# Akamai Guardicore: новий рівень кібербезпеки для вашого бізнесу

Мікросегментація мереж — засіб проти сучасних кіберзагроз. Антон НІКІТІН, Senior Cybersecurity Engineer SEETON (ТОВ «СІТОН ГРУП»), робить огляд рішення для мікросегментації від компанії Akamai.

Щодня зловмисники вигадують нові способи проникнути за периметр вашої мережі. Традиційні методи захисту іноді не в змозі стримати хвилю комплексних атак з використанням, наприклад, ransomware або zero-day вразливостей. Відповіддю на ці виклики є **мікросегментація** — новий підхід до кібербезпеки, який полягає в розділенні мережі на гранульовані та ізольовані зони, зупиняючи зловмисників на їхньому шляху. А серед рішень для мікросегментації особливе місце посідає **Akamai Guardicore** — інструмент, який поєднує простоту, інтуїтивність та функціональність, забезпечуючи захист роботи вашого бізнесу та його кіберстійкість.

## Що таке мікросегментація і чому вона потрібна бізнесу?

Сучасні IT-інфраструктури еволюціонували в складний гібрид з локальних датацентрів, хмарних сервісів, віртуальних машин і контейнеризованих середовищ. Таке розмаїття відкриває для бізнесу низку можливостей, але водночас розширює поверхню для атак на інфраструктуру компанії. Традиційні міжмережеві екрани вже не можуть гарантувати стовідсоткову безпеку, адже периметр мережі розмитий, а кожен сервер чи пристрій — це потенційна точка входу для зловмисників.

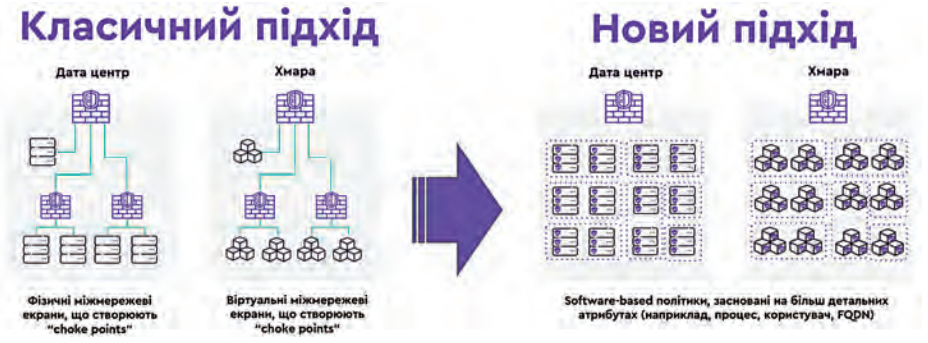


**Рис. 1.** Міжмережеві екрани vs мікросегментація

Мікросегментація вирішує вищеописані проблеми шляхом розділення мережі на дрібні сегменти з індивідуальними політиками безпеки, тим самим захищаючи вашу інфраструктуру від так званого Lateral Movement (поширення мережею). Тобто, коли зловмисник проникає в один сегмент, він не може вільно пересуватися далі, і його діяльність буде заблокована (**рис. 1**). Ви можете сказати: «Я сегментую мережу за допомогою міжмережевих екранів», або: «Я використовую для цього VLAN-и». І справді, ці підходи створюють певний рівень ізоляції. Але запитайте себе: скільки хостів, серверів, віртуальних машин чи контейнерів знаходяться у кожному з таких «сегментів»? Потрібно мати на увазі, що при проникненні в середину мережі компанії зловмисник, потенційно, зможе виконати Lateral movement або завдати шкоди всім хостам у межах даного сегменту. Окрім того, сегментація на рівні міжмережевих екранів працює буквально на мережевому/транспортному рівні, використовуючи лише порт та IP-адресу (в окремих випадках ще й протокол/застосунок, за умови використання NGFW).

Але припустимо, що сегментацію можна реалізувати не на рівні host-to-host, VLAN-ів або на основі IP-адрес та портів, а значно глибше — на рівні від окремого процесу до іншого процесу, навіть якщо вони знаходяться на різних хостах, в різних підмережах або ЦОДах.

Саме так працює **Akamai Guardicore**, про що ми і поговоримо далі.

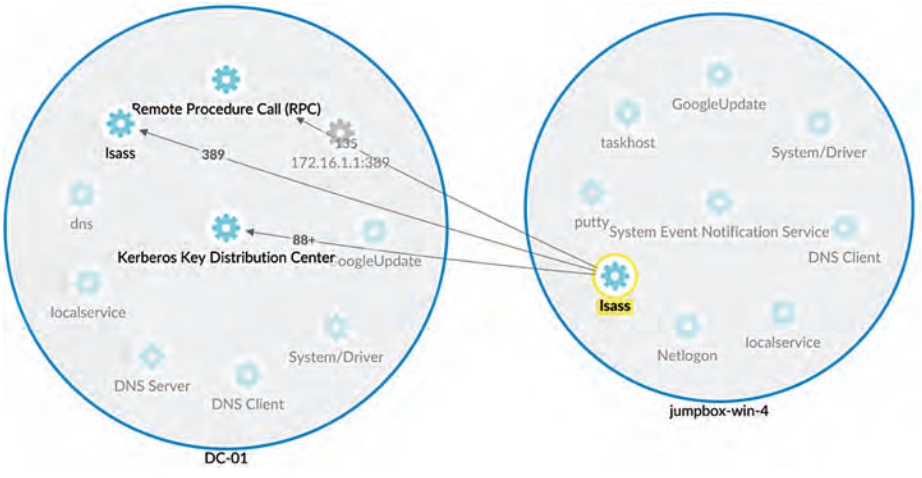


**Рис. 2.** Приклад візуалізації комунікації в Akamai Guardicore

## Як працює Akamai Guardicore?

Уявіть собі детальну мапу IT-інфраструктури компанії, що містить всі комунікації між хостами у форматі: сервер-1 комунікував з сервером-2 по порту 443 шляхом запуску процесу curl.exe користувачем administrator на сервері-1 для комунікації із сервісом nginx, розгорнутому на сервері-2. Цікаво, правда? Одразу можна побачити рівень деталізації інформації порівняно з класичним підходом до сегментації. Для прикладу, на **рис. 2** представлено

варіант комунікації сервісу lsass на сервері Jumpbox-win-4 з сервісами на сервері DC-01. Варто зауважити, що ви маєте змогу контролювати ці комунікації, використавши будь-який з атрибутів (process, port, hostname, IP-address, protocol, user тощо)!

На **рис. 3** зображено приклад детальної інформації про комунікацію між двома сервісами.

«Сегментація на рівні сервісів? — Так. — Сегментація з врахуванням користувачів (identity-based)? — Без питань. Візуалізація мапи мережі? — Легко». Саме так працює Akamai Guardicore, збираючи дані через агенти, мережеві колектори та інтеграції, в тому числі з хмарними провайдерами. Дана інформація перетворюється на динамічну візуалізацію, яка дозволяє спеціалістам з безпеки бачити все: хто, що і коли робить у мережі компанії.

До того ж візуалізація — це не просто мапа. Завдяки штучному інтелекту рішення пропонує готові шаблони політик, які можна налаштувати під потреби бізнесу. Бажаєте захистити критичний застосунок чи зупинити ransomware? Декілька кліків — і політика готова. Більше того, ці політики не залежать від інфраструктури: їх можна застосовувати без складних змін чи простоїв в мережі компанії. Таким чином, Akamai Guardicore дозволяє вам використовувати як проактивний (попередня мікросегментація), так і реактивний (ізоляція та реагування на інциденти) підходи до захисту мережі.

## Чому це важливо саме для вашого бізнесу?

- *Захист від ransomware.* Програми-вимагачі — «біль» для сучасних компаній. Akamai Guardicore ізолює уражені сегменти, не дозволяючи шкідливому ПЗ поширюватися в мережі компанії.
- *Принцип нульової довіри.* Zero Trust — це не просто модний термін, а необхідність. Рішення Akamai Guardicore дозволяє впровадити цей підхід швидко й ефективно, забезпечуючи перевірку, надання та контроль доступу відповідно до політик компанії.
- *Відповідність вимогам.* Рішення Akamai Guardicore забезпечує відповідність GDPR, HIPAA та іншим регуляторним вимогам
- *Захист ключових активів.* Критичні застосунки — серце будь-якого бізнесу. Мікросегментація сегментує та ізолює їх, створюючи надійний бар'єр від загроз.
- *Безпечна хмарна міграція.* Перехід у хмару — це виклик для інформаційної безпеки. Akamai Guardicore забезпечує безперервний захист і видимість на кожному етапі міграції.
- *Безпека віддаленої роботи.* У світі, де співробітники працюють віддалено, захист кінцевих точок і контроль доступу стають критично важливими. Akamai Guardicore вирішує це завдання.
- *Заміна застарілих мережевих екранів.* Забудьте про внутрішні міжмережеві екрани. Akamai Guardicore пропонує гнучкий і сучасний підхід до захисту внутрішньої мережі, що дозволяє перевершити класичний підхід до організації безпеки мережі компанії.

| Type | Action | Source | Destination | Dest. port | Count | Time | Matching Rule |
|---|---|---|---|---|---|---|---|
| ✓ | Allowed | 172.16.100.105<br>jumpbox-win-4<br>lsass<br>C:\Windows\System32\lsass.exe<br>NT AUTHORITY\SYSTEM | 172.16.1.1<br>dc-01.guardicore.local<br>DC-01<br>Kdc<br>C:\Windows\System32\lsass.exe<br>NT AUTHORITY\SYSTEM | 49155 TCP | 1 | 2025-05-15 08:55 | RUL-DEFAULT |

**Рис. 3.** Розгорнуте представлення тієї ж комунікації

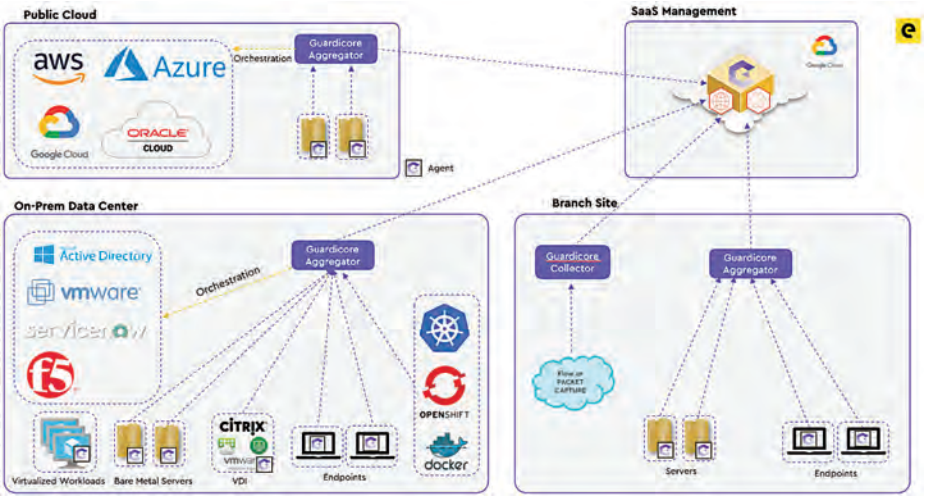


**Рис. 4** Akamai Guardicore — рішення, яке працює у будь-якій інфраструктурі

## Унікальні переваги рішення

Робота Akamai Guardicore не залежить від інфраструктури компанії, оскільки це досягається за рахунок підтримки широкого спектру платформ — від застарілих ОС та майже усіх дистрибутивів Linux до контейнерів, а також безагентного розгортання для, наприклад, IoT-пристроїв (принтерів, камер тощо). Рішення також можна інтегрувати з інструментами безпеки, такими як SIEM, EDR, NGFW тощо. Рішення має декілька варіантів розгортання — у хмарі чи локально, з агентами чи без, що ідеально підходить для інфраструктури будь-якої компанії (**рис. 4**).

## Додаткові функції Akamai Guardicore

- **Візуалізація комунікацій**: Akamai Guardicore автоматизує виявлення та надання динамічного візуального представлення (мапи) для всіх застосунків і робочих навантажень на рівні процесів з ідентифікацією користувацького облікового запису.
- **Сегментація застосунків та мікросегментація**: мапа рішення та інтерфейс для створення та редагування політик дають змогу детально налаштовувати політики безпеки для хостів та виконувати перевірку пристроїв на предмет підозрілих дій, які можуть свідчити про компрометацію хостів.
- **Виявлення компрометації (Breach Detection)** — включає декілька методів виявлення, таких як dynamic deception, виявлення на основі політик, аналіз репутації для файлів, IP-адрес та доменних імен. Додатково Threat Intelligence Firewall надає політики для блокування шкідливих або підозрілих IP-адрес.
- **Автоматичний аналіз** — дозволяє фахівцям з інформаційної безпеки автоматизувати пріоритизацію інцидентів безпеки, тим самим зменшуючи потребу в ручному аналізі за допомогою традиційних інструментів.
- **Реагування на інциденти** — дозволяє в реальному часі ізолювати хости/сегменти, ізолюючи зловмисника або шкідливе ПЗ на ранніх етапах.

*А якщо вас зацікавило рішення класу мікросегментації Akamai Guardicore і у вас з'явилося бажання випробувати його у власній інфраструктурі, — напишіть нам на пошту cs@seeton.pro, і команда* **Cyber Security** *компанії* **Seeton** *допоможе вам у проведенні тестування та впровадженні даного рішення.*