ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТАЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захисту мобільних пристроїв на базі McAfee Mobile Security»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Нікіта МИШКО
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61
МИШКО Нікіта
(прізвище, ім'я)

Керівник к.т.н., доцент БОРСУКОВСЬКИЙ Юрій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

MDM – Управління мобільними пристроями

IAM – управління ідентифікацією та доступом

SIR – Security Incident Response

ШІ – штучний інтелект

ВСТУП

У сучасних умовах стрімкого розвитку інформаційних технологій мобільні пристрої стали невід'ємною частиною роботи в організаціях. Вони використовуються для доступу до корпоративних даних, виконання бізнес-завдань, комунікації та управління процесами. Однак, поряд із перевагами, які забезпечують мобільні пристрої, вони створюють серйозні виклики у сфері інформаційної безпеки.

Мобільні пристрої піддаються різноманітним кіберзагрозам, таким як шкідливе програмне забезпечення, фішингові атаки, несанкціонований доступ до даних та компрометація конфіденційної інформації. Більше того, мобільні пристрої часто використовуються поза межами корпоративної мережі, що ускладнює їхній захист та моніторинг.

В умовах підвищення вимог до конфіденційності, доступності та цілісності інформації в організаціях, впровадження сучасних технологій захисту мобільних пристроїв є критично важливим завданням. Це необхідно не лише для забезпечення безпеки даних, але й для дотримання вимог міжнародних стандартів та законодавства у сфері інформаційної безпеки.

Дослідження у цій сфері дозволяє розробляти ефективні підходи до захисту мобільних пристроїв, враховуючи специфіку роботи організацій та сучасні загрози. Актуальність даної теми зумовлена необхідністю інтеграції мобільних пристроїв у корпоративні інформаційні системи без шкоди для їхньої безпеки, а також постійним зростанням кількості кіберзагроз, які спрямовані на мобільні платформи.

Об'єкт дослідження – захист мобільних пристроїв інформаційної системи організації.

Предмет дослідження – технологія захисту мобільних пристроїв інформаційної системи організації на базі McAfee ePolicy Orchestrator ePolicy.

Метою роботи – розробка варіанту технології захисту мобільних пристроїв інформаційної системи організації та розробка рекомендації щодо її застосування.

Методи дослідження – вивчення літератури з даної теми, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Наукові завдання:

дослідити необхідність управління мобільними пристроями в інформаційній системі організації;

аналіз ризиків використання мобільних пристроїв в інформаційній системі організації;

провести аналіз існуючих технологій захисту мобільних пристроїв інформаційної системи організації;

дослідити методи та засоби захисту мобільних пристроїв інформаційної системи організації

розкрити порядок реалізації технології захисту мобільних пристроїв інформаційної системи організації на базі McAfee ePolicy Orchestrator ePolicy;

надати рекомендації щодо використання McAfee ePolicy Orchestrator ePolicy для захисту мобільних пристроїв інформаційної системи організації.

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

Практичне значення одержаних результатів: запропоновано порядок застосування технології захисту мобільних пристроїв інформаційної системи організації на базі McAfee ePolicy Orchestrator ePolicy, а також розроблено рекомендації для фахівців з кібербезпеки щодо застосування даної технології.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ МОБІЛЬНИХ ПРИСТРОЇВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

1.1. Аналіз необхідності управління мобільними пристроями в інформаційній системі організації

Важливість безпеки мобільних пристроїв неможливо переоцінити. Оскільки щодня все більше людей користуються мобільними пристроями, зростає потреба захищати їх від хакерів. Це робить кібербезпеку мобільних пристроїв важливою сферою, на якій слід зосередитися, гарантуючи захист особистої та робочої інформації від крадіжки та неправомірного використання. Кібербезпека мобільних пристроїв важлива з кількох причин [2, 10,11].

Рис.1.1. Важливість захисту мобільних пристроїв [1]

По-перше, мобільні пристрої часто містять значну особисту інформацію, від контактів і електронних листів до фінансових даних і особистих фотографій. Це робить їх основною мішенню для кіберзлочинців, які хочуть використати цю інформацію для отримання фінансової вигоди або крадіжки особистих даних.

Крім того, мобільні пристрої все частіше використовуються для роботи, доступу до корпоративних мереж і керування конфіденційними бізнес-даними. Без відповідних заходів захисту мобільних пристроїв ці пристрої стають уразливими точками входу для зловмисників, які прагнуть зламати корпоративні системи. Наслідки таких порушень безпеки можуть бути серйозними – від фінансових втрат до шкоди репутації організації.

Зростаюча складність загроз мобільній безпеці, таких як фішинг, зловмисне програмне забезпечення, програми-вимагачі та криптозлом, підкреслює нагальну потребу в надійних заходах мобільної кібербезпеки . Кібербезпека для мобільних пристроїв – це захист самого пристрою та захист даних і мереж, з якими ці пристрої взаємодіють.

Мобільна безпека є критично важливим аспектом загальної кібербезпеки, захищаючи окремих користувачів і організації від потенційної шкоди, спричиненої кібератаками. Забезпечення безпеки мобільних пристроїв є спільною відповідальністю, що вимагає від користувачів, організацій і постачальників рішень безпеки спільної роботи для впровадження ефективних заходів безпеки та практик.

Безпека мобільних пристроїв має велике значення в нашому цифровому світі. Віна діє як щит для персональних пристроїв, які несуть цінну інформацію. До основних переваг захисту мобільних пристрої можна віднести наступне:

1. Комплексний захист особистих і професійних даних: захист мобільного пристрою запобігає несанкціонованому доступу до вашої особистої та робочої інформації, такої як фотографії, електронні листи, контакти та документи компанії. Це забезпечує безпеку ваших особистих даних і захищає бізнес-дані від конкурентів і злодіїв.

2. Захист від кіберзагроз. Ефективні заходи безпеки служать бар'єром проти різноманітних цифрових небезпек, зокрема вірусів, зловмисного програмного забезпечення та фішингових атак. Ці заходи допомагають гарантувати, що хакери не зможуть отримати доступ або пошкодити вашу конфіденційну інформацію.

3. Підвищена впевненість у використанні пристрою. Наявність надійних заходів безпеки дозволяє вам вільніше та впевненіше користуватися своїми мобільними пристроями. Незалежно від того, чи здійснюєте ви покупки в Інтернеті, отримуєте доступ до банківських рахунків чи керуєте робочими завданнями, ви можете робити це, не боячись порушень безпеки.

3. Захист бізнес-інформації та активів. Для компаній безпека мобільних пристроїв дуже важлива для захисту конфіденційних даних компанії, таких як відомості про клієнтів, фінансові записи та стратегічні плани. Це допомагає запобігти витоку даних і несанкціонованому доступу, забезпечуючи безпечне та безпечне продовження бізнес-операцій.

4. Відстеження пристрою та стирання: функції мобільного захисту можуть допомогти знайти ваш пристрій у разі його втрати або викрадення. Якщо відновлення неможливе, ці функції можуть дистанційно заблокувати або стерти пристрій, гарантуючи, що ніхто інший не матиме доступу до вашої особистої інформації. Впровадження надійних заходів безпеки на мобільних пристроях є дуже важливим. Він не тільки захищає окремих людей, але й допомагає компаніям безпечно працювати в нашому все більш цифровому світі.

Рис.1.2. Переваги захисту мобільних пристроїв

Управління мобільними пристроями (MDM) — це перевірена методологія та набір інструментів, які надають робочій силі інструменти та програми для підвищення продуктивності мобільних пристроїв, зберігаючи корпоративні дані в безпеці [1].

Завдяки зрілій платформі MDM відділи безпеки інформаційної системи організації можуть керувати всіма пристроями компанії, незалежно від їх операційної системи. Ефективна платформа MDM допомагає захищати всі пристрої, зберігаючи гнучкість і продуктивність робочої сили організації.

Останніми роками мобільні пристрої стали широко поширеними на підприємствах. Компанії та їхні працівники використовують мобільні пристрої, такі як смартфони, планшети та ноутбуки, для виконання широкого спектру завдань. І оскільки віддалена робота стала важливою, мобільні пристрої стали невід'ємною частиною більшості організацій, будучи життєво важливими інструментами продуктивності та ефективності.

Оскільки корпоративні мобільні пристрої отримують доступ до критично важливих бізнес-даних, вони можуть загрожувати безпеці в разі злому, викрадення або втрати. Таким чином, важливість керування мобільними пристроями зросла так, що керівникам IT та безпеки тепер доручено надавати, керувати та захищати мобільні пристрої у відповідних інформаційних системах організацій.

MDM — це рішення, яке використовує програмне забезпечення як компонент для використання мобільних пристроїв, одночасно захищаючи активи організації, наприклад дані. Організації практикують MDM, застосовуючи програмне забезпечення, процеси та політики безпеки на мобільних пристроях та їхньому використанні. Окрім керування інвентаризацією пристрою та наданням доступу, рішення MDM захищають програми, дані та вміст пристрою. У цьому сенсі MDM і мобільна безпека схожі.

Однак MDM — це підхід, орієнтований на пристрій, тоді як мобільна безпека та уніфіковане керування кінцевими точками еволюціонували до позиції, орієнтованої на користувача. У програмі MDM співробітники можуть отримати

спеціальний робочий пристрій, як-от ноутбуки чи смартфони, або віддалено зареєструвати персональний пристрій. Персональні пристрої отримують рольовий доступ до корпоративних даних і електронної пошти, захищений VPN, GPS-відстеження, захищені паролем програми та інше програмне забезпечення MDM для оптимальної безпеки даних.

Потім програмне забезпечення MDM може відстежувати поведінку та критично важливі для бізнесу дані на зареєстрованих пристроях. А з більш складними рішеннями MDM машинне навчання та ШІ можуть потім аналізувати ці дані. Ці інструменти захищають пристрої від шкідливих програм та інших кіберзагроз. Наприклад, організація може призначити ноутбук або смартфон співробітнику або консультанту, у якому попередньо запрограмовано профіль даних, VPN та інше необхідне програмне забезпечення та програми. У цьому сценарії MDM пропонує найбільший контроль роботодавцю. За допомогою інструментів MDM підприємства можуть відстежувати, контролювати, усувати неполадки та навіть видаляти дані пристрою у разі крадіжки, втрати чи виявлення злому.

Політики MDM надають організаціям розуміння, як організації керуватимуть мобільними пристроями та регулюватимуть їх використання. Щоб налаштувати та опублікувати свої політики та процеси, організації повинні визначити:

Використання парольного захисту

Використовувати відеокамери на пристроях чи ні.

Використовувати підключення до Wi-Fi чи ні

Визначити які налаштування необхідні для пристроїв.

Компоненти засобів управління мобільними пристроями повинні включати наступне:

1. Відстеження пристрою

Кожен пристрій, який організація реєструє або випускає, можна налаштувати для включення GPS-відстеження та інших програм. Програми дозволяють IT-фахівцям підприємства контролювати, оновлювати та усувати неполадки пристрою в режимі реального часу. Вони також можуть виявляти пристрої високого ризику

або несумісні з ними та повідомляти про них, а також віддалено блокувати або стирати дані з пристрою в разі втрати чи викрадення.

2. Мобільний менеджмент

ІТ-відділи закуповують, розгортають, керують і підтримують мобільні пристрої для своїх співробітників, включаючи усунення несправностей функціональних пристроїв. Ці відділи гарантують, що кожен пристрій постачається з необхідними операційними системами та програмами для своїх користувачів, включаючи програми для продуктивності, безпеки та захисту даних, резервного копіювання та відновлення.

3. Безпека програми

Безпека програми може включати упаковку програми, під час якої ІТ-адміністратор застосовує до програми функції безпеки або керування. Потім цю програму повторно розгортають як контейнерну програму. Ці функції безпеки можуть визначити, чи потрібна автентифікація користувача для відкриття програми; чи можна копіювати, вставляти або зберігати дані з програми на пристрої; і чи може користувач ділитися файлом.

4. Управління ідентифікацією та доступом (IAM)

Безпечне керування мобільними пристроями вимагає надійного управління ідентифікацією та доступом (IAM). IAM дозволяє підприємству керувати ідентифікаторами користувачів, пов’язаними з пристроєм. Доступ кожного користувача в організації можна повністю регулювати за допомогою таких функцій, як єдиний вхід (SSO), багатофакторна автентифікація та рольовий доступ.

5. Безпека кінцевої точки

Безпека кінцевих точок охоплює всі пристрої, які мають доступ до корпоративної мережі, включаючи переносні пристрої, датчики Інтернету речей (IoT) і нетрадиційні мобільні пристрої. Безпека кінцевої точки може включати стандартні інструменти безпеки мережі , такі як антивірусне програмне забезпечення та контроль доступу до мережі та реагування на інциденти , фільтрування URL-адрес і захист у хмарі.

Моделі реалізації MDM

MDM можна впроваджувати за допомогою різних моделей залежно від потреб і вимог організації.

Локальний

За допомогою локального MDM інфраструктура розміщується та керується локально самою організацією. Це вимагає від організації придбання та обслуговування необхідного апаратного та програмного забезпечення. Локальний MDM пропонує повний контроль і безпеку, але вимагає вищого рівня технічної експертизи та інвестицій.

Хмарний

Хмарні рішення MDM розміщуються та керуються стороннім постачальником послуг. Організації підключаються до служби MDM через Інтернет. Хмарне MDM пропонує гнучкість, масштабованість і спрощене керування, оскільки постачальник послуг відповідає за обслуговування та оновлення інфраструктури.

Гібрид

Гібридне рішення MDM поєднує в собі елементи як локальних, так і хмарних рішень MDM. Організації можуть розміщувати певні функції та дані локально, а іншими функціями можна керувати в хмарі. Це забезпечує баланс між контролем і гнучкістю, дозволяючи організаціям скористатися як локальною безпекою, так і перевагами хмари.

1.2. Аналіз загроз використання мобільних пристроїв в інформаційній системі організації

Використання мобільних пристроїв в інформаційній системі організації можуть нанести великої шкоди та загрози, тому боротьба з такими загрозами, як фішинг , зловмисне програмне забезпечення , програми-вимагачі та криптозлом, є головною проблемою для мобільних телефонів з кібербезпекою . Важливо мати потужний захист, щоб захистити мобільні пристрої від цих поширених атак.

Розглянемо вплив кожної з перелічених загроз.

Фішинг

Фішинговий електронний лист або SMS-фішинг (смішинг) є великою загрозою для витоку даних.

Рис.1.3. Фішинговий електронний лист або SMS-фішинг (смішинг) як загроза для витоку даних

Фішингові атаки є однією з найпоширеніших загроз мобільній кібербезпеці . Ці атаки зазвичай здійснюються у формі оманливих електронних листів або повідомлень, які обманом змушують користувачів надати конфіденційну інформацію, як-от паролі чи фінансові дані. Оскільки мобільні пристрої використовуються як для особистого, так і для професійного спілкування, ризик стати жертвою спроб фішингу вищий, ніж будь-коли.

Важливо бути обережним із небажаними повідомленнями та електронними листами, особливо тими, які вимагають особистої інформації.

Зловмисне програмне забезпечення та програми-вимагачі

Програми-вимагачі та шкідливі програми є небезпечними кіберзагрозами для мобільних пристроїв.

Рис.1.4. Програми-вимагачі та шкідливі програми є небезпечними кіберзагрозами для мобільних пристроїв

Шкідливе програмне забезпечення та програми-вимагачі становлять серйозну загрозу кібербезпеці мобільних телефонів. Зловмисне програмне забезпечення – це зловмисне програмне забезпечення, призначене для шкоди або використання будь-якого програмованого пристрою чи мережі. Програми-вимагачі – це різновид зловмисного програмного забезпечення, яке блокує або шифрує дані жертви, вимагаючи плату за його випуск.

Мобільні пристрої все частіше стають мішенню таких типів атак, часто через шкідливі програми або скомпрометовані веб-сайти. Оновлення операційної системи та програм є важливим кроком у захисті від цих загроз. Однак люди також повинні навчитися ідентифікувати та захищати себе від цих загроз соціальної інженерії через онлайн-навчання.

Криптоджекінг

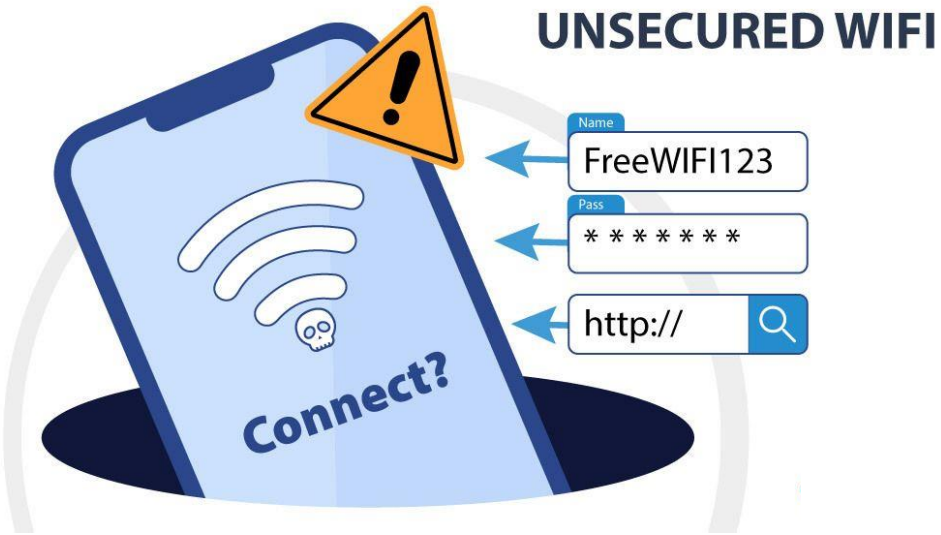
Атаки криптозловмисників дозволяють хакерам використовувати потужність вашого телефону для отримання криптовалюти.

Рис.1.5. Атаки криптозловмисників дозволяють хакерам використовувати потужність мобільного пристрою для отримання криптовалюти

Cryptojacking є новою, але швидко зростаючою загрозою для мобільної кібербезпеки. У ньому хакери використовують обчислювальну потужність мобільного пристрою для майнінгу криптовалют без згоди або відома користувача, по суті це означає, що вони використовують ресурси пристрою для генерації нових цифрових монет. Це може призвести до зниження продуктивності пристрою та збільшення споживання батареї. Користувачі можуть навіть не усвідомлювати, що їхній пристрій зламано, що робить його непомітною та серйозною проблемою.

Незахищений Wi-Fi

Хакери часто створюють підроблені відкриті мережі Wi-Fi, щоб люди могли підключатися до них.



1.6. Підроблені відкриті мережі Wi-Fi

Підключення до незахищених мереж WiFi становить значний ризик для мобільної кібербезпеки . Ці мережі, які часто можна знайти в громадських місцях, таких як кафе чи аеропорти, не шифрують дані. Відсутність шифрування полегшує кіберзлочинцям перехоплення інформації, яку надсилає та отримує ваш пристрій, зокрема паролі, електронні листи та інші конфіденційні дані.

Зручність загальнодоступного Wi-Fi може коштувати конфіденційності та безпеки, тому важливо використовувати захищені мережі або використовувати віртуальну приватну мережу (VPN) для кращого захисту.

Застарілі операційні системи

Застарілі операційні системи становлять значний ризик для безпеки.

Рис.1.7. Застарілі операційні системи становлять значний ризик безпеки

Використання мобільних пристроїв із застарілими операційними системами є значним ризиком для безпеки.

Виробники регулярно випускають оновлення, які виправляють помилки та вразливості безпеки. Коли пристрої працюють із застарілим програмним забезпеченням, вони пропускають ці критичні оновлення, залишаючи їх підданими експлойтам і атакам. Кібербезпека для мобільних пристроїв значною мірою залежить від підтримки операційної системи та всіх програм в актуальному стані, щоб запобігти зловмисникам, які використовують старі вразливості.

Надмірні дозволи програми

Іншою загрозою безпеці мобільних пристроїв є програми, які запитують надмірні дозволи.

Програми, які запитують надмірні дозволи, створюють ще одну загрозу безпеці мобільних пристроїв . Іноді програми вимагають більше доступу до вашого пристрою, ніж це необхідно для їх функціональності, як-от доступ до ваших контактів, місцезнаходження чи навіть камери та мікрофона.

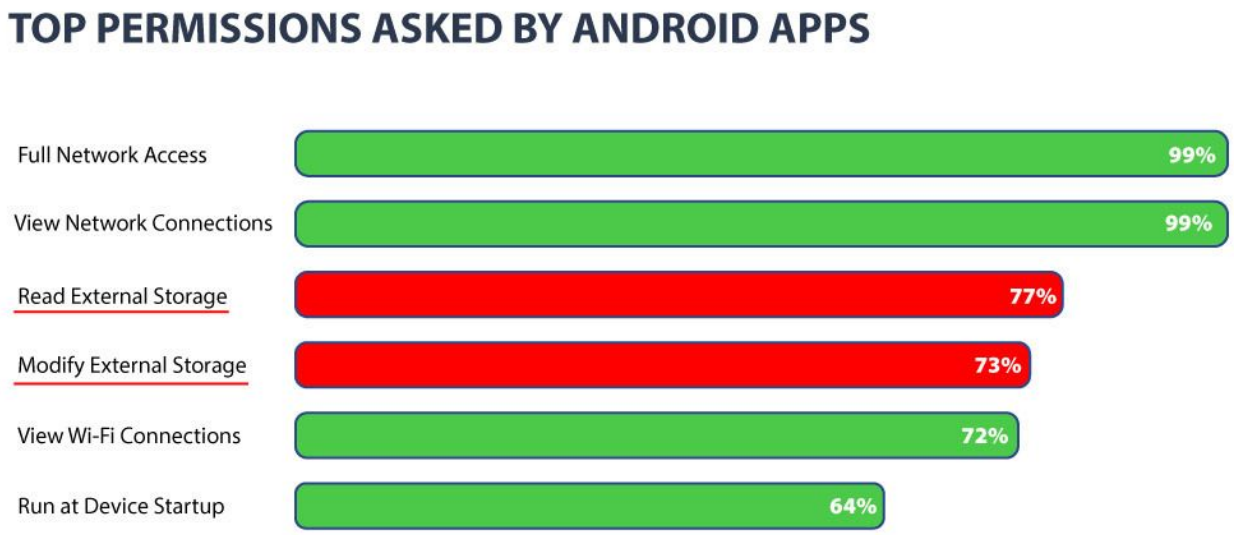


Рис.1.8. Програми, які вимагають надмірних дозволів

Програми, які запитують дозвіл камери, створюють ризик для конфіденційності.

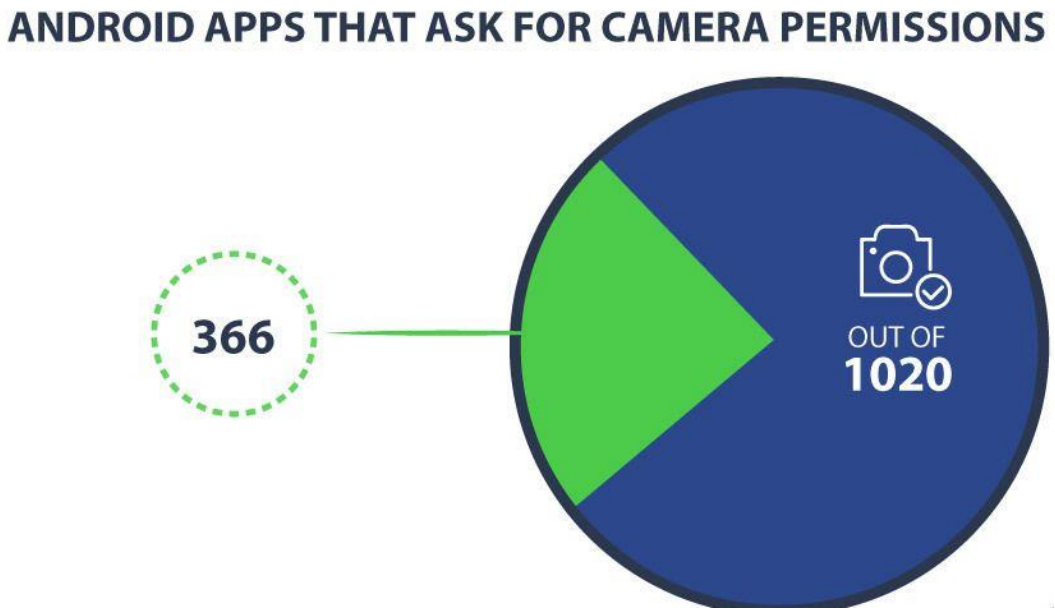


Рис 1.9: Програми, які запитують дозвіл камери, створюють ризик для конфіденційності

Надмірні дозволи програми можуть призвести до непотрібного розкриття даних і ризиків для конфіденційності. Важливо переглянути дозволи, які запитують додатки, перед встановленням і обмежити ці дозволи тими, що строго необхідні для роботи додатка.

1.3. Аналіз технологій захисту мобільних пристроїв інформаційної системи організації

Для аналізу технологій захисту мобільних пристроїв порівняємо найкраще програмне забезпечення для управління мобільними пристроями (MDM), щоб спростити та легко керувати мобільною безпекою для політик Bring Your Own Device (BYOD) [3, 4].

Управління парком пристроїв у різних відділах є відповідальною роботою фахівців. Рішенням є програмне забезпечення MDM, яке дозволить здійснювати необхідний рівень контролю інформаційної системи організації.

Власне кажучи, керування мобільними пристроями (зазвичай називається MDM) — це адміністрування мобільних пристроїв. Смартфони , планшети та все частіше ноутбуки потрапляють під контроль MDM. Нещодавно, з появою Bring

Your Own Device, інструменти керування корпоративною мобільністю (EMM) були включені в MDM.

Однак MDM відрізняється від Уніфікованого керування кінцевими точками (UEM), оскільки це більше стосується всіх інших кінцевих точок пристроїв, від апаратного забезпечення IoT до принтерів , настільних комп'ютерів і переносних пристроїв.

Різні основні функції MDM забезпечують віддалену доступність пристроїв для аудиту, оновлення по повітрю (OTA), ефективну роботу програмного забезпечення та доступність пристроїв для віддаленої діагностики та усунення несправностей. Програмне забезпечення MDM працює на сервері або системі адміністратора та може використовуватися для нагляду за широким спектром пристроїв. Open Mobile Alliance випустив протокол під назвою OMA Device Management, специфікацію, яку використовують більшість інструментів MDM. Його можна знайти на кількох смартфонах, КПК та інших мобільних пристроях.

Хоча використання програмного забезпечення MDM можна вважати нещодавньою розробкою, керування мобільними пристроями бере свій початок у минулому.

TechRadar нещодавно переглянув ключові функції ряду програмного забезпечення для керування мобільними пристроями, щоб допомогти вам вибрати з найкращих доступних пакетів MDM.

Критерії, які слід враховувати при виборі технології для управління мобільними пристроями (MDM) [4, 5]:

Функції безпеки

Підтримка платформ (iOS, Android, Windows, macOS)

Варіанти розгортання (хмарне або локальне)

Зручний інтерфейс

Управління програмами

Відповідність і забезпечення виконання політики

Можливості віддаленого керування

Звітність та аналітика

Інтеграційні можливості

Масштабованість

Вартість і ліцензування

Досвід користувача

Підтримка та оновлення

Геозонування та відстеження місцезнаходження

Підтримка контейнеризації та BYOD

Методи аутентифікації користувача

Резервне копіювання та відновлення даних

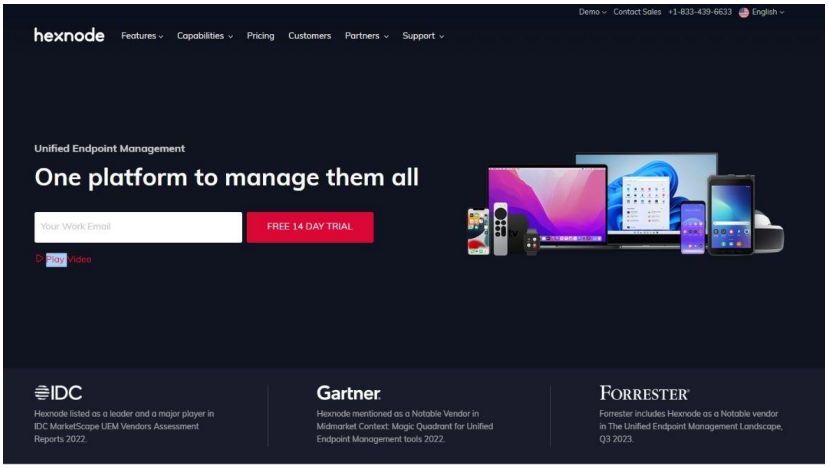
Репутація постачальника

Дотримання правил конфіденційності

Навчання та документація

Розглянемо найбільш популярні технології управління мобільними пристроями.

Hexnode, підрозділ корпоративного програмного забезпечення Mitsogo Inc., є постачальником кібербезпеки, який спеціалізується на рішеннях для керування мобільними пристроями (MDM). Їх однойменна платформа дозволяє IT-командам і командам безпеки керувати всіма пристроями, включно з мобільними пристроями та пристроями IoT, у їхній мережі, включаючи додатки, вміст і ідентифікаційні дані, пов’язані з цими пристроями, за допомогою єдиної уніфікованої платформи.



Why businesses love Hexnode UEM

1.10. Техгологія Hexnode

З центральної консолі керування Hexnode адміністратори можуть контролювати всі мобільні пристрої, підключені до корпоративної мережі, з підтримкою операційних систем Android, iOS, Fire OS і Windows. Адміністратори можуть налаштовувати політику незалежності від платформи, розгортати програми, переглядати звіти про працездатність і відповідність пристрою та віддалено вирішувати проблеми безпеки за допомогою функцій MDM. Варіанти усунення несправностей включають шифрування, віддалене блокування та стирання, автоматичне блокування та моніторинг екрана. Hexnode також пропонує вбудований інструмент захисту електронної пошти, який гарантує, що корпоративні електронні листи відкриваються лише на схвалених пристроях, допомагаючи зменшити поширення компрометації облікового запису. Hexnode особливо сильний у плані захисту парку пристроїв BYOD: у режимі Smart Kiosk захищений контейнер ізолює особисті та робочі дані користувачів, перетворюючи мобільні пристрої на спеціально створені кіоски, щоб забезпечити безпечний доступ до певних додатків і безпечний перегляд. Якщо цей параметр увімкнено, адміністратори можуть віддалено налаштовувати периферійні параметри та переглядати екран пристрою в режимі реального часу за допомогою функцій MDM.

Hexnode порівняно легко розгорнути завдяки інтеграції з Active Directory, Google Workspace і Microsoft 365, що спрощує процес налаштування MDM. Користувачі хвалять платформу за широкі можливості автоматичного звітування, а також за рівень підтримки, що надається командою Hexnode, документацією продукту та форумами спільноти. Ми рекомендуємо Hexnode як надійне рішення MDM для будь-якого бізнесу, якому потрібна краща видимість своїх мобільних пристроїв, особливо тих, які мають значну кількість пристроїв BYOD [5].

IBM Security MaaS360 з Watson

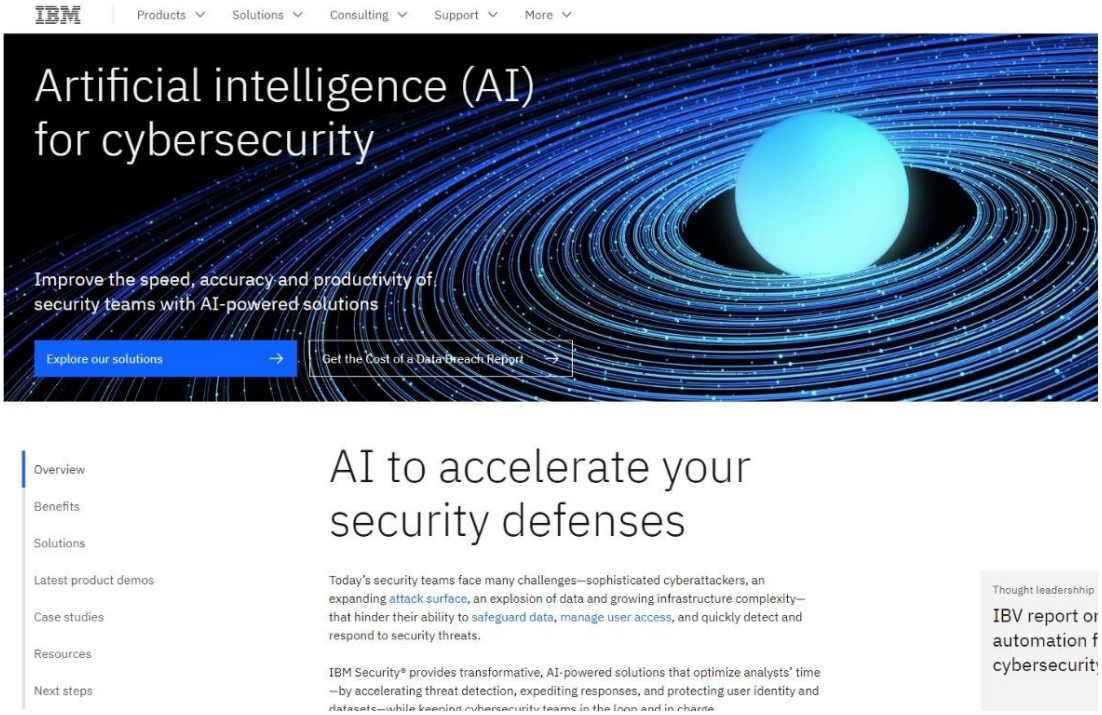


Рис.1.11. технологія IBM Security MaaS360 з Watson

IBM Security — це глобальний постачальник рішень для керування мобільними пристроями (MDM), аналітики, IT-інфраструктури, управління IT та розробки програмного забезпечення. MaaS360 з Watson — це рішення IBM для керування кінцевими точками на основі штучного інтелекту, створене для допомоги IT-командам в управлінні та захисті пристроїв Android, iOS, Windows і Mac, включаючи пристрої IoT, а також у нагляді за програмами та вмістом на цих пристроях.

MaaS360 із Watson дає змогу IT-командам і командам безпеки відстежувати використання пристроїв і програм у їхній мережі та створювати звіти про ці аспекти, а також про безпеку та відповідність пристрою, розширюючи можливості MDM. Адміністратори можуть налаштувати засоби безпеки, такі як єдиний вхід (SSO) і тунелювання на рівні програми, щоб полегшити безпечний віддалений доступ до бізнес-додатків і зменшити ризик порушення ідентифікаційних даних у разі втрати або викрадення пристрою. Ці політики можна застосовувати як до корпоративних пристроїв, так і до пристроїв BYOD. Крім того, адміністратори

можуть встановити додаткові заходи безпеки для BYOD або персональних пристроїв, наприклад обмеження зберігання даних і створення корпоративних персонажів і контейнерів. Функція Mobile Threat Management на платформі визначає та усуває шкідливі та підозрілі програми, перш ніж вони зможуть скомпрометувати пристрій і мережу. Watson Advisor від IBM, використовуючи аналітику на основі штучного інтелекту, надає інформацію про ризики мобільних пристроїв, допомагаючи компаніям ефективно виявляти, сортувати та вирішувати інциденти.

Користувачі високо оцінюють MaaS360 з Watson за зручні процеси реєстрації пристроїв і розповсюдження додатків, а також широкий спектр функцій безпеки, які він пропонує в сфері рішень MDM. IBM також надає цілодобову підтримку через чат, телефон та електронну пошту, обслуговуючи IT-спеціалістів і співробітників служби безпеки з різним рівнем технічних знань, гарантуючи, що користувачі можуть максимізувати можливості платформи. Незважаючи на те, що MaaS360 із Watson задовольняє потреби малого та середнього бізнесу та підприємств, пропонуючи адаптивну ціну для кожного користувача, масштабованість і повну інтеграцію з існуючою інфраструктурою, ми рекомендуємо платформу особливо для малого та середнього бізнесу.

ManageEngine Mobile Device Manager Plus

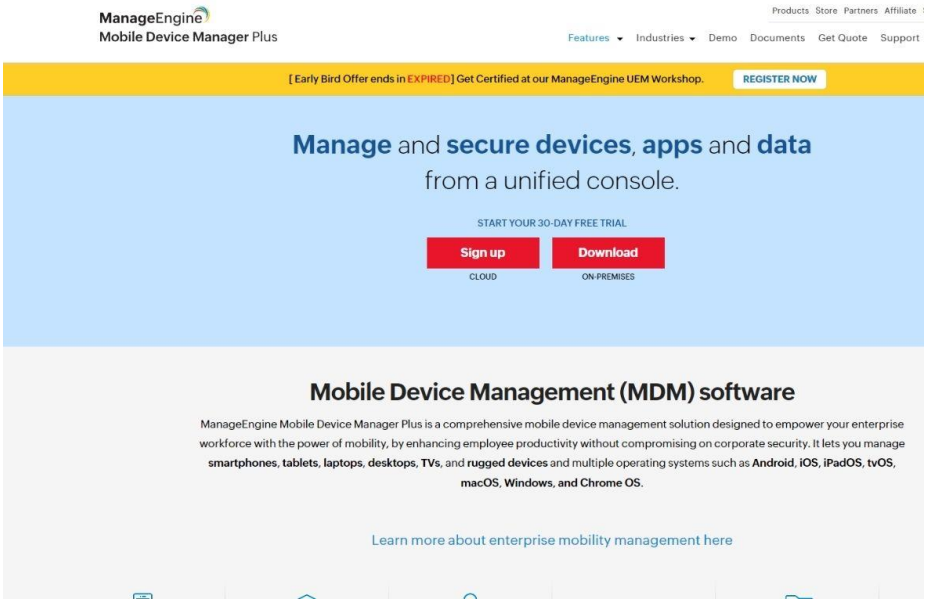


Рис.1.12. ManageEngine Mobile Device Manager Plus

ManageEngine є підрозділом Zoho Corporation, який спеціалізується на рішеннях для керування мобільними пристроями (MDM) і надає програмне забезпечення для керування IT, розроблене для того, щоб допомогти компаніям оптимізувати та інтегрувати свої IT-процеси. Mobile Device Manager Plus — це надійне рішення MDM від ManageEngine, яке пропонує комплексне керування пристроями, програмами та безпекою, а також контейнеризацію для різних типів пристроїв. Це стосується смартфонів, планшетів, ноутбуків, настільних ПК, надійних пристроїв і навіть пристроїв Інтернету речей, таких як телевізори. Mobile Device Manager Plus сумісний із широким спектром операційних систем, включаючи Android, iOS, tvOS, macOS, Windows і Chrome OS, усіма ними можна централізовано керувати через єдиний інтерфейс.

З консолі адміністратора IT-спеціалісти та служби безпеки можуть легко реєструвати й автентифікувати мобільні пристрої, налаштовувати політики двофакторної автентифікації (2FA), керувати налаштуваннями периферійних пристроїв і контролювати спільне використання пристроїв. Адміністратори можуть створювати власні звіти за допомогою інтуїтивно зрозумілого засобу створення звітів із функцією перетягування та планувати автоматичне створення звітів у таких форматах, як PDF, CSV і XLS. Платформа також пропонує низку варіантів усунення несправностей, включаючи функцію чату, віддалений перегляд екрана, віддалене сканування, перезапуск, стирання, функції вимкнення та повний автоматичний віддалений доступ. Mobile Device Manager Plus чудово керує додатками, дозволяючи адміністраторам ефективно розподіляти та керувати додатками між різними типами пристроїв і операційними системами, створювати профілі для розділення робочих і особистих додатків, а також активувати режим термінала, обмежуючи функціональність пристрою авторизованими корпоративними додатками. Крім того, платформа включає додаткові функції безпеки, такі як керування доступом на основі ролей, єдиний вхід, шифрування даних, можливості VPN і можливість обмежити сторонні резервні копії.

ManageEngine Mobile Device Manager Plus надає гнучкі тарифні плани та пропонує варіанти хмарного та локального розгортання. Користувачі цінують зручний інтерфейс платформи та потужні можливості дистанційного керування для ефективного усунення несправностей. Ми рекомендуємо Mobile Device Manager Plus як надійне рішення MDM, призначене для малих і середніх організацій із різними типами пристроїв, яким потрібне інтуїтивно зрозуміле рішення MDM із вбудованими функціями безпеки.

Компанія McAfee, заслужений лідер у розробці рішень інформаційної безпеки, повідомила про реліз нової, 11-ї версії Enterprise Mobility Management (EMM).

Одним із ключових нововведень стала повна інтеграція EMM із єдиною консоллю ePolicy Orchestrator. Тепер керування мобільними пристроями нічим не відрізняється від керування робочими станціями. Інтеграція несе в собі гнучкішу схему застосування політик: глобально, окремо по платформах (iOS, Android, Windows Phone), окремо по групах (наприклад, для співробітників одного відділу), вибірково для конкретного користувача (наприклад, для керівника або ТОП менеджера) та нарешті політика може бути призначена для конкретного пристрою.

Керування великою кількістю пристроїв стало простіше завдяки груповим операціям, які адміністратор системи може виконувати через консоль ePO (оновлення статусу пристрою, очищення даних, розблокування, розгортання пакета та інші).

Отже, надалі буде досліджено технололгію McAfee Mobile Security із єдиною консоллю ePolicy Orchestrator.

2 МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА ПРИКЛАДІ РІШЕННЯ MCAFEE EPOLICY ORCHESTRATOR

2.1. Архітектура та компоненти рішення McAfee ePolicy Orchestrator

McAfee EPO є ключовим компонентом платформи управління безпекою McAfee, яка забезпечує уніфіковане керування безпекою кінцевої точки, мережі та даних, що скорочує час реагування на інциденти, посилює захист, спрощує керування ризиками та безпекою за допомогою автоматизації, наскрізної видимості мережі та безпеки [5, 6].

За допомогою EPO можна виконувати завдання безпеки мережі та багато іншого:

керувати мережевою безпекою та забезпечуйте її за допомогою призначення політик і завдань клієнта;

оновлювати файли визначення виявлення, антивірусні механізми та інший вміст безпеки, необхідний програмному забезпеченню безпеки, щоб забезпечити безпеку ваших керованих систем;

керувати пристроями;

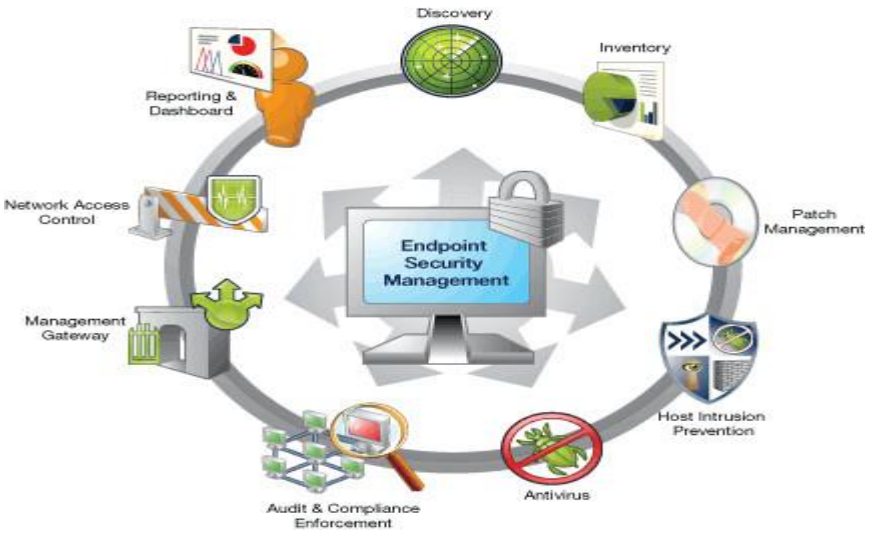


Рис.2.1. Можливості технології McAfee ePolicy Orchestrator

створювати звіти за допомогою вбудованого майстра системи запитів, які відображають інформативні налаштовані користувачем діаграми та таблиці з даними безпеки мережі [6].

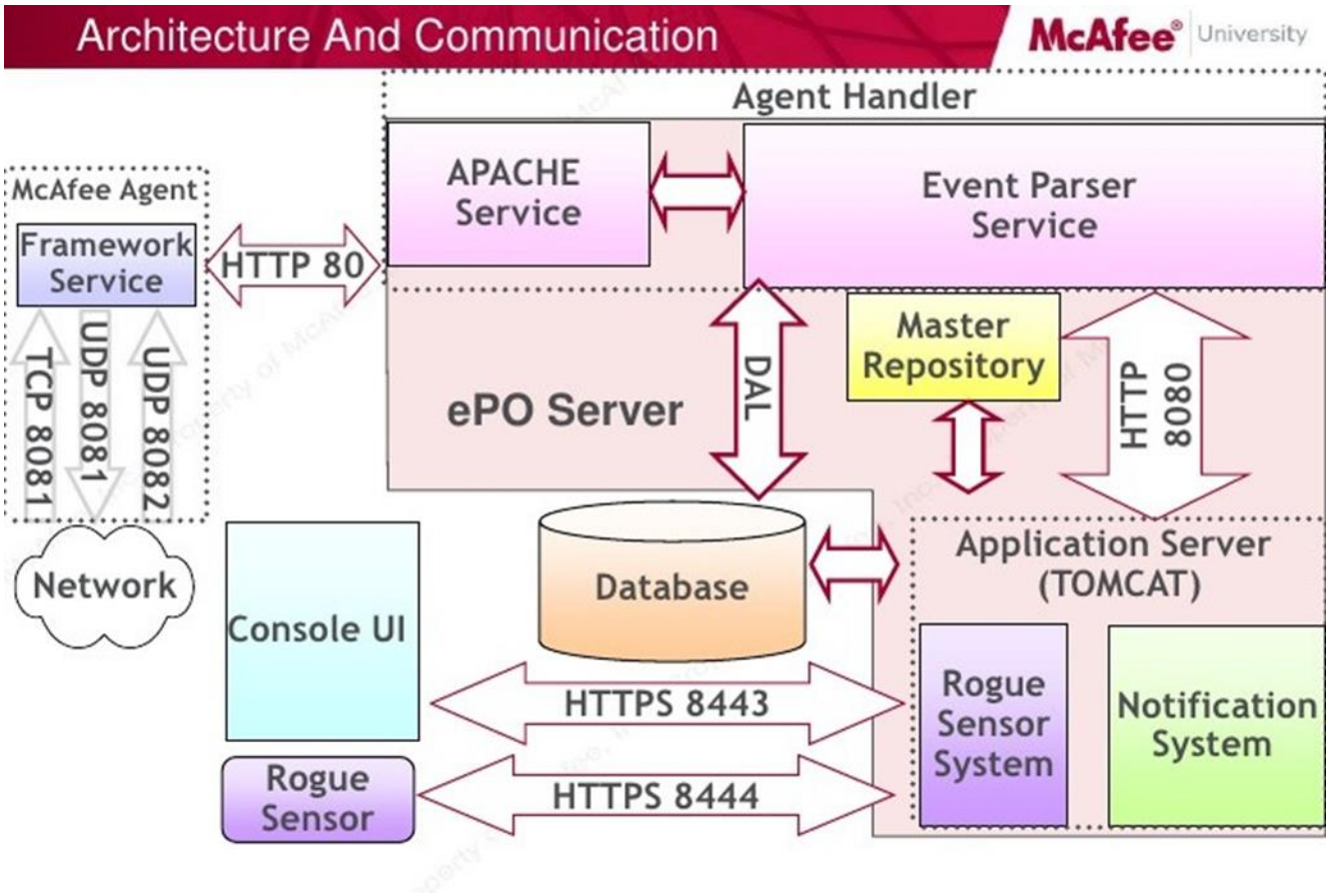


Рис.2.2. Архітектура McAfee ePolicy Orchestrator [6]

До основних компонент архітектури McAfee ePolicy Orchestrator входять:

1. Сервер McAfee ePO - центр керованого середовища. Сервер забезпечує політику безпеки, завдання, контролює оновлення та обробляє події для кожної керованої системи.

2. База даних – центральний компонент для зберігання всіх створених і використовуваних даних.

3. McAfee Agent – може розглядатися як засіб контролю за інформацією між ЕРО та кінцевими системами. Агент отримує оновлення, забезпечує виконання завдань, виконання політики та пересилає події. Він використовує окремий безпечний канал даних для передачі даних на сервер. Агента також можна налаштувати як Суперагента.

4. Головне сховище – центральне розташування для всіх оновлень і підписів McAfee, що розміщено на сервері ePO. Головне сховище отримує вказані користувачем оновлення та підписи з McAfee або з визначених користувачем сайтів джерел.

5. Розподілені репозиторії – локальні точки доступу, стратегічно розміщені в середовищі для агентів, щоб отримувати підписи, оновлення продукту та встановлення продукту з мінімальним впливом на пропускну здатність. Залежно від типу мережі, можна налаштувати як спільні розподілені сховища SuperAgent, HTTP, FTP або UNC.

6. Віддалені обробники агентів – сервер, який можна встановити в різних мережевих розташуваннях, щоб допомогти керувати зв'язком агентів, балансуванням навантаження та оновленнями продуктів. Обробники віддалених агентів складаються з сервера Apache і аналізатора подій. Вони можуть допомогти вам керувати потребами великих або складних мережевих інфраструктур, дозволяючи більше контролювати зв'язок між агентом і сервером.

7. Зареєстровані сервери – використовуються для реєстрації інших серверів на вашому сервері EPO. Зареєстровані типи серверів включають:

Сервер LDAP – використовується для правил призначення політики та для автоматичного створення облікового запису користувача.

Сервер SNMP – використовується для отримання перехоплення SNMP. Додайте інформацію про сервер SNMP, щоб EPO знав, куди надіслати пастку.

Сервер бази даних – використовується для розширення розширених інструментів звітності, які надаються разом з EPO.

В загальному, архітектура McAfee ePolicy Orchestrator, з урахуванням всіх компонетів буд виглядати наступним чином, як це представлено на рис. 2.3

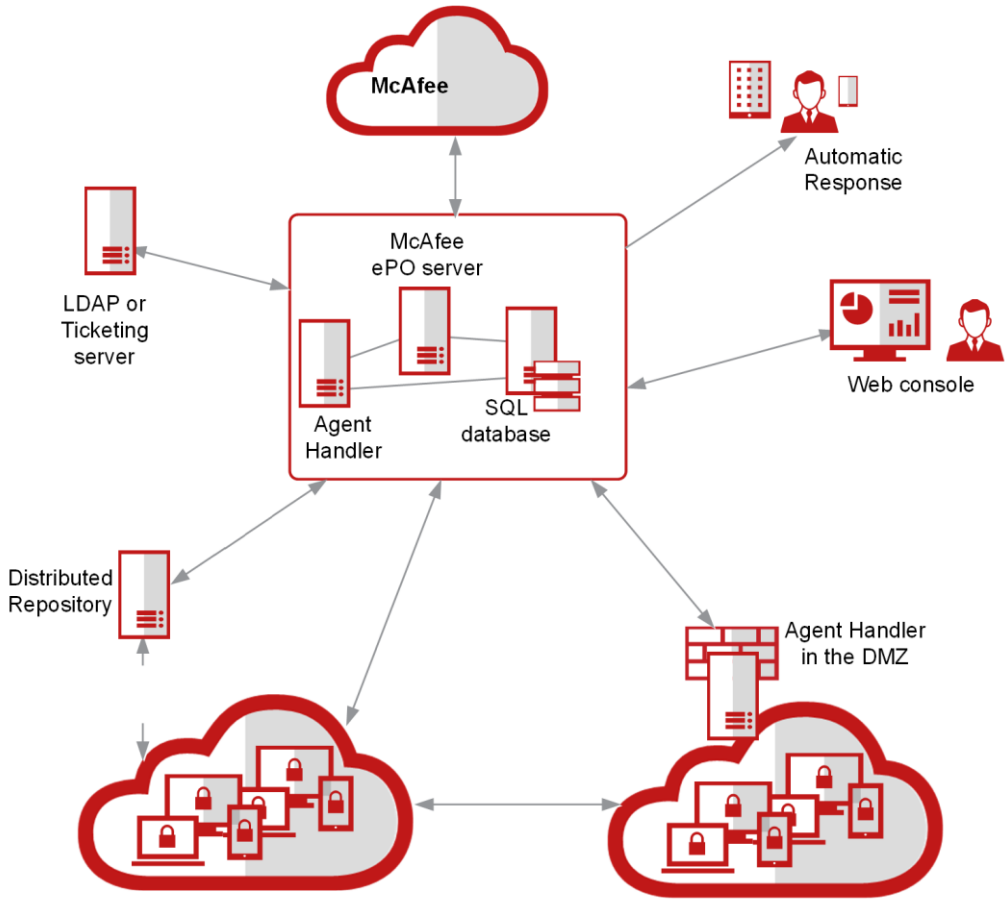


Рис. 2.3. Загальна архітектура McAfee ePolicy Orchestrator

McAfee ePO забезпечує загальну платформу адміністрування для всіх продуктів та інтегрується з понад 130 додатками сторонніх розробників.

McAfee ePO пропонує високоякісні варіанти створення звітів у формі широкого спектру попередньо встановлених шаблонів або параметрів налаштування.

Крім іншого, він також пропонує:

Можливість деактивації та блокування облікових записів адміністратора.

Обмеження можливості входу лише з визначених IP-адрес.

Автоматичне тегування, розширене властивостями продукту.

Покращене обслуговування бази даних – обслуговує завдання, що виконують технічне обслуговування для підвищення продуктивності.

Визначення інтервалу оновлення політики та надсилання подій.

Правила, визначені для груп користувачів, конкретних користувачів і організаційних підрозділів (або комбінація кількох параметрів), визначених у структурі каталогу AD/LDAP.

Контроль доступу до журналів, інформаційних панелей і керування політикою на основі ролей та ідентичності користувача в AD і підтримки автентифікації за допомогою клієнтських сертифікатів.

Можливість інтеграції з декількома доменами AD, опціональна частота синхронізації інформації.

Визначення привілейованих користувачів без блокування, визначеного політикою (лише моніторинг).

Політики, визначені для клієнтів онлайн і офлайн (як підключених, так і відключених від мережі).

Політики зворотної сумісності зі старими версіями.

Отже, McAfee ePolicy Orchestrator є гарною технологією, яка дозволить захицати мобільні пристрої з єдиної консолі. Крім цього вона дозволяє моніторити всі події безпеки, відповідно до встановлених політик та створювати необхідні звіти.

2.2. Функціональність McAfee ePolicy Orchestrator

Архітектура McAfee ePolicy Orchestrator розроблена як надзвичайно гнучкий інструмент. Перспектива встановлення та налаштування є дуже простою. Програмне забезпечення відповідає класичній моделі клієнт-сервер, у якій клієнтська система (система) звертається до сервера для отримання інструкцій щодо встановлення в кожну систему у вашій мережі. Після розгортання агента в системі системою можна керувати за допомогою EPO Box. Захищений зв’язок між сервером і керованою системою є зв’язком, який з’єднує всі компоненти EPO.

Сервер EPO та його компоненти взаємодіють у безпечному мережевому середовищі.

1. Сервер EPO підключається до сервера оновлення McAfee, щоб отримати найновіший вміст безпеки.

2. База даних EPO зберігає всі дані про керовані системи в мережі, включно з властивостями системи, інформацією про політику, структурою каталогу та іншими відповідними потребами сервера даних для підтримки систем в актуальному стані.

3. Агенти McAfee розгортаються в системах, щоб полегшити: застосування політики, оновлення розгортання продуктів.

4. Керовані системи Захищений зв’язок між агентом і сервером (ASSC) відбувається через регулярні проміжки часу між системами та сервером. Якщо в мережі встановлено віддалені обробники агентів, агенти спілкуються із сервером через відповідні обробники на основі призначень.

5. Користувачі входять до консолі EPO для виконання завдань керування безпекою, таких як виконання запитів для звітування про стан безпеки або робота з керованими політиками безпеки програмного забезпечення.

6. Сервер оновлень McAfee розміщує найновіший вміст безпеки, за допомогою якого EPO отримує вміст через заплановані проміжки часу.

7. Розподілені репозиторії, розміщені на локальному вмісті безпеки мережевого хосту, щоб агенти могли швидше отримувати оновлення.

8. Remote AH допомагає масштабувати мережу для обробки більшої кількості агентів за допомогою одного сервера EPO.

9. Сповіщення про автоматичну відповідь надсилаються адміністраторам безпеки, щоб повідомити їх про подію.

3 ТЕХНОЛОГІЯ ЗАХИСТУ МОБІЛЬНИХ ПРИСТРОЇВ ОРГАНІЗАЦІЇ НА БАЗІ MCAFEE EPOLICY ORCHESTRATOR

3.1 Варіант технології McAfee ePolicy Orchestrator з оробниками агентів

Технологія захисту мобільних пристроїв McAfee ePolicy Orchestrator ePolicy працює на базі сервера ePolicy Orchestrator (ePO) 4.5, який відокремлює служби сервера, що працюють із запитами агентів, і додав логіку управління, що дозволяє розгортати екземпляри цих служб. Саме використання обробника агентів в інфраструктурі організації дозволяє управляти, захищати та моніторити стан мобільних пристроїв (рис.3.1)

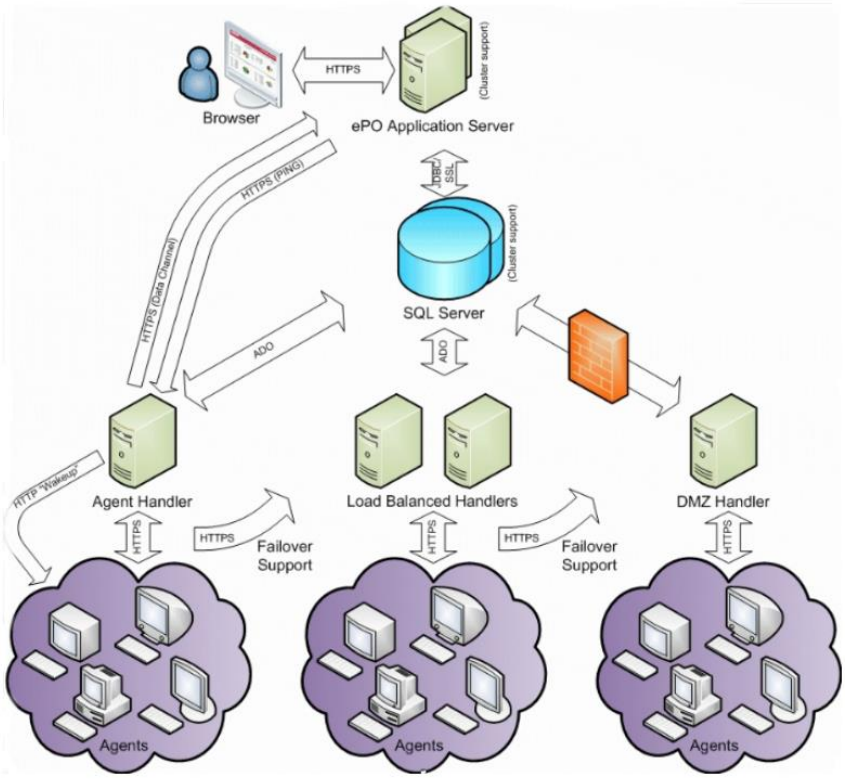


Рис.3.1. Розгортання обробника агентів в McAfee ePolicy Orchestrator

Цей новий компонент інфраструктури ePO отримав назву "Обробник агентів". В ePO 4.0 і попередніх версіях існував єдиний сервер ePO, до якого агенти могли підключатися і отримувати оновлення політик і завдань. Оскільки сервер

ePO відповідає за обробку кожного агента, що підключається до нього, існувало обмеження на розмір розгортання, з яким міг впоратися сервер ePO. Єдиною можливістю збільшити масштабованість одного сервера ePO було перенесення бази даних. В іншому випадку сервер ePO можна було б масштабувати вертикально (за допомогою більшого та швидшого обладнання), а не горизонтально (за допомогою більшої кількості серверів для розподілу навантаження). Впровадження обробників агентів у версії 4.5 дає клієнтам можливість нарощувати логічну інфраструктуру ePO горизонтально, додаючи кілька обробників агентів для масштабування підключення агентів.

Серверне обладнання середнього класу коштує дешевше, ніж сервери високого класу. Використання обробників агентів допомагає економічно ефективніше масштабувати більші інсталяції ePO, не розбиваючи організацію на частини і не використовуючи кілька серверів ePO. Оскільки обробники агентів можна додавати за потреби, вони дозволяють розгортати ePO разом з компанією. Причини для розгортання декількох обробників агентів включають в себе наступні:

Масштабованість - якщо ваш сервер ePO перевантажений, обробляючи велику кількість запитів агентів.

Відмовостійкість - якщо ви хочете дозволити агентам переносити збої між кількома фізичними пристроями і не хочете кластеризувати сервер ePO.

Топологія - якщо вам потрібно керувати системами за NAT або в зовнішній мережі, за умови, що обробник агентів може продовжувати мати високошвидкісне з'єднання з центральною базою даних.

Впровадження обробників агентів у поєднанні з новою версією McAfee Agent 4.5 забезпечує відмовостійкість загальної інфраструктури ePO до втрати одного або декількох обробників агентів. McAfee Agent 4.5 можна налаштувати з резервним списком обробників агентів.

Обробники агентів координують роботу між собою, а сервер додатків спілкується з віддаленими обробниками агентів. Як основний механізм зв'язку використовується черга в базі даних. Обробники агентів часто (приблизно кожні десять секунд) перевіряють робочу чергу і виконують запитувані дії. Типові дії

включають пробудження агентів, розгортання та повідомлення по каналу передачі даних. Це одна з причин, чому кожен обробник агентів потребує відносно швидкого з'єднання з базою даних з низькою затримкою.

У будь-якій інсталяції ePO 4.0 запущено три служби. Їх можна знайти за адресою: Пуск |> "Пуск".

Запустити| Services.msc:

• Сервер додатків (MCAFEETOMCATSRV)

• Сервер Apache (MCAFEEAPACHESRV)

• Парсер подій (MCAFEEEVENTPARSERSRV)

Сервер Apache та аналізатор подій відповідають за зв'язок з McAfee Agent. Ці дві служби працюють разом, щоб отримувати оновлені події та властивості від агентів і надсилати оновлені політики та завдання, призначені адміністраторами в консолі ePO.

Сервер додатків (Tomcat) містить інтерфейс користувача і планувальник завдань сервера.

В ePO 4.5 інсталяція первинного сервера ePO включає всі три служби, наприклад, Apache і Tomcat. У логічному сервері ePO є лише один основний сервер ePO (Рис.3.2).

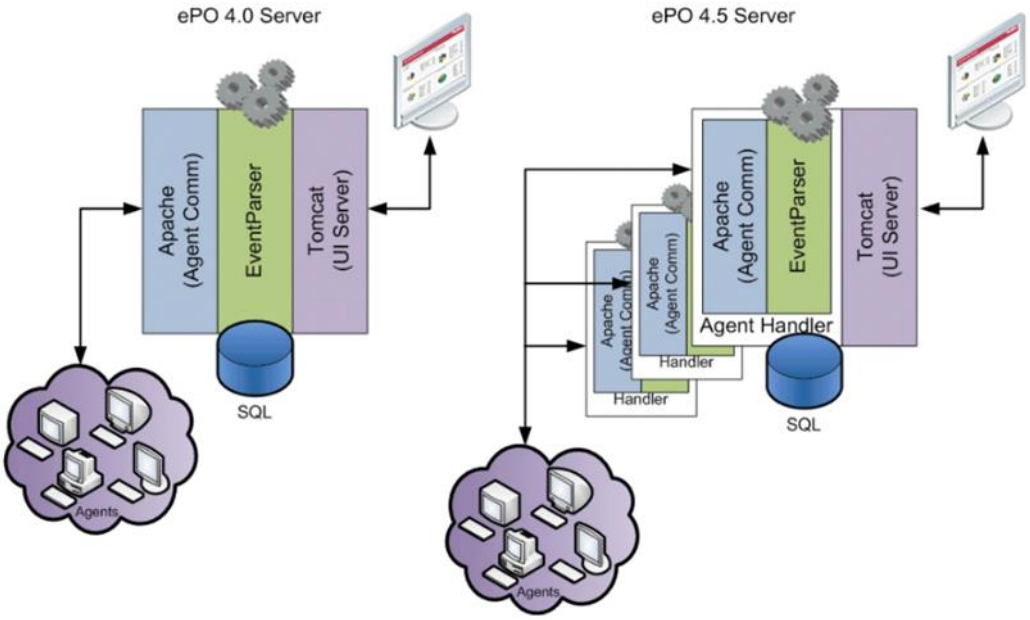


Рис.3.2. Інсталяція Обробника агентів

Інсталяція Обробника агентів включає лише сервер (Apache) та служби аналізатора подій

Невелика кількість обробників агентів може бути розгорнута на окремому обладнанні і співіснувати в межах однієї логічної інфраструктури ePO (рис.3.2).

Обробник агентів інсталюється як частина основного сервера ePO. Цього буде достатньо для багатьох невеликих інсталяцій ePO; у таких випадках додатковий обробник агентів не потрібен.

Для встановлення додаткових обробників агентів у складі сервера ePO 4.5 доступний другий інсталятор, який дозволяє адміністратору встановити обробник агентів на окремому сервері та підключити обробник агентів до основного сервера ePO. Після встановлення додатковий обробник агентів автоматично налаштований на роботу з основним сервером ePO для розподілу вхідних запитів агентів. Консоль ePO можна використовувати для налаштування правил призначення обробника для підтримки більш складних сценаріїв, наприклад, обробник агентів в DMZ або за брандмауером.

Сервер ePO є центральним рішенням для управління продуктами McAfee, а з впровадженням програми SIA інтеграційні SDK доступні і для сторонніх партнерів. Оскільки кількість продуктів, інтегрованих з ePO, збільшується, спроба отримати політику або надіслати події на ePO зростає зі збільшенням навантаження на сервер. Розгортання ePO, в якому використовується лише Virus Scan Enterprise, може забезпечити управління близько 200 тис. систем за допомогою одного сервера. Але в міру розгортання додаткових продуктів і керування ними на тому ж сервері навантаження зменшується максимальна кількість систем, якими можна керувати за допомогою одного і того ж обладнання. Впровадження обробників агентів забезпечує можливість горизонтального масштабування інфраструктури ePO шляхом додавання додаткових серверів для управління еквівалентною або більшою кількістю агентів в рамках одного логічного розгортання ePO.

У ePO 4.0 і попередніх версіях недоступність сервера ePO (наприклад, через оновлення, мережу тощо) не дозволяла агентам отримувати оновлення політик і

завдань, а також звіти події та властивості. Після розгортання декількох обробників агентів, вони можуть бути доступні агентам як кандидати на відмову. Це дозволяє серверу додатків і будь-якій кількості обробників агентів або вийти з ладу, або перейти в автономний режим, при цьому агенти можуть отримувати оновлені завдання або політику від обробника(ів) агентів, що працюють в режимі онлайн.

Поки обробник агентів підключений до бази даних, він може продовжувати обслуговувати агентів, включаючи будь-які зміни в політиці або завданнях, які були внесені до властивостей агентів або користувачем до того, як сервер додатків було виведено в офлайн. Обхід відмов доступний лише в McAfee Agent 4.5. Тоді як ePO 4.0 і попередні версії агента розуміють лише одне розташування сервера.

Файл конфігурації, який надається разом з McAfee Agent 4.5, містить список обробників агентів, що налаштовується. McAfee Agent 4.5 виконуватиме збій за списком обробників агентів доти, доки список не закінчиться або доки він не зможе зв'язатися з дійсним, увімкненим обробником агентів. Однією з проблем використання декількох обробників агентів для обходу відмови є те, що оскільки McAfee Agent 4.0 знає лише про один сервер, додавання обробників агентів не допомагає забезпечити обхід відмови або балансування навантаження для попередніх версій McAfee Agents 4.5.

В ePO 4.0, якщо агент знаходився в мережі NAT, ним можна було керувати, але він не міг безпосередньо звертатися до сервера ePO. Адміністратори не могли виконувати прямі маніпуляції з цими системами. Агенти не могли бути розбуджені сервером, тому вся комунікація повинна була ініціюватися агентом, що збільшувало затримку для певних операцій, ініційованих користувачем. В ePO 4.5 обробник агентів можна розмістити всередині NAT, і він зможе звертатися до систем у регіоні NAT для пробудження, доступу до каналів передачі даних і так далі.

Роумінг. У багатьох організаціях є підгрупа користувачів, які переміщуються між сайтами. Завдяки підтримці та налаштуванню декількох обробників агентів, роумінговий користувач може підключитися до найближчого обробника агента. Це можливо, тільки якщо обробники агентів з усіх місць були налаштовані за

списоком обхідних шляхів. За бажанням адміністратора, політику та сортування систем можна змінити так, щоб роумінгова система отримувала різні політики в кожному місці.

Сумісність. Важливим аспектом реалізації обробника агента було забезпечення безперешкодної зворотної сумісності з версіями McAfee Agent 3.6 і 4.0. Ці версії агента не мали концепцію декількох обробників агентів, тому для сервера ePO доступний лише один запис.

Отже, навіть якщо для обходу відмови налаштовано кілька обробників агентів, агентам 3.6 і 4.0 надсилається лише перший обробник у списку. Отже, обхід відмови з боку агента недоступний для застарілих агентів. Однак, якщо обробники агентів об'єднані у віртуальну групу, використовуючи або програмні або апаратні балансувальники навантаження, єдиний груповий запис буде надіслано цим агентам. Це дає змогу забезпечити балансування навантаження та відмовостійкість навіть для застарілих агентів.

Кеш сховища. McAfee Agent за замовчуванням використовує основний сервер ePO (той самий сервер, що й Tomcat) як головне сховище. Це означає, що агенти будуть повертатися до обробника агентів, якщо вони не зможуть зв'язатися зі своїм налаштованим сховищем для отримання вмісту та оновлень продуктів. Оскільки обробник агентів може бути запущений не на тій же машині, що і справжній головний сховище (на сервері додатків ePO), він повинен обробляти ці запити. Обробники агентів прозоро обробляють запити на програмне забезпечення та кешують необхідні файли після завантаження з основного сховища.

Керування обробниками агентів. Керування обробниками агентів виконується в Меню | Конфігурація | Обробники агентів. У цьому меню відкривається сторінка де налаштовуються правила призначення обробників.

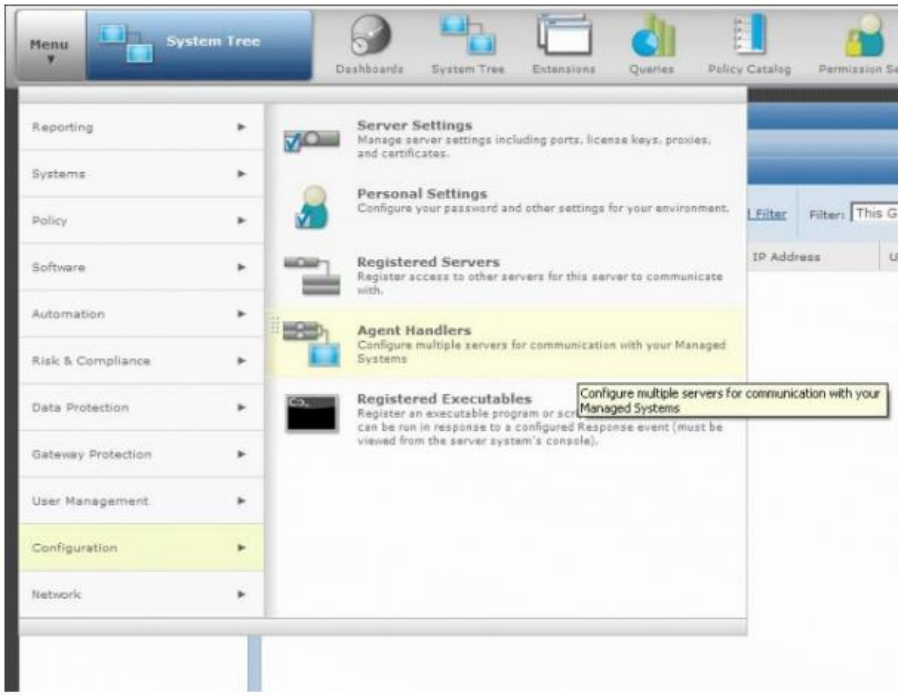


Рис.3.3. Пункт меню обробника агентів

Після встановлення обробника агента він з'явиться у списку доступних обробників агентів, який можна знайти у верхньому лівому елементі на сторінці управління обробниками агентів.

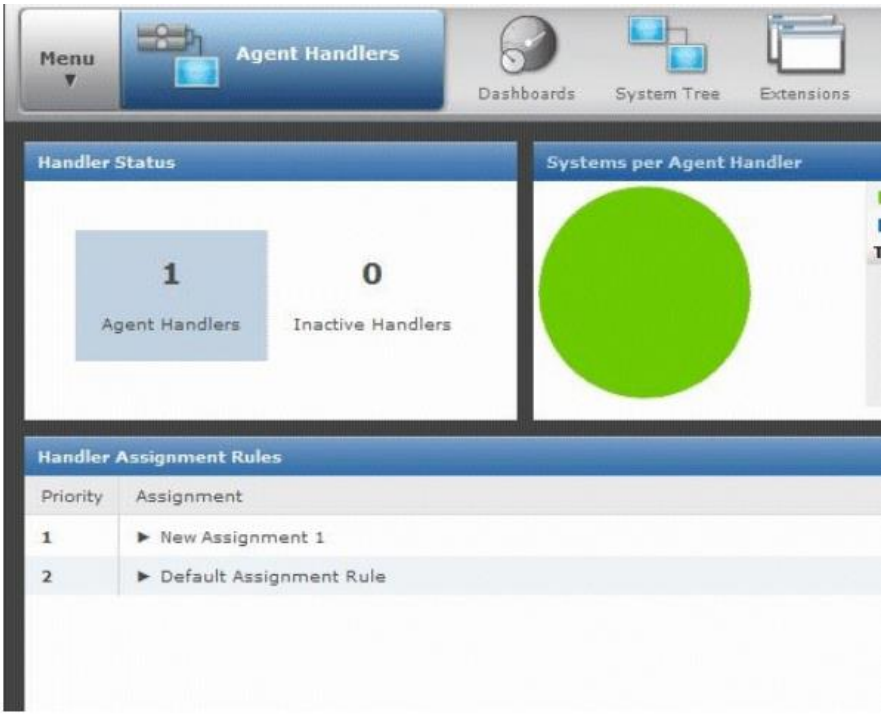


Рис.3.4. Меню управління обробником агента

Рис.3.5. Список обробників агентів

Обробники агентів можуть бути об'єднані в групи обробників для призначення як єдине ціле в правилах призначення обробників. Крім того, якщо ви використовуєте балансувальник навантаження або якщо ваш обробник агентів може бути відомий під різними IP-адресами в більш ніж одному сегменті мережі, ви можете створити віртуальні обробники агентів для використання в правилах призначення. Введіть віртуальне DNS-ім'я та IP-адресу на сторінці. Групи, і віртуальний обробник агентів буде доступний для призначення.

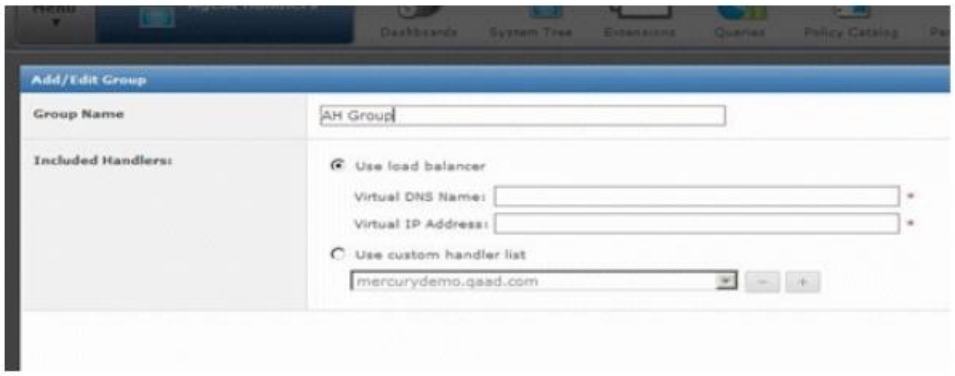


Рис.3.6. Обробники груп та віртуальних агентів

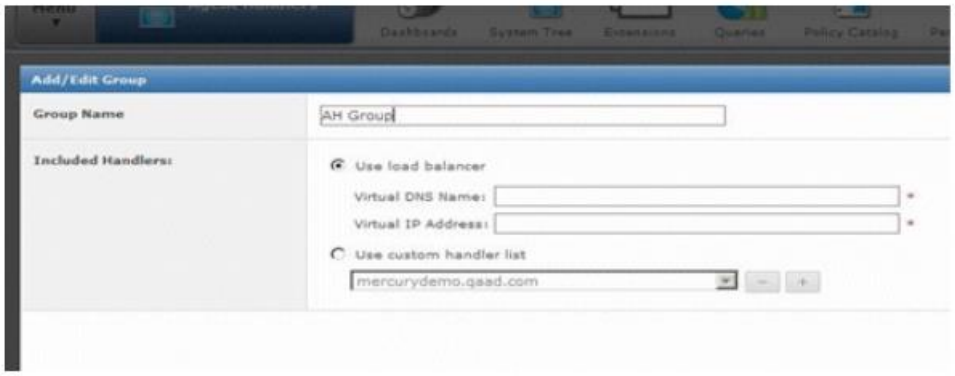


Рис.3.7. Правила призначення обробників агентів

Адміністратор може створювати правила призначення обробників, щоб вказати обробники агентів і їх порядок для кожної системи. Це дозволяє адміністраторам встановлювати основні та резервні обробники агентів по-різному для різних областей дерева.

Отже, технологія McAfee ePolicy Orchestrator з використанням обробників агентів дозволить балансувати навантаження на сервер, що в свою чергу дозволить захищати та моніторити мобільні пристрої організації.

3.2. Технологія інтеграції клієнтського середовища організації до McAfee ePolicy Orchestrator

McAfee ePO з технологією реагування на інциденти безпеки (SIR) з підключенням клієнтського середовища Now Platform. Користувач із цією роллю також за потреби призначає роль аналітика інцидентів безпеки. Користувач із цією роллю взаємодіє та аналізує інциденти безпеки в продукті SIR [7].

Підключення до системи та потік даних

Рис. 3..8. ілюструє клієнтське

середовище. Сервер Now Platform MID потрібен, щоб Now Platform міг підключатися до сервера McAfee ePO (консолі) через плагін розширення ServiceNow . Після підключення необхідно використовувати можливості платформи Now, щоб ініціювати сканування зловмисного програмного забезпечення, ізолювати хост-машини та відновлювати їх у своїй мережі, отримувати результати останнього сканування та збирати системні відомості про ваші активи. Коли ці можливості повертають результати з ваших активів, які відповідають вашим критеріям пошуку, дані завантажуються через сервер MID у ваш екземпляр Now Platform . Дані відображаються у пов’язаних списках інциденту безпеки Now Platform Security Incident Response (SIR). На наступному малюнку показано потік даних для однієї групи кінцевих точок, якими керує одна консоль McAfee ePO .

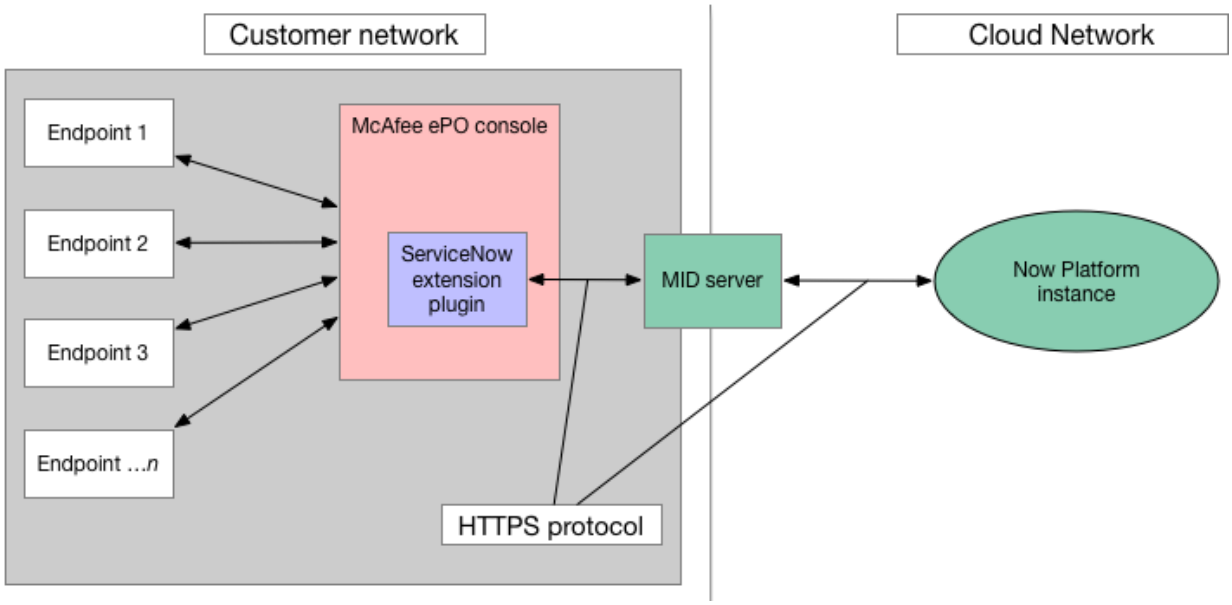


Рис.3.8. Інтеграція клієнтського середовища до Now Platform

Як показано на 3.9, ця інтеграція може підтримувати більше однієї консолі McAfee ePO. Одна група кінцевих точок може керуватися однією консоллю McAfee ePO , а інша група кінцевих точок – іншою консоллю McAfee ePO . Дані з кількох консолей McAfee ePO надходять через один сервер MID. Однак ви також можете віддати перевагу налаштуванню кількох серверів MID, якщо цього вимагає ваша організація.

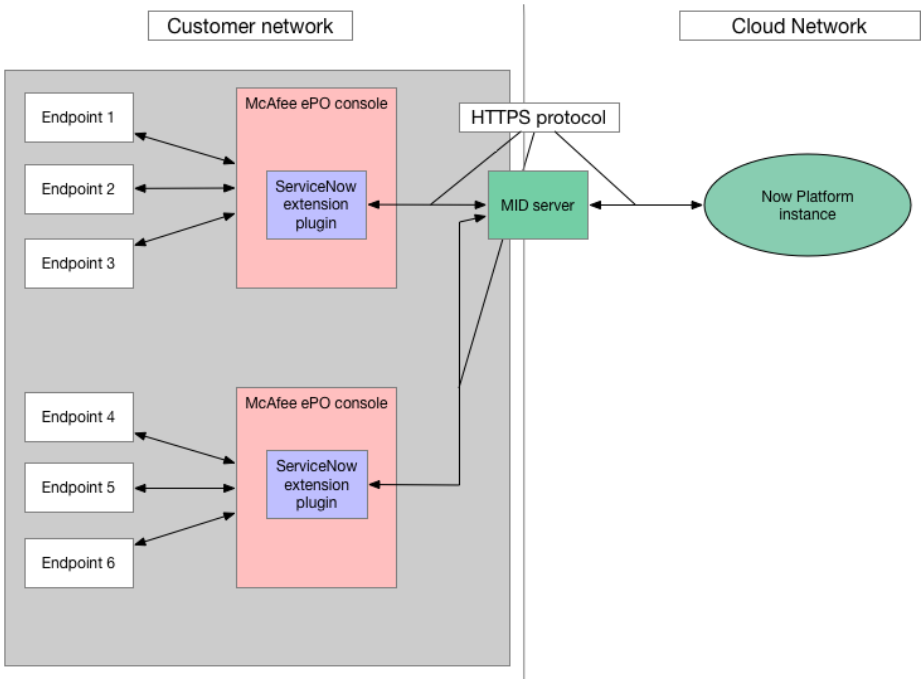


Рис.3.9. Інтеграція до декількох консолей McAfee ePO

Робочі процеси для інтеграції McAfee ePO попередньо налаштовані та розроблені спеціально для цієї інтеграції. Ви можете редагувати ці робочі процеси відповідно до потреб вашої організації. Робочі процеси включають наступні боти з робочі цикли:

Security Operations Інтеграція McAfee EPO – отримати відомості про хост:

Security Operations Інтеграція McAfee EPO - ініціювати сканування шкідливих програм;

Security Operations Інтеграція McAfee EPO - Isolate Host;

Security Operations Інтеграція McAfee EPO – Список загроз;

Security Operations Інтеграція McAfee EPO - видалення ізоляції;

Інтеграція вимагає, щоб MID-сервер спілкувався через з'єднання протоколу HTTPS із консоллю McAfee ePO .

Для реагування на інциденти в McAfee ePO потрібно налаштовувати відповідні ролі:

– Користувач з роллю системного адміністратора (admin) для встановлення програми.

– Користувач із роллю адміністратора інцидентів безпеки (sn_si.admin) налаштовує програму, створює, активує та видаляє профілі.

– Користувач із роллю аналітика інцидентів безпеки (sn_si.analyst) працює з інцидентами безпеки. Завдання включають вручну запуск профілів від інцидентів безпеки. Якщо на етапі конфігурації в профілі вибрано параметр затвердження, користувачі з цією роллю також надсилають запити на ізоляцію хостів і повернення їх у мережу.

Для того щоб McAfee ePO виконував реагування на інцидент безпеки потрібен плагін (com.snc.si_dep). Цей плагін автоматично встановлює всі залежності, необхідні для підтримки продукту реагування на інциденти безпеки Його встановлюють і активують перш ніж інсталювати та активувати інші програми Security Operations, необхідні для інтеграції.

Розглянемо порядок налаштування консолі McAfee ePO для інтеграції з системою реагування на інциденти безпеки (SIR).

Тут необхідна роль: адміністратор McAfee ePO

Як користувач із правами адміністратора McAfee ePO переконайтеся, що ви встановили Servicenow.zip плагін розширення на вашій консолі McAfee ePO . Цей плагін розширення потрібен для інтеграції

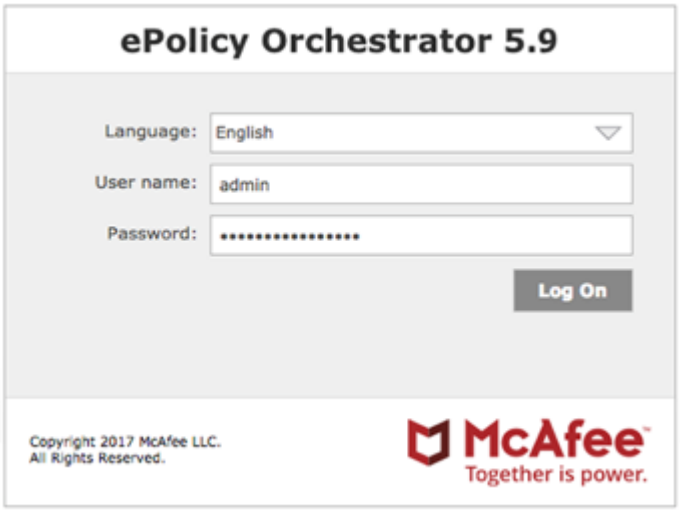
Плагін розширення ServiceNow підключає ваш екземпляр Now Platform до вашої консолі McAfee ePO . Це підключення дозволяє посилатися на теги безпеки, які ви створюєте на консолі McAfee ePO для ізольованого хоста, і ініціювати дії сканування зловмисного програмного забезпечення до профілів можливостей у вашому екземплярі Now Platform .

Мітки безпеки у вашій консолі McAfee ePO мають збігатися з тегами безпеки в записах можливостей у вашому екземплярі Now Platform .

У наступних кроках показано, як установити плагін розширення, створити тег безпеки на консолі McAfee ePO та призначити дію для тегу.

1. Якщо ви не встановили плагін розширення ServiceNow на консолі McAfee ePO, необхідно виконати наведені нижче дії, щоб установити його.

2. Увійдіть у свою консоль McAfee ePO за допомогою свого імені користувача та пароля McAfee.



3.10. Вхід до консолі McAfee ePO

3. У розділі Програмне забезпечення натисніть посилання Розширення (рис.3.11).

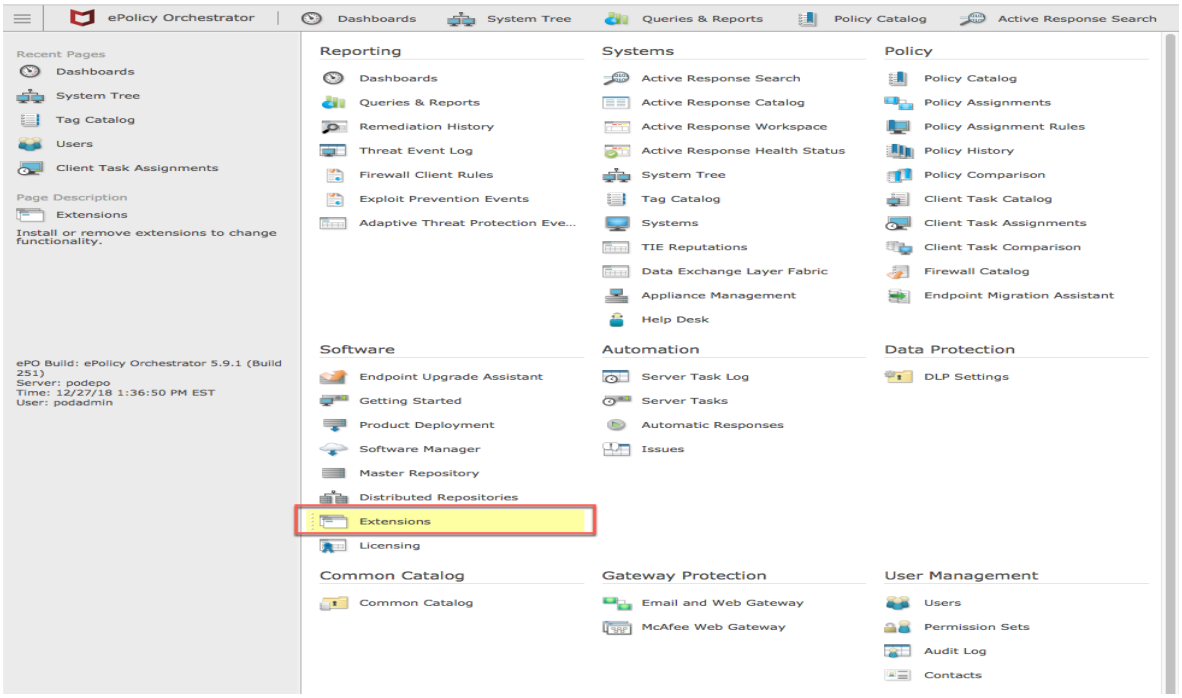


Рис.3.11. Розділ розширення

4. На сторінці розширень, що відобразиться, натисніть «Установити розширення» (рис.3.12)

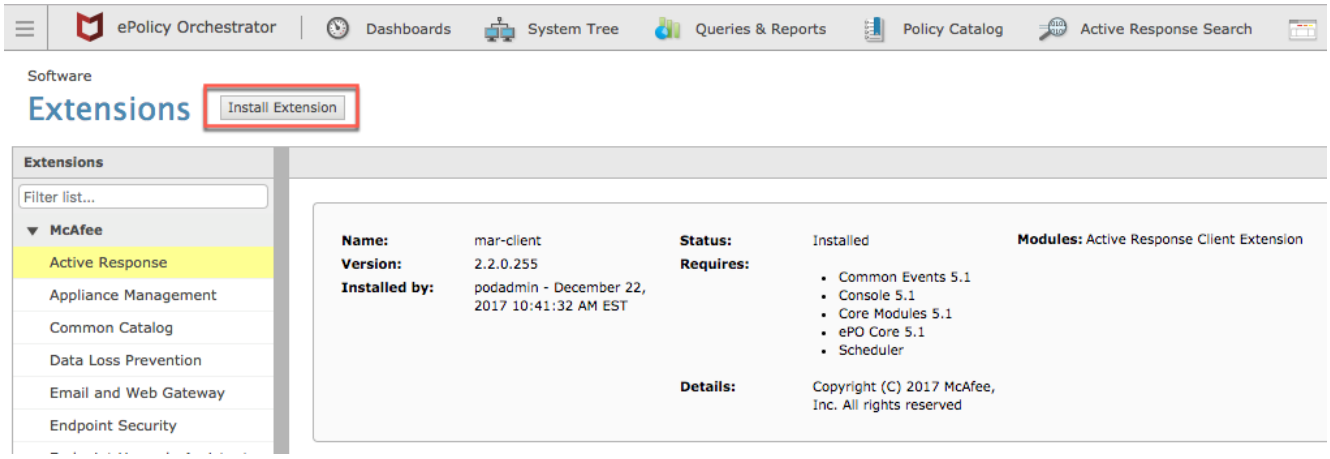


Рис.3.12. «Установити розширення»

5. У діалоговому вікні «Установити розширення» натисніть «Вибрати файл » і перейдіть доServicenow.zipy вашій системі та натисніть OK, щоб завантажити його(рис.3.13).

Після завершення завантаження відобразиться сторінка програмних розширень із переліком плагіна розширення ServiceNow (3.13).

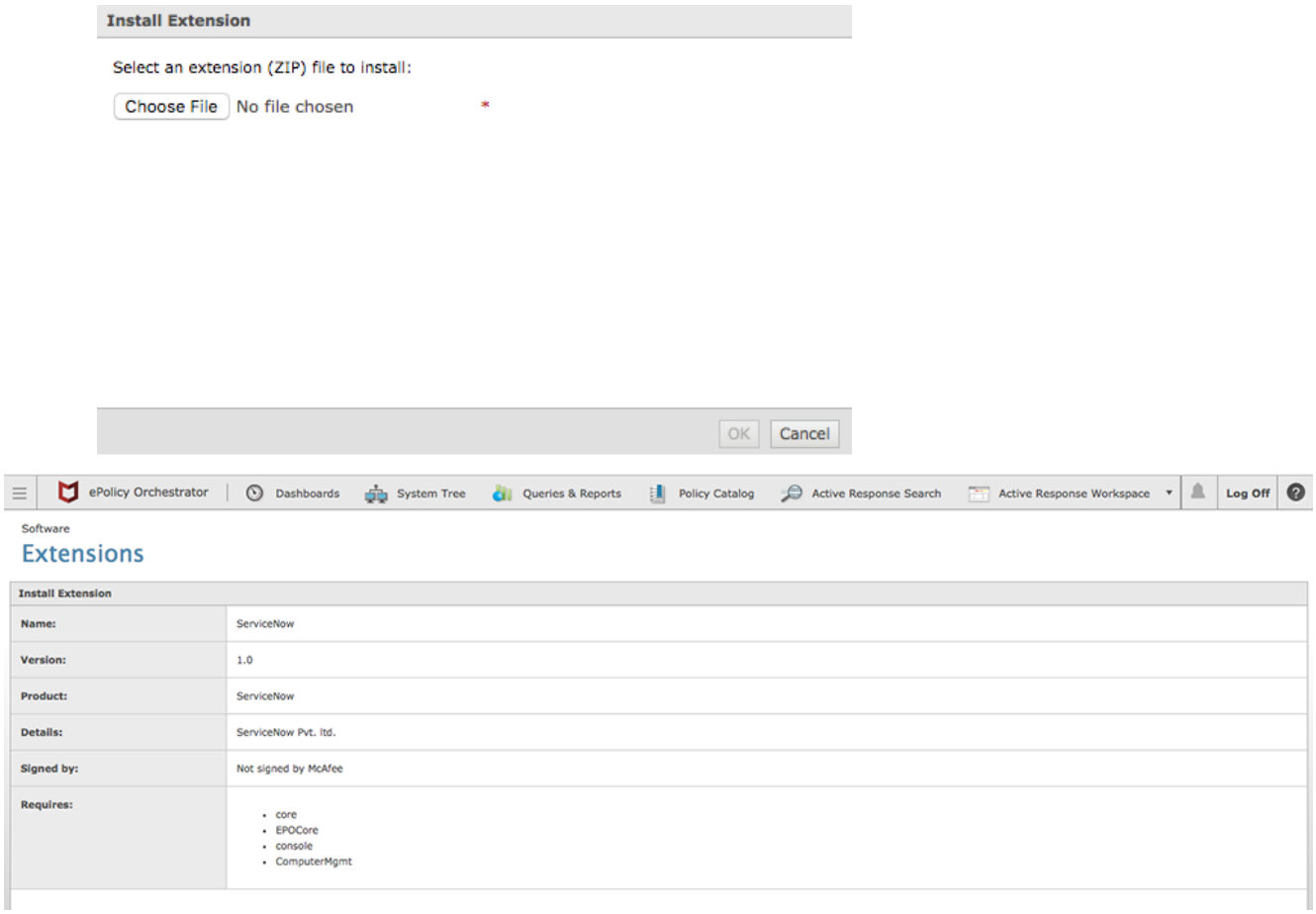


Рис.3.13. Встановлене розширення плагіна ServiceNow на консолі McAfee ePO

6. Створення тегів безпеки в консолі McAfee ePO для ініціювання сканування зловмисного програмного забезпечення та ізоляції дій хоста.

а) перейдіть на домашню сторінку та натисніть посилання Каталог тегів (3.14).

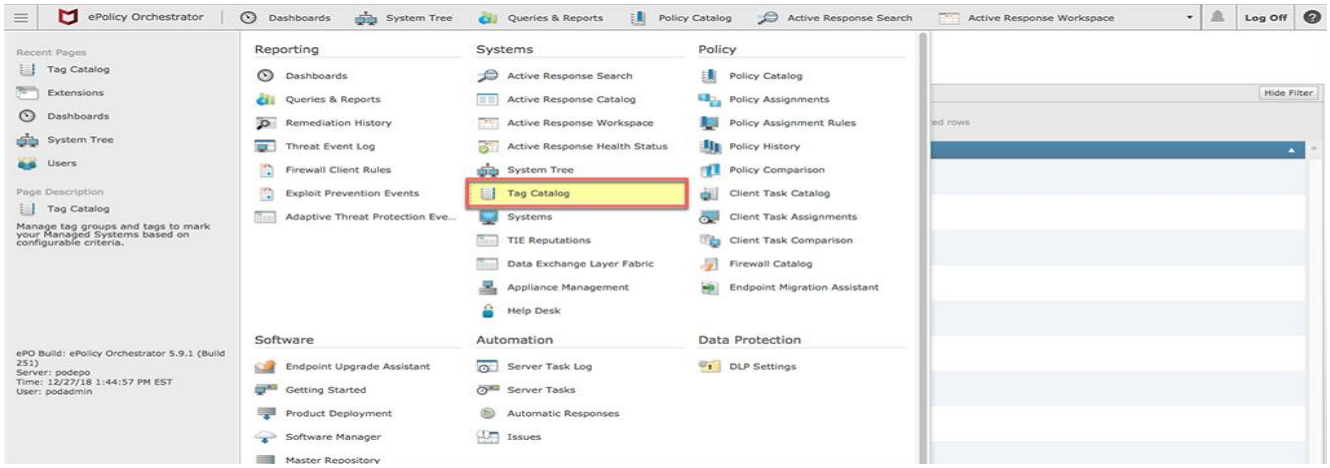


Рис.3.14. Каталог тегів

б) на сторінці каталогу тегів, що відобразиться, натисніть «Новий тег» .

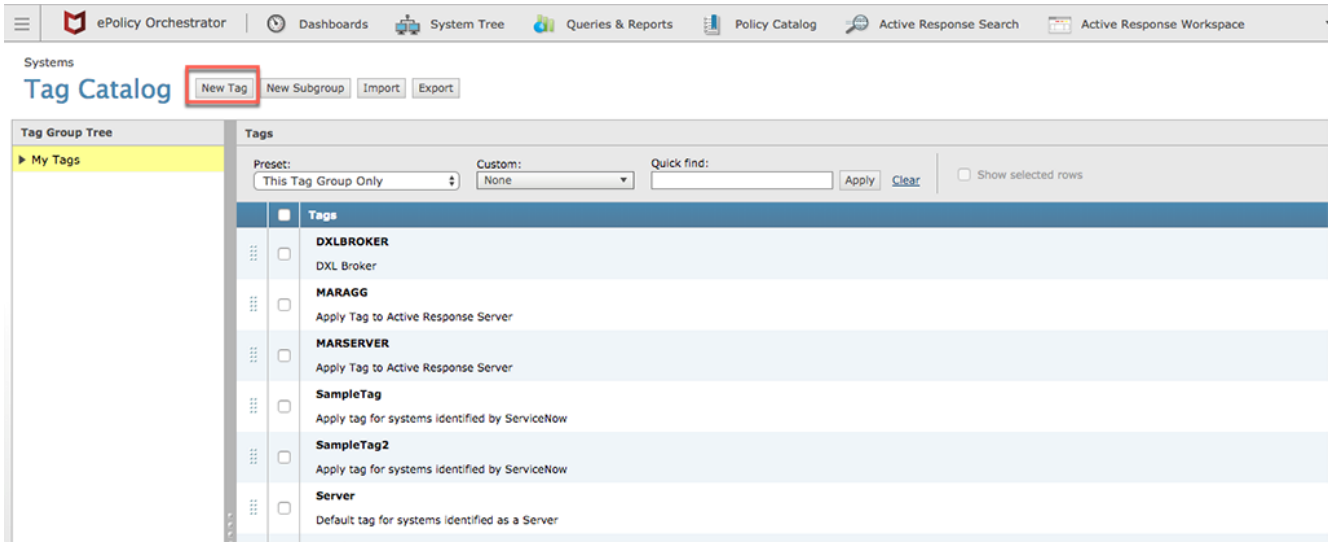


Рис.3.15. Новий тег

с) вибравши крок Опис на панелі перебігу, що відображається, введіть ім’я та опис для тегу (Рис. 3.16).

На рис 3.16 показано приклад відображення тегу із назвою та описом для можливості сканування зловмисного ПЗ. Це ім’я тегу – це те, що збігається та на яке посилається ваш екземпляр Now Platform .

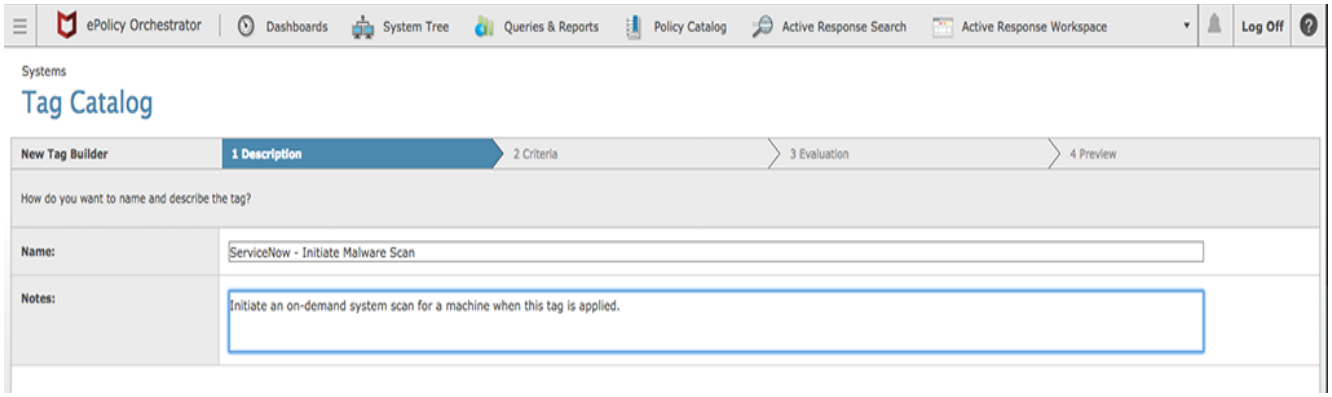


Рис.3.16. Тег із назвою та описом для можливості сканування зловмисного ПЗ

d) Щоб перейти до кроку Критерії, клацніть Критерії на панелі виконання.

Повідомлення, які відображаються, вказують на те, що цьому тегу наразі не призначено жодних дій і що тег можна застосувати лише вручну.

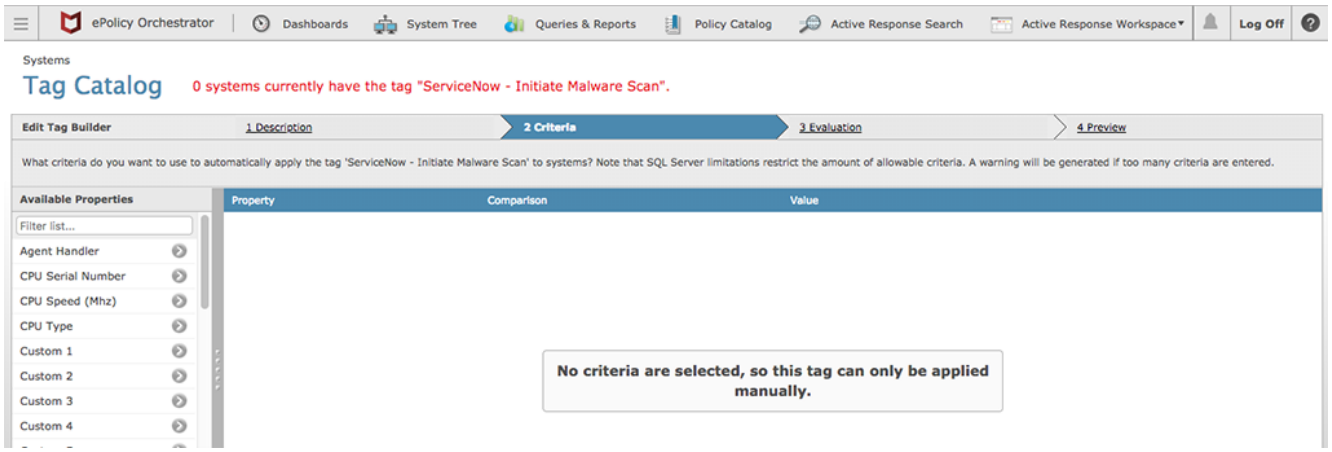


Рис.3.17. Тег критеріїв

e) щоб продовжити, натисніть «Оцінка» на панелі виконання, як це показано на рис 3.18.

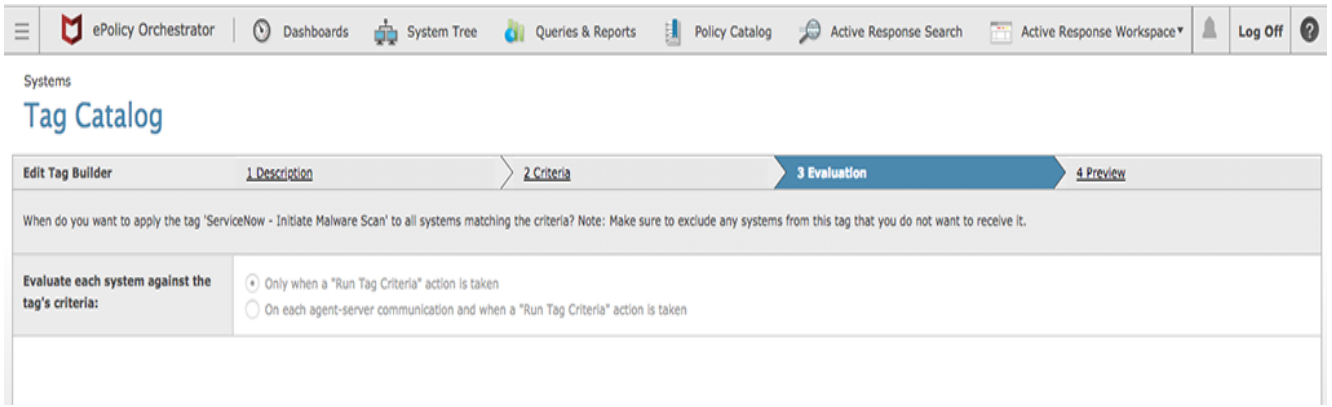


Рис. 3.18. Оцінка тегів

f) Відкривши сторінку каталогу тегів етапу оцінки, залиште параметри на цій сторінці за замовчуванням і на панелі перебігу натисніть «Попередній перегляд» рис.3.19.

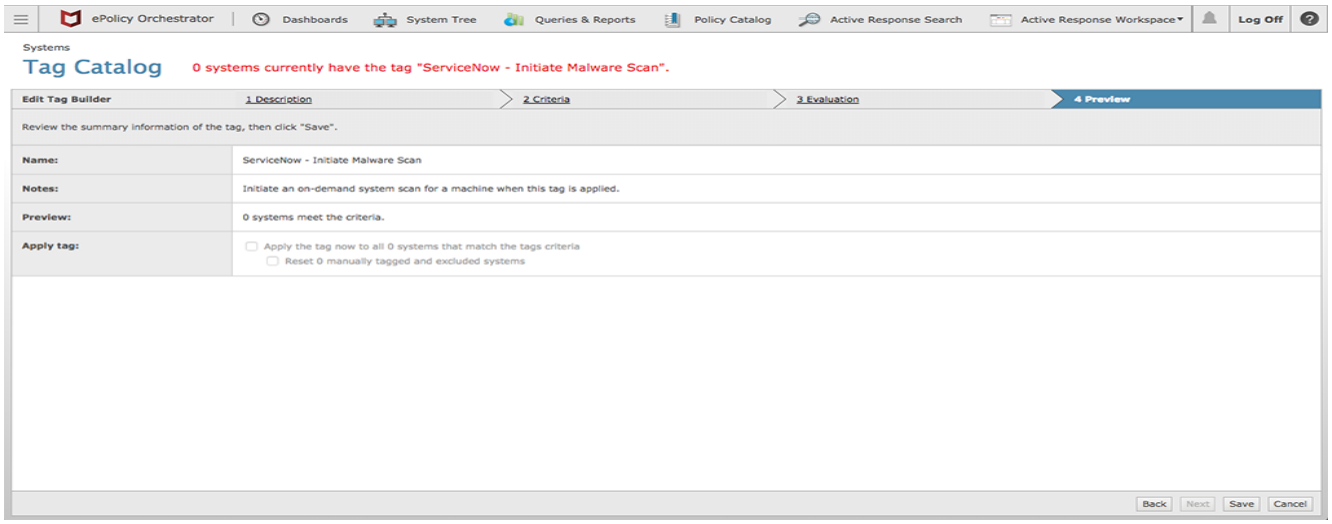


Рис. 3.19. «Попередній перегляд»

g) на сторінці попереднього перегляду в нижньому правому куті сторінки натисніть « Зберегти» , щоб зберегти запис.

Новий тег відображається в каталозі тегів, як показано на рис.3.20.

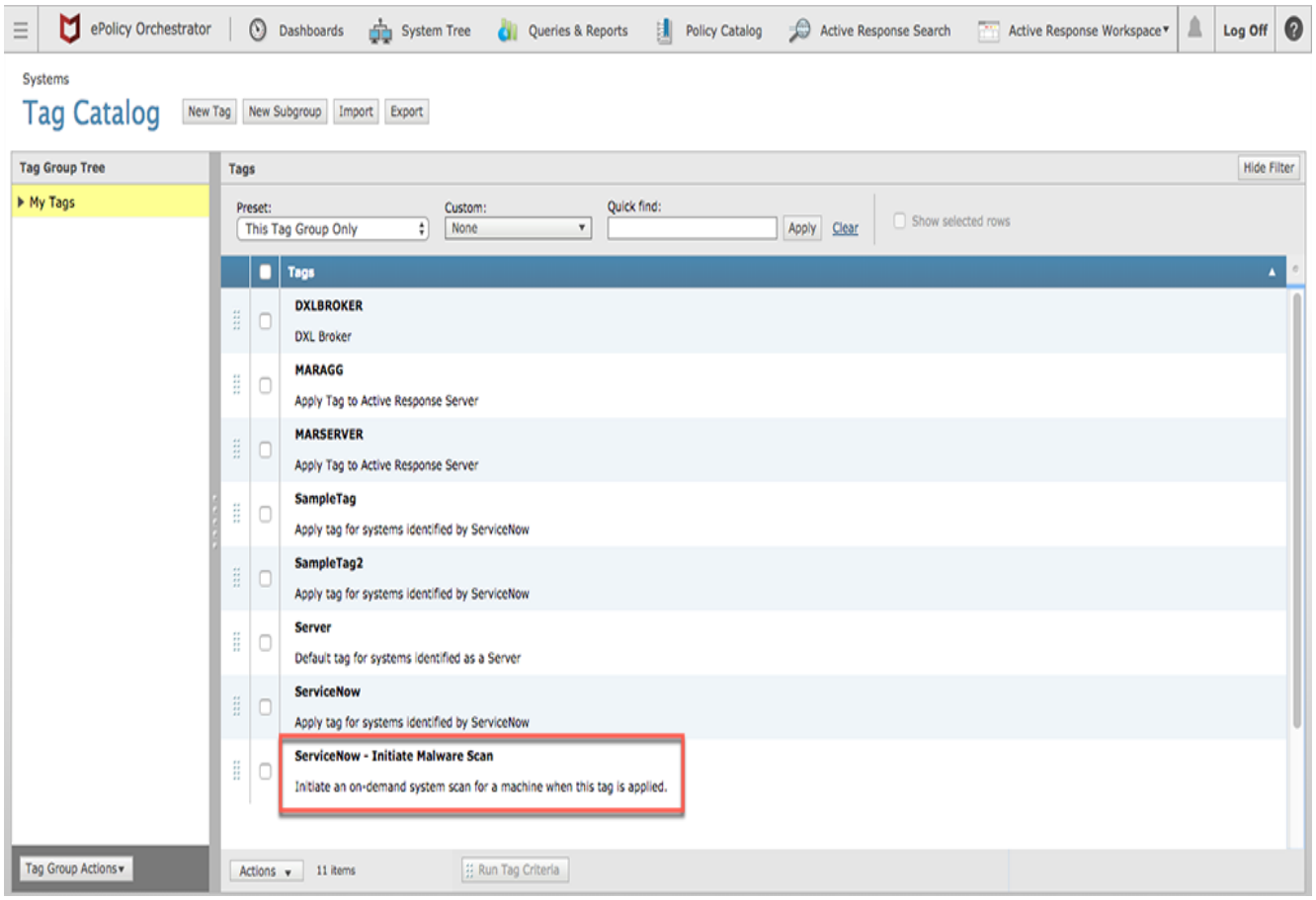


Рис.3.20. Новий тег у каталозі

7. Створіть тег безпеки для дії ізоляції хоста, повторивши попередні кроки.

Після створення обох тегів можна призначати дії для нових тегів.

8. Щоб додати дію до нового тегу, виконайте наведені нижче дії.

а) перейдіть на домашню сторінку та в розділі «Політика» натисніть посилання «Призначення завдань клієнта» рис.3.21.

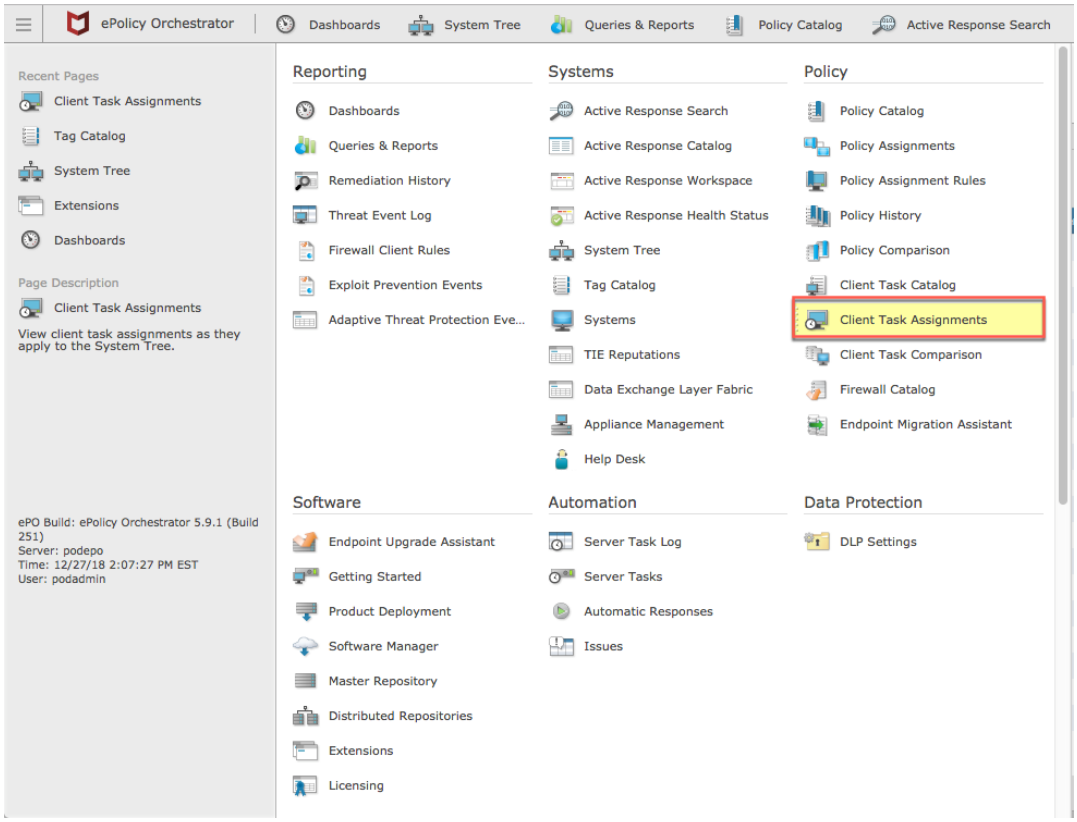


Рис.3.20. Призначення завдань клієнта

b) на сторінці дерева систем, яка відображається, у нижній частині сторінки розгорніть меню «Дії» та виберіть «Нове призначення клієнтського завдання» (рис.3.21).

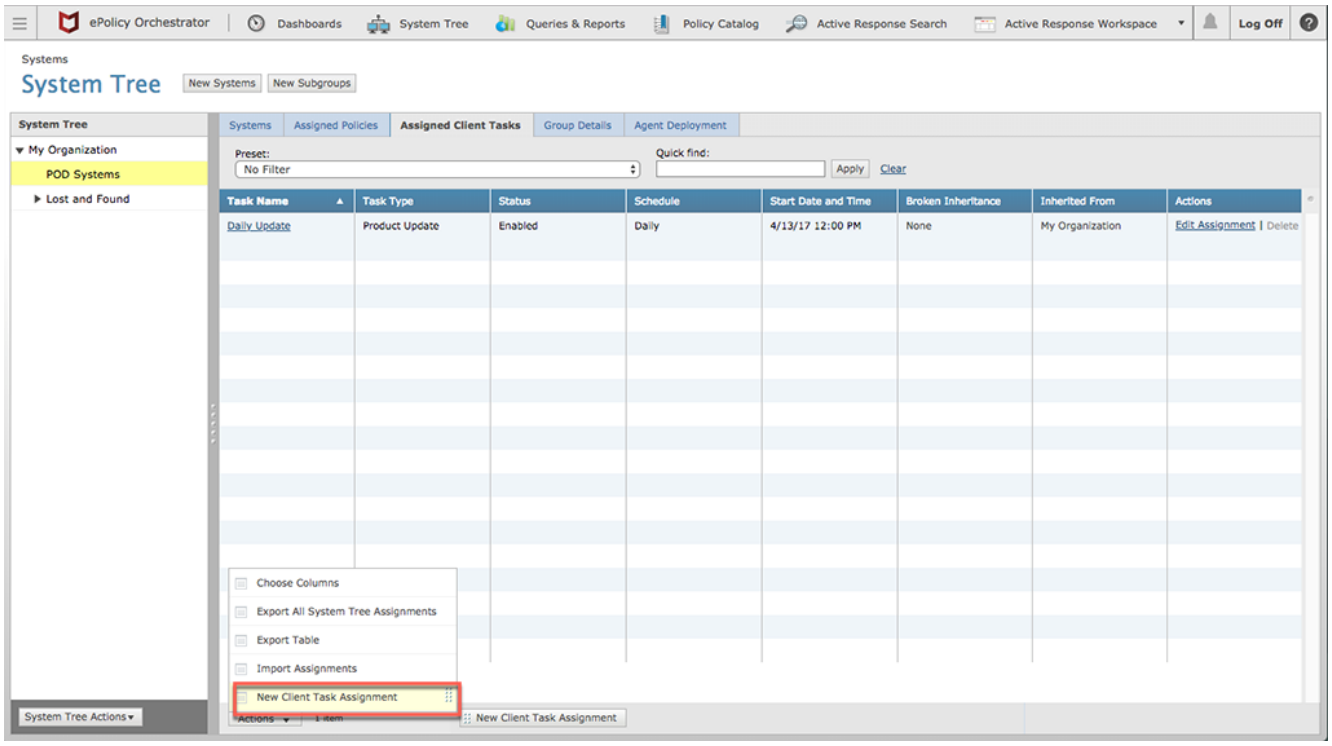


Рис.3.21. Нове призначення клієнтського завдання

с) на сторінці, яка відобразиться, перейдіть до пункту Запобігання загрозам безпеки кінцевої точки > Сканування за вимогою на основі політики > Сканування за вимогою — повне сканування , вибравши шлях, як показано на рис.3.22.

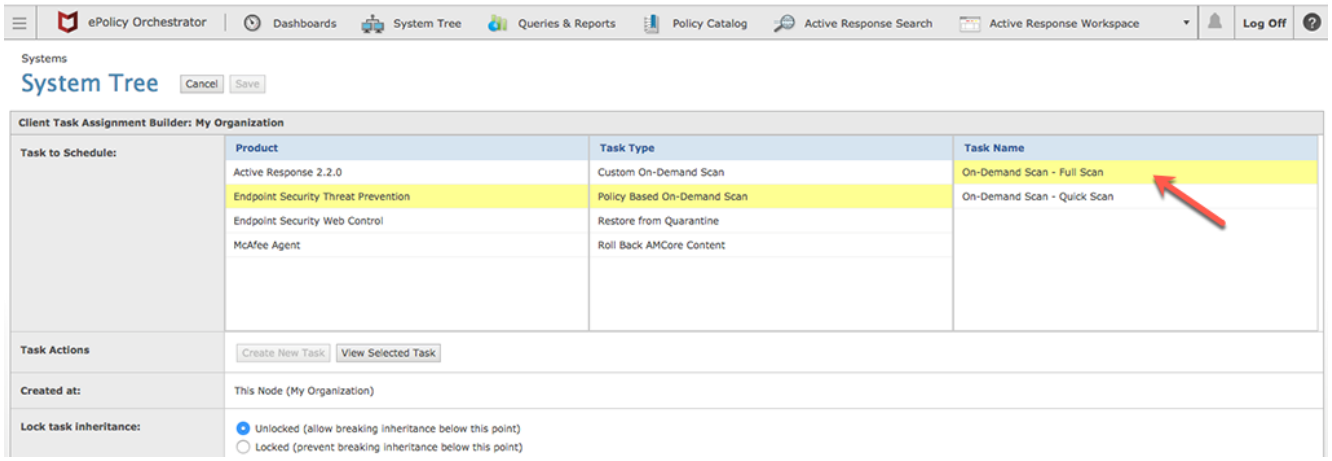


Рис.3.22 .Налаштоване завдання

Налаштування тегу та призначення завдання закінчено.У розділі «Теги» під перемикачем і поруч мають буди теги, з’явиться тег «Ініціювати сканування шкідливих програм».

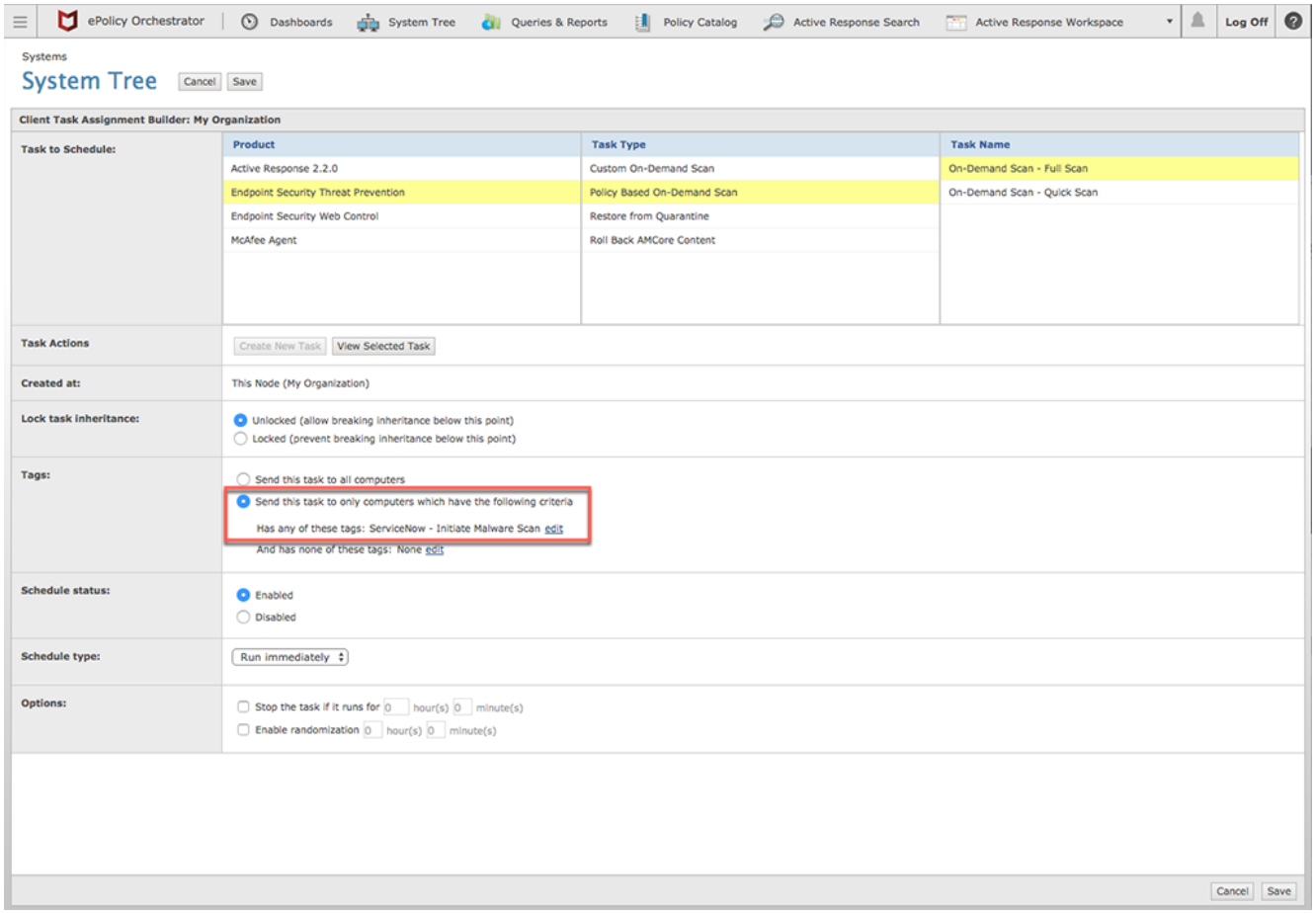


Рис. 3.23. Налаштований тег «Ініціювати сканування шкідливих програм».

На сторінці «Дерево системи» завдання відображається у списку «Призначені завдання клієнта» (вкладка).

Отже відповідно до процедури налаштування плагіну завдань адміністратор встановив плагін розширення, створили теги безпеки та призначили завдання своїм тегам до пристроїв організації. Тепер вся інформація щодо безпеки пристроїв організації моніториться адміністратором безпеки, що дозволить йому вчасно реагувати на інциденти безпеки.

3.3. Рекомендації застосування технології захисту мобільних пристороїв McAfee Mobile Security

Мобільні пристрої стали невід'ємною частиною робочого процесу в більшості організацій. Вони надають працівникам гнучкість та мобільність, але водночас створюють нові вектори для кібератак. Тому захист мобільних пристроїв є критично важливим завданням для фахівців з кібербезпеки. Основні кроки для захисту мобільних кроків повинні включати:

1. Розробка політики безпеки мобільних пристроїв.

Використання особистих пристроїв для роботи, допустимі додатки, правила зберігання даних тощо.

Необхідно проводити регулярні тренінги та інформування про потенційні загрози та правила безпеки.

Визначення наслідків порушення політики.

2. Застосовати технологію управління мобільними пристроями в інформаційній системі організації.

Оберіть MDM-систему, яка відповідає потребам організації та забезпечує необхідний рівень контролю.

Настройте MDM для віддаленого управління пристроями, встановлення політик, блокування несанкціонованих додатків, шифрування даних тощо.

Регулярно оновлюйте MDM-систему та профілі пристроїв.

3. Захист пристроїв повинен включати паролі та шифрування даних, захист вд крадіжок.

4. Захист мережі повинен включати VPN та захищений W-Fi.

Використання VPN дозволить застосовувати шифрування трафіку між мобільним пристроєм та корпоративною мережею.

Обмежений доступ до незахищених Wi-Fi мереж дозволить зменшити ризики витоку інформації.

Контроль використання мобільних мереж та налаштвання аутентифікації для доступу до корпоративних ресурсів організації зменшить ризики несанкціонованого доступу до інфраструктури організаціх.

При використанні мобільних пристроїв приділяти увагу безпекі додатків:

Створіть список дозволених додатків, які можуть бути встановлені на пристрої.

Перед встановленням додатків перевіряйте їх на наявність шкідливого коду.

Регулярно оновлюйте всі встановлені додатки.

5. Підвищення обізнаності безпеки при роботі з мобільними пристроями.

Проводьте регулярні тренінги для підвищення обізнаності користувачів про кіберзагрози та правила безпеки.

Навчайте користувачів розпізнавати фішингові атаки та не відкривати підозрілі посилання та файли.

Попереджайте про ризики соціальної інженерії та нерозголошення конфіденційної інформації.

Захист мобільних пристроїв є складним завданням, яке вимагає комплексного підходу. Поєднання технічних заходів та підвищення обізнаності користувачів дозволить мінімізувати ризики, пов’язані з використанням мобільних пристроїв в організації.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було отримано наступні результати:

Виявлено, що останнім часом організації використовують мобільні пристрої для виконання своїх бізнес-процесів. Це в свою чергу підвищило ризики безпеки інформаційних ресурсів організацій, що може призвести до витоку даних та несанкціонованому доступу до інформаційної системи організацій.

Для захисту мобільних пристроїв в організації проведено аналіз застосування технології управління мобільними пристроями для захисту особистої та робочої інформації від крадіжки та неправомірного використання. Використання такої технології обумовлення різними типами атак, які можуть бути використано зловмисниками для отримання конфіденційної інформації або несанкціонованому доступу до інформаційної системи організації.

В роботі проведено порівняльний аналіз різних рішень, які надають можливості захисту та управління мобільними пристроями організації. В результаті порівняння було обрано технологію McAfee Mobile Security з консоллю управління ePolicy Orchestrator. Теке управління мобільними пристроями нічим не відрізняється від керування робочими станціями. Інтеграція несе в собі гнучкішу схему застосування політик: глобально, окремо по платформах (iOS, Android, Windows Phone), окремо по групах (наприклад, для співробітників одного відділу), вибірково для конкретного користувача (наприклад, для керівника або ТОП менеджера) та нарешті політика може бути призначена для конкретного пристрою.

В роботі досліджено методи та засоби організації McAfee EPO є ключовим компонентом платформи управління безпекою McAfee, яка забезпечує уніфіковане керування безпекою кінцевої точки, мережі та даних, що скорочує час реагування на інциденти, посилює захист, спрощує керування ризиками та безпекою за допомогою автоматизації, наскрізної видимості мережі та безпеки.

Розроблено технологія захисту мобільних пристроїв McAfee ePolicy Orchestrator ePolicy працює на базі сервера ePolicy Orchestrator (ePO) 4.5, який

відокремлює служби сервера, що працюють із запитами агентів, і додав логіку управління, що дозволяє розгортати екземпляри цих служб. Саме використання обробника агентів в інфраструктурі організації дозволяє управляти, захищати та моніторити стан мобільних пристроїв.

В роботі запропоновано технологію інтеграції McAfee ePolicy Orchestrator ePolicy з підключенням клієнтського середовища Now Platform. Така інтеграція дозволяє налаштовувати теги безпеки для адміністратора безпеки.

Крім того, в роботі надано загальні рекомендації щодо організації безпеки мобільних пристрої в організації, які надають вектор задач що підвищить захист мобільних пристроїв в інформаційній системі організації.

Отже використання McAfee ePolicy Orchestrator ePolicy дозволить організаціям підвищити рівень кібербезпеки та захистити свої дані від витоку конфіденційної інформації та несанкціонованого доступу до інформаційної системи.

ПЕРЕЛІК ПОСИЛАНЬ

1 Ibm. (2024, September 03). Mobile device management. URL: https://www.ibm.com/topics/mobile-device-management (Дата звернення: 12.10.2024).

2. Keepnet Labs. (2024, November 18). What Is Mobile Security: Threats & Components - Keepnet. Keepnet Labs. URL: https://keepnetlabs.com/blog/what-is-mobile-security-threats-and-components (дата звернення: 12.10.2024).

3. Inc. (2024, November 19). Unified Endpoint Management Tools. URL: https://www.gartner.com/reviews/market/unified-endpoint-management-tools (дата звернення: 20.10.2024).

4. Nield, D., Wolfe, B. M., & Cawley, C. (2024). Best MDM solution of 2024. TechRadar. URL: https://www.techradar.com/best/best-mdm-solutions (дата звернення: 25.10.2024).

5. Top 10 Best Mobile Device Management (MDM) Solutions 2024. (2024, October 24). URL: from https://www.cpdevice.com/best-mobile-device-management-mdm-solutions (дата звернення: 25.10.2024).

6. McAfee ePolicy Orchestrator. | LinkedIn.. URL: https://www.linkedin.com/pulse/little-mcafee-epo-neeraj-vats (дата звернення: 01.11.2024).

7. Sockalingam, H. (2024, August 01). Архітектура інтеграції для McAfee ePO. URL: https://www.servicenow.com/docs/bundle/xanadu-security-management/page/product/secops-integration-mcaffee-epo/concept/mcafee-epo-integration-architecture.html (дата звернення: 015.11.2024).

8. Curran, K., Maynes, V., & Harkin, D. (2015). Mobile device security. Int. J. Inf. Comput. Secur., 7(1), 1. doi: 10.1504/IJICS.2015.069205

9. Mitrea, T., & Borda, M. (2020). Mobile Security Threats: A Survey on Protection and Mitigation Strategies. International conference KNOWLEDGE-BASED ORGANIZATION, 26(3), 131–135. doi: 10.2478/kbo-2020-0127

10. Cinar, A. C., & Kara, T. B. (2023). The current state and future of mobile security in the light of the recent mobile security threat reports. Multimed. Tools Appl., 82(13), 20269–20281. doi: 10.1007/s11042-023-14400-6

11. Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model. Symmetry, 12(5), 754. https://doi.org/10.3390/sym12050754.