарний провайдер і хмарний споживач спільно контролюють ресурси в хмарної системі» (Рис.1.6) [11].

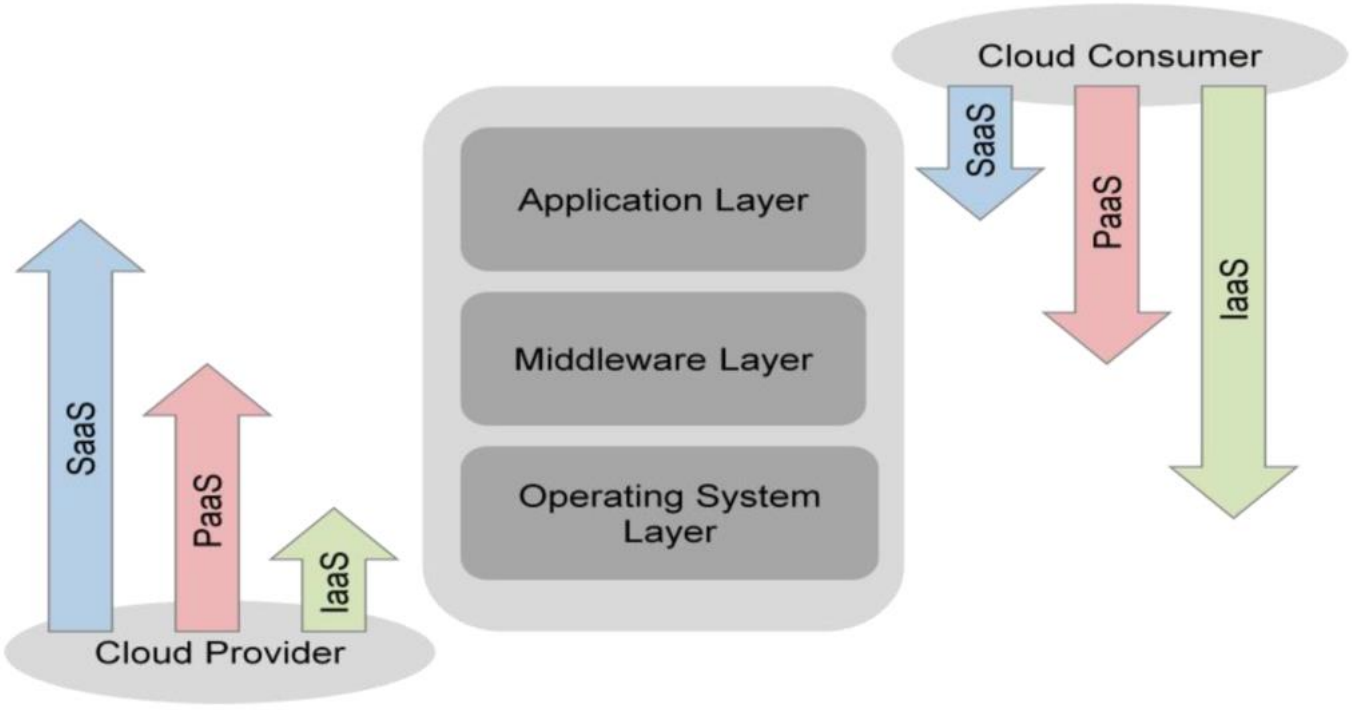

Рис. 1.6. Зона відповідальності постачальника та користувача хмарних сервісів стандарту NIST SP 500-292

1.2.5 Характеристика моделей обслуговування хмарних обчислень

Слід визнати, що існує розмежування засобів управління хмарної моделлю, яке буде варіюватися в залежності від використовуваної реалізації і споживання необхідних послуг, і це буде визначати обов'язки сторін-учасників процесу і допомагати управляти хмарним середовищем. Щоб постачальник хмарних послуг міг надати адекватні можливості транзакцій, необхідно визначити достатні вимоги.

При традиційному способі отримання послуг або ресурсів власник інфраструктури відповідає за управління всіма компонентами використовуваного ним апаратного і програмного забезпечення. Зазвичай користувачеві потрібен якийсь час, щоб отримати доступ до нового ресурсу, але при необхідності його можна точно налаштувати.

Традиційна інфраструктура часто пов'язана з застарілими базовими додатками (можливо, заснованими на старіших технологіях), які досить важко перенести в хмарні парадигми. Здатність до швидкої адаптації, стандартизація та інші явні переваги хмари не є достатніми причинами для перенесення. В інших випадках жорсткі вимоги безпеки і місцеве законодавство вимагають від користувачів, щоб дані розташовувалися поблизу або перебували під повним адміністративним контролем.

Інфраструктура як послуга (IaaS)

Інфраструктура як послуга (IaaS) - це хмарне решение, в рамках якого постачальник надає користувачу доступ до обчислювальних ресурсів, таким як сервери, сховище і мережі. Компанії використовують свої власні платформи і додатки в інфраструктурі постачальника послуг.

Основні функції

• замість того щоб купуваті обладнання и негайно оплачувати його, користувачі оплачують IaaS за запит.

• інфраструктура масштабується залежно від потреб в обчіслювальній потужності и пам'яті.

• підприємства економлять витрати на покупку і обслуговування свого власного апаратного забезпечення.

• дані знаходяться в хмарі, тому немає єдиної точки відмові.

• підтрімується віртуалізація завдання адміністрування, що дозволяє звільніті час для виконання іншої роботи.

Відповідальність компанії починається з рівня операційної системи, а доступність і надійність наданої інфраструктури забезпечує постачальник.

Є кілька варіантів використання, в яких може бути вигідна ця модель послуг. Компанії, які не мають власного центру обробки даних, розглядають IaaS як швидку і дешеву інфраструктуру для своїх бізнес-проектів, які при необхідності можна розширити або припинити. Ще приклад використання IaaS - це традиційні компанії, яким потрібні обчислювальні потужності для обробки змінних робочих навантажень з меншими капітальними витратами. В обох випадках компанії будуть платити тільки за послуги, які вони використовують.

Платформа як послуга (PaaS)

Платформа як послуга (PaaS) - це хмарне рішення, в рамках якого користувачам надається хмарна середовище, в якому вони можуть здійснювати розробку, управління і доставку додатків. Крім сховища та інших обчислювальних ресурсів, користувачі можуть використовувати готові інструменти для розробки, налаштування та тестування своїх власних додатків.

Основні функції

• PaaS надає платформу з інструментами для тестування, розробки і розміщення додатків в тому ж середовищі.

• Організації отримують можливість зосередитися на розробці, не турбуючись про базову інфраструктуру.

• Постачальники керують захистом, операційними системами, серверним програмним забезпеченням і резервним копіюванням.

• Полегшується спільна робота, навіть якщо співробітники працюють віддалено.

Для компаній-розробників, які хотіли б реалізувати гнучкі методології розробки, найбільше підходить модель PaaS. Постачальники PaaS надають безліч послуг, які можна використовувати всередині додатків. Ці послуги завжди будуть доступними і сучасними. PaaS забезпечує дуже простий спосіб тестування і створення прототипів нових додатків. Це дозволяє економити гроші при розробці нових послуг і додатків. Додатки можна випускати швидше, ніж зазвичай, для отримання відгуків користувачів.

Економіка API - нова парадигма в сфері розробки, і хмара надає досконалу платформу для її реалізації.

Програмне забезпечення як послуга (SaaS)

Сьогодні моделі надання послуг SaaS є загальноприйнятими в багатьох компаніях, які хотіли б отримувати вигоду від використання додатків без необхідності обслуговування та оновлення інфраструктури та компонентів. Додатки для пошти, управління ресурсами підприємства (ERP), спільної роботи і офісні додатки - найбільш затребувані рішення SaaS. Основні переваги моделі SaaS - це гнучкість і еластичність.

Програмне забезпечення як послуга (SaaS) - це хмарне рішення, в рамках якого забезпечується доступ користувачів до хмарного програмного забезпечення постачальника. Його користувачі не встановлюють додатки на свої власні локальні пристрої. Додатки знаходяться у віддаленій хмарної мережі, доступ до якої здійснюється через веб-інтерфейс або API. Додаток дозволяє користувачам зберігати і аналізувати дані і спільно працювати над проектами.

Основні функції

• Постачальники SaaS надають користувачам програмне забезпечення і додатки на основі передплати.

• Користувачам не потрібно встановлювати або оновлювати ПО, а також керувати ним; це роблять постачальники SaaS.

• Дані в хмарі захищені: збій обладнання не призводить до втрати даних.

• Використання ресурсів масштабується залежно від потреб у послугах.

• Програма є доступною майже з будь-якого пристрою, підключеного до мережі Інтернет, і практично в будь-якій точці світу.

Приклади моделей хмарного сервісу та сервіси провайдера:

Програмне забезпечення як послуга - Amazon WorkSpaces, Google G Suite, Microsoft Office 365 і т. д.

Інфраструктура як послуга - Amazon EC2, віртуальні машини Azure, Google Compute Engine і т. д.

Платформа як послуга - Amazon Elastic Beanstalk, веб-сайти Azure, Google App Engine і т. д.

Функціонування як послуга - AWS Lambda, Функції Azure, Хмарні функції Google і т. д.

1.3. Аналіз та вибір брокерів безпечного доступу в хмарі CASB

1.3.1 Функціональні можливості CASB

Виділимо найбільш актуальні завдання щодо забезпечення безпеки використання хмар [3,4,5,7]:

видимість використовуваних хмарних сервісів;

контроль над їх використанням;

забезпечення захисту хмарних даних від неправомірного спотворення або видалення,

запобігання витоку інформації;

захист даних від зовнішніх і внутрішніх загроз, що передаються в хмари і зберігаються на їхньому боці;

захист від хмарних шкідливих програм і їх поширення.

Системи CASB на початку свого розвитку були в основному зосереджені на контролі доступу до бек-офісних додатків, що поставляються як Software as a Service

(SaaS), таким як CRM, ERP, HR, спільне використання файлів (EFSS), хмарні додатки типу G Suite і Microsoft Office 365 і служби технічної підтримки (Service desk). Зараз же область їх застосування включає в себе інструменти для контролю доступу до більш широкого спектру хмарних сервісів: Platform as a Service (PaaS) і Infrastructure as a Service (IaaS).

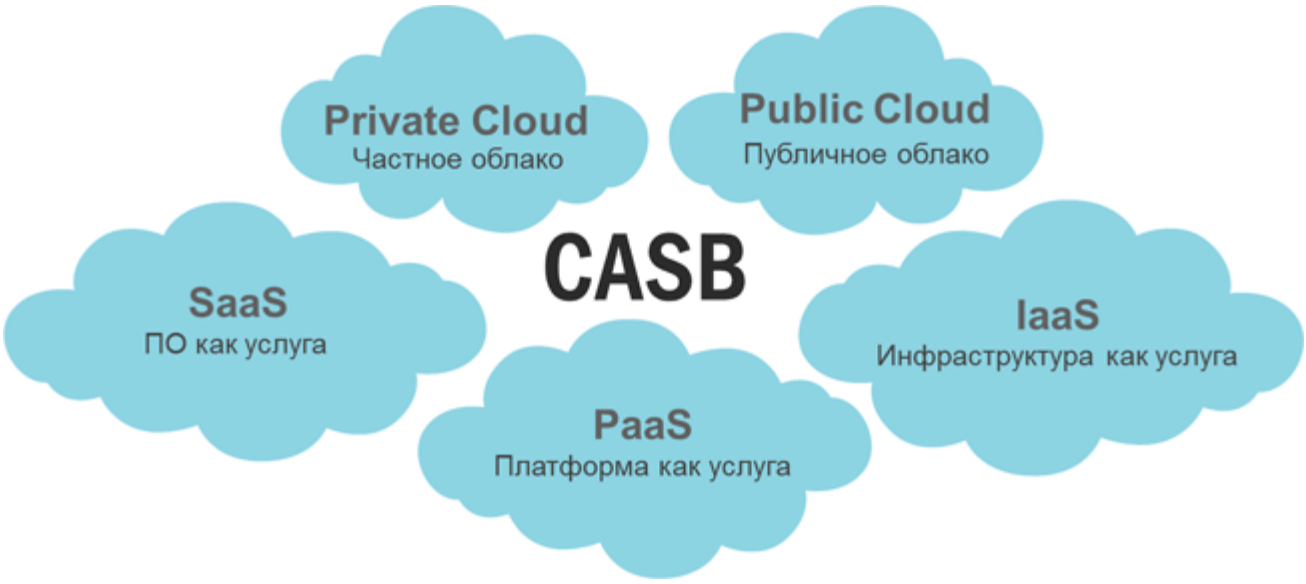

Рис.1.7. Хмарні сервіси CASB

Хмарні сервіси системи CASB (Рис.1.7) допомагають організаціям контролювати хмарні додатки і сервіси, як офіційно дозволені політиками ІБ компаній до використання, так і не дозволених, які вважаються неправомірними. CASB надає видимість, необхідну для забезпечення безпеки хмарних додатків, і можливість швидко і ефективно реагувати на зовнішні та внутрішні загрози. Провідні аналітичні агентства до цього класу рішень відносять такі основні функціональні блоки: наочність, захист даних, захист від загроз і відповідність вимогам регулюючих органів. Розглянемо більш докладно, яка функціональність може входити в кожен з цих блоків. (Рис. 1.8)

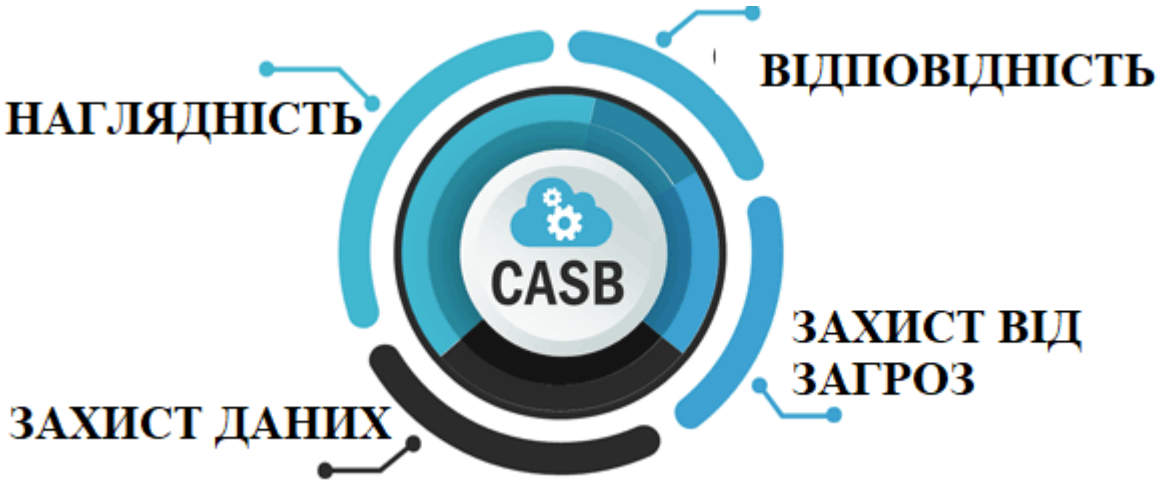

Рис.1.8. Основні функціональні блоки CASB

Наглядність у цей функціональний блок в першу чергу входить пошук і виявлення всіх використовуваних організацією дозволених і недозволених хмарних додатків і сервісів. Відсутність наглядності використовуваних хмар призводить не тільки до того, що немає видимості використовуваних ресурсів, а й немає розуміння в цілому, наскільки компанія схильна до ризиків інформаційної безпеки щодо переміщення в хмару або щодо даних, що зберігаються вже там. Очевидно, що несанкціоноване використання хмар в організаціях, так зване «тіньове IT» може привести до втрати критичних для компанії даних або до різних варіантів негативного впливу на них і на інфраструктуру організації в цілому. Після виявлення всіх використовуваних ресурсів в хмарі, система CASB дозволяє забезпечувати наочне уявлення: до яких хмарних додатків / сервісів співробітники мають доступ і хто дійсно користується цими сервісами, з яких саме пристроїв і якого місця розташування. Далі дозволяє провести аналіз і оцінити ризики конкретних використовуваних хмарних сервісів і вжити необхідних заходів щодо забезпечення безпеки.

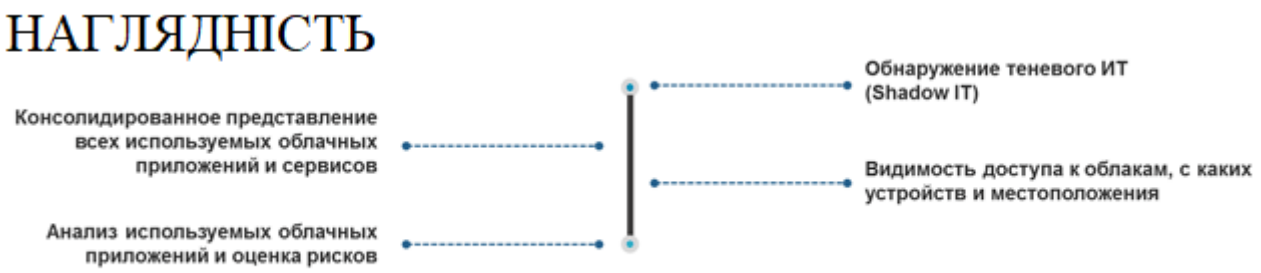

Рис.1.9. Основна функціональність блоку наглядність

Захист даних у першу чергу, для забезпечення захисту даних CASB надає інструменти управління правами доступу до хмар для запобігання несанкціонованому використанню сервісів і недозволених додатків, контролю доступу до ресурсів з різних пристроїв, а також застосування політик розмежування прав доступу до критичних даних. CASB контролює доступ користувачів до всіх використовуваних хмарних сервісів, в тому числі надає можливість не тільки розмежовувати доступ до них, а й забороняти використання певних хмарних сервісів, в залежності від встановлених політик ІБ кожної конкретної організації (Рис.1.10).

Також CASB підтримує різні політики розмежування прав доступу користувачів до даних, що знаходяться в хмарах і, при необхідності, блокує доступ до ресурсів з неавторизованих пристроїв і доступ до даних без відповідних привілеїв. Деякі системи CASB надають можливість інтеграції з існуючими на інфраструктурі системами IDM / IGA з управління обліковими записами і призначеним для користувача доступом. Із застосуванням механізму поведінкового аналізу UEBA рішення класу CASB дозволяють виявити аномальні активності з правами доступу або дії підозрілих облікових записів.

Моніторинг подій в хмарі і виявлення підозрілих активностей, а також оповіщення в режимі реального часу дозволяють перехопити шахрайські дії, своєчасно заблокувати такого роду активності і, при необхідності, облікові записи, для запобігання подальшого поширення неправомірних дій.

По-друге, CASB включає в себе можливість виявлення критичних даних, що зберігаються або переміщуються в хмарні сервіси, їх категоризації і / або класифікації та подальшого контролю над ними. Для запобігання витоку важливої інформації спочатку застосовується пошук критичного контенту і подальша його захист в санкціонованих хмарних додатках, а також виявлення критичної інформації на шляху до несанкціонованих додатків і застосування режиму блокування, в залежності від налаштувань і встановлених політик. Дана функціональність цілком повторює функціональність систем класу DLP, тільки орієнтована на хмарне середовище. Деякі CASB-системи не мають вбудованих DLP-функцій, але можуть використовувати сторонні DLP-інструменти, надаючи інтерфейс взаємодії через API ICAP або RESTful до існуючих на мережі DLP-систем. Деякі CASB пропонують вбудовані функції контролю і захисту даних DCAP (Data-Centric Audit and Protection) або також можливість інтеграції.

По-третє, в якості додаткового захисту даних CASB представляє функціональність шифрування, або токенізації даних в хмарних платформах. При повному або вибірковому шифруванні структурованих полів, яке налаштовується в хмарних додатках, а також неструктурованих даних в хмарних платформах і шифрування контенту «на льоту», забезпечує додатковий захист даних. Зловмисникам не дуже цікаві зашифровані дані, їх неможливо використовувати оперативно в своїх цілях без додаткових витрат на їх розшифровку. Залежно від конкретного вендора, рішення CASB підтримують різні типи шифрування даних і способи управління ключами.

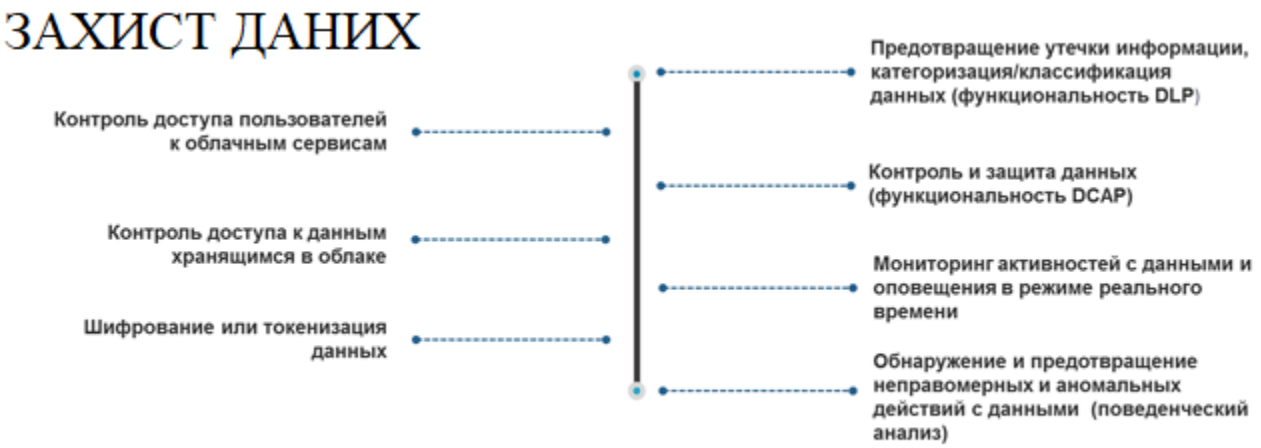

Рис.1.10. Основна функціональність по захисту даних

Захист від загроз. Системи класу CASB включають в себе функціональність по виявленню, нейтралізації та усунення шкідливих програм в хмарних платформах. Відповідно до недавніх досліджень Netskope і Ponemon Institute, одна з трьох організацій схильна до впливу шкідливого коду і не знає про це. Більш того, 31% організацій зазнали негативні впливи на свої критичні дані, викликані хмарними шкідливими програмами [8-10].

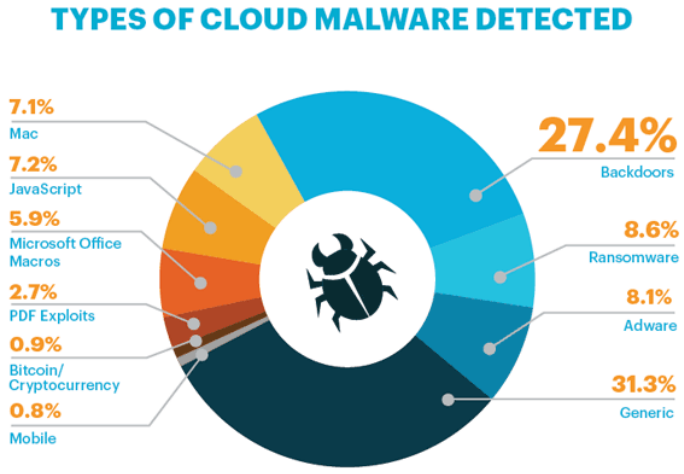

Рис 1.11. Типи зафіксованих хмарних шкідливих програм в процентному співвідношенні, за даними Netskope Clould report, вересень 2019р.

Хакери йдуть туди, де знаходяться менш захищені і не менш цінні дані, а на сьогоднішній момент це хмара. В даний час спостерігається зростання числа інцидентів, пов'язаних з хмарними шкідливими програмами і вірусами-вимагачами в хмарах. Це пов'язано з тим, що шкідливе ПЗ може ховатися в хмарних сервісах, і організації не можуть захистити себе, тому що вони або не знають про використання співробітниками конкретного хмарного сервісу з шкідливим кодом в ньому, або просто не контролюють його.

У зв'язку з тим, що користувачі багатьох організацій мають неконтрольований доступ до хмарних додатків / сервісів, які можуть бути спочатку скомпрометовані або користуються зараженими файлами в хмарах, виникає ризик швидкого поширення шкідливої програми по всьому периметру корпоративної мережі і нанесення більш глобального збитку організації. Наприклад, скомпрометовані привілейовані облікові записи дозволяють отримати розширений доступ до всіх хмарних сервісів і даними організації, що дозволить в подальшому зловмисникові отримати доступ і до локально розташованих даних і інфраструктурі в цілому, наприклад, при проведенні цілеспрямованої атаки.

CASB, в залежності від рішення конкретного виробника, пропонує різні методи запобігання хмарним загрозам і кібератак, такі як поведінкова аналітика, антивірусне сканування, застосування машинного навчання для встановлення шаблонів поведінки, використання аналітики загроз в реальному часі від постачальників хмарних сервісів. У деяких виробників CASB-систем є власні аналітичні центри, які спеціалізуються на вивченні хмарних вірусів і специфіки хмарних атак, а також дають можливість використовувати додаткові інструменти, наприклад пісочницю.

Рішення CASB забезпечує можливість виявлення, карантину і нейтралізації шкідливих програм, а також блокування доступу до шкідливих хмарних додатків, реєструючи і наочно відображаючи всі підозрілі дії.

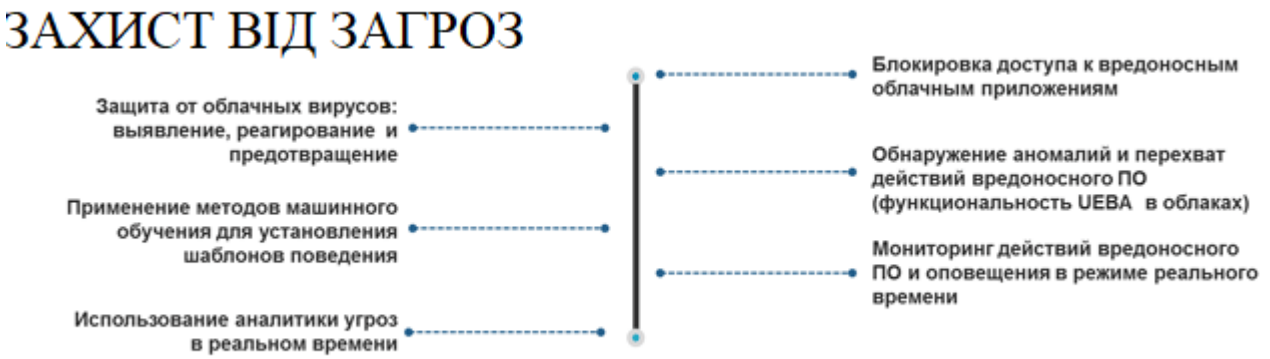

Рис. 1.12. Основна функціональність по захисту від загроз

Відповідність. Необхідність відповідати вимогам внутрішніх і зовнішніх регуляторів не пропадає навіть при частковому переході організацій в хмару. CASB допомагає дотримуватися встановлених внутрішньої політики інформаційної безпеки і демонструвати відповідність нормативним вимогам зовнішніх регуляторів, забезпечуючи комплексний захист хмарних ресурсів. Рішення CASB надає єдину консоль візуалізації, моніторингу та звітності по всіх використовуваних хмарним додаткам і сервісам, єдину бізнес-орієнтовану платформу з реагування та розслідування інцидентів інформаційної безпеки (рис.1.3).

Рис. 1.13. Опис функціонального блоку відповідність

1.3.2 Принцип роботи CASB

CASB є уніфікований інструмент контролю за всіма хмарними додатками, ресурсами і сервісів, контролює взаємодію між хмарними додатками і зовнішнім

світом за допомогою проксі-режиму (Proxy) та / або API-режиму, що дозволяє виявляти потенційні загрози, і орієнтований на високий рівень захисту хмарної середовища [2,3,4].

Системи CASB можуть розгортатися як у локальній, так і в хмарної середовищі, а також у гібридної комбінації з використанням локальних і хмарних контрольних точок, в залежності від потреб та вимог до побудови систем безпеки конкретної організації. Впровадження CASB в хмарному виконанні помітно більш популярно, ніж в локальному, і стає все більш привабливим варіантом для більшості випадків використання. Проте, локальні варіанти розгортання мають право на існування.

Залежно від конкретного вендора системи CASB, як згадувалося вище, підтримують різні архітектурні можливості підключення до хмар:

- API
- Proxy
- Гібридний виконання (Рис.1.14).

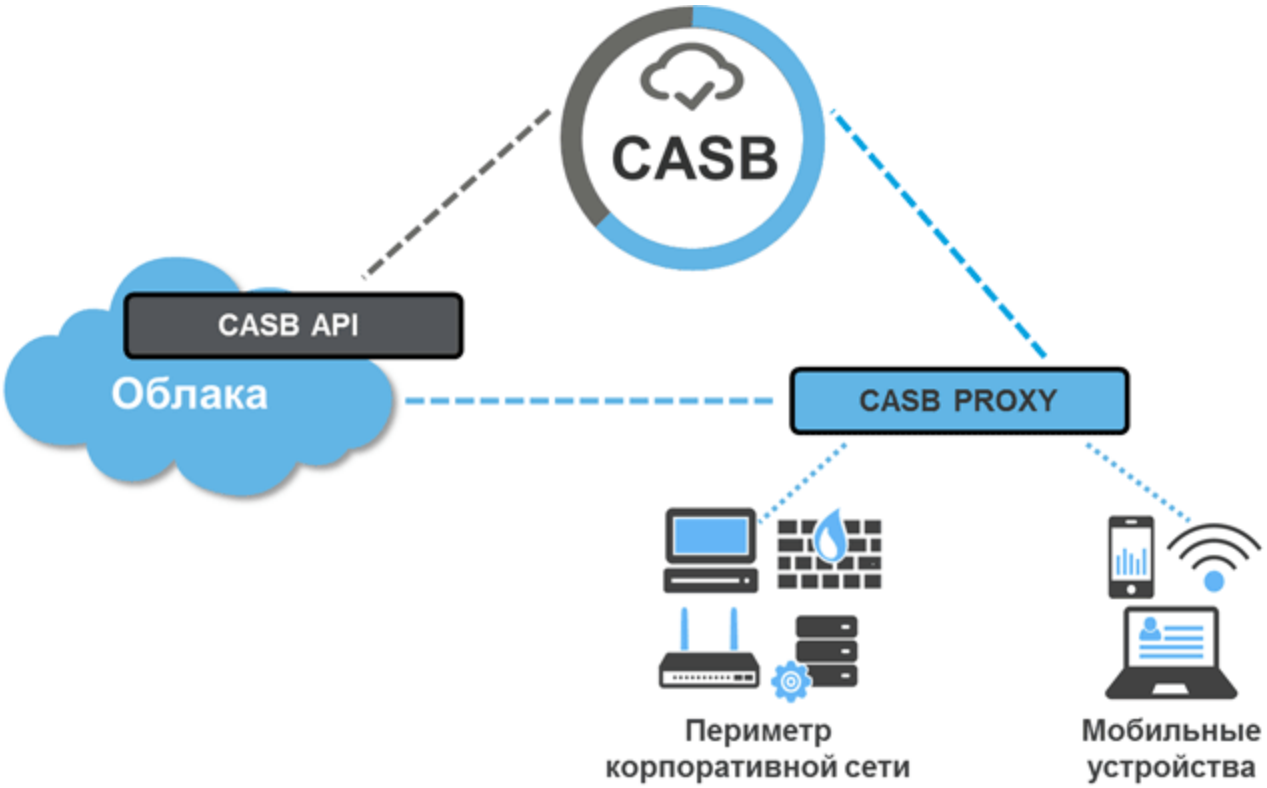

Рис. 1.14. Гібридне виконання роботи CASB

1.3.3 Вибір постачальника Cloud Access Security Brokers

Головним питанням залишається, який підхід обрати до розгортання CASB-рішення, що будуть найбільш правильним. Все залежить від конкретної організації, від ландшафту використовуваних в ній хмарних додатків / сервісів, від використовуваних ІБ-рішень в інфраструктурі і від стратегії по забезпеченню інформаційної безпеки в цілому. Хоча варто відзначити, що Gartner у своєму звіті Magic Quadrant for Cloud Access Security Brokers виділяє в фаворитах гібридний підхід як найбільш повний за функціональними можливостями (Рис 1.15). У цьому ж звіті при бажанні можна почерпнути більш детальну інформацію про згадані підходах, їх достоїнства і недоліки.

Рис. 1.15. Magic Quadrant for Cloud Access Security Brokers

Світовий ринок рішень CASB Через швидке впровадження організаціями хмарних сервісів постачальники CASB-систем в даний час активно борються за лідерство. Більшість глобальних гравців систем інформаційної безпеки здійснили покупки нішевих гравців, що спеціалізуються на хмарної безпеки, тим самим поповнивши свої портфелі рішеннями класу CASB. Варто згадати, що 3 січня 2018

року компанія McAfee закрила угоду з придбання рішення CASB компанії Skyhigh Networks і тим самим розширила свій список пропонованих рішень одним з сильних продуктів цього класу. Провідні аналітичні агентства Gartner, KuppingerCole, IDC, Forrester в своїх звітах згадують наступних вендорів в даному класі рішень зі своїми підходами в реалізації і функціональними можливостями:

- Bitglass (Bitglass CASB 2)
- CensorNet (CensorNet Unified Security Service, CensorNet Secure Web Gateway);
- CipherCloud (CipherCloud Platform);
- Cisco (CISCO Cloudlock);
- Forcepoint (Forcepoint CASB);
- IBM (IBM Cloud Security Enforcer);
- Microsoft (Microsoft Cloud App Security);
- Netskope (Netskope Active Platform);
- Oracle (Oracle CASB Cloud Service);
- Symantec (Symantec CloudSOC).

Висновки до розділу 1

1. Проведено аналіз використання хмарних сервісів для корпоративних інформаційних систем, в результаті якого було визначено основні види кібербезпеки, які можуть негативно вплинути на роботу корпоративної системи.

2. Визначено моделі розгортання хмар, в залежності від потреб бізнес-процесів та моделі обслуговування в хмарі, які відповідають міжнародним стандартам.

3. Проведено аналіз функціональних блоків CASB та вибір основних постачальників CASB. Відповідно Magic Quadrant for Cloud Access Security Brokers обрано кращій варіант для подальшого дослідження Microsoft Cloud App Security.

2 МЕТОДИ ТА ЗАСОБИ ПОБУДОВИ CASB НА БАЗІ MICROSOFT CLOUD APP SECURITY

2.1. Призначення Microsoft Cloud App Security

Як було розглянуто в попередньому розділі хмари підвищуть гнучкість в роботі співробітників і IT-фахівців. Але такий перехід в хмару викликають певні труднощі в захисті організації. Для того щоб отримати максимальну користь від хмарних сервісів і додатків, IT-фахівцям потрібно обрати критерій за яким будуть надаватися доступ та контроль доступу для захисту критично важливих даних компанії [1].

Microsoft Cloud App Security - це брокер безпечного доступу в хмару (CASB), який підтримує різні режими розгортання, який включає збір даних журналів, з'єднувачі API і зворотні проксі-сервери. Цей засіб забезпечує широкі можливості візуалізації, контроль переміщення даних і складну аналітику для ідентифікації та усунення кіберзагроз у всіх хмарних службах Майкрософт і сторонніх постачальників.

Брокер CASB допомагає компанії отримати повне уявлення про використання хмарних ресурсів додатками SaaS і хмарними службами. В основному CASB використовується для виявлення тіньових IT та управління додатками. Крім того, компанія несе відповідальність за управління хмарної платформою і її захист, включаючи IAM, віртуальні машини, обчислювальні ресурси, дані і сховище, мережеві ресурси і багато іншого. Таким чином, якщо компанія використовує або планує використовувати хмарні сервіси в своєму портфелі мережевих служб, швидше за все, необхідно використовувати CASB для вирішення інших унікальних завдань щодо контролю та захисту середовища компанії. і захистити конфіденційні бізнес-дані.

Організація повинна захистити своїх користувачів і конфіденційні дані від різних методів, застосовуваних зловмисниками. Брокери CASB надають широкий набір можливостей для захисту середовища відповідно до таких принципів:

Видимість: виявлення всіх хмарних служб, призначення кожній з них рівень ризику, виявлення всіх користувачів і сторонніх додатків, які можуть увійти в систему.

Безпека даних: виявлення і контроль використання конфіденційних відомостей (DLP), застосування заходів відповідно до мітками класифікації вмісту.

Захист від загроз: забезпечення адаптивного контролю доступу (AAC), аналіз поведінки користувачів і сутностей (UEBA), усунення шкідливих програм.

Відповідність вимогам: надання звітів і панелей моніторингу для демонстрації управління хмарою, допомога в забезпеченні відповідності нормативним вимогам і вимогам до місця розташування даних.

Як видно з основних принципів Microsoft Cloud App Security, вони повністю відповідають функціональним блокам концепції CASB.

2.2 Архітектура Microsoft Cloud App Security

Розглянемо архітектуру Cloud App Security, яка надасть основне уявлення щодо методів та засобів роботи в хмарному середовищі компанії.

Cloud App Security дозволяє отримувати інформацію про хмарі за рахунок використання наступних засобів:

Cloud Discovery використовується для зпівставлення і визначення хмарного середовища і хмарних додатків, які використовує компанія;

застосовує і скасовує санкціонування додатків в хмарі;

використовує *прості* в розгортанні з'єднувачі додатків, які застосовують переваги інтерфейсів API постачальників, для моніторингу і контролю додатків, до підключаються працівники компанії.

використовує *захист* на основі Управління умовним доступом до додатків, забезпечуючи можливість відстеження і контролю доступу та дій, які виконуються в ваших хмарних додатках;

забезпечує *безперервний контроль* завдяки установці політик і їх постійного налаштування.

Дана архітектура забезпечує забезпечує роботу платформи Cloud App Security основним призначенням якої є [1]:

виявлення та адміністрування використання тіньових IT. Визначає хмарні додатки, IaaS і служби PaaS, які використовує компанія. Аналізувати шаблони використання, а також оцінка рівня ризику і готовності бізнес-процесві використовувати більш ніж 16 000 додатків SaaS, запобігаючи виникненню більш ніж 80 типів ризиків. Це дозволить забезпечити безпеку і відповідніть вимогам щодо управління бізнес-процесів компанії.

захист конфіденційних даних в будь-якому місці в хмарі. Надає можливість аналізувати, класифікувати і захищати конфіденційні відомості від розкриття при зберіганні. При використанні готових політик і автоматизовані процеси допоможе при застосування засобів управління в реальному часі до всіх хмарних додатків.

захист від кіберзагроз та аномалій. Визначається незвичайна поведінка хмарних додатків для ідентифікації програм-шантажистів, скомпрометованих користувачів або шахрайських програм, аналізує шаблони використання з високим ризиком, а також автоматично застосовує виправлення, щоб запобігти ризикам для компанії.

оцінка відповідності хмарних додатків. Оцінка, чи відповідають хмарні додатки відповідним вимогам, включаючи відповідність нормативним вимогам і галузевим стандартам. Дозволяє запобігти витоку даних для невідповідних додатків і обмежує доступ до контрольованих даних.

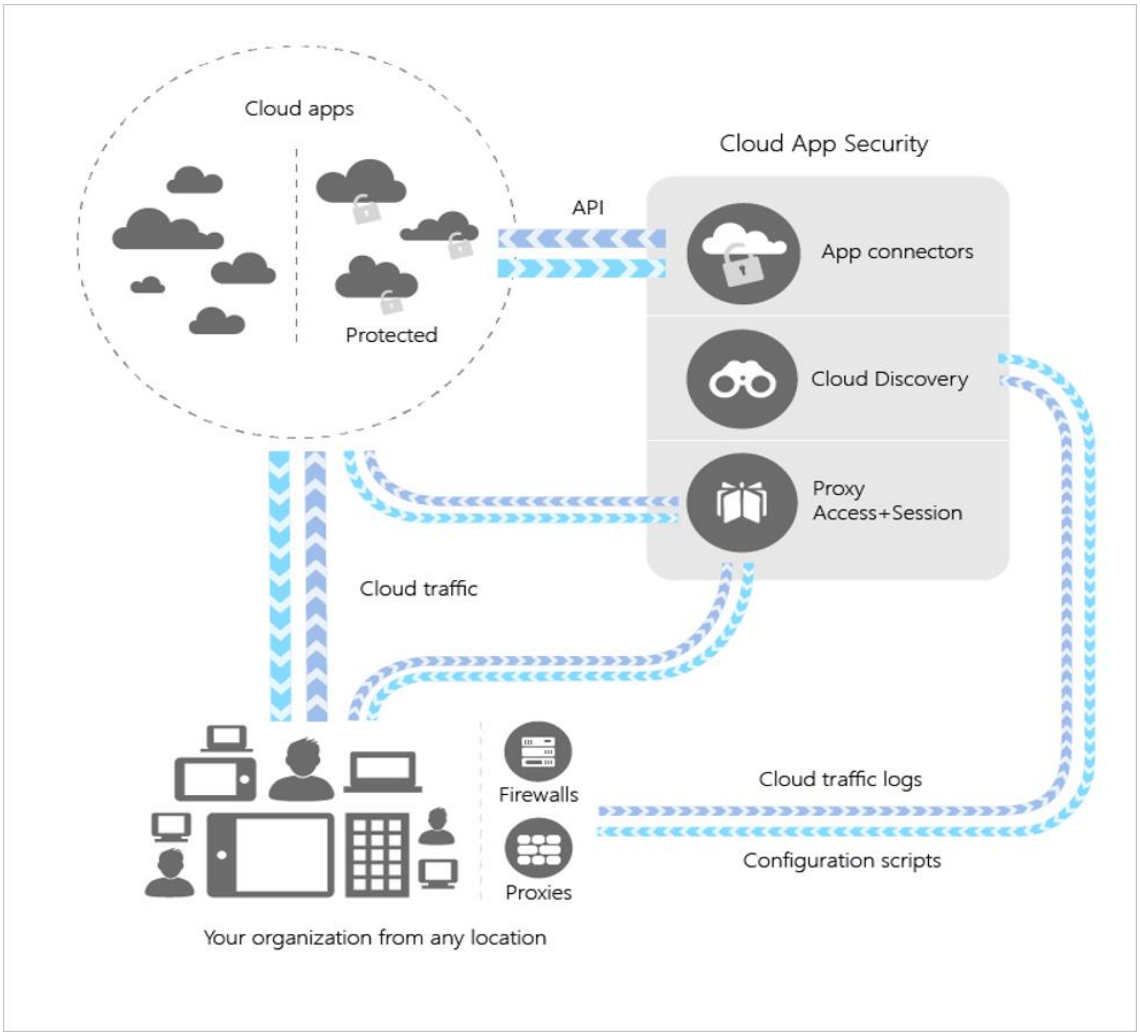

Рис.2.1. Архітектура Microsoft Cloud App Security

Розглянемо ці засоби більш детально.

Cloud Discovery використовує журнали трафіку для динамічного виявлення і аналізу хмарних додатків, що використовуються компанією. Для створення звіту про миттєвий знімок використання хмари організацією дозволяє вручну відправити файли журналу з брандмауера або проксі-сервера для аналізу. Щоб налаштувати безперервні звіти, використовують збирачі журналів Cloud App Security для періодичного перенаправлення журналів компанії.

Застосування і скасування санкціонування додатків. Можна використовувати Cloud App Security, щоб застосовувати або скасовувати санкціонування додатків в організації за допомогою каталогу хмарних додатків. Команда аналітиків Майкрософт має у своєму розпорядженні великий каталог, який постійно поповнюється, що містить більше 16 000 хмарних додатків, які ранжуються і оцінюються відповідно до галузевих стандартів. Компанія може використовувати каталог хмарних додатків, щоб оцінити ризик для хмарних додатків на основі нормативних сертифікацій, галузевих стандартів і рекомендацій. Це дозволяє налаштувати оцінку і вагу різних параметрів відповідно до потреб компанії. На основі цих оцінок Cloud App Security повідомляє, наскільки небезпечним є додаток. Оцінка ґрунтується більш ніж на 80 факторах ризику, які можуть впливати на середу.

З'єднувачі додатків використовують API постачальників хмарних додатків, щоб інтегрувати хмару Cloud App Security з іншими хмарними додатками. З'єднувачі додатків розширюють управління і захист. Вони також надають доступ до інформації безпосередньо з хмарних додатків для аналізу Cloud App Security.

Щоб підключити додаток і продовжити захист, адміністратор програми дозволяє Cloud App Security доступ до додатка. Потім Cloud App Security запитує журнали подій в додатку і сканує дані, облікові записи і хмарний вміст. Cloud App Security може примусово застосовувати політики, виявляти загрози та надавати системі управління дані для вирішення проблем.

Cloud App Security використовує API, надані хмарним постачальником. Кожна програма має власну платформу і обмеження API. Cloud App Security працює з постачальниками додатків над оптимізацією використання API для досягнення оптимальної роботи. Беручи до уваги різні обмеження, що накладаються додатками на API (наприклад, регулювання, обмеження API, динамічне зрушення вікон API), підсистеми Cloud App Security використовують допустимі ресурси. Деякі операції, такі як сканування всіх файлів клієнтів, вимагають великого числа викликів API і тому

розтягуються на більш тривалий час. Деякі політики можуть виконуватися протягом декількох годин і навіть днів.

Захист на основі функції управління налаштуванням умовного доступу для додатків. Управління умовним доступом до додатків Microsoft Cloud App Security використовує архітектуру на основі зворотного проксі-сервера. Це рішення надає можливості, за допомогою яких можна в реальному часі відстежувати і контролювати доступ до хмарного середовища, а також виконувати в ньому дії. За допомогою захисту на основі функції управління налаштування умовного доступу для додатків можливо використовувати такі можливості:

запобігання витоку даних за допомогою попереджування блокування скачування файлів;

налаштування правил примусового шифрування даних, що зберігаються в хмарі або скачуваних з нього;

отримання інформації про незахищені кінцеві точки для відстеження дій на некерованих пристроях;

управління доступом з розташувань за межами корпоративної мережі і з ненадійних IP-адрес.

Управління політиками. Дає можливість використовувати політики для визначення поведінки користувачів в хмарі. Використання політики, дозволяє виявляти небезпечну поведінку, порушення або підозрілі точки даних і дії в хмарному середовищі. При необхідності є можливість використовувати політики, щоб впровадити процеси виправлення для повного усунення ризиків. Типи політик пов'язані з різними типами відомостей, які потрібно зібрати про хмарне середовище, і декількома типами коригувальних дій, які можуть знадобитися.

Рис. 2.2 Кругова діаграма безпеки Zero Trust

Проста кругова діаграма безпеки Zero Trust, в основі якої лежить механізм примусового виконання, що забезпечує оцінку політики в реальному часі. Механізм забезпечує захист, аналізуючи сигнали, застосовуючи загально-організаційні політики та аналітику загроз, а також забезпечуючи перевірку і аутентифікацію особистості і безпеку пристроїв. Вона умовно надає доступ до даних, додатків, інфраструктурі і мережі, забезпечуючи безперервну і повну видимість і аналітику, а також автоматизацію процесів.

2.3 З'єднувачі додатків API

З'єднувачі додатків використовують API постачальників хмарних додатків, щоб інтегрувати хмару Cloud App Security з іншими хмарними додатками. З'єднувачі додатків розширюють управління і захист. Вони також надають доступ до інформації безпосередньо з хмарних додатків для аналізу Cloud App Security.

Щоб підключити додаток і продовжити захист, адміністратор програми надає Cloud App Security доступ до додатків. Потім Cloud App Security по запиту збирає журнали дій в додатку і сканує дані, облікові записи і хмарний вміст. Cloud App

Security може примусово застосовувати політики, виявляти загрози та надавати рекомендації по застосуванні дій системі управління для вирішення проблем.

Cloud App Security використовує API, надані хмарним постачальником. Кожна програма має власну платформу і обмеження API. Cloud App Security працює з постачальниками додатків над оптимізацією використання API для досягнення оптимальної роботи. Якщо взяти до уваги різні обмеження, що накладаються додатками на API (наприклад, регулювання, обмеження API, динамічний зрушення вікон API), підсистеми Cloud App Security використовують допустимі ресурси. Деякі операції, такі як сканування всіх файлів в клієнті, вимагають великого числа викликів API і тому розтягуються на більш тривалий час. Деякі політики можуть виконуватися протягом декількох годин і навіть днів.

2.4 Cloud Discovery

Cloud Discovery використовує журнали трафіку для динамічного виявлення і аналізу хмарних додатків, що використовуються компанією. Для створення звіту про негайний знімок використання хмари організацією можна вручну відправити файли журналу з брандмауера або проксі-сервера для аналізу. Щоб налаштувати безперервні звіти, використовують збирачі журналів Cloud App Security для періодичного перенаправлення журналів.

2.5 Захист на основі функції управління налаштуваннями умовного доступу для додатків Proxy Access

Управління умовним доступом до додатків Microsoft Cloud App Security використовує архітектуру на основі зворотного проксі-сервера. Таке рішення надає засоби, за допомогою яких можна в реальному часі відстежувати і контролювати доступ до хмарного середовища, а також виконувати в ній дії. За допомогою захисту

на основі функції управління налаштуваннями умовного доступу для додатків є можливість використовувати такі можливості:

• запобігання витоку даних за допомогою попереджувального блокування скачування файлів;

• налаштування правил примусового шифрування даних, які зберігаються в хмарі або скачуються з нього;

• отримання інформації про незахищені кінцеві точки для відстеження дій на некерованих пристроях;

• управління доступом з розташувань, які знаходяться за межами корпоративної мережі і з ненадійних IP-адрес.

2.6. Управління політиками Microsoft Cloud App Security

Microsoft Cloud App Security використовує політики для визначення поведінки користувачів в хмарі. Використання політики необхідне для того, щоб виявляти небезпечну поведінку, порушення або підозрілі точки даних і дії в хмарному середовищі. При необхідності є можливість застосовувати політики, щоб впровадити процеси виправлення для повного усунення ризиків. Типи політик пов'язані з різними типами відомостей, які потрібно зібрати про хмарної середовищі, і декількома типами коригувальних дій, які можуть знадобитися.

Висновки до розділу 2

3 ТЕХНОЛОГІЯ РОЗГОРТАННЯ ТА ВИКОРИСТАННЯ MICROSOFT CLOUD APP SECURITY

3.1. Розгортання Microsoft Cloud App Security

Для розгортання Microsoft Cloud App Security у компанії повинна бути ліцензія на використання Cloud App Security. Microsoft Cloud App Security - це служба підписки на основі користувачів. Кожна ліцензія розрахована на кожного користувача на місяць. Microsoft Cloud App Security можна ліцензувати як окремий продукт або як частину декількох різних планів ліцензування. Коли ми говоримо про «повну пропозицію CASB», мається наувазі що це пропозиція, яка включає всі можливості Cloud App Security, Office 365 Cloud App Security і Cloud App Discovery.

Коли отримано ліцензію на Cloud App Security, приходить повідомлення до електронної пошти з інформацією про активацію і посиланням на портал Cloud App Security.

Для налаштування Cloud App Security необхідні права глобального адміністратора або адміністратора безпеки в Azure Active Directory або Office 365. Важливо розуміти, що у користувача, якому призначена роль адміністратора, будуть однакові дозволи для всіх хмарних додатків, на які підписана компанія. Це не залежить від того, де була призначена ця роль: в центрі адміністрування Microsoft 365, на класичному порталі Azure або за допомогою модуля Azure AD для Windows PowerShell.

Для роботи з порталом Cloud App Security використовується Internet Explorer 11, Microsoft Edge (останньої версії), Google Chrome (останньої версії), Mozilla Firefox (останньої версії) або Apple Safari (останньої версії).

Доступ до порталу Cloud App Security отримується на сторінці https://portal.cloudappsecurity.com. Портал можна також відкрити через Центр адміністрування Microsoft 365, виконавши такі дії:

1. Перебуваючи в Центрі адміністрування Microsoft 365, в бічному меню клацніть *Показати всі*, а потім виберіть *Безпека*.

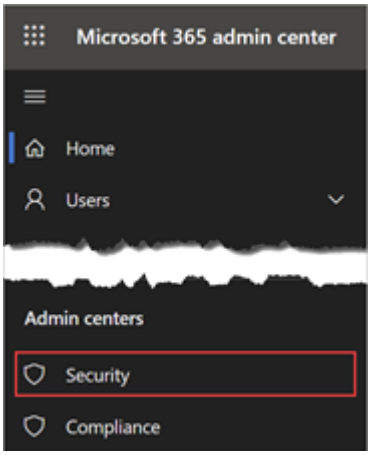

Рис. 3.1. Центр адміністрування Microsoft

2. На сторінці відомостей про безпеку Microsoft 365 клацніть *Інші ресурси*, а потім виберіть *Cloud App Security*.

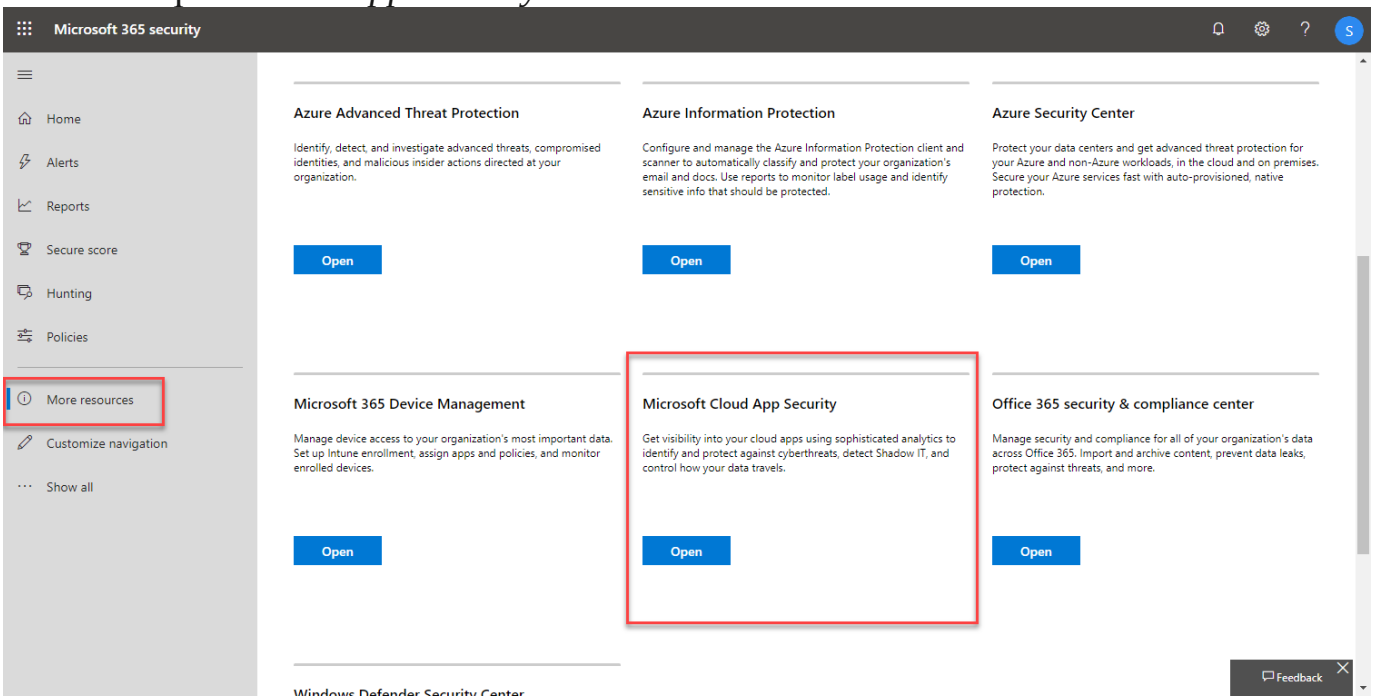

Рис. 3.2. Сторінка відомостей про безпеку Microsoft 365

Розглянемо основні налаштування Microsoft Cloud App Security.

Етап 1. Встановлення миттєвої видимості, захисту та дій управління для додатків. Основною задачею даного етапу є підключення додатків:

1. У меню «Параметри», яке викликається значком шестерні, виберіть *З'єднувачі* з додатками.

2. Клацніть знак "плюс", щоб додати і вибрати програму.

3. Щоб підключити додаток, виконайте дії з налаштування.

Дане налаштування необхідно для з'єднання програми щоб забезпечити більш високий рівень видимості, який дає можливість вивчати пов'язані з ними дії, файли і облікові записи в хмарному середовищі.

Етап 2. Управління хмарними додатками за допомогою політик

Основною задачею даного етапу є створення політик:

1. Послідовно виберіть *Управління> Шаблони*.

2. Виберіть зі списку шаблон політики, а потім натисніть (+) Створити політику.

3. Налаштуйте політику (виберіть фільтри, дії та інші параметри), а потім виберіть Створити.

4. На вкладці Політики виберіть політику, щоб переглянути відповідні їй елементи (дії, файли, оповіщення). Створювати політику необхідно для кожної категорії ризику, щоб охопити всі сценарії безпеки хмарної середовища.

Політики використовують для моніторингу тенденцій, перегляду загроз безпеки, а також створення звітів, що настроюються і сповіщень. За допомогою політик можна створювати дії системи управління, а також налаштовувати захист від втрати даних і управління загальним доступом до файлів.

Етап 3. Налаштування Cloud Discovery

Основною задачею даного етапу є включення Cloud App Security для перегляду використання хмарних додатків:

1. Забезпечте інтеграцію з ATP в Microsoft Defender, щоб автоматично використовувати Cloud App Security для моніторингу пристроїв Windows 10 в корпоративній мережі і за її межами.

2. При використанні платформи Zscaler її необхідно інтегрувати з Cloud App Security.

3. Щоб домогтися повного покриття, створіть безперервний звіт Cloud Discovery:

1. У меню "*Параметри*", яке викликається значком шестерні, виберіть Параметри Cloud Discovery.

2. Виберіть *Автоматична* відправка журналів.

3. На вкладці *Джерела* даних додайте свої джерела.

4. На вкладці *Збирачі даних журналу* налаштуйте збірник журнальних даних.

Налаштування звітів Cloud Discovery необхідно для видимості тіньових IT в компаніїд уже важлива. Проаналізувавши журнали, можна легко визначити, ким і на яких пристроях використовуються ті чи інші програми.

Етап 4. Індивідуальне налаштування

Основною задачею даного етапу є додавання відомостей про компанію

Введення установок електронної пошти

1. У меню "*Параметри*", яке викликається значком шестерні, виберіть Параметри пошти.

2. У розділі *Посвідчення відправника* листа введіть адреси електронної пошти та псевдонім.

3. У розділі *Дизайн* листа передайте використовуваний організацією шаблон листів.

Налаштування повідомлень адміністратора

1. На панелі навігації виберіть ім'я користувача, а потім перейдіть в розділ *Параметри користувача*.

2. У розділі *Повідомлення* налаштуйте методи, які необхідно задати для системних повідомлень.

3. Виберіть *Зберегти*.

Налаштування метрик оцінки

1. У меню "*Параметри*", яке викликається значком шестерні, виберіть параметри Cloud Discovery.

2. В меню "*Параметри*", яке викликається значком шестерні, виберіть параметри Cloud Discovery.

3. У розділі *Метрики оцінки* налаштуйте важливість різних значень ризику.

4. Виберіть *Зберегти*.

Тепер оцінки ризику, задані для виявлених додатків, налаштовані в точній відповідності з потребами і пріоритетами організації.

Індивідуальні налаштування середовища необхідно для того щоб деякі компоненти працювали найкраще, коли вони налаштовані відповідно потреб. Можливо надавати користувачам поліпшені можливості для роботи за допомогою власних шаблонів електронної пошти. Для цього необхідно визначити, які повідомлення будуть отримуватися, і налаштувати метрику оцінки ризику відповідно до переваг компанії.

Етап 5. Впорядкування даних відповідно потреб

Основною задачею даного етапу є налаштування важливих параметрів.

Створення тегів IP-адрес

1. У меню "*Параметри*", яке викликається значком шестерні, виберіть параметри Cloud Discovery.

2. В меню "*Параметри*", яке викликається значком шестерні, виберіть Діапазони IP-адрес.

3. Клацніть знак "плюс", щоб додати діапазон IP-адрес.

4. Введіть для діапазону IP-адрес відомості, розташування, категорію тегів.

5. Виберіть команду Створити.

Тепер при створенні політик, а також при фільтрації та створення безперервних звітів можна використовувати теги IP-адрес.

Створення безперервних звітів

1. У меню "*Параметри*", яке викликається значком шестерні, виберіть Параметри Cloud Discovery.

2. У розділі *Безперервні* звіти виберіть Створити звіт.

3. Виконайте дії з налаштування.

4. Виберіть команду Створити.

Тепер є можливість переглядати виявлені дані відповідно до власних уподобань, наприклад по бізнес-одиницям або діапазонів IP-адрес.

Додавання доменів

1. У меню "*Параметри*", яке викликається значком шестерні, виберіть Параметри.

2. У розділі *Відомості* про організацію додати внутрішні домени своєї організації.

3. Виберіть *Зберегти*.

Ці параметри забезпечують більш ефективне управління можливостями консолі. За допомогою тегів IP-адрес простіше створювати політики відповідно до своїх потреб, точно фільтрувати дані і багато іншого. Використовувати представлення даних для групування даних по логічним категоріям.

3.2. Технологія виявлення і контролю тіньових IT у мережі

За допомогою Cloud Discovery є можливість виявити використовувані додатки, визначити їх ризик, налаштувати політики для визначення нових ризикованих додатків і зробити ці програми несанкціонованими, щоб вони спочатку блокувалися проксі-сервером або брандмауером.

• Виявлення і визначення тіньових IT

• Оцінка та аналіз

• Управління додатками

• Розширені звіти про виявлення тіньових IT

• Контроль санкціонованих додатків

Розглянемо технологію як виявляти і контролювати тіньові IT у мережі компанії.

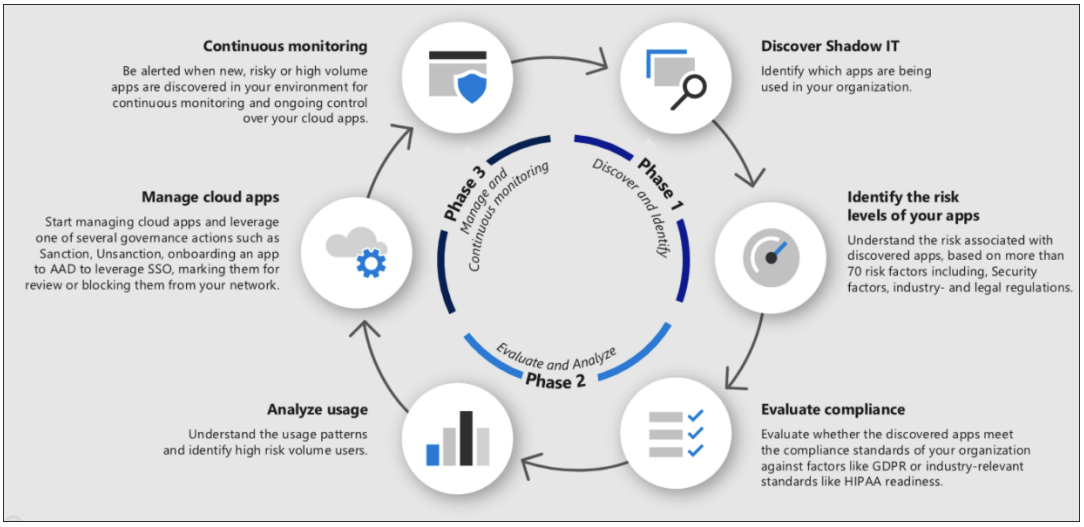

Рис.3.2. Етапи виявлення тіньових IT

Етап 1. Виявлення і визначення тіньових IT

1. *Виявлення тіньових IT*. Використовується Cloud Discovery для оцінки системи безпеки своєї організації - це допомагає дізнатися, що насправді відбувається в мережі. Це можна зробити за допомогою будь-якого з наступних методів:

- Щоб швидко почати роботу з Cloud Discovery, використовуйте інтеграцію з ATP в Microsoft Defender. Початкова підтримка інтеграції дозволяє відразу ж почати збір даних хмарного трафіку на пристроях під управлінням Windows 10 всередині і поза вашої мережі.

- Щоб охопити всі підключені до мережі пристрої, важливо розгорнути збір журналів даних Cloud App Security на брандмауерах та інших проксі-серверах, який буде збирати дані з кінцевих точок і відправляти їх в Cloud App Security для аналізу.

- Інтеграція Cloud App Security з проксі-сервером. Cloud App Security спочатку підтримує інтеграцію з рядом сторонніх проксі-серверів, включаючи Zscaler.

Так як в різних групах користувачів, регіонах і бізнес-групах використовуються різні політики, можливо, є сенс створити для них окремі звіти про тіньові IT. Запустивши Cloud Discovery в своїй мережі, ознайомтеся з створюваними безперервними звітами і панеллю моніторингу Cloud Discovery, щоб отримати повне

уявлення про використовувані у вашій організації додатках. Рекомендується переглядати їх за категоріями, так як часто несанкціоновані програми застосовуються в робочих цілях, якщо потрібна функція в санкціонованих відсутня.

2. *Визначення рівнів ризику додатків*. Каталог хмарних додатків Cloud App Security дозволяє детально аналізувати ризики, пов'язані з кожним виявленим додатком. Каталог ризиків Cloud App Security включає більше 16 000 додатків, які оцінюються більш ніж по 80-ти факторам ризику. Фактори ризику включають як загальну інформацію про програму (в яких регіонах вона використовується, хто його видавець), так і засоби безпеки (підтримка шифрування неактивних даних, журнал аудиту призначених для користувача дій).

- На порталі Cloud App Security в розділі *Виявлення* клацніть *Виявлені* додатки. Відфільтруйте список виявлених додатків в організації, про що цікавлять вас факторам ризику. Наприклад, ви можете використовувати розширені фільтри, щоб знайти всі додатки з оцінкою ризику нижче 8.
- Щоб отримати докладні відомості про фактори ризику безпеки програми, клацніть його ім'я і перейдіть на вкладку *Відомості*.

Етап 2. Оцінка і аналіз.

1. *Оцінка відповідності.* Перевірте, чи сертифіковані додатки які відповідні стандартам вашої організації, таким як HIPAA, SOC2 і GDPR.

На порталі Cloud App Security в розділі *Виявлення* клацніть *Виявлені додатки*. Відфільтруйте список виявлених додатків в організації, які цікавлять вас за фактором ризику відповідності. Наприклад, використовуйте запропонований запит, щоб відфільтрувати додатки, які не відповідають вимогам.

Щоб отримати докладні відомості про фактори ризику відповідності додатки, клацніть його ім'я і перейдіть на вкладку *Відомості.* Дочекайтеся отримання повідомлення, якщо виявлений додаток пов'язаний з нещодавно опублікованими порушенням безпеки, виявлено порушення безпеки програми необхідно виявити всіх

користувачів, IP-адреси і пристрої, які зверталися до уразливого додатка за останні 90 днів, і застосуєте відповідні засоби контролю.

2. *Аналіз використання*. Тепер, коли виявлено, чи варто використовувати додаток в організації, дізнайтеся, хто і як його використовує. Якщо воно використовується тільки в обмеженому ряді випадків, можливо, це нормально. Однак якщо воно застосовується все частіше, то ви напевно захочете знати про це, щоб прийняти рішення про можливе блокування. Для цього:

- На порталі Cloud App Security в розділі *Виявлення* клацніть *Виявлені додатки* і виберіть конкретний додаток для аналізу. На вкладці *Використання* показано, скільки активних користувачів працюють з додатком і скільки трафіку воно створює. З цього ви вже зможете в цілому зрозуміти, що відбувається з додатком. Потім, якщо ви захочете дізнатися, хто конкретно використовує додаток, ви можете розкрити більш докладні відомості, клацнувши *Всіх активних користувачів.* Це важлива дія дасть вам актуальну інформацію: наприклад, якщо ви виявите, що всі користувачі певної програми - з відділу маркетингу, то можливо, такий додаток необхідно організації. Якщо воно пов'язане з високим ризиком, слід запропонувати альтернативу, перш ніж блокувати його.

- Дізнайтеся докладніше про використання виявлених додатків. Переглядайте піддомени і ресурси, щоб дізнатися про конкретні дії, доступі до даних і використанні ресурсів в хмарних службах.

3. Виявлення альтернативних додатків: знайдіть в каталозі хмарних додатків більш безпечні програми, які забезпечують такий же бізнес-функціонал, як у виявлених додатків з ризиком, але на відміну від них відповідають політиці вашої організації. Розширені фільтри дозволять шукати додатки тієї ж категорії, які відповідають різним використовуваним вами параметрам контролю безпеки.

Етап 3. Управління додатками

Управління хмарними додатками. Cloud App Security допомагає контролювати використання додатків у вашій організації. Визначивши в ній типові дії і шаблони

поведінки, ви можете створювати власні теги для класифікації додатків відповідно до їх бізнес-статусом і обгрунтуванням використання. Ці теги потім можна застосовувати для конкретних цілей моніторингу, наприклад для виявлення великих обсягів вхідного трафіку в додатках, позначених тегом хмарного сховища з високим ризиком. Тегами додатків можна управляти в розділі *Параметри Cloud Discovery> Теги додатків.* Надалі ви можете використовувати ці теги для фільтрації на сторінках Cloud Discovery і створювати з їх допомогою політики.

Рекомендується управляти виявленими додатками за допомогою колекції Azure Active Directory (Azure AD): У Cloud App Security також використовується власна інтеграція з Azure Active Directory, яка дозволяє управляти виявленими додатками в колекції Azure Active Directory. Для додатків, які вже відображаються в колекції Azure Active Directory, можна використовувати єдиний вхід і управляти ними за допомогою Azure Active Directory. Для цього знайдіть рядок потрібної програми, клацніть три точки в кінці рядка і виберіть Керувати додатком в Azure Active Directory.

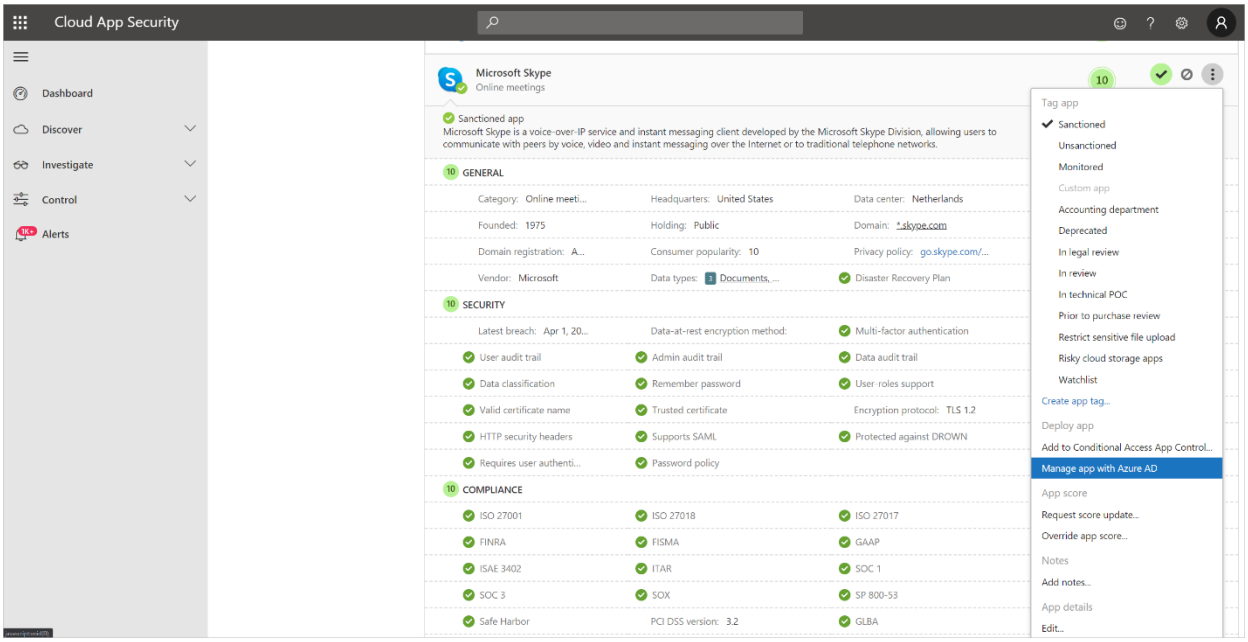

Рис. 3.3. Вікно керування додатками

Безперервний моніторинг. Провівши детальний аналіз додатків, можливо, необхідно створити політики їх моніторингу та необхідні елементи управління.

Тепер прийшов час створити політики, щоб отримувати автоматичні оповіщення про важливі для вас події. Наприклад, ви можете створити політику виявлення додатків, яка буде повідомляти про різке збільшення обсягів скачування або трафіку в сюжеті вашого додатку. Для цього слід включити політики *Незвичайна поведінка* у виявлених користувачів, Перевірка додатків хмарного сховища на відповідність і *Нове ризикований додаток*. Слід також налаштувати політику для повідомлень по електронній пошті або текстовими повідомленнями.

Відкрийте сторінку попереджень і використовуйте фільтр *Тип політики*, щоб знайти попередження виявлення додатків. При виявленні будь-то додатків, відповідних політикам, рекомендуємо провести додатковий аналіз, наприклад зв'язавшись з їх користувачами, щоб отримати обгрунтування їх застосування в організації. Потім повторіть дії на етапі 2, щоб оцінити ризик додатку. Після цього прийміть рішення про подальші дії: затвердите додаток для майбутнього використання або щоб позначити його як несанкціоноване, щоб доступ до нього користувачам блокувався брандмауером, проксі-сервером або захищеним веб-шлюзом.

Етап 4. Розширені звіти про виявлення тіньових IT

Крім установок звіту, доступних в Cloud App Security, є можливість інтегрувати журнали Cloud Discovery в Azure Sentinel для подальшого вивчення і аналізу. Після переміщення даних в Azure Sentinel, можна переглядати їх на панелях моніторингу, виконувати запити за допомогою мови запитів Kusto, експортувати запити в Microsoft Power BI, інтегрувати їх з іншими джерелами і створювати власні оповіщення.

Етап 5: Контроль санкціонованих додатків

1. Щоб увімкнути управління додатками через API, підключіть додатки за допомогою API для безперервного моніторингу.

2. Захист додатоків за допомогою *Управління умовним доступом до додатків*.

Слід пам'ятати, що хмарні додатки щодня оновлюються, і постійно виходять нові хмарні програми. Через це співробітники весь час використовують нові додатки, тому важливо відстежувати, перевіряти та оновлювати ваші політики, а також контролювати, які програми використовують користувачі і як вони з ними працюють. Ви завжди можете відкрити панель моніторингу Cloud Discovery і дізнатися, які нові додатки зараз використовуються, а потім знову виконати етапи для забезпечення захисту вашої організації і її даних.

3.3 Розробка рекомендацій застосування технології забезпечення захищеного доступу до хмарних сервісів Microsoft Cloud App Security

Для ефективного застосування технології забезпечення захищеного доступу до хмарних сервісів корпоративних інформаційних систем фахівцям із кібербезпеки необхідно дотримуватися рекомендацій.

Так, для вибору технології CASB, щодо визначення технології забезпечення доступу до хмарних сервісів необхідно зрозуміти, які саме дані необхідно контролювати, як проводити аналітику для ідентифікації и усунення кіберзагроз у хмарних сервісах Можливість швидкого розгортання та централізоване управління дозволяє управляти хмарними додатками. Для впровадження CASB в корпоративній інформаційній мережі необхідно визначити:

- мету впровадження CASB в компанії;
- роль і місце провайдера при надані хмарних сервісів, з точки зору кібербезпеки;
- визначити типи додатків, які відповідають політиці безпеки компанії.
- проводити постійний моніторинг додатків, які дозволять адміністратору безпеки виявити тіньові IT;
- Виявлення та оцінка хмарних додатків;
- Застосовувати політики управління хмарою;

- Проводити постійну класифікація, маркування і захист конфіденційних даних при зберіганні в хмарі.
- Проводити постійний моніторинг активності користувачів, щодо використовуваних даних.

Виконання цих даних рекомендацій дозволить компанії забезпечити кібербезпеку доступу до хмарних сервісів, які будуть відповідати політиці безпеки компанії, рекомендаціям міжнародних стандартів.

Висновки до розділу 3

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми технологію забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи, встановлена основні завдання щодо їх захисту.

Проаналізовано існуючі технології забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи. Досліджено технологію забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи на базі рішення Microsoft Cloud App Security. Визначено методи та засоби забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи, які реалізовані в Microsoft Cloud App Security.

Встановлено основні функції та принципи роботи програмного комплексу Microsoft Cloud App Security. Визначено архітектуру Microsoft Cloud App Security для розуміння загального стану хмари в додатках SaaS і хмарних сервісах, і тому виявлення тіньових IT і управління додатками є ключовими варіантами використання.

У роботі запропоновано технологію забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи Microsoft Cloud App Security. Для виконання цих завдань використовується Cloud Discovery, який забезпечує динамічне виявлення та аналізу хмарних додатків, які використовує компанія. Розроблено рекомендації фахівцям із кібербезпеки щодо застосування технології забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи.

Таким чином, правильна реалізація технології забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи на базі рішення Microsoft Cloud App Security має забезпечити ефективний захист корпоративних даних та кібербезпеку корпоративної інформаційної системи підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1 Інтернет ресурс. Хмарні сервіси на базі Microsoft для бізнесу [Електронний ресурс] режим доступу: https://www.lankey.ru/oblachnie-servisi/ .

2. Інтернет ресурс. CASB [режим доступу https://www.anti-malware.ru/analytics/Market_Analysis/cloud-access-security-broker].
3 CASB A Complete Guide - 5STARCooks (September 29, 2019)- 2020. – 302p.

4. Cloud Access Security Broker A) Complete Guide - 5STARCooks (September 6, 2019)– 2020. – 298p.

5. Using Oracle CASB Cloud Service., Release 20.1.1.0 [Електронний ресурс] режим доступу: https://www.lankey.ru/oblachnie-servisi - Oracle - July 2020 -727p

6. Осьмак Д.П. Технологія забезпечення захисту хмарних сервісів на базі рішення Microsoft Cloud App security [Електронний ресурс]. - Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки».- Київ, ДУТ.- с. 129-132[режим доступу:http://www.dut.edu.ua/uploads/p_1739_27992763.pdf]

7. Charles J. Brooks, Philip R. Craig, Donald ShortCybersecurity Essentials. – SYBEX. 2018. – 450p.

8. Chris Moschovitis Cybersecurity Program Development for Business: The Essential Planning Guide. – WILEY. 2018.- 224p.

9. Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams, Abdul Aslam Enterprise Cybersecurity Study Guide. – 2018. – 737p.

10. Implementing the NIST Cybersecurity Framework. – ISACA. – 2016.- 108p.

11. Стандарт NIST SP 500-292 NIST Cloud Computing Reference Architecture [Електронний ресурс] режим доступу: https://bigdatawg.nist.gov/_uploadfiles/M0008_v1_7256814129.pdf.

SP 800-145

12. Стандарт NIST: The NIST Definition of Cloud Computing [Електронний ресурс] режим доступу: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

13. Технічна документація: Microsoft Cloud App Security overview [електронний ресурсъ режим доступу:]https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)