CLOUD SECURITY BLUEPRINT

ARCHITECTURES AND SOLUTIONS

IT specialist

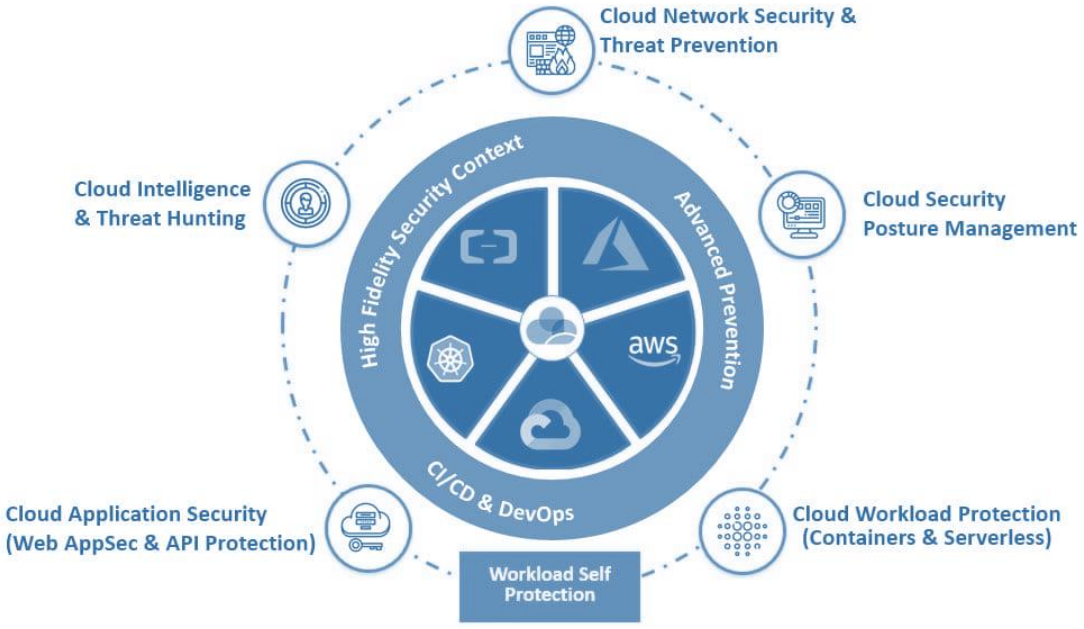
CHECK POINT

Опис

У даному документі розглянуто основні хмарні концепції (модель спільної відповідальності, нульова довіра), проблеми, які має вирішувати сучасна хмарна архітектура безпеки, а також виклики, з якими зіштовхуються компанії при побудові захисту в хмарних середовищах, а саме: збільшення площі атак, зниження видимості, динамічні та тимчасові навантаження, автоматизовані процеси DevOps, надмірні привілеї та численні хмарні середовища.

У документі описано архітектурні принципи хмарної безпеки, необхідні для ефективного вирішення завдань інформаційної безпеки в хмарі. Принципи включають:

- ✓ Розширений захист від загроз для периметру мережі
- ✓ Захист від різних векторів атак, таких як: ідентифікація, адміністрування та захист даних
- ✓ Проєктування архітектури таким чином, щоб зберегти безпеку частиною хмарного середовища
- ✓ Сегментація для мінімізації поверхні атаки та зменшення радіусу ураження
- ✓ Гнучкість, автоматизація та еластичність додатків без шкоди для безпеки
- ✓ Побудова уніфікованого захисту незалежно від особливостей хмарної платформи



Збільшення хмарних технологій

Згідно інформації зі звіту Flexera про стан хмарних технологій Rightscale 2019, впровадження хмарних обчислень відбувається в більшості організацій будь-якого розміру: 94% опитаних повідомили, що їх організація використовує публічну хмару. Ми також бачимо, що підприємства продовжують використовувати гібридні та Multi-Cloud стратегії (див. рис. 1). Впровадження гібридної хмари зросло з 51% до 58%, а використання Multi-Cloud зросло з 81% до 84% порівняно з попереднім роком.

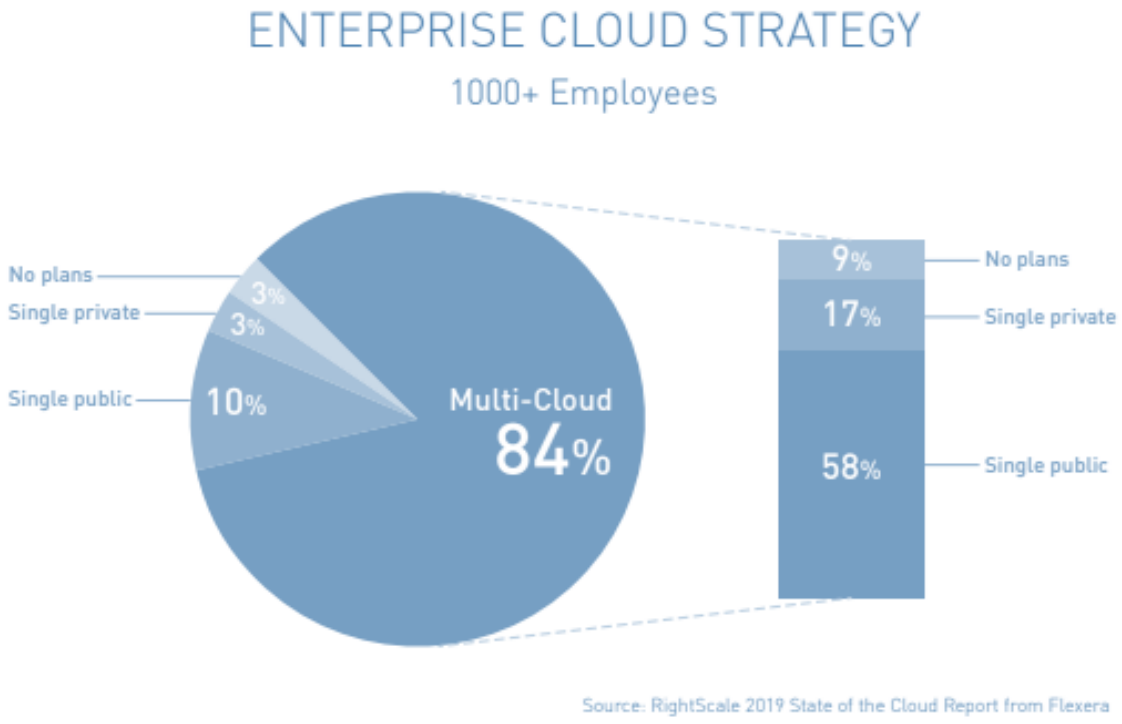


Рисунок 1 Зростання корпоративних гібридних і Multi-Cloud інфраструктур

Гнучкість бізнесу, продуктивність, операційна ефективність і рентабельність, безсумнівно, є ключовими факторами впровадження публічної хмари підприємства. Публічна хмара дозволяє швидше отримувати та розгортати ресурси комп'ютерної мережі. Після розгортання ці ресурси можна збільшити або зменшити за потреби, щоб задовольнити попит.

У цьому документі описано ключові концепції безпеки хмари та принципи архітектури, які повинні лежати в основі плану безпеки хмари.

Концепції хмарної безпеки

У цьому розділі розглянуто дві ключові концепції, які підприємство має розуміти, щоб реалізувати ефективний проєкт безпеки.

Розуміння моделі спільної відповідальності публічної хмари

Перенесення робочих навантажень і даних у публічне хмарне середовище означає, що відповідальність за безпеку розподіляється між вами та вашим постачальником хмарних послуг. Безпека хмарної інфраструктури (включно з фактичним розташуванням фізичних центрів обробки даних, приладами мережевої комунікації та обладнання для зберігання даних, таких як маршрутизатори, комутатори та балансувальники навантаження, системами опалення, вентиляції, кондиціонування, енергопостачання тощо) забезпечується постачальником. Клієнт несе відповідальність за використання власних інструментів хмарного постачальника для захисту активів і робочих навантажень, які він виконує в хмарі, включаючи код програми, дані програми та доступ до програми, зберігаючи при цьому відповідність за нормативними вимогами і найкращими практиками безпеки.

За визначенням, модель спільної відповідальності змінюється при використанні служб IaaS, PaaS або SaaS (див. рис. 2 на основі діаграми з веб-сайту Microsoft Azure). У той же час більшість типових хмарних реалізацій використовують поєднання цих моделей обслуговування, що часто є причиною загальної плутанини: хто за що відповідає?

RESPONSIBILITY ZONES

Responsibility	SaaS	PaaS	IaaS	On-prem	
Data governance & rights management	●	●	●	●	Always retained by customer
Client endpoints	●	●	●	●	
Account & access management	●	●	●	●	
Identity & directory infrastructure	◑	◑	●	●	Varies by Service Type
Application	○	◑	●	●	
Network controls	○	◑	●	●	
Operating System	○	○	●	●	
Physical hosts	○	○	○	●	Transfers to Cloud Provider
Physical network	○	○	○	●	
Physical data center	○	○	○	●	

○ Cloud Provider ● Customer

Based on a diagram in the Azure website

Рисунок 2 Зони спільної відповідальності в моделях хмарних сервісів

Amazon Web Services (AWS) лаконічно підсумовує це на своєму веб-сайті:

«...клієнт має виконувати всі необхідні завдання з конфігурації та керування безпекою. Клієнти, які розгортають Amazon EC2, несуть відповідальність за керування гостьовою операційною системою (включно з оновленням безпеки), будь-яким прикладним програмним забезпеченням або утилітами, встановленими клієнтом на робочих машинах і за конфігурацію наданого AWS брандмауера на кожній робочій машині. Ця модель спільної відповідальності замовника/AWS також поширюється на IT-контроль. Подібно до того, як відповідальність за управління IT-середовищем розподіляється між AWS та її клієнтами, так само розподіляються управління, експлуатація та перевірка засобів спільного контролю IT...»

Коротко кажучи, клієнти хмари не повинні бути переконані, що «хмара безпечна». Насправді, відповідальність клієнтів хмари за безпеку є значною, і до неї ніколи не слід ставитися легковажно.

Нульова довіра і чому ви повинні це прийняти

Forrester заявляє у своєму звіті Predictions 2019 Transformation goes pragmatic, що «у 2019 і в 2020 році Zero Trust стане спеціальним стандартом у США».

Як випливає з назви, основний принцип Zero Trust полягає в тому, щоб не довіряти нікому і нічому, перевіряючи все. Існують зловмисники як у мережі, так і за її межами, і за замовчуванням користувачам і машинам ніколи не слід автоматично довіряти. Потрібно припустити, що весь трафік, незалежно від місця розташування, є зловмисним, доки він не буде перевірений (тобто авторизований, переглянутий і захищений).

Zero Trust, наприклад, сприяє стратегії управління найменшими привілеями, згідно з якою користувачі отримують доступ лише до ресурсів, необхідних для виконання своїх обов'язків. Крім того, сучасні програми часто надають широкі привілеї компонентам, з яких складається розподілена архітектура. Веб-додатки особливо вразливі. Наприклад, якщо розробник не заблокував порти або не реалізував дозволи згідно принципу «за потреби», хакер, який захопить програму, матиме привілеї для редагування бази даних.

Крім того, мережі Zero Trust використовують мікросегментацію – метод створення безпечних зон у центрах обробки даних і хмарних розгортаннях, який сегментує робочі навантаження одне від одного, захищає все всередині зони та застосовує політики для захисту трафіку між зонами. Це робить безпеку мережі набагато детальнішою. Також важливо постійно перевіряти та реєструвати весь внутрішній і зовнішній трафік, щоб відстежувати шкідливі дії в реальному часі.

В описаному вище звіті Forrester чітко зазначено, що ми повинні:

«створювати безпечні мікропериметри, використовувати обфускації для підвищення безпеки даних, обмежувати надмірні привілеї користувачів для зменшення ризику, використовувати автоматизацію аналітики для покращення виявлення безпеки та реагування. Необхідно відкинути ідею довіреної внутрішньої та ненадійної зовнішньої мережі. Групи безпеки повинні перевіряти та захищати всі ресурси незалежно від місця розташування, обмежити та суворо контролювати доступ для всіх користувачів, пристроїв, каналів і моделей хостингу, а також реєструвати й перевіряти весь внутрішній і зовнішній трафік».

Завдяки цим та іншими методам Zero Trust сприяє безпеці, яка є всеосяжною та проактивною в усій мережі, а не лише на периметрі. Застосування принципів нульової довіри ефективно мінімізує поверхню, а також радіус атаки на мережу, коли вона відбувається.

Також важливо постійно перевіряти та реєструвати весь внутрішній і зовнішній трафік, щоб відстежувати шкідливі дії за допомогою можливостей захисту в реальному часі.

Розширені виклики хмарної безпеки

Оскільки публічна хмара не має чітких периметрів або портів виходу/входу, організація, яка переходить до хмари, потрапляє в принципово іншу реальність безпеки. Ця нова реальність безпеки стає ще складнішою при застосуванні сучасних хмарних підходів, таких як автоматизовані методи CI/CD, розподілені безсерверні архітектури та ефемерні активи, як-от «функції як послуга» та контейнери.

У цьому розділі ми обговоримо передові проблеми безпеки та численні ризики, з якими стикаються сучасні організації, орієнтовані на хмару.

Збільшена поверхня атаки

Зловмисне програмне забезпечення, Zero-Day, захоплення облікового запису та багато інших загроз стали повсякденною реальністю. Загальнодоступне хмарне середовище стало великою та дуже привабливою поверхнею для атак хакерів, які намагаються використовувати погано захищені вхідні порти хмари, щоб отримати доступ і скомпрометувати робочі навантаження та дані в хмарі. Кожна організація, яка використовує публічну хмару, повинна розуміти, що вона значно збільшує поверхню атаки на себе, просто використовуючи її.

Відсутність видимості та відстеження

Загалом компанії мають менший доступ до хмарних інфраструктур, ніж до локальних. У моделі IaaS хмарні постачальники мають повний контроль над інфраструктурним рівнем і не розкривають його своїм клієнтам. Відсутність видимості та контролю ще більше поширена в хмарних моделях PaaS і SaaS.

Якщо говорити точніше, хмарні ресурси часто стають невидимими, ними важко керувати, що створює серйозні проблеми в забезпеченні безпеки. Без інструментів оркестрування наступного покоління клієнти хмари не можуть ефективно ідентифікувати та кількісно оцінити свої хмарні активи або візуалізувати своє хмарне середовище.

Робочі навантаження постійно змінюються

Хмарні ресурси надаються та виводяться з експлуатації динамічно, швидко та гнучко. Традиційні інструменти безпеки просто нездатні забезпечити дотримання політики захисту в такому гнучкому та динамічному середовищі. Потрібні нові інструменти та підходи, щоб захистити сучасні постійно мінливі та ефемерні робочі навантаження.

DevOps, DevSecOps і автоматизація

Організації, які прийняли високоавтоматизовану культуру DevOps безперервної інтеграції та безперервного розгортання (CI/CD), повинні переконатися, що відповідні засоби контролю безпеки визначені та вбудовані в код і шаблони на ранніх етапах циклу розробки. Зміни, пов'язані з безпекою, впроваджені після того, як робоче навантаження було розгорнуто, можуть підірвати безпеку організації, а також збільшити час виходу на ринок.

Детальне керування привілеями та ключами

Незвично, що ролі користувачів хмари налаштовані лояльно, надаючи широкі привілеї, що перевищують ті, що призначені або необхідні. Одним із поширених прикладів є надання дозволів на видалення або запис бази даних користувачам, які не навчені або просто не потребують видалення чи додавання активів.

Подібна ситуація на рівні програми, де неправильно налаштовані ключі та привілеї створюють ризики безпеці через витік ключів або погано захищені сеанси.

Щоб підтримувати принцип нульової довіри, привілеями користувачів і програм потрібно керувати на дуже детальному рівні за допомогою гнучких і динамічних інструментів керування доступом.

Multi-Cloud середовище

Кожен постачальник хмарних послуг пропонує інструменти та послуги, які допомагають клієнтам контролювати та захищати свої хмарні ресурси. Рекомендується інтегрувати ці інструменти хмарних постачальників у ваш існуючий стек безпеки, щоб допомогти виконати вашу роль у моделі спільної відповідальності.

Однак важливо пам'ятати, що засоби безпеки кожного постачальника застосовуються лише до його власних хмарних служб. Щоб узгоджено керувати безпекою в гібридних і Multi-Cloud середовищах, яким сьогодні віддають перевагу, організації потрібні інструменти керування конфігурацією, автоматичного виправлення та оркестровки, які безперебійно працюють між постачальниками публічних, приватних хмар і випадків локального розгортання.

Відповідність і правила

Під час роботи в хмарі необхідно враховувати дотримання відповідних законів або галузевих нормативних вимог. Щоб виконати свою частину моделі спільної відповідальності, що стосується відповідності, усі провідні постачальники хмарних технологій погодилися з більшістю відомих програм акредитації, таких як PCI, NIST,

HIPAA та GDPR. Однак клієнти несуть відповідальність за забезпечення відповідності їх робочого навантаження та процесів даних.

Крім того, враховуючи погану видимість і динаміку хмарного середовища, процес аудиту відповідності може бути трудомістким, якщо клієнти не використовують інструменти, які виконують у реальному часі безперервні перевірки відповідності на наявність неправильних конфігурацій, включаючи попередження та автоматичне виправлення за потреби.

Принципи архітектури хмарної безпеки

У цьому розділі розглянуто архітектурні принципи, які повинні бути враховані в будь-якому розгортанні хмари корпоративного рівня, якщо воно збирається вирішувати проблеми обмеженої видимості, необхідності детальної авторизації та керування привілеями, плавної інтеграції з автоматизованими процесами CI/CD, узгодженості між складними інфраструктурами та дотримання вимог відповідності.

Безпека периметра мережі з розширеним захистом від загроз

В останні роки спостерігається явне зростання як частоти атак, так і складності цих атак. Хмара розширює поверхню атаки організації та загалом створює нові виклики безпеці з точки зору того, як ми виконуємо сканування вразливостей і захищаємо веб-додатки.

Як зазначалося вище (див. Розуміння моделі спільної відповідальності), у моделі обслуговування IaaS постачальник відповідає за безпеку «хмари», тоді як клієнт повинен взяти на себе відповідальність за безпеку того, що «в» хмарі. Це покладає на клієнта відповідальність за впровадження найкращого у своєму класі вдосконаленого захисту та запобігання загрозам на периметрі мережі (тобто головних вузлах, через які трафік входить і виходить із ресурсів у хмарному середовищі) відповідно до моделі спільної відповідальності.

Інші вектори атак, які потрібно захистити

Інші вектори атак, на які мають бути спрямовані проєкти захисту хмари:

DATA	Дані, що залишаються, мають бути захищені на ресурсах хмарного сховища, таких як Amazon S3, Azure Storage та Google Cloud Storage Bucket. Дані під час пересилання мають бути зашифровані за допомогою таких інструментів, як помічник монтування Amazon EFS, шифрування Azure на стороні клієнта або на стороні сервера та шифрування GCP під час передавання.
COMPUTE	Окрім стандартних віртуальних машин, хмарна архітектура безпеки повинна враховувати сучасні високорозподілені та динамічні архітектури додатків, які базуються переважно на безсерверних архітектурах, мікросервісах, функціях як сервіс (FaaS), інфраструктурі як код (IaC) тощо. Дизайн також має забезпечувати захист передових хмарних продуктів PaaS, які підтримують ці архітектури та сервіси, зокрема AWS Lambda, Azure Functions, Google Cloud Functions, Amazon API Gateway, Amazon Elastic Container Registry та Azure API Management.
MESSAGING	Подібним чином сучасні веб-додатки часто використовують повідомлення для обміну даними між своїми розподіленими компонентами. Для керованих служб обміну повідомленнями, таких як Google Cloud's Cloud Pub/Sub, Azure Service Bus і Amazon Simple Notification Service (SNS), необхідно запровадити захист периметра.
IDENTITY	Ідентифікація в хмарних середовищах складається з доступу до хмарного середовища (наприклад, надання нової машини), а також доступу до кожного конкретного сервісу (наприклад, RDP-доступ до цієї нової машини). Клієнти мають ідентифікувати та авторизувати користувачів, які бажають отримати доступ до їхніх публічних хмарних ресурсів. Для служб контролю доступу постачальників, таких як AWS Identity and Access Management (IAM) і Azure Active Directory, необхідно запровадити захист на рівні керування. До того ж клієнт повинен використовувати групи безпеки для динамічного контролю доступу користувачів, які ввійшли в систему, до ресурсів у хмарі.

Безпека за проєктом

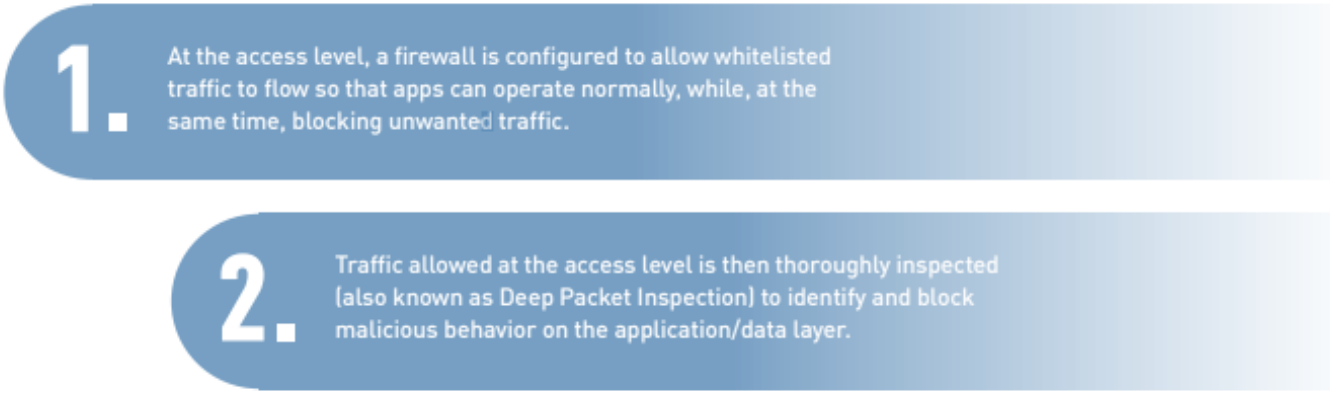
Неправильна конфігурація є однією з основних причин витоку даних у хмарі. «Безпека за проєктом» означає, що архітектура безпеки хмари повинна, де це можливо, використовувати характеристики «проєкту» хмарної інфраструктури для досягнення незмінної безпеки (тобто безпеки, яка не може бути скомпрометована неправильною конфігурацією політики або іншими шляхами). Наприклад, може існувати вимога, щоб певне хмарне сховище даних ніколи не виходило в мережу Інтернет. Замість конфігурації брандмауера найкращою практикою «безпеки за проєктом» було б ніколи не мати жодного з'єднання між сховищем і хабом, що виходить в мережу Інтернет.

Цей підхід до безпеки є ще одним прикладом того, як Zero Trust можна і потрібно використовувати для ефективного захисту хмарних ресурсів.

Сегментація та мікросегментація

Нещодавнє дослідження Proofpoint про понад 100 000 несанкціонованих входів у мільйони облікових записів хмарних користувачів, що контролюються, показує, що кожне третє порушення включало сторонній рух між двома або більше точками в мережі. Після порушення периметра мережі зловмисник зміг заразити інші машини в цій мережі. Така поведінка підсилює необхідність впровадження фундаментального принципу моделі нульової довіри, яка полягає в подальшому сегментуванні мережі за програмами чи службами та розміщенні найкращого в своєму класі захисту між цими сегментами, щоб зловмисник не міг вільно пересуватися.

Щоб реалізувати сегментацію як частину моделі Zero Trust, а також дозволити програмам безпечно спілкуватися одна з одною, безпеку для кожного сегмента мережі потрібно забезпечити двома точками контролю безпеки:



Хмарна архітектура безпеки організації повинна сприяти автоматизації процесів і завдань із самого початку.

Спритність

За вимогою характеристики гнучкості та масштабування публічної хмари повинні надавати можливість розгорнути та керувати робочим навантаженням для вашого бізнесу з найвищою гнучкістю та швидкістю. Сучасна ефективна бізнес-практика неможлива, якщо для отримання серверів і послуг потрібні тижні або якщо робочі процеси безпеки є виснажливими та трудомісткими.

Ваша хмарна архітектура безпеки повинна культивувати та бути гнучкою, гарантуючи, що швидкість не сприятиме втраті контролю чи бізнес-ризику. Цей принцип підтримується шляхом делегування прав власності, що надає DevOps, між різними зацікавленими сторонами в організації, власниками програм та іншими особами з розширеними рівнями повноважень над їхніми ресурсами та середовищами. Використовуючи інфраструктуру як код та інші методи, команди DevOps можуть динамічно та програмно впроваджувати захист контролю доступу всередині та між своїми власними робочими навантаженнями, залишаючи захист периметра та розширену безпеку командам мережі та безпеки.

Автоматизація. Ефективність. Еластичність.

Хмарна автоматизація — це широкий термін, який стосується процесів та інструментів, які організація використовує для зменшення ручних зусиль, пов’язаних із наданням і керуванням хмарними ресурсами. Це різко контрастує із застарілими підходами безпеки, які значною мірою покладаються на ручний захист робочих навантажень і ресурсів. Якщо гнучкість бізнесу обмежена вузькими місцями безпеки, вони будуть або уникнені, або просто розкриті достатньо широко, щоб не заважати, що може піддати організацію більшому ризику.

Зменшення людського фактора в операціях захисту хмари за допомогою автоматизації та програмних операцій не тільки підтримує гнучкість бізнесу та операційну ефективність, але й зменшує ризик людської помилки (тобто неправильної конфігурації), яка є дуже важливим фактором порушень безпеки. Хмарна архітектура безпеки організації повинна сприяти автоматизації процесів і завдань від самого початку. Це починається на етапі підготовки середовища (наприклад, за допомогою попередньо налаштованих шаблонів) і продовжується повсякденними операціями, такими як використання динамічних адаптивних політик безпеки, які не потребують втручання людини.

Безмежність

Для корпоративних клієнтів стає звичайною практикою використовувати Multi-Cloud стратегію (тобто використання кількох постачальників хмарних обчислень в одному середовищі). Незважаючи на те, що ця стратегія має багато переваг, використання безлічі нових технологій від кількох хмарних провайдерів у різних географічних місцях несе з собою кілька проблем безпеки, зокрема:

- ✓ Застосування узгодженої політики безпеки в усіх середовищах.
- ✓ Встановлення уніфікованого та централізованого управління системою безпеки організації (тобто виявлення, усунення та вирішення інцидентів безпеки з одного місця).
- ✓ Безпечне з'єднання різноманітних хмарних середовищ у багатьох місцях.
- ✓ Дозволяє програмам легко та безпечно спілкуватися одна з одною незалежно від їх розташування.
- ✓ Отримання видимості транспортних потоків усередині та ззовні.

Таким чином, ефективна хмарна архітектура безпеки повинна бути незалежною від хмарної платформи. Архітектура повинна підтримувати уніфіковану політику в публічних/приватних і локальних середовищах, дозволяючи командам безпеки зосереджуватися на безпеці, а не на механізмі перемикання контекстів між інструментами безпеки та послугами, що стосуються постачальників.

Відповідність

Як обговорювалося вище в розділі «Відповідність і правила», хмара створює значні проблеми щодо відповідності та аудиту відповідності. Хмарна архітектура безпеки організації має забезпечувати відповідність робочих навантажень і даних, а також безпроблемне проведення аудитів навіть у складних Multi-Cloud і гібридних інфраструктурах.

Резюме

Основними факторами впровадження хмари є гнучкість, коротший час виходу на ринок і здатність швидше впроваджувати інновації. Завдання для CISO полягає в тому, як підтримати потреби бізнесу щодо впровадження та трансформації хмари без шкоди для безпеки чи швидкості.

У цьому документі ми пояснюємо, чому клієнти повинні переглянути свою стратегію хмарної безпеки та запровадити хмарні архітектури безпеки, які надають:

- Більш гнучкі та еластичні рішення безпеки
- Усі бізнес-переваги роботи в хмарі, але в безпечний спосіб
- Розширений і комплексний захист від загроз

Однак, оскільки компанії переносять сучасні та традиційні робочі навантаження в публічну хмару, важливо, щоб вони розуміли свою роль у моделях спільної відповідальності хмарних постачальників. У моделі обслуговування IaaS, наприклад, постачальник відповідає за безпеку самої інфраструктури, але клієнти повинні взяти на себе відповідальність за захист своїх власних даних, програм і робочих навантажень. Це завдання стає ще складнішим при додаванні інших хмарних служб, таких як PaaS і SaaS.

Інструменти, які пропонують постачальники хмарних технологій, щоб допомогти клієнтам упровадити безпечне розгортання хмарних технологій, часто є недієвими перед обличчям сучасних загроз. Також важко керувати Multi-Cloud та гібридними середовищами, використовуючи фрагментований стек, що складається з інструментів, призначених для постачальника.

Враховуючи складність і масштаби сучасного ландшафту загроз, хмарна безпека повинна застосовувати підхід нульової довіри, за якого користувачі чи машини за замовчуванням не довіряють один одному. Користувачам слід надати лише мінімальні привілеї, тобто ті, які їм дійсно потрібні для виконання своїх завдань. Увесь трафік має бути перевірений, а поверхні атак потрібно мінімізувати за допомогою ефективної сегментації мережі. Мікросегментація мереж, визначених програмним забезпеченням і архітектурою розподілених додатків ще більше підвищує рівень безпеки.

Є кілька ключових принципів, які повинні лежати в основі будь-якої хмарної архітектури безпеки:

- ✓ Розширений захист для мереж, а також векторів атак даних, обчислень, обміну повідомленнями та ідентифікації.
- ✓ Систематичне розділення всіх потоків трафіку (до, з і всередині хмарних середовищ).

- ✓ Сегментація за додатком або службою та мікросегментація хостів, що працюють в одному сегменті або віддалено.
- ✓ Культивування гнучкості для DevOps і напрямків бізнесу без шкоди для корпоративної безпеки.
- ✓ Автоматизація, ефективність і гнучкість, щоб не відставати від швидкості бізнесу, одночасно зменшуючи ризик людської помилки та неправильні конфігурації завдяки вбудованому захисту в код.
- ✓ Незалежна від платформи архітектура без меж, у якій політики безпеки можуть узгоджено застосовуватися в усіх середовищах.

IT Specialist LLC

Українська компанія-інтегратор, заснована в 2014 році.
Ми об'єднали в одну команду висококласних, досвідчених і сертифікованих фахівців сучасного ринку IT.

- **120** діючих сертифікатів спеціалістів компанії
- **200+** успішно реалізованих проектів із топ-вендорами у світі
- **24/7** технічна підтримка та SLA

CHECK POINT

CHECK POINT STARS PARTNER

CHECK POINT YOU DESERVE THE BEST SECURITY CLOUDGUARD PARTNER

CHECK POINT YOU DESERVE THE BEST SECURITY CLOUD SECURITY PARTNER

CHECK POINT YOU DESERVE THE BEST SECURITY HARMONY PARTNER