ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«Технологія захисту інформаційної системи компанії на базі хмарних сервісів»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Стрічко Сергій Сергійович
(прізвище та ініціали)
Керівник Дмітрієв В.Є.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"___"_____ 2021 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Стрічко Сергія Сергійовича
(прізвище, ім'я, по батькові)

1. Тема магістерської роботи:
Технологія захисту інформаційної системи компанії на базі хмарних сервісів

керівник магістерської роботи Дмітрієв В.Є., ст.викладач
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «11» жовтня 2021 року №170.

2. Строк подання студентом магістерської роботи 15.12.2021 р.

3. Вихідні дані до магістерської роботи
Корпоративна інформаційна система;
Хмарні сервіси;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблеми забезпечення управління захистом інформаційної системи компанії на базі хмарних сервісів.
2. Дослідження методів та засобів управління безпекою хмарних сервісів.
3. Технологія управління доступом на базі хмарних сервісів.

5. Перелік графічного матеріалу

1. Тема магістерської роботи.

2. Об’єкт, предмет, мета та наукові завдання дослідження.

3. Результати аналізу підходів та змісту захисту інформаційної системи компанії на базі хмарних сервісів.

4. Результати аналізу методів та засобів управління захистом інформаційної системи компанії на базі хмарних сервісів

5. Варіанти реалізації управління захистом інформаційної системи компанії на базі хмарних сервісів.

6. Рекомендації щодо застосування методів та засобів управління захистом інформаційної системи компанії на базі хмарних сервісів

7. Висновки за результатами роботи.

6. Дата видачі завдання 15.02.2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми управління захистом інформаційної системи компанії на базі хмарних сервісів.	15.02.2021 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	15.03.2021 р.	
3.	Аналіз методів та засобів управління захистом інформаційної системи компанії на базі хмарних сервісів.	12.04.2021 р.	
4.	Розроблення рекомендацій щодо управління захистом інформаційної системи компанії на базі хмарних сервісів.	15.05.2021 р.	
5.	Оформлення результатів дослідження.	22.05.2021 р.	
6.	Підготовка доповіді до захисту.	28.05.2021 р.	

Студент _____ Стрічко С.С.
(підпис) прізвище та ініціали

Керівник магістерської роботи _____ Дмітрієв В.Є.
(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА
на магістерську роботу

студента Стрічко Сергія Сергійовича
на тему: Технологія захисту інформаційної системи компанії на базі хмарних сервісів

Актуальність: Використання хмарних сервісів компаніями сьогодні стає все більш популярним. Це пов'язано з можливістю підвищення ефективності виконання бізнес-процесів компанії, зменшення витрат на підтримку власної інфраструктури. Але такий перехід у хмари, вимагає інші підходи для забезпечення роботи та доступу до хмари, де зберігаються данні копманії. Тому тема магістерської роботи, щодо управління захистом інформаційної системи на базі хмарних сервісів є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу в роботі було визначено підходи управління захистом інформаційної системи компанії на базі хмарних сервісів.
2. Досліджено методи та засоби управління захистом інформаційної системи компанії на базі хмарних сервісів».
3. Розроблення рекомендацій щодо застосування методів та засобів управління захистом інформаційної системи компанії на базі хмарних сервісів».
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. У бакалаврській роботі бажано було б визначити більш детально методи автентифікації до хмарних сервісів користувачів інформаційної системи компанії.
2. У роботі не завжди застосовуються посилання на використані джерела інформації.

Висновок: Враховуючи недоліки, магістерська робота заслуговує оцінку **добре**, а студент **Стрічко С.С.** присвоєння кваліфікації: магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

Підпис засвідчую
Підпис особи, що засвідчує (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент **Стрічко С.С.** до захисту магістерської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія захисту інформаційної системи компанії на базі хмарних сервісів»
Магістерська робота і рецензія додаються.

Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Стрічко С.С. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2020 року по 2022 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту, факультету (відділення) _____ Журенко О.В.
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студент **Стрічко С.С.** обрав тему роботи, метою якої було дослідження методів та засобів управління захистом інформаційної системи компанії на базі хмарних сервісів. Перелік використаних джерел свідчить про вміння студентом розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Муренк М.В. показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану магістерську роботу студента Стрічко С.С. на оцінку **«добре»** та присвоїти йому кваліфікацію: магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

.

Керівник магістерської роботи _____ Дмітрієв В.Є.
(підпис) (прізвище та ініціали)
“____” _____ 2021 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент Муренко М.В.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

“____” _____ 2021 року

РЕФЕРАТ

Текстова частина магістерської роботи: 50 сторінок, 12 рисунків, 7 джерел.

Об'єкт дослідження – процес управління захистом інформаційної системи компанії на базі хмарних сервісів.

Предмет дослідження – технологія управління захистом інформаційної системи компанії на базі хмарних сервісів.

Мета роботи – розробити технологію та рекомендації щодо застосування методів та засобів управління захистом інформаційної системи компанії на базі хмарних сервісів.

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

В роботі проведено аналіз використання хмарних сервісів для підвищення ефективності виконання бізнес-процесів компанії. На основі отриманих результатів визначено вимого до архітектури безпеки хмарних технологій міжнародних стандартів. В результаті було запропоновано методи та засоби щодо управління захистом інформаційної системи компанії на базі хмарних сервісів.

В роботі запропоновано рішення щодо управління захистом доступу на базі хмарних сервісів Netskope. Для даного рішення визначено архітектуру, вимоги та функціональні можливості. На основі проведеного дослідження розроблено рекомендації щодо управління захистом інформаційної системи компанії на базі хмарних сервісів.

Галузь використання – кібербезпека хмарного доступу.

ІНФОРМАЦІЙНА СИСТЕМА, ЗАГРОЗИ, ХМАРНІ СЕРВІСИ, ВИТОК АРХІТЕКТУРА, ФУНКЦІЇ, CASB, ДАНІ, МЕТОДИ ТА ЗАСОБИ, ШИФРУВАННЯ, ФОРМАТ, GPDR, ЗАКОН ЗАХИСТ, МЕТОДИ ТА ЗАСОБИ

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІТ – інформаційні технології

ПЗ – програмне забезпечення

GPDR – General Data Protection Regulation

NIST – National Institute of Standards and Technology

NAC - Network Access Control

CSP – постачальник хмарних послуг

CASB - Брокер безпеки хмарного доступу

ВСТУП

Актуальність дослідження. Наслідки поширення хмарних і мобільних пристроїв означають, що дані і користувачі знаходяться за межами локальної інфраструктури безпеки. Там, де успадковані системи безпеки могли ефективно контролювати трафік локальної мережі, CASB взяли на себе моніторинг і аутентифікацію доступу в хмарі для користувачів корпоративної інформаційної системи.

Оскільки організації впровадили віддалену роботу і дозволили персональні пристрої (BYOD) для персоналу, хмара пропонує відкритий доступ до некерованих або несанкціонованим пристроїв, які користувач може аутентифікувати. Все викликає вразливість системи безпеки, оскільки дані, які зберігаються у відповідних хмарних додатках, можуть бути завантажені без особливих зусиль. Без CASB отримання прозорості безлічі точок доступу є серйозною перешкодою на шляху підвищення безпеки. Тому застосування технологій CASB при переході компаній у хмари є самим надійним засобом для збереження конфіденційної, комерційної інформації. Тому тема магістерської роботи щодо забезпечення безпеки хмарних сервісів є своєчасною та актуальною.

Об'єкт дослідження – процес управління захистом інформаційної системи компанії на базі хмарних сервісів.

Предмет дослідження – технологія управління захистом інформаційної системи компанії на базі хмарних сервісів.

Мета роботи – розробити технологію та рекомендації щодо застосування методів та засобів управління захистом інформаційної системи компанії на базі хмарних сервісів.

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

Завдання магістерської роботи:

провести аналіз вимог управління захистом інформаційної системи компанії на базі хмарних сервісів;

проаналізувати основні загрози використання хмарних сервісів;

визначити методи та засоби управління захистом інформаційної системи компанії на базі хмарних сервісів.;

дослідити архітектуру та функції управління захистом інформаційної системи компанії на базі хмарних сервісів;

розробити рекомендації управління захистом інформаційної системи компанії на базі хмарних сервісів.

Практичне значення одержаних результатів: рекомендації щодо управління захистом інформаційної системи компанії на базі хмарних сервісів. можуть бути використані у сфері забезпечення кібербезпеки.

Апробація результатів: результати магістерської роботи доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки».

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЙНОЇ СИСТЕМИ КОМПАНІЇ НА БАЗІ ХМАРНИХ СЕРВІСІВ

1.1. Аналіз застосування хмарних сервісів в інформаційні системі компанії

Використання хмарних сервісів дозволяє співробітникам виконувати свою роботу швидше, простіше і гнучкіше, ніж традиційні інструменти. Ось кілька причин, за якими будь-яка організація повинна подумати про використання хмари:

Гнучкість бізнесу: люди хочуть працювати продуктивно зараз; Вони не хочуть чекати наступного випуску програмного забезпечення. Багато хмарні сервіси випускаються частіше ніж традиційне програмне забезпечення, що дозволяє компанії, щоб скористатися новітніми функціями.

Вибір пристрою: хмара дає людям гнучкість працювати на будь-якому пристрої - настільному комп'ютері, ноутбуці, планшеті або смартфоні - в будь-який час і в будь-якому місці .

Співпраця: хмара дозволяє колегам і бізнес-партнерам безперешкодний обмін даними і доступ до них.

Мінімальні витрати: розгортання, підтримка і оновлення локального програмного забезпечення може бути дорогим. Можливість зменшити витрати на ведення бізнесу, а також більш точну відповідність витрат можна використовуючи хмарні сервіси.

Хмарні сервіси (public cloud services) - це програми і платформи, які «живуть» і працюють на серверах хмарних провайдерів. Головна особливість хмарних додатків полягає в тому, що створивши акаунт на такій платформі, користувач може отримувати доступ до необхідної інформації з будь-якого пристрою в будь-якій точці світу. Для цього необхідно створити логін і пароль. Використовувати хмарні служби не тільки зручно, але й безпечно. Так якщо з телефоном або комп'ютером щось трапиться, дані не зникнуть.

Схожа ситуація і з бізнесом. Принцип роботи хмарних платформ досить проста. Хмарне сховище надається користувачеві в необхідному обсязі, оплачується за фактом використання і позбавляє від необхідності купувати власну IT-інфраструктуру для зберігання даних і керувати нею. Це забезпечує гнучкість, швидку масштабованість і надійність. Наприклад, зберігати необхідну програму в хмарному сховищі набагато безпечніше, ніж на сервері, який знаходиться під столом в офісі. Сервер може вийти з ладу, заразитися вірусом, або взагалі перестати працювати. А в період більшого попиту на ресурси компанії, власник може просто замовити більше ресурсів у хмарного провайдера і не переживати, що сайт «ляже».

Хмарні сховища даних дозволяють розміщувати і зберігати великий об'єм інформації, на відміну від традиційних серверів і ПК.

Для надання послуг хмарних сервісів існують моделі.

Хмарні оператори виділяють три найбільш поширені з них:

IaaS (Infrastructure as a Service - інфраструктура як послуга) - надання замовнику в оренду обчислювальних ресурсів у вигляді віртуальної інфраструктури.

PaaS (Platform as a Service - Платформа як Послуга) - клієнт отримує повноцінну віртуальну платформу з різними інструментами та сервісами.

SaaS (Software as a Service - програмне забезпечення як Послуга) - клієнт отримує в своє розпорядження певні програмні продукти за допомогою мережі інтернет.

Розглянемо хмарні сервіси для бізнесу.

Хмарні корпоративні сервіси допомагають вирішувати найрізноманітніші завдання. Наприклад, побудувати віртуальну IT-інфраструктуру, розгорнути резервне сховище даних, запускати власні програми та багато іншого. Для того щоб підібрати оптимальні хмарні рішення, потрібно розуміти, які саме продукти пропонуються зараз на цьому ринку.

Основними видами хмарних сервісів є:

Віртуальний сервер

Це є найпоширеніший тип. Доступ до обчислювальних ресурсів, дискового простору і операційній системі. Скориставшись цією послугою, компанія уникне витрат на закупівлю та обслуговування фізичних серверів. Тобто, компанія орендуєте практично скільки завгодно хмарних обчислювальних ресурсів на будь-який час.

Приватна хмара для бізнесу

Орендувавши сервер, компанія можете почати роботу з панеллю керування (наприклад, vCloud Director) на машині з потрібними їй характеристиками і операційною системою. Фактично цей віртуальний сервер працює на фізичному обладнанні хмарного провайдера, разом з безліччю інших. Якщо компанії необхідно збільшити обчислювальні потужності, це можна зробити за невеликий час, зробивши необхідне замовлення у провайдера.

Використання такої послуги буде дешевше і зменьшаться витрати на резервне копіювання.

Використання віртуальної інфраструктури значно зменшить фінансові витрати компанії на виконання своїх бізнес процесів.

Хмарне сховище

Тут є можливість отримати доступ до системи зберігання даних (СЗД), яка дасть можливість завантажувати, видаляти і сортувати файли будь-якого формату. Тобто, це особиста мережева папка, з якої є можливість робити все те ж саме, що і з папками на своєму комп'ютері. Якщо не вистачатиме місця, можна оперативно збільшити його обсяг до потрібного. Крім того, ці ресурси можна використовувати, для зберігання резервних копій (бекапів). Тут є можливість самостійно вирішувати, яка частота резервного копіювання буде комфортною. У разі проблем є можливість відновити всі з хмарні копії.

Середовище для розробки ПО

Ще один вид хмарних сервісів - платформні. Вони можуть включати готові бази даних (БД) і системи управління ними (СУБД), засоби розробки,

балансувальник навантаження, середовище запуску контейнеризованих додатків, інструменти бізнес-аналітики та інше. З їх допомогою можливо повноцінно розробити, протестувати і розгорнути додаток, а потім оновлювати його.

Висока доступність, підтримка безлічі користувачів і масштабування платформних сервісів підвищує ефективність розробки. Крім того, при використанні не буде проблем з ліцензіями на необхідне програмне забезпечення. Всі ці питання вирішує хмарний провайдер і його робота повністю легальна. Засоби розробки скоротять час на запуск нових додатків, тому що безліч компонентів вже вбудовані в платформу. Деякі провайдери можуть дати вам середовище розробки не для однієї, а для безлічі платформ, наприклад, для мобільних і на базі браузера. Таким чином, процес створення нових додатків стане ще зручніше і швидше. Приклади таких сервісів - IBM Bluemix, Heroku, Google App Engine.

Додатки в хмарі

Це повноцінне програмне забезпечення, спочатку створене для спільної роботи без прив'язки до місця і обладнання. Користувачі підключаються до них через інтернет, як правило, за допомогою браузера. Вся інфраструктура знаходиться в центрі обробки даних провайдера. Стабільна робота веб-додатків - його зона відповідальності.

Використання цих додатків підвищує і мобільність роботи, тому що ці продукти доступні практично звідки завгодно, єдина умова - постійне інтернет-підключення. Це хороша технічна база для створення ефективно працюючої розподіленої команди.

Таким чином, робота з цими програмами буде набагато дешевше, ніж покупка ліцензій для кожної машини окремо. До цього типу належать усі популярні сервіси для роботи, які запускаються в хмарі - Gmail, Google Docs, Trello, а також корпоративне ПО: SimpleOne, Microsoft Office 365, 1С в хмарі і багато інших.

Тому виділимо переваги використання хмарних сервісів.

По перше не потрібно думати про обслуговування. Створення та обслуговування IT-інфраструктури, її безпеку, надійність і працездатність - завдання хмарного провайдера.

Незалежно від того, яку модель буде обрано (може вийти декілька), ваші корпоративні дані зберігаються в хмарі, тому є ризик отримати доступ несанкціонованих користувачів до корпоративних даних.

Тому при використанні хмари, необхідно розглянути можливість створення чітких політик запобігання втраті даних у хмарі (DLP), які допоможуть керувати тим, що зберігається в хмарі, як вони зберігаються та що залишається на місці.

1.2. Аналіз вимог до безпеки хмарних сервісів

Еталонна архітектура хмарних обчислень NIST - це загальна концептуальна модель високого рівня, яка є потужним інструментом для обговорення вимог, структур і операцій хмарних обчислень. Модель не прив'язана ні до яких конкретних продуктів, послуг або еталонної реалізації постачальника і не визначає розпорядчих рішень, що перешкоджають інноваціям. Вона визначає набір суб'єктів, дій і функцій, які можуть використовуватися в процесі розробки архітектури хмарних обчислень. Вона містить набір представлень і описів, які є основою для описаних характеристик щодо використання стандартів хмарних обчислень.

Еталонна архітектура хмарних обчислень NIST фокусується на вимогах до хмарних послуг. Вона описує операційні тонкощі хмарних обчислень.

Побудова еталонної архітектури хмарних обчислень NIST необхідна для розуміння різних хмарних сервісів в контексті загальної концептуальної моделі хмарних обчислень;

Еталонна архітектура описує п'ять основних учасників з їх ролями та обов'язками, що використовують хмарні обчислення. Еталонна архітектура хмарних обчислень NIST визначає п'ять основних дійових осіб (рис 1.1):

споживач хмари,

постачальник хмари,

хмарний сервіс.

аудитор,

хмарний брокер і хмарний оператор.

Ці ключові люди грають ключову роль в сфері хмарних обчислень. Кожен суб'єкт - це об'єкт (людина або організація), який бере участь в транзакції або процесі і / або виконує завдання в хмарних обчисленнях.

Наприклад, споживач хмари - це фізична особа або організація, які набувають і використовують хмарні продукти і послуги.

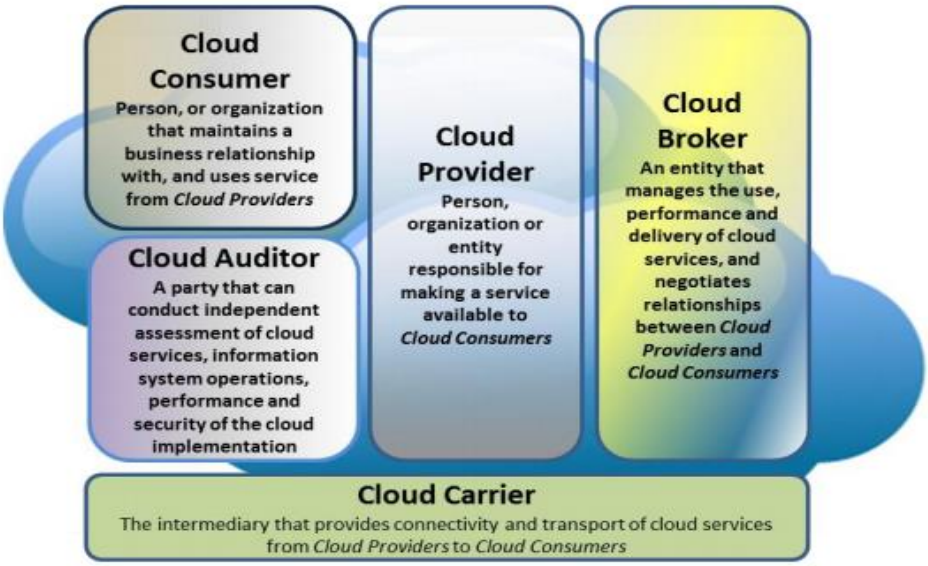

Рис. 1.1. Дійові особи хмарних обчислень [1]

Постачальником продуктів і послуг є постачальник хмарних послуг.

Використання різних пропозицій послуг (програмне забезпечення, платформа або інфраструктура), дозволених постачальником хмарних послуг, може відбутися зміщення у рівні відповідальності за деякі аспекти обсягу контролю, безпеки і конфігурації (рис 1.2).

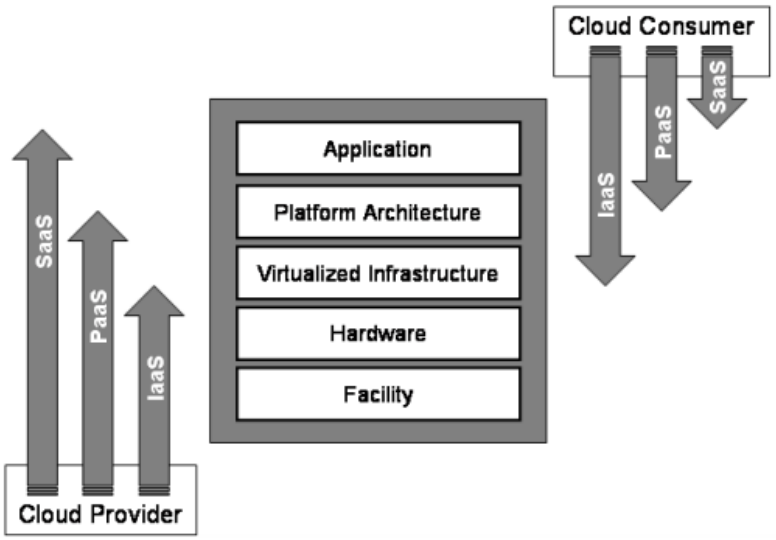

Рис.1.2. Рівні відповідальності

Так хмарний брокер виступає в якості посередника між споживачем і постачальником і допомагає споживачам долати складнощі пропозицій хмарних послуг, а також може створювати хмарні послуги з доданою вартістю.

Cloud Auditor забезпечує цінну невід'ємну функцію для уряду, проводячи незалежний моніторинг продуктивності і безпеки хмарних сервісів.

Хмарний постачальник - це організація, яка несе відповідальність за передачу даних, щось на зразок розподільника енергії в електромережі.

На рис. 1.3. показано взаємодію між дійовими особами в хмарних обчисленнях NIST. Споживач хмар може отримувати хмарні послуги у хмарного провайдера безпосередньо або через хмарного брокера. Хмарний аудитор проводить незалежний аудит і може зв’язатися з іншими для збору необхідної інформації.

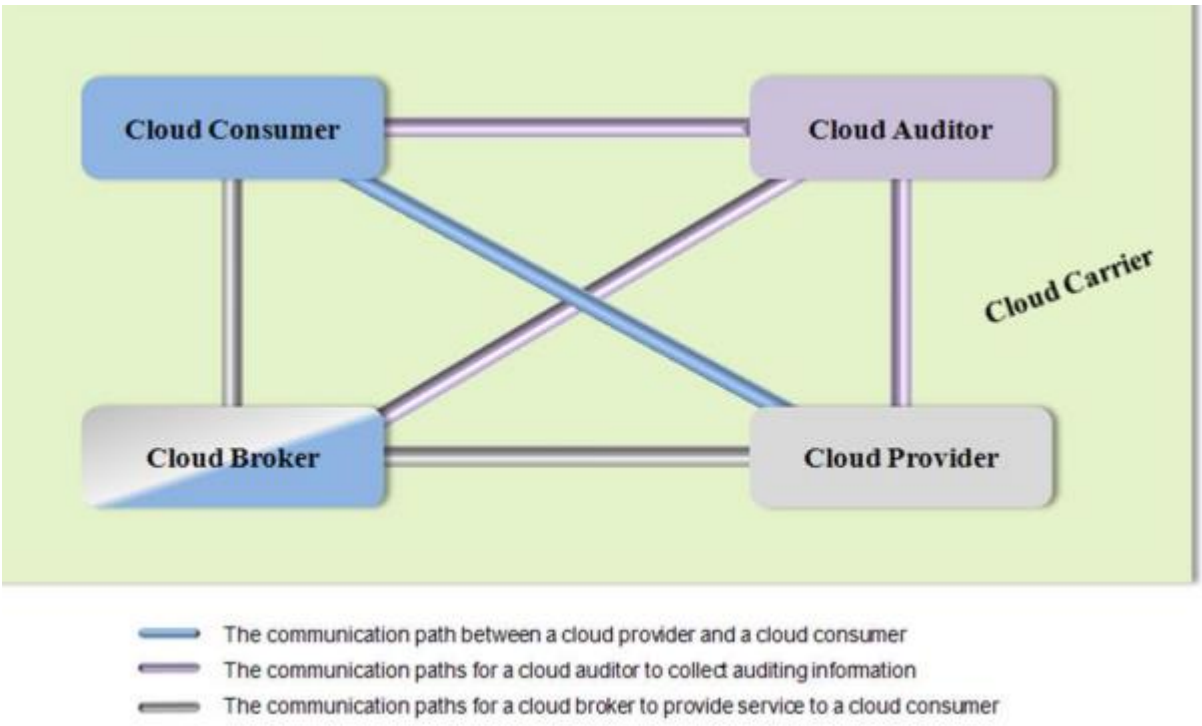

Рис. 1.3. Взаємодія між дійовими особами хмарних обчисленнях NIST [1]

Таким чином використання хмарних сервісів вимагають від компаній приділяти велику увагу безпеці своєї корпоративної інформаційної системи.

1.3. Аналіз загроз безпеці хмарного середовища

Як було вже сказано, компанії все частіше переходять до хмари, і використовують хмарні інфраструктури. Все це призводить до того, що зростаючий обсяг чутливих даних і функціональні можливості переходять до хмари. Тому хмарна безпека стає все більш важливою для забезпечення кібербезпеки організації.

Згідно Cloud Cloud Alliance за 2019 рік визначено одинадцять загроз безпеці хмари.

Порушення даних - пов'язано з тим, що компанії переміщують велику кількість своїх даних в хмару. Саме ці хмарні дані стають метою для кіберзлочинців.

Невірне налаштування конфігурації та недостатній контроль таких змін. Проблеми з невірною конфігурацією є головною причиною появи порушенн в хмарних даних. Хмарне середовище достатньо відрізняється від локально розгорнутих мереж, і організації, які переміщують свої сховища даних в хмару, як правило не завжди вірно налаштовують параметри безпеки, які надані постачальником хмарних послуг (CSP). Як результат, конфіденційні дані потрапляють туди, де їх можна легко отримати.

Відсутність стратегії та архітектури хмарної безпеки.

При переміщенні своєї архітектури до хмари багато організації думають, що їх інструменти, політики та стратегії безпеки будуть працювати так само, як і в локальній інфраструктурі. Однак архітектура хмари показує, що організації просто зменшили видимість інфраструктури і їм необхідно налаштувати специфічні для хмар контроль безпеки, що надаються їх постачальниками хмар. Невдало розроблена стратегію безпеки збільшує ймовірність того, що важливі елементи керування та налаштування конфігурації інформаційної системи будуть не помічені, що відкриє організацію для проведення атаки.

Недостатня особистість, довіреність, доступ та керування ключами

Хмара розроблена так, щоб бути більш доступною, ніж локальна інфраструктура. Вона знаходиться за мережним периметром організації та має бути доступною через Інтернет. Тому, управління доступом до хмарної інфраструктури дуже важливе. Викрадені дані користувача можна використати для отримання прямого доступу до хмарних ресурсів компанії.

Викрадення рахунку

У хмарі облікові записи хмарних служб та записи мають відповідні дозволи. Зловмисник, який зможе отримати доступ до облікових даних або записів, зможе отримати повний контроль над програмами та даними, що містяться в хмарномій інфраструктурі компанії.

Внутрішня загроза. Приблизно 60% випадків хмарної безпеки пов'язано з інсайдерськими загрозами. У більшості випадків працівник може піддати дані організації загрозі за необережністю.

Небезпечні інтерфейси та API. Як і всі API, хмарні API розроблені для викриття внутрішньої функціональності системи, що дозволяє користувачам взаємодіяти з нею з мінімальними витратами. Якщо не забезпечити доступ до API, система може бути атакована, оскільки несанкціоновані користувачі можуть здійснювати масовий збір даних.

Слабка контрольна площина. Площина управління в хмарі призначена для того щоб забезпечити власнику хмарної інфраструктури повний контроль над операціями в ній. Якщо організація використовує хмарні ресурси зі слабкою або не налаштованою площиною управління, вона не буде мати повний контроль над її операціями.

Обмежена видимість використання хмар

Ця загроза виникає, коли організації не мають загальну видимість операцій, що виконуються в їх хмарній інфраструктурі. Законні користувачі можуть використовувати несанкціоновані програми в хмарній інфраструктурі організації (або тіньові IT).

Зловживання та нечесне використання хмарних сервісів

Кіберзлочинці все частіше використовують хмару інфраструктуру з метою впровадження та запуску своїх атак. Оскільки такі атаки приходять з домену CSP, вони здаються законними. Тому організаціям необхідно розгортати рішення безпеки, які можуть переглядати попередні доменні імена та визначати хороший або зловмисний трафік.

1.4. Визначення методів та засобів управління захистом інформаційної системи компанії на базі хмарних сервісів

На сьогодні IT-відділи мають обмежену видимість щодо хмарних сервісів, особливо з "тіньовими IT". Вони не мають ефективного способу відстежувати використання служб або контролювати конфіденційні дані після їх завантаження. Щоб подолати цю проблему в безпеці, можна використати брокерів безпеки хмарного доступу (CASB).

Перевага CASB полягає в тому, що це дозволяє організації використовувати хмару без шкоди для безпеки або відповідності стандартам кібербезпеки.

Поєднуючи функції безпеки в межах однієї точки забезпечення для всіх хмарних служб, CASB різко зменшують складність захисту даних у хмарі.

Для безпечного переходу на хмарні технології, компаніям доцільно використати брокерів безпеки хмарного доступу.

Брокер безпеки хмарного доступу (CASB) (іноді вимовляється як cas-bee) - це локальне або хмарне програмне забезпечення, яке розміщуються між користувачами хмарних сервісів і хмарними додатками і може відстежувати всі дії і забезпечувати дотримання політик безпеки компанії. CASB пропонує різні послуги, які можуть включати моніторинг активності користувачів, попередження адміністраторів про потенційно небезпечних діях, забезпечення дотримання політики безпеки і автоматичне запобігання шкідливих програм, пошук тіньових додатків, тощо..

Використання CASB може забезпечити безпеку та управління хмарною інфраструктурою компанії. Тобто забезпечити, «безпеку» - як запобігання подій високого ризику, та «управління» - моніторинг і пом'якшення подій високого ризику.

Брокери, які забезпечують безпеку, знаходяться між користувачем і хмарою. З архітектурної точки зору це може бути досягнуто за допомогою проксі-агентів на кожному граничному пристрої або без агента без будь-якої конфігурації на кожному пристрої. Безагентний CASB забезпечує швидке розгортання і

забезпечує безпеку на всіх пристроях, керованих компанією або некерованих BYOD. Безагентний CASB також використовує конфіденційність користувачів, перевіряючи лише корпоративні дані. CASB на основі агентів складний в розгортанні і ефективний тільки на пристроях, керованих корпорацією. Агентський CASB зазвичай перевіряє як корпоративні, так і особисті дані.

CASB, які забезпечують управління, можуть використовувати API для перевірки даних і активності в хмарі, щоб попередити про ризикові події після події. Інша можливість управління CASB полягає в перевірці журналів брандмауера або проксі-сервера на предмет використання хмарних додатків.

Згідно з дослідженнями. Gartner – CASB є важливим елементом стратегій хмарної безпеки, який допомагає керівникам служб безпеки та управління ризиками відкривати хмарні сервіси і оцінювати ризики хмарних обчислень. Вони виявляють і захищають конфіденційну інформацію, виявляють і усувають загрози, а також забезпечують ефективне управління хмарою і дотримання нормативних вимог.

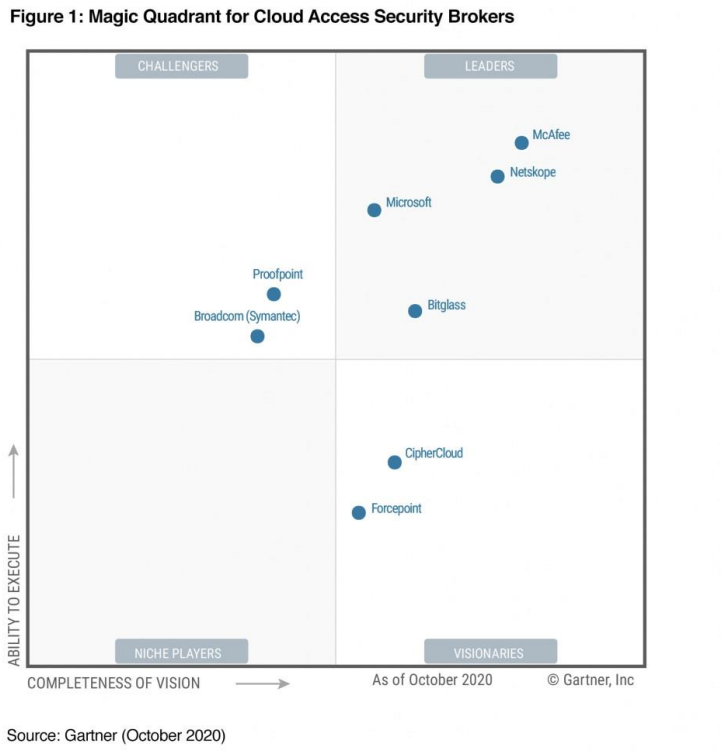

Рис. 1.4. Gartner Magic Quadrant CASB

До квадранту увійшли такі компанії як:

- Bitglass;
- Broadcom (Symantec);
- CipherCloud;
- Forcepoint;
- McAfee;
- Microsoft;
- Netskope.

Проведемо аналіз щодо переваг та недоліків даних технологій.

Netskope - постачальник засобів безпеки, який прискорює процес цифрової трансформації за допомогою перевіреної платформи безпеки, орієнтованої на дані, інтелектуального хмарного середовища. Netskope простий у використанні і має технічну підтримку.

Переваги:

Покращує компліанс і управління ризиками

Підтримка безпека і управління

До недоліків можна віднести що дане рішення дороге.

Netskope має найвищий рейтинг в нашому аналізі і вийшла на перше місце в таких областях за рахунок здатності виявляти і управляти хмарними додатками, як керованими, так і некерованими. Шлюзи безпеки допомагають запобігти витоку конфіденційних даних небезпечними інсайдерами або кіберзлочинцями, які проникли за периметр безпеки.

Підхід, орієнтований на дані, прийнятий в Netskope Security Cloud, дозволяє забезпечувати видимість і захист даних в реальному часі від загроз щоразу, коли будь-який ПК або мобільний пристрій підключається до хмари.

McAfee MVISION відповідає вимогам, управління фінансовими, репутаційними ризиками і захисту інтелектуальної власності.

Переваги:

Високі рейтинги щодо виявлення аномалій, автоматизації та інтелекту.

Недоліки: досить складна у розгортанні.

Що стосується вартості, McAfee MVISION знаходиться на одному рівні з Proofpoint і Cisco CloudLock, і відразу після Netskope. Виходячи з організації, відомої своїми пропозиціями щодо захисту від вірусів і безпеки, MVISION приділяє першочергову увагу безпеці, аналізу загроз і штучного інтелекту (AI). Кінцеві точки і хмарна безпеку MVISION захищають дані за рахунок централізованого управління і узгодження аналітики, автоматизації та аналізу загроз.

Пропозиція CASB, заснована на глибокому розумінні, забезпечується майже мільярдом датчиків по всьому світу, а сучасна аналітика забезпечує одні з кращих інтелектуальних можливостей.

Cisco Cloudlock. Забезпечує надійну безпеку в поєднанні з простотою розгортання робить Cisco Cloudlock.

Cisco Cloudlock хмарне рішення CASB, яке використовує API для управління ризиками. Cisco використовує алгоритми машинного навчання для виявлення будь-яких аномалій на основі набору факторів і дій, щоб запобігти будь-якій загрозі для хмарної інфраструктури. Технологія запобігання витоку даних (DLP) постійно відстежує хмарне середовище. Брандмауер Cloudlock Apps гарантує, що всі хмарні додатки, підключені до корпоративної IT-інфраструктури, регулярно виявляються і контролюються.

Переваги:

забезпечує надійну безпеку;

легкість розгортання;

автоматизація процесів.

До недоліків можна віднести, що відповідність і видимість можуть бути краще.

Bitglass забезпечує надійнубезпеку, управління і унікальний підхід до захисту хмарного середовища.

Bitglass - це хмарний CASB, який можна розгорнути в контейнері докерів для задоволення вимог локального клієнта. Він поєднує в собі підходи прямого і зворотного проксі-сервера і API, а його зворотний проксі-сервер на основі

браузера без агента допомагає відловлювати загрози, які можуть бути пропущені мережевими зворотними проксі-серверами. Bitglass підтримує мобільні і некеровані пристрої, включаючи можливості управління мобільними пристроями.

Переваги:

Унікальний безагентний підхід на основі браузера;

Забезпечення безпеки і управління;

Технічна підтримка.

Як недолік, розгортання може бути складним завданням.

Proofpoint пропонує надійний захист і функціональність.

Proofpoint прагне задовольнити потреби клієнта з обмеженим бюджетом. Пропозиція CASB захищає основні хмарні пропозиції і гарантує, що підприємства отримують орієнтовану на людей видимість і контроль над хмарними додатками. Інструмент дозволяє підприємствам структурувати рівні доступу до користувачів і сторонніх додатків на основі виявлених параметрів ризику. Одне з найважливіших переваг Proofpoint - детальний огляд інформації про користувачів і будь-яких ризиків для даних. Інсайти поділяються на три класи: глобальний, призначений для користувача і рівень додатків. Протокол CASB пропонує контроль для управління підозрілими входами в систему, діями і попередженнями DLP.

Переваги:

легкість розгортання;

забезпечення безпеки;

технічна підтримка.

Як недолік виділено, що керування звітами користувачів може бути складним завданням.

Fortinet FortiCASB забезпечує надійну безпеку.

Fortinet піддалася більш незалежному тестуванню, ніж більшість постачальників засобів забезпечення безпеки, тому не дивно, що FortiCASB зайняв перше місце в рейтингу «Виявлення та реагування». Користувачі також позитивно оцінюють продуктивність компанії, відповідність вимогам, видимість і

загальні можливості. Підтримка вище середнього, а розгортання - приблизно середнє. Єдина область, в якій компанія відстає, - це ціна.

Тож для подальших досліджень та розробки рекомендацій захисту хмарних сервісів надамо перевагу Netskope, яка має самий високий рейтинг.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ БЕЗПЕКОЮ ХМАРНИХ СЕРВІСІВ

2.1. Роль і місце Netskope CASB в забезпеченні хмарної безпеки

Розглянемо архітектуру та принцип роботи CASB.

Рішення CASB рогортається в хмарному середовищі та контролює взаємодію користувачів та додатоки через API та / або проксі-сервер. Також існує можливість використання локальних та гібридних режимів.

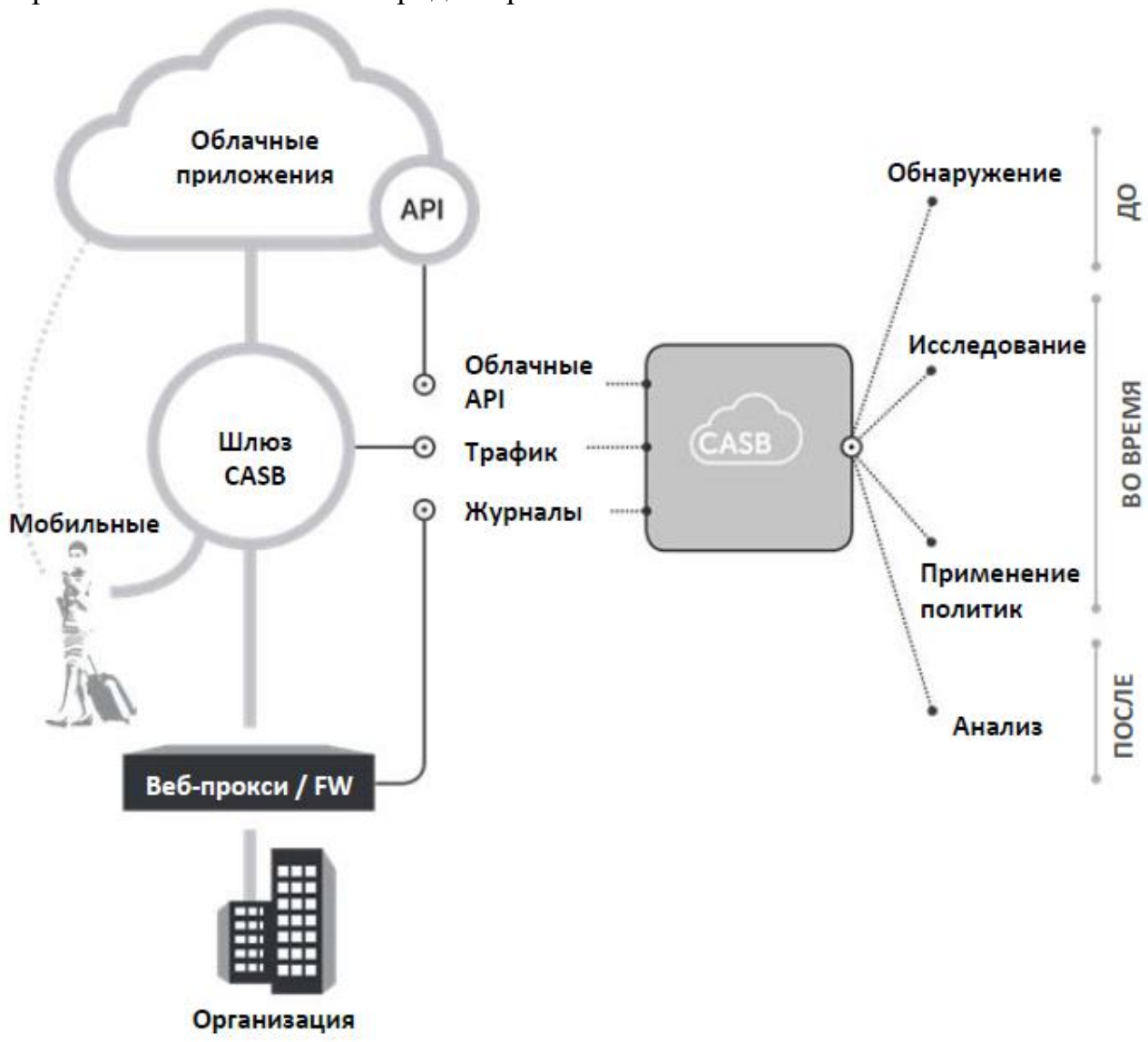

Рис.2.1. Архітектура та принцип роботи CASB

Вибір архітектури розробки CASB залежить від інфраструктури та потреб конкретної організації.

Визначимо основні можливості CASB

Виявляти і визначати оцінку ризику для всіх хмарних служб. CASB виявляють і визначають оцінку ризику кожної визначеної служби. Це дозволяє вирішити, чи прийнятні послуги для комерційного використання.

Забезпечують адаптивний контроль доступу. Дозволяє контролювати доступ користувачів на основі ряду умов, таких як групові чи організаційні підрозділи у корпоративному середовищі, атрибути пристроїв або інші фактори, такі як мережа або геолокація.

Відстежує та налаштовує сповіщення про діяльність адміністратора та користувача. Допомагає зрозуміти діяльність адміністратора та користувачів, наприклад, чи обмінюються користувачі конфіденційними даними за межами компанії, завантажують їх на несанкціонований пристрій чи посилюють привілеї в межах служби. Вони також можуть попередити вас про аномальні дії або дії, які можуть призвести до витоку даних (див. рис.2.1).

Доступ в хмару трансформує організацію. Вона змінює те, як відбувається швидкість виконання бізнес процесів компанії, оскільки все стає більш інтуїтивно зрозумілим, пов'язаним, відкритим і спільним, і ці зміна поширюються на SaaS, IaaS і веб-середовища. Але це в свою чергу створює нові проблеми і ризики, які не можуть вирішити успадковані рішення безпеки. Для цього необхідно забезпечити безпеку, яка може захистити дані і користувачів, де б вони не знаходилися.

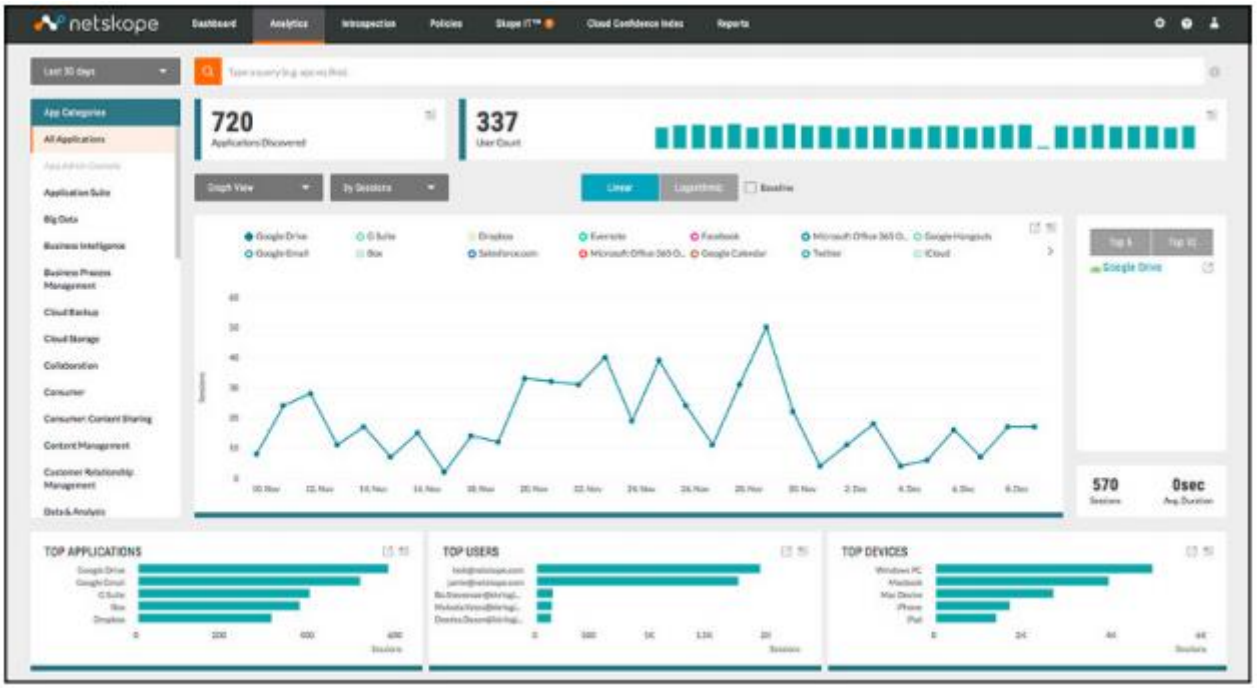

Рис.2.1. Моніторинг хмарних сервісів

Netskope пропонує хмарні сервіси на своїй хмарній платформі безпеки, як це показано на рис. 2.2.

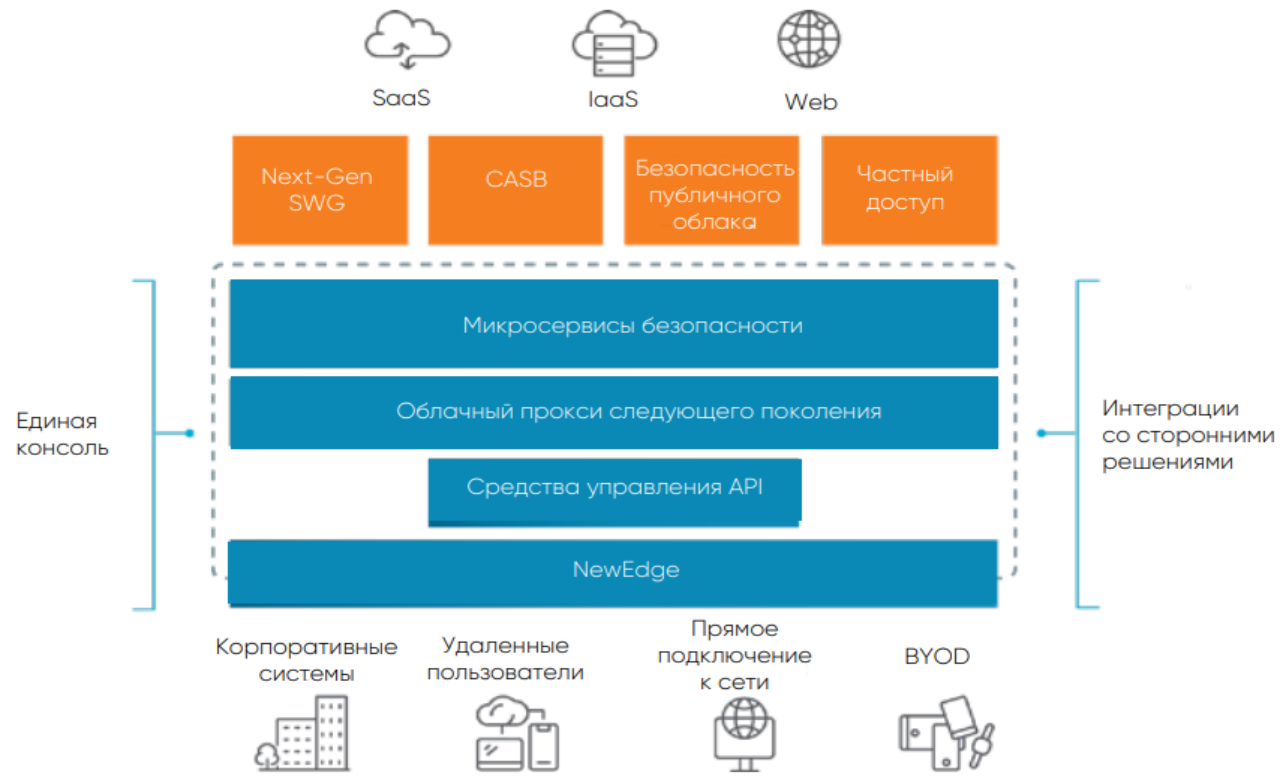

Рис.2.2. Netskope хмарна платформа безпеки

Хмара прискорює бізнес і покращує безпеку, а Netskope доповнює ці переваги єдиної консоллю і уніфікованими засобами контролю на основі політик, для того включатися в розрив поєднання інструментів SWG + CASB + DLP та забезпечило веб-захист нового покоління.

Платформа Netskope дає ряд переваг заточеним під хмару організаціям, включаючи орієнтовану на дані структуру для захисту даних і користувачів в будь-якому місці; розумну хмарну аналітику для безпечної роботи з хмарою і веб-ресурсами; а також передову глобальну потужну архітектуру для оперативного і масштабованого захисту.

Особливості хмарної платформи Netskope.

1. Візуалізація і контроль веб-трафіку, додатків і хмарних сервісів. Netskope надає API-проксі для призначених для користувача додатків. Це дозволяє розуміти контент і контекст тисяч додатків, на що не здатні традиційні рішення SWG. Прості в розгортанні хмарні рішення з прямим або зворотним проксі – при включенні в розрив - забезпечують візуалізацію і гранулярний контроль на основі політик для веб-трафіку, додатків і хмарних сервісів.

Данна особливість надає такі можливості:

• Виявлення в ході аналізу (при включенні в розрив) або за допомогою журналів з можливістю шифрування полів персональних даних в цілях конфіденційності;

• URL-фільтрація по більш ніж 100 категоріях для більш ніж 200 мов, що покриває 99,9% активного інтернет-простору;

• Рейтинги динамічних веб-сторінок по 70 категоріям + призначені для користувача категорії, категорії додатків і категорії YouTube;

• Включається в розрив CASB, що забезпечує візуалізацію і гранулярний контроль на основі політик для більш ніж тисячі керованих і некерованих додатків;

• Cloud Confidence Index ™ (CCI) - рейтинги ризику для більш ніж 36 000 додатків і хмарних сервісів з використанням більше 50 атрибутів CSA.

2. Виявлення шкідливого ПЗ і загроз Багаторівневий хмарний захист включає в себе захист від шкідливих програм, аналіз скриптів до їх виконання, евристику, пісочницю та виявлення аномалій на основі машинного навчання під управлінням команди Netskope Threat Research Labs.

Данна особливість надає такі можливості:

• Понад 40 джерел інформації про загрози + призначені для користувача хеш індикаторів компрометації і URL-канали;

• Аналіз поведінки користувачів і сутностей (UEBA) для виявлення компрометації доступу і аномалій;

• Хмарна пісочниця, стороння підтримка пісочниць Checkpoint, Juniper, Palo Alto Networks;

• Експорт даних через REST API + обмін відомостями про загрози на форматі вихідного коду.

3. Запобігання витоків даних (DLP). Політики "дозволити / заборонити" не підходять для бізнес-підрозділів, де прийнято вільне використання додатків з публікацією, передачею, вивантаженням або завантаженням даних в один клік. Засобам контролю на основі політик потрібно розуміти контент і контекст, а значить, без DLP тут не обійтися. Netskope надає визнану систему DLP для веб-трафіку, додатків і хмарних сервісів.

Данна особливість надає такі можливості:

• Хмарна система DLP з 3000 + ідентифікаторами даних, підтримкою 1000+ типів файлів і 40+ готових шаблонів політик;

• Виявлення даних різними методами, включаючи користувацькі регулярні вирази, цифрові відбитки, точне зіставлення даних, аналіз близькості, збіг по шаблонах і ключові слова, витяг метаданих та оптичне розпізнавання символів (API-режим);

• Система DLP може сповіщати, дозволяти, блокувати, видавати повідомлення для ознайомлення співробітників з корпоративними правилами поведінки, замінювати файли заглушками, токенізіровати або шифрувати дані

(структуровані і неструктуровані), відправляти на зберігання для судових потреб або в карантин;

• Базується на машинному навчанні виявлення даних, що передаються між корпоративними і особистими екземплярами додатків, для виявлення інсайдерів і витоку даних

4. Розширена веб-аналітика і звітність. Засоби контролю на основі політик визначає і задає Netskope Cloud XD, який інтелектуально і з акцентом на користувача візуалізує використання веб-сайтів, додатків і хмарних сервісів для аналітики та звітності. Cloud XD синтезує дані про веб-активності і витягує з них ті відомості про відвідування веб-сайтів і сторінок.

• Рішення дозволяє співробітникам центрів безпеки (SOC) швидко розслідувати сповіщення, розуміючи контент і контекст дій на веб-сайтах, в додатках і хмарних сервісах;

• Аналітика в режимі реального часу дозволяє будувати зведені дашборди і звіти;

• Деталізація по конкретному користувачеві, сайту і сторінці;

• Гнучкий механізм ситуативних запитів, що дозволяє 90 днів (більше - за окремим контрактом) витягувати багаті метадані про дії на веб-сайтах і в додатках;

• Функціонал експорту даних і відкритий API інтегруються зі сторонніми рішеннями.

2.2. Визначення основних функцій щодо забезпечення безпеки хмарних сервісів CASB

Оцінку готовності впровадження хмарної служби на підприємстві визначається відповідними функціями згідно виконання відповідних критеріїв у наступних функціональних областях:

✓ Сертифікати та стандарти;

✓ Захист даних;

✓ Контроль доступу;

✓ Аудит;

✓ Аварійне відновлення і безперервність бізнесу;

✓ Юридична інформація та конфіденційність;

✓ Уразливості і експлойти.

Коли конфіденційні або ділові дані знаходяться за межами компанії, керівник берете на себе рівень власного ризику. Ви зберігаєте дані і - залежно від функціональності загальнодоступної хмари - втрачаєте можливість мати фізичний доступ до серверів, на яких розміщена ваша інформація. Як результат, конфіденційні, регульовані або інші дані будуть під загрозою через властивості хмарних служб, в яких вони перебувають. Тому як користувачу хмарних служб необхідно переконатися, що вбудовані можливості безпеки, які необхідні компанії, доступні у хмарних послугах, якими користується ваша організація. Важливо, що коли дані виходять з-під контролю компанії та зберігаються в хмарі, вибрані служби застосовують заходи безпеки для захисту ваших даних та дотримання політик компанії.

Хмарні служби повинні відповідати нормативно-правовій стороні, для того щоб забезпечити зменшення ризику:

Сертифікати та стандарти: Ваші послуги та дані, які знаходяться в хмарі, повинні відповідати вимогам нормативних актів та галузевих вказівок, які притаманні для компанії.. Це є на панелі управління хмарою “Загальні сертифікати хмарної безпеки”, де показано ключові сертифікації, які слід враховувати.

Захист даних: Послуги, що містять ваші корпоративні дані, повинні дозволити вам захистити ці дані відповідно до ваших вимог. Це може включати

• Класифікація ваших даних та забезпечення доступу та політики захисту даних на основі рівнів класифікації;

• Захист конфіденційних та регульованих даних за допомогою надійного шифрування та корпоративних ключів;

• Відокремлення екземпляра хмарної служби від екземплярів інших клієнтів, щоб унеможливити потрапляння даних або пошкоджених даних одного клієнта, що можуть впливати на дані іншого.

Контроль доступу: Ваші служби повинні пропонувати засоби контролю доступу та забезпечення дотримання правил, які рівноцінними локальним органам управління. Сюди можна включити функції багатофакторної автентифікації, підтримка єдиного входу та детальний контроль доступу.

Відновлення після стихійних лих та безперервність бізнесу: Послуги повинні відповідати планам та процесам аварійного відновлення. Ці деталі повинні відображати вимоги щодо безвідмовної роботи та доступу до даних залежно від важливості даних компанії.

Шифрування: Служби, що зберігають конфіденційні або персональні дані, повинні використовувати шифрування даних у стані спокою та надавати вибір, як керувати цими ключами шифрування відповідно до ваших правил.

Аудити та оповіщення: Служби, які займаються критичними бізнес-процесами, містять конфіденційні дані або мають доступ до ваших корпоративних систем, повинні пропонувати надійні функції реєстрації та попередження про доступ до даних (див. Рис. 2.3). Це допоможе вам виявити підозрілі дії, як це відбувається, а також виконати розслідування після підозри на подію.

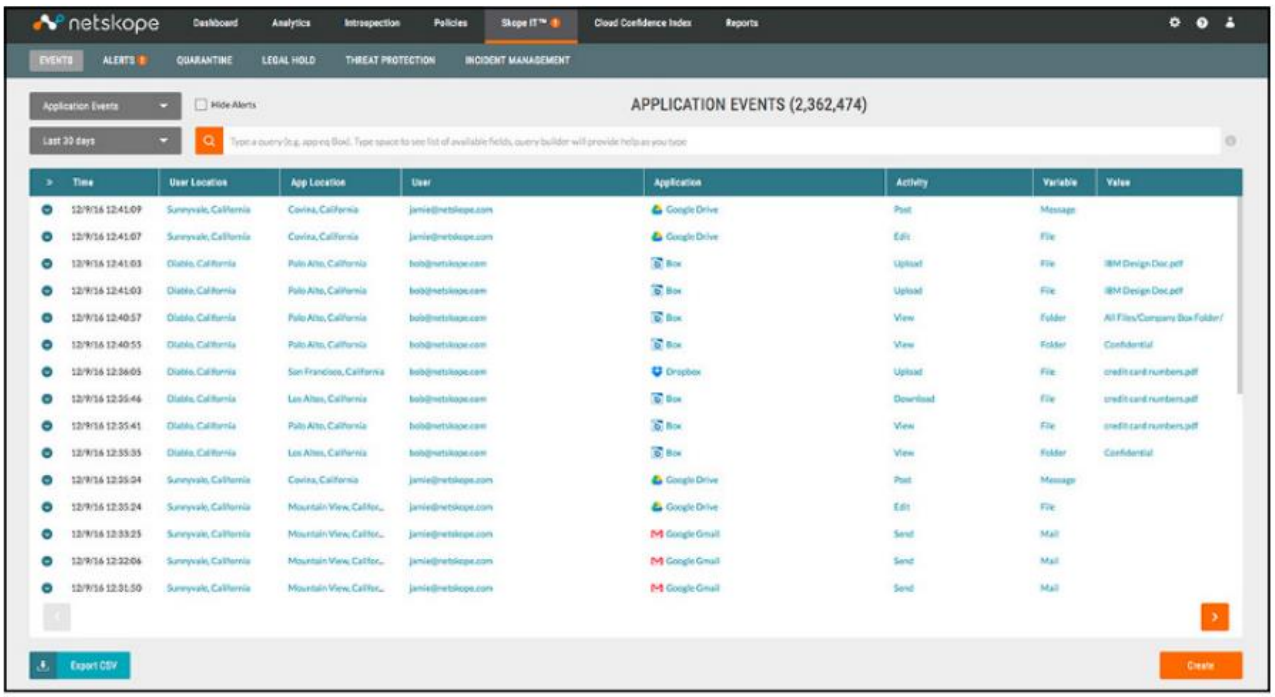

Рис.2.3. Аудит та оповіщення

2.3. Засоби забезпечення безпеки витоку даних CASB

Для забезпечення захисту даних, які знаходяться в хмарі, необхідно застосовувати засоби CASB запобігання втрати даних (DLP). Це дозволить застосовувати політики DLP включаючи користувача, хмарну службу або категорію, активність тощо. Профіль DLP Netskope складається:

Особиста інформація:

- PHI: Захищена медична інформація
- PCI: Інформація про платіжні картки;

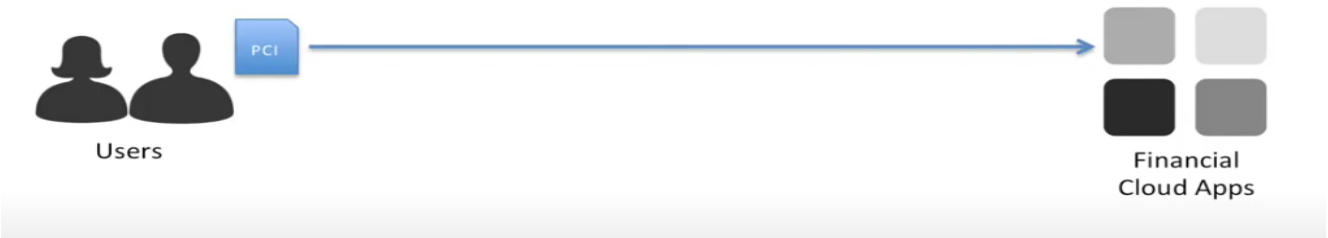

Рис. 2.4. PCI: Інформація про платіжні картки

- Конкретні ключові слова, словники ключових слів, відбитки пальців або точна відповідність вмісту;
- Вихідний код.

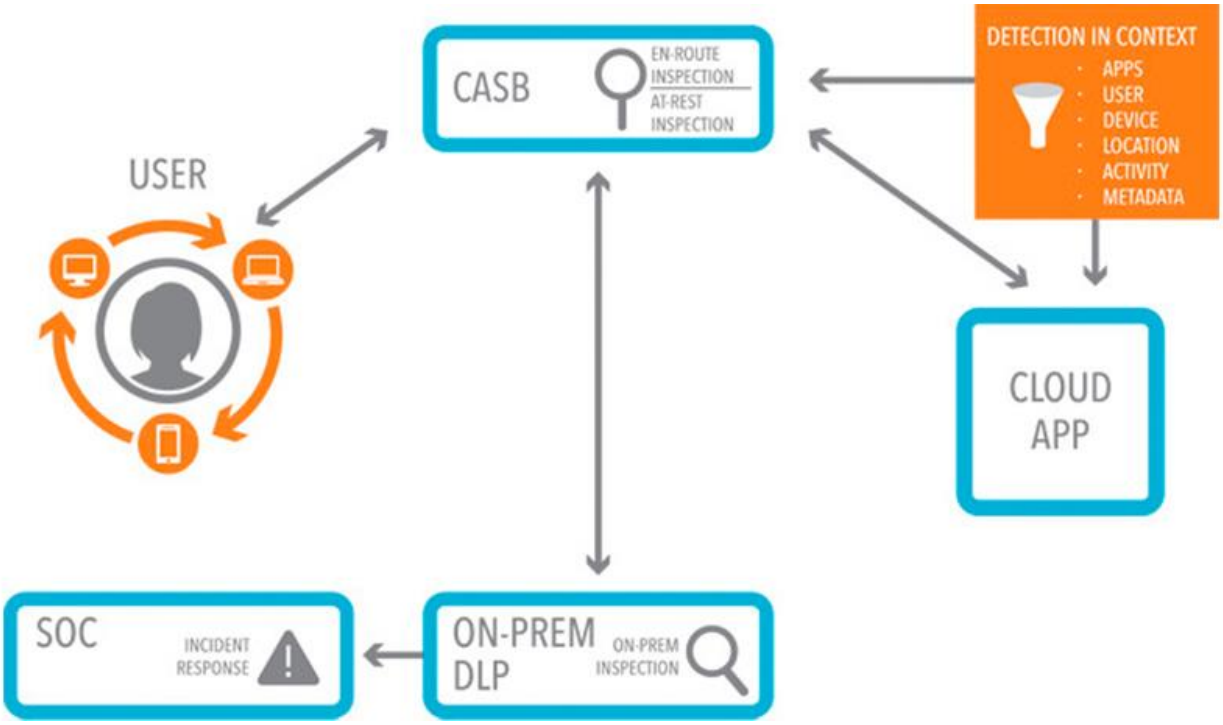

Рис. 2.5. DLP Netskope

DLP Netskope дозволяє створювати власні профілі. Профілі, можна застосовувати до будь-якого користувача, групи користувачів, хмарної служби, екземпляра або категорії хмарних служб, розташування, пристрою, класифікації пристроїв, активності тощо (рис.2.6).

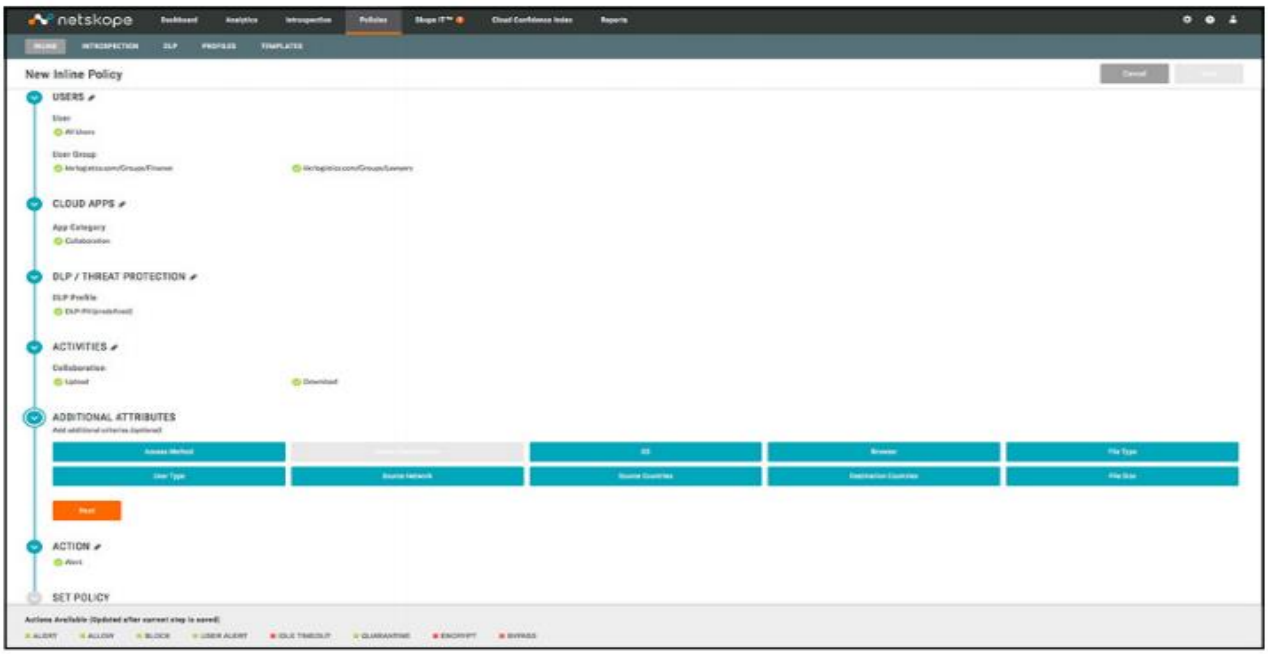

Рис. 2.6. DLP Netskope - власні профілі

Наприклад, медична компанія хоче виявляти порушення PHI, необхідно створити профіль DLP за допомогою заздалегідь визначеного словника, що містить сотні класифікаторів, пов'язаних з PHI (ім'я пацієнта, номер соціального страхування, медичні процедури, ліки тощо). Ви також повинні мати можливість створити власний профіль, використовуючи регулярні вирази, формувати відбитки пальців, точну відповідність, власні словники ключових слів щоб запобігти будь-яким порушенням.

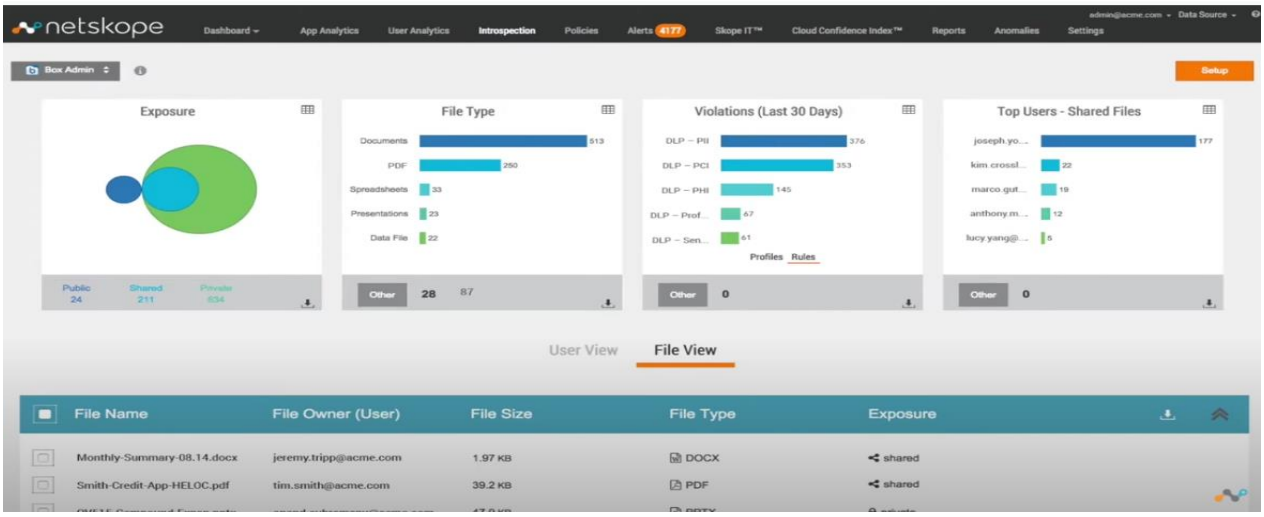

Рис. 2.7. Попередження про порушення

На основі порушень DLP можна створювати звіти. Наприклад, є можливість дізнатися, які користувачі найчастіше порушують правила PCI, або найпопулярніші служби та пристрої, що використовуються для порушення правил PHI в організації. Можливо надіслати ці звіти іншим працівникам та зупинити таку діяльність, що порушує політику. На рис. 2.7. показано звіт про відповідність в інтерфейсі Netskope. Його також можна завантажити у форматі PDF або запланувати його доставку іншим користувачам.

Рис.2.7. Приклад звіту порушення правил PHI в організації

3 ТЕХНОЛОГІЯ УПРАВЛІННЯ ДОСТУПОМ НА БАЗІ ХМАРНИХ СЕРВІСІВ

3.1. Рекомендації щодо застосування хмарного DLP Netskope

Важливість захисту даних від витоку є дуже важливою. Тому надамо загальні рекомендації щодо створення профілів DLP для компаній:

Обов'язково необхідно фахівцям з кібербезпеки створювати відповідні профілі DLP для своїх хмарних служб, включаючи PII, PHI, PCI тощо.

Засновуйте профілі DLP на стандартних галузевих ідентифікаторах та правилах та включайте розширений контекст (послуги, користувачі, час, місцезнаходження та діяльність користувачів) у свої політики DLP.

Відкривайте вміст у спокійному стані, який уже перебуває у ваших хмарних послугах, і вживайте таких заходів, як зміна власника, вміст на карантині або шифрування вмісту.

Встановіть політики DLP, які набувають чинності не лише в одній службі, але й у цілій категорії, якщо вони вам потрібні.

На рис. 3.1 показано, як можна налаштувати політику DLP.

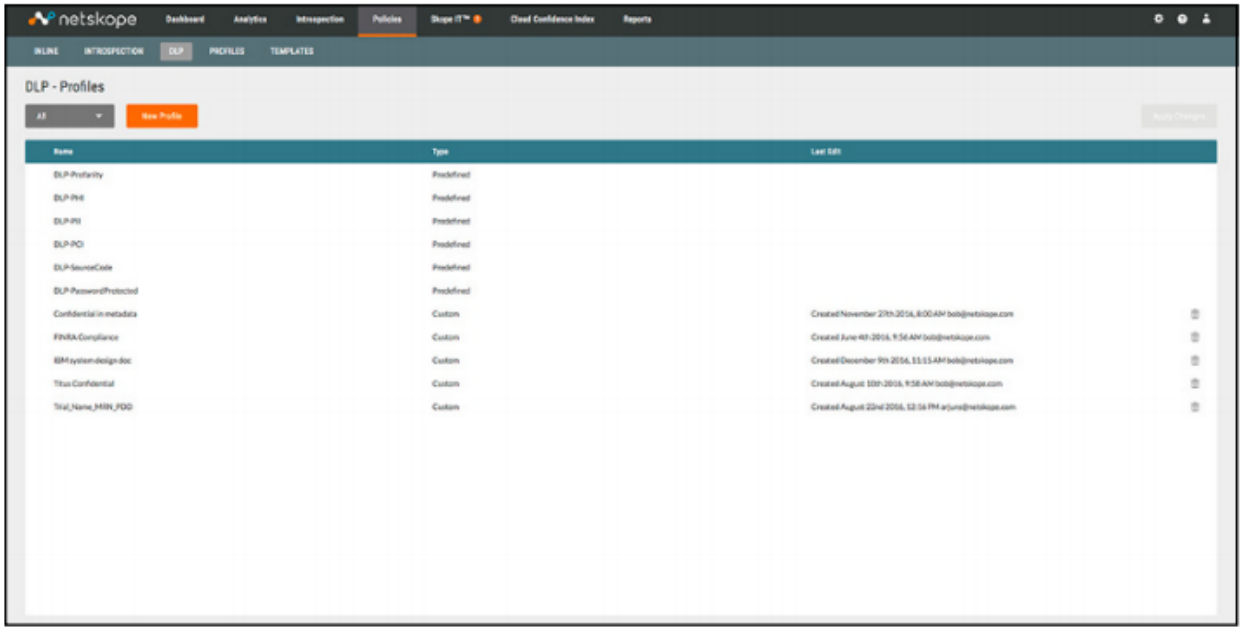

Рис.3.1 Налаштування профілю DLP

Переконайтеся, що ваші політики DLP можуть бути застосовані в режимі реального часу до того, як відбудеться порушення даних або викриття.

Дотримання даних вимог дозволить:

- отримайте повну видимість даних всюди
- зупинити ненавмисне або несанкціоноване переміщення даних, навіть по електронній пошті;
- запобігти крадіжці даних на некеровані пристрої;
- спростите захист даних;
- навчати користувачів безпечній поведінці в режимі реального часу;
- забезпечити відповідність нормативним вимогам.

3.2. Технологія захисту віддалених користувачів при роботі з хмарними сервісами

Розглянемо та надамо рекомендації щодо захисту віддалених користувачів при роботі з хмарними сервісами .

Багато організацій мають труднощі з забезпеченням належної безпеки для віддалених співробітників і все частіше стикаються з проблемами віддаленого доступу в сучасному світі, орієнтованому на хмарні технології. Як група, віддалені співробітники підходять для переходу на хмарне рішення безпеки; це може значно знизити ризики, і вдосконалити для користувача досвід.

При оцінці вибору щодо кращого захисту віддалених співробітників, надамо рекомендації для забезпечення безпеки компанії за допомогою хмарного рішення. По кожній з рекомендації надамо пояснення проблеми і ризику, варіант як Netskope може допомогти вирішити проблему, і як ви можете перевірити і оцінити ваш поточний стан безпеки.

Дана технологія дозволяє:

- Враховувати хмарні загрози;
- Виявлення і крадіжка даних;
- Компроментація доступу та аномалії;

Гнучкість і глобальні характеристики;

Запровадження нульової довіри доступу мережі.

1. Хмарні загрози

Сьогодні організації зазвичай використовують понад 2400 хмарних сервісів і додатків, з яких відомо, що більше 1600 з них є загрозою.

Хмара - це нова поверхня для атак. Головна атака на основі хмарних обчислень - це фішинг. Головна мета фішингу - облікові дані співробітників для хмарних додатків і електронної пошти. Успадковані засоби захисту веб-безпеки, орієнтовані на репутацію в Інтернеті для запуску захисту, або рішення для кінцевих точок, які шукають шкідливе навантаження.

Існують приклади використання хмарних сервісів, хмарних додатків і хмарного сховища для обходу застарілих засобів захисту на всіх етапах ланцюжка кібератак. У добре відомих хмарних сервісах є довірені домени і дійсні сертифікати, і вони можуть бути внесені до білого списку, щоб обійти захист. Це забезпечує доступ до атак з «червоної доріжки» для віддалених співробітників, які зазвичай витрачають до 89% свого дня на доступ до хмари.

Кіберзлочинцям тепер потрібна хмарна ідентифікація більше, ніж номер кредитної картки. Облікові дані SaaS (30,8%) перевершили фішингові атаки на платіжні системи (19,8%) і фінансові установи (19,4%).

Рекомендація:

Використання Netskope Next Gen Secure Web Gateway (NG SWG) захищає всіх користувачів і пристрої, з будь-якого місця, за допомогою хмарного захисту. Netskope має можливість декодувати трафік тисячі хмарних сервісів і хмарних додатків, щоб моніторити активність і дані, а також забезпечувати розширений захист від загроз.

Протестуйте свій стек безпеки, щоб оцінити, скільки ваших хмарних сервісів і хмарних додатків, керованих і некерованих, можна перевірити на предмет змісту і контексту. Переконайтеся, що у вас є метадані, наприклад,

легітимний користувач, тип пристрою, хмарне додаток, рівень ризику, екземпляр додатку, активність користувача і передані дані.

Це дозволить розслідувати атаку хмарного фішингу з боку шахрайського примірника некерованого хмарного додатка і визначити чи є у вас необхідна видимість і метадані.

2. Виявлення і крадіжка даних

Хмарні дані охоплюють чотири вектора, які можут привести до виявлення і крадіжці даних. Статистика: у 20% користувачів конфіденційні дані переміщаються між хмарними додатками, і 37% цих даних пов'язані з порушеннями DLP.

По-перше, визначені і перевірені керовані хмарні сервіси, включаючи Microsoft Office 365 і G Suite by Google Cloud, часто потрапляють в білий список. Таким чином, віддалені співробітники можуть випадково або навмисно переміщати дані між корпоративними і особистими даними цих хмарних сервісів.

По-друге, організація має лише кілька керованих хмарних сервісів, зазвичай менше 2%, в той час як використання різноманітного набору некерованих хмарних сервісів становить 98%.

Некеровані хмарні додатки зазвичай вільно приймаються бізнес-підрозділами, а окремі користувачі і дані часто можуть легко передаватися в ці служби.

По-третє, звичайним явищем є переміщення даних між категоріями хмарних додатків, включаючи переміщення даних між додатками хмарного сховища, від хмарного сховища до додатків для спільної роботи і від хмарного сховища до веб-пошти. Вам необхідно виявляти, а потім управляти переміщенням конфіденційних і особистих даних між небажаними категоріями, додатками і екземплярами. І, нарешті, без розуміння ризику, пов'язаного з хмарними додатками, неможливо обмежити доступ або дії користувачів для тих хмарних додатків, дані в яких можуть бути піддані ризику компрометації. Розуміння того, які програми становлять менший ризик (наприклад, Microsoft OneDrive, Box) в порівнянні з додатками, що представляють більш високий ризик (наприклад,

WeTransfer, Zippyshare), допоможе групі безпеки встановити відповідні політики захисту даних для віддалених співробітників.

Використання Netskope NG SWG захищає віддалених співробітників за допомогою хмарної системи запобігання втрати даних (DLP). Netskope DLP добре розбирається в цьому, на основі контексту, екземпляр,у категорії ризику. Ці характеристики, яких немає в застарілих засобах захисту Інтернету, можуть бути використані для побудови ефективної політики захисту даних безпосередньо в хмарі.

Netskope - це єдина хмарна платформа безпеки з уніфікованими політиками захисту як хмари, так і Інтернету. Це означає, що політики DLP можуть застосовуватися до вмісту веб-сторінок, файлів і форм, а також до тисяч хмарних сервісів і додатків.

Рекомендація. Протестуйте свій стек безпеки за всіма правилами; застосовуйте правила DLP і політику між конфіденційними даними компанії на основі особистих примірників керованих хмарних додатків, або керованих на прикладі некерованих хмарних додатків. Крім того, якщо у вашому поточному стеку безпеки є видимість для віддалених співробітників, перевірте чи може він змінювати профіль переміщення хмарних даних між категоріями хмарних додатків або надавати оцінку ризиків хмарних додатків, щоб допомогти з вибором і включенням хмарних додатків з меншим ризиком для використання бізнес-підрозділами та співробітниками.

3. Компроментація доступу та аномалії

Ідентифікація та доступ до хмари - це новий периметр, тому не дивно, що фішингові облікові дані для доступу до хмари тепер є метою номер один для кіберзлочинців, набагато випереджаючи мету платіжного та фінансового фішингу.

Коли фішинг виявлено, необхідно провести превентивні дії для захисту підприємства. Тобто необхідно якомога швидше виявити використання цих скомпрометованих облікових даних і пов'язані з ними шкідливі дії. Для виявлення

компрометації доступу і аномальної поведінки необхідно мати великі метадані, зібрані з тисяч хмарних сервісів і додатків, а також розуміння контексту для моделей і сценаріїв використання машинного навчання (ML). Застарілі засоби захисту не бачать хмарних сервісів, оскільки вони не можуть декодувати контент і контекст, залишають віддалених співробітників незахищеними, а операції безпеки не мають можливості виявляти або досліджувати компрометацію доступу і аномалії.

Слід пам’ятати: атаки з використанням хмари можуть використовувати фішингові облікові дані з використанням довірених доменів, які мають діючі сертифікати SSL і які обходять захист кінцевих точок, оскільки немає виявленого корисного навантаження.

Рекомендації. Netskope надає аналітику поведінки користувачів і сутностей (UEBA) на основі великих метаданих, які він збирає від віддалених користувачів, де б вони не знаходилися і до яких хмарних додатків і веб-сайтам вони зверталися. Виявлення аномалій машинного навчання Netskope UEBA дозволяє виявляти зламані облікові записи, зловмисників і крадіжку даних. Подальші відомості і попередження надаються шляхом послідовного аналізу правил дій, таких як масові завантаження, масові видалення, рідкісні події, географічна близькість і аналіз, доступ з країн з високим ризиком і множинні невдалі спроби входу в систему. Тому завдання команди безпеки виявити або дослідити підозрювану компроментацію доступу або аномальної поведінки користувачів в хмарних додатках.

Для цього перевірте свій поточний стек безпеки, змоделювавши підозрілу поведінку крадіжки даних. Завантажте 10 або більше файлів з корпоративного примірника керованого хмарного додатка, а потім завантажте їх в особистий екземпляр некерованого хмарного додатка, почекайте 20 хвилин і потім видаліть файли з особистого примірника. Це дозволить отримати повідомлення про ці дії, отримати одне або два попередження, і використовувати дані для створення деталізованих засобів управління політиками.

4. Гнучкість і глобальні характеристики

Кіберзлочинці почали застосовувати хмари швидше, ніж більшість законних організацій, багато з яких все ще намагаються убезпечити використання хмари за допомогою пристроїв веб-безпеки, в які вони інвестували багато років назад. віддалені працівники часто підключаються через ці VPN-з'єднання. Це обладнання зазвичай обмежене в обчислювальних ресурсах і ємності сховища, що вимагає від служби безпеки міняти вимоги безпеки на користь наданої продуктивності.

Зашифрований трафік SSL / TLS (HTTPS) зараз становить 84% у всьому світі, а ефективний захист вимагає інтенсивних обчислювальних циклів для декодування і перевірки вмісту і контексту використання хмари і Інтернету. Такі підходи, як внесення трафіку в білий список, щоб спробувати поліпшити взаємодію з користувачем, вибіркове включення захисту на основі ризику або репутації, неможливість декодувати JSON-трафік на основі API в хмарі або просто дозвіл віддаленим працівникам обходити заходи безпеки - все це величезні ризики. в хмарному середовищі. Сучасний підхід до безпеки для віддалених співробітників, який масштабується і забезпечує оптимальну взаємодію з користувачем, може бути реалізований тільки з хмари.

Рекомендації

Netskope надає хмарні мікросервіси безпеки на єдиній глобальній платформі з продуктивністю за запитом і масштабованість для перевірки зашифрованого трафіку, декодування хмарних сервісів і додатків, фільтрації веб-трафіку і застосування розширеного захисту даних і загроз. Netskope також надає глобальну мережеву інфраструктуру загальнодоступних точок присутності (PoP) з високою пропускною здатністю з неперевершеною пірінговою взаємодією з такими сервісами, як Amazon Web Services (AWS), Microsoft Azure і Google Cloud Platform (GCP), що забезпечує безпечний шлях до Інтернету для віддалених співробітників з будь-якої точки світу. Ця мережева інфраструктура, яка називається NewEdge ™, забезпечує безпечне і зручне взаємодія з користувачем при використанні Netskope Security Cloud.

Порівняйте можливості захисту вашого застарілого пристрою з можливостями хмарного захисту Netskope. Створіть свої власні тести або використовуйте інструмент перевірки безпеки Netskope - netskopesecuritycheck.com. Якщо користувачі обходять існуючі заходи безпеки, перебуваючи поза офісом, подумайте про впровадження хмарного захисту. Ці засоби захисту можуть замінити або розширити функційні можливості обладнання в вашому центрі обробки даних.

5. Застосування принципів нульової довіри доступу до мережі

Міграція приватних додатків в загальнодоступну хмару і широке поширення хмарних додатків усувають необхідність в корпоративних центрах обробки даних. Управління застарілими рішеннями VPN, які забезпечують зворотний зв'язок пристроїв з традиційними центрами обробки даних, пов'язані з деякими ризиками, пов’язаних з небажаною і обтяжливою взаємодією з користувачем.

По-перше, залучення віддалених користувачів через віртуальні приватні мережі через центральні центри обробки даних до додатків і ресурсів, розміщених в загальнодоступних хмарних середовищах, призведе до зниження продуктивності і тривалого періоду прийому-передачі. По-друге, наявність відкритих портів і сервісів для VPN-підключень до мережевого середовища забезпечує відкриту поверхню для атак. І, нарешті, віддалені віртуальні приватні мережі надають зламаним обліковим записам або зловмисникам доступ і, що ще більш небезпечно, можливість горизонтального переміщення всередині корпоративної мережі.

Переваги NETSKOPE

Netskope пропонує захист віддалених користувачів за допомогою рішень доступу до мережі з нульовим довірою (ZTNA), на базі рішення Netskope Private Access (NPA), що дозволить забезпечити прямий доступ тільки до авторизованих додатків в центрі обробки даних або загальнодоступній хмарі. NPA не вимагає відкритих портів або сервісів і, отже, виключає будь-яку можливість для

зовнішнього впливу і атак. NPA - це хмарне рішення і добре масштабується,. На відміну від пристроїв VPN, не потрібно турбуватися про паралелізм користувачів або вичерпання ресурсів. Тому необхідно відмовитися від застарілого рішення VPN на користь ZTNA.

Рекомендації

При порівнянні можливостей віддаленого доступу через VPN та Netskope Private Access, можна зробити висновок, що ускладняється доступ віддалених співробітників до приватних додатків в загальнодоступних хмарних середовищах з використанням традиційних віртуальних приватних мереж віддаленого доступу. Netskope забезпечує для віддалених користувачів впровадження ZTNA більш ефективно, ніж традиційні рішення VPN. Рішення NPA може бути розгорнуто протягом декількох годин. Крім того, NPA є частиною тієї ж хмарної платформи Netskope, яка забезпечує всі переваги для захисту доступу віддалених співробітників до хмари і Інтернету.

Тому як висновок: віддалені співробітники повинні бути головним пріоритетом для хмарного захисту та бути орієнтованої на хмару.

Тож для ефективної роботи з хмарними сервісами необхідно виділити віддалених співробітників в групу і забезпечити їм необхідну безпеку за допомогою глобально доступного до хмарного безпечного веб-шлюзу нового покоління (NG SWG). Необхідно використовувати Netskope для управління доступом в Інтернет, що забезпечить захист даних, шифрування хмарних сервісів і додатків для забезпечення контролю політик користувачів. Необхідно віддаленим співробітникам надати безпечний і прямий доступ до корпоративних центрів обробки даних і загальнодоступних хмарних середовищ за допомогою Netskope Private Access, рішення ZTNA, яке є інтегрованою можливістю платформи Netskope.

ВИСНОВКИ

Хмарні технології все частіше застосовують для підвищення ефективності виконання бізнес-процесів компаній. Для фахівців кібербезпеки при переході на хмарні технології необхідно знати методи та засоби, які необхідно застосувати при такому переході. Саме ці питання були розглянуто в даній магістерській роботі.

Таким чином в бакалаврській роботі отримано наступні результати:

Проведено аналіз застосування хмарних сервісів в інформаційні системі компанії в результаті якого визначено основні причини для переходу компаній в хмару.

На основі проведеного аналізу проведено аналіз вимог міжнародного стандарту NIST, щодо архітектури хмарних обчислень, учасників процесу та зони відповідальності між користувачем та надавачем послуг.

В роботі визначено основні методи та засоби забезпечення безпеки при використанні хмарних сервісів.

Для обраного рішення Netskope було визначено архітектуру, основні функціональні можливості та принцип роботи CASB.

Розроблено рекомендації захисту даних віддалених користувачів при використанні хмарних сервісів. Фахівцям з кібербезпеки необхідно створювати відповідні профілі DLP для своїх хмарних служб, включаючи PII, PHI, PCI, використовувати веб-шлюзу нового покоління NG SWG для захисту даних, інтегрувати доступ до хмарного середовища на базі Netskope Private Access з рішенням ZTNA.

ПЕРЕЛІК ПОСИЛАНЬ

1. Хмарні сервіси [Електронний ресурс] – Режим доступу: https://gmsseguridad.com/wp-content/uploads/2020/10/Netskope.pdf

2. NIST_SP-500 [Електронний ресурс] – Режим доступу: https://www.nist.gov/system/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf .

3. Guidelines on Security and Privacy in Public Cloud Computinghttps [Електронний ресурс] – Режим доступу://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf .

4. Cloud Access Security Brokers (CASB) Reviews and Ratings [Електронний ресурс] – Режим доступу: https://www.gartner.com/reviews/market/cloud-access-security-brokers/

5. CASB [Електронний ресурс] – Режим доступу: https://www.esecurityplanet.com/products/casb-security-vendors/#netskope.

5. Designing a SASE Architecture For Dummies, Netskope Special. – Copyright.- 2021 . – 66 p.

6. Cloud Security For Dummies®, Netskope 2nd Edition. - Copyright.- 2017.- 57p.

7. П'ять принципів безпеки віддаленого доступу [Електронний ресурс] – Режим доступу: https://resources.netskope.com/ebooks/5-reasons-to-choose-cloud-security-for-remote-workers

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)