ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ДОСЛІДЖЕННЯ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КІНЦЕВИХ ТОЧОК У КОРПОРАТИВНИХ СИСТЕМАХ ЗА ДОПОМОГОЮ SYXSENSE»

Виконав студент 6 курсу, групи БСДМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Сільченко І. Д.
(прізвище та ініціали)
Керівник Кожухівський А. Д.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н. С.
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"___"_____ 2022 року

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

Сільченко Івану Денисовичу
(прізвище, ім'я, по батькові)

1. Тема магістерської роботи: «Дослідження та забезпечення безпеки кінцевих точок у корпоративних системах за допомогою Syxsense»

керівник магістерської роботи д.т.н., професор Кожухівский А. Д.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «12» жовтня 2022 року № 122.

2. Строк подання студентом магістерської роботи 15.12.2022 р.

3. Вихідні дані до магістерської роботи
корпоративна інформаційна система;
комплексне рішення забезпечення захисту кінцевих точок у корпоративних системах з Syxsense;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблеми забезпечення захисту кінцевих точок корпоративної інформаційної системи.
2. Аналіз методів та засобів захисту кінцевих точок на прикладі Syxsense.
3. Результати аналізу методів та засобів захисту кінцевих точок на прикладі Syxsense.
4. Розроблення рекомендацій щодо застосування методів та засобів захисту кінцевих точок корпоративної інформаційної системи.

5. Перелік графічного матеріалу

1. Тема магістерської роботи.

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

3. Результати аналізу проблеми забезпечення кібербезпеки корпоративної інформаційної системи.

4. Результати аналізу існуючих методів та засобів захисту кінцевих точок корпоративної інформаційної системи.

5. Призначення та склад програмного комплексу Syxsense.

6. Технологія застосування програмного продукту Syxsense

7. Розроблення рекомендацій щодо застосування методів та засобів захисту кінцевих точок корпоративної інформаційної системи.

8. Висновки за результатами роботи.

6. Дата видачі завдання 26.09.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми забезпечення захисту кінцевих точок.	26.09.2022 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	14.10.2022 р.	
3.	Аналіз проблеми забезпечення кібербезпеки корпоративної інформаційної системи.	05.11.2022 р.	
4.	Аналіз методів та засобів захисту кінцевих точок на прикладі Syxsense.	25.11.2022 р.	
5.	Розроблення рекомендацій щодо застосування методів та засобів захисту кінцевих точок корпоративної інформаційної системи.	09.12.2022 р.	
6.	Оформлення результатів дослідження.	14.12.2022 р.	
7.	Підготовка доповіді до захисту.	15.12.2022 р.	

Студент Сільченко І. Д.

(підпис) прізвище та ініціали

Керівник магістерської роботи Кожухівський А. Д.

(підпис) прізвище та ініціали

РЕФЕРАТ

Текстова частина магістерської роботи: 84 сторінки, 34 рисунки, 20 джерел, 1 таблиця.

Об'єкт дослідження – процес забезпечення захисту кінцевих точок корпоративної інформаційної системи.

Предмет дослідження – методи та засоби захисту кінцевих точок корпоративної інформаційної системи на базі рішення Syxsense Endpoint Security.

Мета роботи – розробити рекомендації щодо застосування методів та засобів захисту кінцевих точок корпоративної інформаційної системи підприємства.

Методи дослідження – аналіз джерел інформації за темою роботи, вивчення документації по експлуатації, відтворення процесу забезпечення захисту кінцевих точок.

Незалежно від того, наскільки сильно бізнес захищає свою мережу безпеки та дані, він все одно залишається вразливим, оскільки кіберзлочинці стають все більш досконалими у своїх методах атак. Як наслідок, єдиним рішенням є постійне вдосконалення плану кібербезпеки у мережі, і одним з мережевих рішень для підвищення рівня її безпеки є кінцеві точки.

В роботі було виконано дослідження засобів захисту кінцевих точок корпоративної інформаційної мережі. Було проведено аналіз проблеми забезпечення безпеки корпоративної мережі. Також, було розроблено рекомендації щодо захисту кінцевих точок корпоративної мережі з використанням програмного продукту Syxsense Endpoint Security.

Впроваджено варіант технології забезпечення захисту кінцевих точок. Встановлено рекомендації щодо застосування даної технології.

Галузь використання – кібербезпека кінцевих точок у корпорат системах.

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, ЗАХИСТ КІНЦЕВИХ ТОЧОК, ТЕХНОЛОГІЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК, МІЖМЕРЕЖЕВИЙ ЕКРАН, ПОПЕРЕДЖЕННЯ ЗАГРОЗ, КОНТРОЛЬ ІНТЕРНЕТУ, АДАПТИВНИЙ ЗАХИСТ ВІД ЗАГРОЗ, EDR-ТЕХНОЛОГІЇ.

ABSTRACT

Master`s thesis: 84 pages, 34 figures, 20 sources, 1 table.

Object of research - the process of providing protection of endpoints of corporate information system.

Subject of research - methods and means of protection of endpoints of corporate information system on the basis of Syxsense Endpoint Security solution.

Purpose - to develop recommendations for the use of methods and means of protecting the endpoints of the corporate information system of the enterprise.

Research methods - analysis of information sources on the topic of work, study of operating documentation, reproduction of the process of endpoint protection.

No matter how much a business protects its security network and data, it still remains vulnerable as cybercriminals are becoming more sophisticated in their attack methods. As a result, the only solution is to continuously improve the cybersecurity plan in the network, and one of the network solutions to improve its security is endpoints.

In this work, a study of the means of protecting the endpoints of the corporate information network was carried out. The problem of ensuring the security of the corporate network was analyzed. Also, recommendations were developed to protect the endpoints of the corporate network using the Syxsense Endpoint Security software product.

A variant of endpoint protection technology was introduced. Recommendations for the use of this technology have been established.

Scope - cybersecurity of endpoints in corporate systems.

KEYWORDS - CORPORATE INFORMATION SYSTEM, CYBERSECURITY, ENDPOINT PROTECTION, ENDPOINT PROTECTION TECHNOLOGY, METHODS AND MEANS OF ENDPOINT PROTECTION, FIREWALL, THREAT

PREVENTION, INTERNET CONTROL, ADAPTIVE THREAT PROTECTION, EDR-TECHNOLOGY.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ …… 12

ВСТУП ……..…… 13

1 **АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ……** 15

1.1 Призначення, структура, функції та умови функціонування корпоративної інформаційної системи…….. 15

1.2 Аналіз проблеми забезпечення захисту кінцевих точок корпоративної інформаційної системи……. 18

1.3 Мета та завдання захисту кінцевих точок корпоративної інформаційної системи…… 22

1.4 Аналіз існуючих методів та засобів захисту кінцевих точок корпоративної інформаційної системи…….. 26

2 **АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КІНЦЕВИХ ТОЧОК НА ПРИКЛАДІ SYXSENSE ENDPOINT SECURITY……..** 40

2.1 Призначення, основні функції та склад програмного комплексу Syxsense Endpoint Security…….. 40

2.2 Основні функції та принципи роботи модуля Syxsense Manage…….. 46

2.3 Основні функції та принципи роботи модуля Syxsense Secure…… 51

3 **РОЗРОБЛЕННЯ ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК НА БАЗІ РІШЕННЯ SYXSENSE ENDPOINT SECURITY** ……..…… 59

3.1 Технологія застосування програмного комплексу Syxsense Endpoint Security…….. 59

3.2 Рекомендації щодо застосування технології забезпечення захисту кінцевих точок ……. 75

ВИСНОВКИ …….. 80
ПЕРЕЛІК ПОСИЛАНЬ 82
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 84

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп’ютер

ЦОД – центр обробки даних

СЗІ – системи захисту інформації

СУБД – системи управління базами даних

ABAC – Attribute-Based Access Control

ACL – Access Control List

ACM – Access Control Mechanism

API – Application Programming Interface

ZTNA – Zero Trust Network Access

IAM – Identity and Access Management

SSO – Single Sign-On

BYOD – Bring-Your-Own-Device

EPP – Endpoint Protection Platform

ERP – Enterprise Resource Planning System

EDR – Endpoint Detection & Response

IoT – Internet of Things

ВСТУП

Актуальність дослідження. Сучасний світ не стоїть на місці та постійно розвивається. Найактивніше всього у 21-му столітті розвивається сфера технологій, яка охоплює собою дуже багато нових відкриттів та захоплюючих витворів. Але, нажаль, з іншого боку медалі можна побачити також і зріст кіберзлочинності.
На сьогодняшній день існує дуже багато типів кібератак. У зв’язку із цим, зростає необхідність в тому, щоб не тільки зупиняти ці кібератаки, а й запобігати їх появи. Тому, зараз дуже важливо, аби кожна корпоративна інформаційна система підприємства мала змогу захиститися від них шляхом добре розробленного програмного забезпечення та кваліфікованих кадрів.

Кінцеві точки завжди були якщо не головним, то одним із основних джерел загроз інформаційній безпеці підприємства. При цьому саме поняття кінцевої станції істотно розширилося за останні кілька років, особливо з розвитком мобільних платформ.

І тепер в область визначення «кінцевої точки» входять не тільки персональні комп'ютери користувачів і корпоративні сервера, але й мобільні пристрої (ноутбуки, смартфони, планшети) та пристрої IoT (Internet of Things).

З цієї ж самої причини значно збільшилася кількість векторів атак, як на корпоративні мережі, так і на звичайних домашніх користувачів. Стрімкий розвиток концепції BYOD (Bring Your Own Device) своєчасно внесло свої корективи в розмивання периметру організацій та збільшення векторів атак. Якщо раніше смартфони, домашні комп'ютери і ноутбуки користувачів не надавали великого комерційного інтересу для зловмисників, то з перенесенням на них частини корпоративних функцій вони стали вельми бажаними цілями для атак.

Наведені аргументи актуалізують тему даної роботи, зміст якої становить дослідження технології забезпечення захисту кінцевих точок на базі рішення Syxsense.

Об'єкт дослідження – процес забезпечення кіберзахисту кінцевих точок.

Предмет дослідження – технологія захисту кінцевих точок.

Мета роботи – розробити варіант технології впровадження системи забезпечення захисту кінцевих точок та рекомендації щодо її застосування.

Наукові завдання:

дослідити значення проблеми необхідності забезпечення захисту кінцевих точок;

з'ясувати, яким чином підприємство має забезпечити захист корпоративної інформаційної системи;

проаналізувати проблеми забезпечення кібербезпеки корпоративної інформаційної системи;

розробити варіант технології забезпечення захисту кінцевих точок та рекомендації щодо застосування даної технології.

провести аналіз існуючих методів та засобів захисту кінцевих точок корпоративної інформаційної системи.

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

Практичне значення одержаних результатів полягає в розробці рекомендацій щодо застосування програмного продукту Syxsense для захисту кінцевих точок корпоративної інформаційної системи.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

1.1. Призначення, структура, функції та умови функціонування корпоративної інформаційної системи підприємства

Захист кінцевих точок - це практика захисту даних і робочих процесів, пов'язаних з окремими пристроями, які підключаються до вашої мережі. Платформи захисту кінцевих точок (EPP) працюють, перевіряючи файли при вході в мережу. Сучасні платформи захисту використовують потужне хмарне сховище для постійно зростаючої бази даних, звільняючи кінцеві точки від потоку, пов'язаного зі зберіганням всієї цієї інформації на місці і обслуговуванням, необхідним для підтримки цих баз даних в актуальному стані. Доступ до цих даних у хмарі також забезпечує більшу швидкість і масштабованість.

Розвиток інформаційних технологій та засобів автоматизації, збільшення обсягів оброблюваної інформації та динамічність зовнішнього середовища вимагає прийняття оперативних, раціональних та адекватних управлінських рішень. Для досягнення найвищої ефективності виробничої діяльності організації та підвищення мотивації співробітників необхідно створити сприятливий соціально-психологічний клімат в трудовому колективі, сформувати налагоджений зворотний зв'язок, розвинути довірчі відносини між керівництвом і підлеглими, побудовані на усвідомленні спільних інтересів і потреб організації.

Сьогодні у сфері захисту інформаційних активів використовуються інноваційні рішення, які дозволяють здійснювати безперервний моніторинг кіберзагроз та оперативно реагувати на інциденти. Інформаційна безпека є одним з першочергових пріоритетів у формуванні надійного підприємства.

Інформаційна безпека сучасної організації передбачає забезпечення захищеності інформаційного середовища, спрямованого на досягнення його

цілісності, автентичності, конфіденційності, а також доступності для авторизованих користувачів. Це забезпечується комплексом організаційно-технічних засобів і виконанням режимних заходів, спрямованих на надійний захист корпоративного контенту від випадкового і навмисного впливу, а також наявністю механізмів відмовостійкості і резервуванням функцій системи, що дозволяє гнучко підлаштовувати можливості системи під поточні корпоративні завдання інформаційної безпеки. Основними завданнями захисту інформації, що міститься в автоматизованій системі в процесі електронної взаємодії, є: запобігання поширенню, модифікації, знищенню, копіюванню, блокуванню і незаконному копіюванню інформації з обмеженим доступом.

КІС призначені для підтримки більшості бізнес-процесів (бажано всіх, якщо це можливо) всього підприємства (або декількох підприємств), збору та аналізу інформації про підприємство і зовнішнє середовище з метою вирішення завдань управління підприємством як по вертикалі (від первинної інформації до підтримки прийняття рішень вищим керівництвом), так і по горизонталі (всі сфери діяльності та технологічні операції). Такі системи характеризуються високою швидкодією і надзвичайною простотою використання, проте функціональні можливості таких систем в частині аналізу, як правило, вкрай обмежені.

КІС допомагають керівникам аналізувати важливу інформацію та за допомогою відповідних інструментів спрямовувати її на створення стратегічних рішень в організації. Наприклад, КІС допомагають керівникам сформувати більш точне та актуальне цілісне уявлення про діяльність організації, а також про конкурентів, постачальників та клієнтів.

Таке розуміння концепції КІС пов'язане з усвідомленням того, що корпоративний інформаційний простір - це щось досить складне, а не просто набір декількох програм. Спочатку було визнання того, що це інтегроване середовище обробки даних, а звідси і використання іншого терміну - інтегрована інформаційна система. Потім, поступово, сформувалося розуміння, що це не просто середовище обробки даних, а, в першу чергу, сукупність методів і підходів до управління різнорідними і багатоформними даними, вилучення інформації з існуючих ІС, в

першу чергу, у формах, необхідних для забезпечення управління підприємством.

Корпоративні інформаційні системи допомагають керівникам аналізувати важливу інформацію та використовувати відповідні засоби безпеки, щоб спрямувати її на створення стратегічних рішень в організації. Наприклад, КІС допомагають керівникам виробити більш точне і актуальне цілісне уявлення про діяльність організації, а також про конкурентів, постачальників і клієнтів.

Корпоративна інформаційна система повинна мати наступні властивості:

функціональна повнота системи (характеризується кількістю одноразово врахованих параметрів діяльності підприємства);

забезпечення формування звітності та обліку одночасно за міжнародними стандартами;

локалізація інформаційної системи: облік національного законодавства і системи розрахунків, інтерфейс і довідкова система національною мовою;

забезпечення розмежування доступу до даних і функцій;

попередження про спроби несанкціонованого доступу до інформації;

забезпечення авторизації інформації, реєстрації часу введення та модифікації даних, протоколювання віддалених даних;

можливість безперервного розвитку системи за рахунок наявності засобів адаптації та супроводу системи;

можливість консолідації інформації: на рівні підприємства (для об'єднання інформації філій, дочірніх підприємств тощо), на рівні окремих завдань та часових періодів.

Компанії, які дозволяють співробітникам приносити власні пристрої, такі як ноутбуки або смартфони, часто стикаються з проблемами безпеки кінцевих точок. Без добре продуманої політики використання власних пристроїв (BYOD), пристрої, що належать співробітникам, можуть поставити під загрозу безпеку інформації компанії або мережі.

За оцінками організацій, близько 45% корпоративних даних зберігається на кінцевих пристроях. Ці ноутбуки, планшети і смартфони становлять величезний ризик для безпеки даних.

Зростаюча вразливість кінцевих пристроїв у всій галузі означає, що дані легше скомпрометувати, ніж будь-коли. Щоразу, коли працівник підключається до публічної мережі Wi-Fi, завантажує підозрілий додаток або стає мішенню фішингової афери, ризик зростає.

Це особливо важливо, оскільки кінцеві пристрої не тільки піддають свої дані можливому витоку, вони також служать потенційним каналом для порушення безпеки всієї мережі.

Політики безпеки, особливо ті, що стосуються захисту принесених з собою пристроїв, є важливою частиною захисту кінцевих пристроїв від атак. Але найбільшою причиною вразливості є якість навчання та обізнаність співробітників. Необережні дії можуть серйозно вплинути на цілісність захищеної мережі:

- Втрачені або неналежним чином виведені з експлуатації пристрої: співробітники, які втрачають пристрої, підключені до мережі компанії, можуть піддавати цю мережу атакам.

- Погане застосування оновлень безпеки: Застарілі ОС та додатки можуть призвести до будь-якої кількості вразливостей на пристрої, який має доступ до конфіденційної інформації компанії.

- Співробітники відключають/вмикають шифрування: люди частіше налаштовують безпеку на своїх пристроях і переробляють налаштування відповідно до своїх потреб. Це може призвести до появи небажаних точок доступу.

За допомогою проактивної, постійно діючої технології IT-спеціалісти можуть уникнути цих проблем, зберігаючи при цьому відповідність вимогам безпеки та зменшуючи ризики.

1.2. Аналіз проблеми забезпечення захисту кінцевих точок корпоративної інформаційної системи.

Для сучасних інформаційних систем забезпечення безпеки корпоративної інформаційної системи є складним і багатовекторним завданням. Одним з її

ключових напрямків є захист робочих станцій і серверів.

У сьогоднішніх реаліях організаціям необхідна грамотна оцінка найбільш актуальних загроз для їх інформаційних систем, а також аналіз фінансових і репутаційних ризиків від можливих дій зловмисників.

Основними проблемами забезпечення кібербезпеки на підприємствах можна вважати:

недостатня кваліфікація персоналу на підприємствах;

невміння запобігати та протидіяти кібератакам та шкідливому програмному забезпеченню;

неналежне використання захисного програмного забезпечення;

недостатній розвиток стратегічно правильних засобів захисту інформації в корпоративній системі;

неправильний підхід або відсутність управління ризиками;

крадіжка інформації через підключені пристрої.

Потрібно звернути увагу на зміну картини загроз. За останні кілька десятиліть шкідливі програми сильно еволюціонували: якщо раніше це були результати звичайної цікавості та перевірки сил, то сьогодні мова йде про виключно кримінальні операції, а саме масовані DDoS-атаки, шпигунські програми, рекламне ПЗ, фішинг, руткіти тощо.

Нещодавнє дослідження SANS у 2017 році щодо безпеки кінцевих точок підкреслює важливість впровадження комплексного рішення з безпеки кінцевих точок. Деякі з ключових висновків цього дослідження включають

53% опитаних організацій зіткнулися з одним або декількома порушеннями, які почалися на їх кінцевих точках, а 74% не змогли визначити, чи була система повністю відновлена.

Платформи захисту кінцевих точок (EPP) і традиційні антивірусні рішення відрізняються в деяких ключових аспектах.

Кіберзлочинці постійно змінюють свою тактику, намагаючись обійти системи інформаційної безпеки організацій. В даний час більшість фахівців з інформаційної безпеки розуміють, що наявність прогалин неминуча. Зловмисник

буде обходити існуючі системи безпеки і переміщатися по мережі, викрадаючи параметри доступу і підвищуючи привілеї, поки не знайде конфіденційну інформацію, щоб вкрасти або зашифрувати з метою викупу. Визначення типу загрози та миттєве реагування на неї зараз є найважливішими складовими будь-якої системи безпеки.

У 2019 році аналітики Solar JSOC вперше зафіксували різке зростання кібератак (приблизно на 40%), причому всі вони мали цільову спрямованість - контроль над IT-інфраструктурою, на тлі чого відбулося зниження на 15% кількості атак, скоєних з метою крадіжки грошей [16]. У попередні роки картина була прямо протилежною: кількість атак, спрямованих на викрадення грошей, щорічно зростала на десятки відсотків, інтерес кіберзлочинців до інфраструктури був незначним. Експерти пов'язують таку ситуацію з тим, що середній рівень захищеності банків, які найчастіше слугували мішенню для кіберзлочинців, значно підвищився. Це змушує хакерів шукати більш вразливі цілі.

Станом на 2019 рік найпопулярнішими методами злому корпоративних інфраструктур залишалися зараження шкідливим програмним забезпеченням (віруси, трояни, шпигунські програми тощо) та використання вразливостей у веб-додатках (веб-портали, електронна пошта, особисті кабінети тощо). Частота їх використання зросла на 11% та 13% відповідно. Але якщо в 2018 році основним функціоналом шкідливого ПЗ було шифрування даних, то в 2019 році - майнінг криптовалют.

Але, на тлі зростання зовнішніх атак, експерти Solar JSOC відзначають і позитивну тенденцію: організації стали приділяти більше уваги захисту своєї інформаційної інфраструктури, в тому числі завдяки цьому вперше за 5 років знизилася частка критичних інцидентів (з 19% до 16%).

Незважаючи на те, що серед кіберзлочинців вважається доброю практикою забирати адміністративні права у бізнес-користувачів, багато організацій насправді не поспішають вносити зміни. Без усіх адміністративних прав бізнес-користувачі можуть мати проблеми з виконанням деяких завдань або запуском певних програм, які необхідні їм для виконання своїх щоденних робочих обов'язків.

Наприклад, користувачеві може знадобитися використовувати в робочих цілях додаток, для запуску якого потрібні певні права. Або користувачеві можуть знадобитися права для встановлення або оновлення авторизованого довіреного додатку. Якщо повністю відібрати адміністративні права у таких користувачів, вони будуть змушені звертатися до служби підтримки кожного разу, коли їм знадобляться такі права для виконання своєї повсякденної роботи.

На додаток до компромісів в продуктивності, пов'язаних з обмеженням прав бізнес-користувачів, багато організацій також не наважуються обмежувати права IT-адміністраторів на серверах Windows. В ідеальних умовах системні адміністратори, власники додатків і адміністратори баз даних мають свій власний набір дозволів на кожному сервері, до якого вони мають доступ [5]. На практиці розподіл обов'язків може бути ускладнений, і адміністратори залишаються з набагато більшими правами, ніж їм дійсно потрібно для виконання своєї роботи. Без рольової політики дозволів, яка розмежовує обов'язки IT-адміністраторів, чутливі системи можуть бути легко пошкоджені недосвідченими користувачами, скомпрометовані інсайдерськими зловмисниками або скомпрометовані досвідченими кіберзлочинцями, які отримують несанкціонований доступ до привілейованих облікових записів.

У той же час зросла мобільність кінцевих користувачів, вони застосовують бездротові технології Wi-Fi і GPRS, віртуальні приватні мережі, підключаються до корпоративної мережі віддалено з дому, на вулиці, в аеропорту, на гостьових ПК. Виходячи з цього, зовсім непростою задачею є захист користувача, який весь час змінює місце та засіб доступу в мережу.

Аби вирішити сучасні проблеми захисту кінцевих точок мережі потрібно занадто багато технологій. Використовувати для цього продукти від різних виробників (або від одного ненадійного виробника) - значить звести ефективність і зручність управління та обслуговування практично до нуля. Саме з цієї причини, більшість відомих постачальників в області систем безпеки випустили комплексні засоби захисту корпоративних мереж. Як правило, такі засоби є багатоярусними системами захисту, а також модуль управління всією системою.

Задля забезпечення функціонування корпоративної інформаційної системи необхідно, аби КІС була описана характерними законами управління, які регламентують управлінські дії на дану систему. Також, вона має охоплювати всі можливі комплексні функції для управління бізнес процесами підприємства, а саме: постачання, маркетинг та продажі, фінанси, сервісне обслуговування тощо.

Зміни, що відбуваються в організації споживання корпоративних ІТ-ресурсів, серед яких перш за все слід зазначити розширення спектру використовуваних в офісах пристроїв доступу, а також вихід користувачів за традиційний периметр захисту (що пов'язано з ростом популярності віддаленої роботи поза офісом, мобільністю персоналу і поширенням публічних хмарних ІТ-сервісів, призначених для підтримки корпоративної роботи), обумовлюють необхідність перегляду підходів до побудови захисту кінцевих точок, що забезпечують доступ користувачів до корпоративних ІТ-ресурсів.

1.3. Мета та завдання захисту кінцевих точок корпоративної інформаційної системи

Слід пам'ятати, що і в умовах масштабних змін, що відбуваються в сучасних ІТ, основними *завданнями* захисту кінцевих точок, що підтримують призначений користувачеві доступ до корпоративних ІТ-ресурсів, за своєю суттю залишаються колишніми: вони включають забезпечення кожному співробітнику безперебійного доступу лише до тих ресурсів, які приписані йому бізнес-роллю, тільки при виконанні умов, передбачених політиками безпеки (визначальними час та місце підключення, тип пристрою підключення і встановлені на ньому системи захисту інфомації (СЗІ), дозволений набір і оновлення програмного забезпечення (ПЗ), канали доступу тощо).

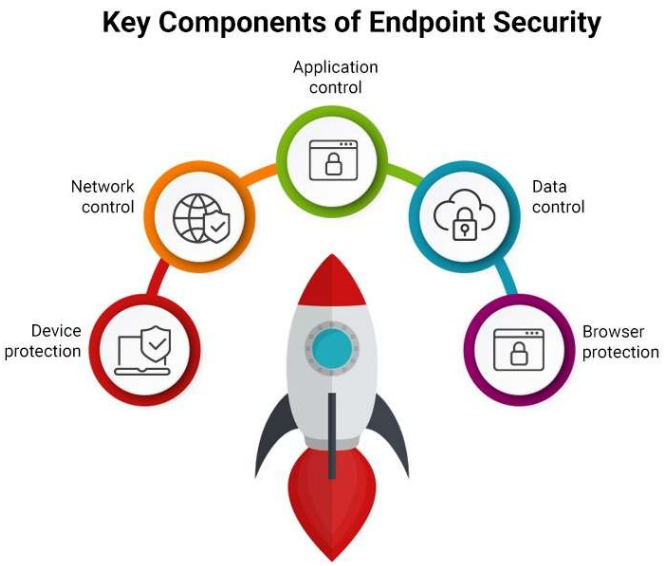


Рис. 1.1 Ключові компоненти захисту кінцевих точок

Вирішення цих завдань спрямоване на мінімізацію ймовірності таких загроз кібербезпеки (КБ), як несанкціоновані дії з даними, атаки на канал передачі інформації між централізованими ресурсами та кінцевою точкою, авторизація іншої особи під ім'ям реального користувача. Засоби захисту, що використовуються для цієї мети, досить добре відомі. Це антивіруси, засоби аутентифікації (наприклад, електронний підпис), засоби захисту каналу (наприклад, VPN). Для мобільних точок доступу додатково потрібно буде встановити криптографічний захист даних, що зберігаються на носіях інформації (в першу чергу знімних носіях типу флешок) і персональний міжмережевий екран.

Якщо для кінцевих точок (ноутбуків, нетбуків, ультрабуків і т.д.), уніфікованих поки що з точки зору апаратної архітектури і операційного середовища, проблем з вибором засобів захисту не виникає, то різноманітність платформ для смартфонів і планшетів вимагає від розробників засобів захисту розробляти спеціальні підходи практично для кожного типу пристроїв, що використовуються на підприємстві.

Основна мета захисту кінцевих точок очевидна - забезпечити захист системи підприємства при доступі до корпоративної мережі з віддалених, бездротових або мобільних пристроїв.

Рис. 1.2 Приклади кінцевих точок

Будь-який комп'ютер або ноутбук, підключений до мережі підприємства, може використовуватися для розповсюдження шкідливих програм. Необхідно робити обов’язковий аналіз як корпоративних комп'ютерів, так і особисті пристрої співробітників в рамках політики використання особистих пристроїв (BYOD), а також зовнішні ПК, які підключаються до офісної мережі через VPN.

Мобільні телефони вимагають особливої уваги. Небезпечно підключати особисті пристрої до офісної мережі перед установкою на них мобільного антивіруса з останніми оновленнями програмного забезпечення. Персонал, який використовує особисті пристрої, також повинен пройти навчання в рамках політики використання особистих пристроїв.

Також, важливо пам’ятати, що під загрозою є не тільки мобільні пристрої і комп'ютери, а ще й інші пристрої, які підключаються до вашої мережі, такі як принтери, факси. Вони вважаються потенційно вразливими і також повинні бути захищені.

Сервери - один з найбільш традиційних типів кінцевих точок. Їх особливо важливо захистити, оскільки на них зберігаються або обробляються бізнес-дані, електронна пошта і ділова документація. Для цієї конфіденційної інформації потрібен особливий рівень захисту.

Тобто, на підприємстві важливо знати, що усі кінцеві точки захищені від потенційних загроз, а також приділяти увагу таким *складовим*:

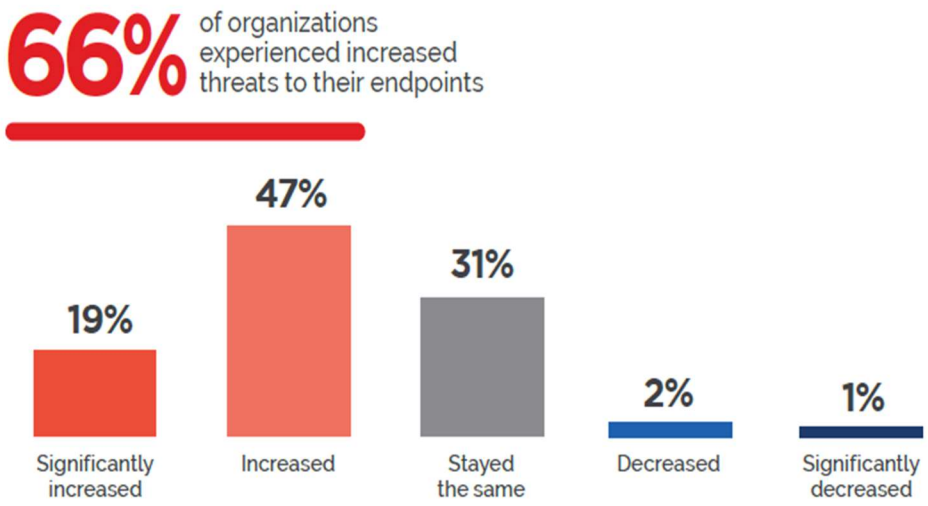
операційні системи - чи працюють всі пристрої на підприємстві під управлінням Windows 8 або більш пізньої версії? Серверне програмне забезпечення 2012 року або більш нове? Більш старі версії могли не отримати виправлення або оновлення для захисту від щодо нових помилок безпеки, а це значить, що пристрої будуть піддаватися більшому ризику проникнення шкідливих програм;

кількість пристроїв - чи контролються всі пристрої, які отримують доступ до корпоративної мережі? У підприємства повинен бути постійний доступ до їх апаратного забезпечення, і його повинні регулярно оновлювати;

оновлення програм - чи оновлені програми на підприємстві та чи є можливість оновлювати їх разом із програмним забезпеченням на всіх пристроях, підключених до корпоративної мережі? У старих версіях програмного забезпечення можуть бути проломи, уразливості nf помилки, якими без праці скористаються хакери. Часто для усунення таких помилок випускаються виправлення, тому необхідно регулярно оновлювати все програмне забезпечення компанії;

зумовлені політики - чи діють на підприємстві зумовлені універсальні політики безпеки (процедури на випадок порушень, мінімальні вимоги до паролів і централізовані перевірки безпеки)? Ручних та спеціальних засобів контролю і правил недостатньо для забезпечення максимальної безпеки підприємства;

заходи забезпечення безпеки - чи в курсі підприємство останніх розробок в сфері кібербезпеки? Сфера кібербезпеки постійно розвивається, а це значить, що завжди є нові розробки, які дозволяють краще зрозуміти кіберзлочинність або посилити заходи безпеки.



1.3. Підвищення рівня загрози для кінцевих точок у 2022 році

1.4. Аналіз існуючих методів та засобів захисту кінцевих точок корпоративної інформаційної системи

До основних заходів щодо забезпечення інформаційної безпеки організації відносяться:

аналіз потенційних і реальних ситуацій, що створюють кіберзагрози для організації;

оцінку характеру загроз інформаційній безпеці;

прийняття та всебічний розподіл заходів щодо виявлення загрози;

реалізацію заходів щодо запобігання загрозам її комерційним інтересам.

Багаторівнева схема захисту інформації та інфраструктури з використанням комплексних рішень кібербезпеки дозволяє мінімізувати ризики та виключити економічні витрати на ліквідацію наслідків кібератак. Правильна організація стану інформаційної безпеки даних покликана запобігати виникненню ризиків за допомогою превентивних заходів, а не усувати їх негативні наслідки. Вжиття превентивних заходів є основою вирішення завдань систем захисту інформації, які полягають у забезпеченні безпечного режиму зберігання документованої інформації, захисту даних, що передаються каналами зв'язку, розмежування прав доступу до окремих категорій документів, резервного копіювання та аварійного відновлення інформаційних систем у разі збоїв програмного та апаратного забезпечення.

Формування безпечного електронного документообігу в компанії передбачає контрольований рух конфіденційних документів через суворо регламентовані пункти прийому, обробки, узгодження, виконання та зберігання в умовах організаційної та технологічної захищеності носія інформації і записаних на ньому корпоративних даних. Однак у житті заходи захисту повинні бути адекватними ймовірності реалізації конкретного виду кіберзагрози в потенціалі з урахуванням масштабів збитків у разі її реалізації, включаючи витрати на придбання засобів захисту. Необхідно забезпечити автоматизацію доступу до робочих процесів для належного захисту файлів, що зберігаються на електронних носіях, від несанкціонованого доступу та впливу шкідливого програмного забезпечення. Наступний ефективний захист комплексний метод.

Комплексний захист корпоративних інформаційних ресурсів вимагає проведення на постійній основі аудиту інформаційної безпеки, який є ефективним інструментом отримання об'єктивної оцінки поточного рівня захищеності компанії від передбачуваних кіберзагроз. Результати аудиту є основою для формування стратегії розвитку системи захисту інформації в автоматизованих інформаційних системах організації, що сприяє підвищенню рівня захисту цінних інформаційних активів від виявлених вразливостей в поточній системі безпеки та управління. Система інформаційної безпеки організації складається з комплексу управлінських рішень, спрямованих на своєчасне виявлення несанкціонованого доступу та запобігання можливим загрозам. Функціонуюча система оцінки інформаційної безпеки повинна бути комплексною, враховувати всі фактори ризику, які впливають на стан інформаційної безпеки. До об'єктів захисту корпоративної інформації відносяться наступні елементи:

об'єкти забезпечуючої інформаційної інфраструктури, що складаються з програмно-технічних комплексів зберігання та обробки даних;

об'єкти автоматизованих систем управління та інформаційних систем (автоматизовані робочі місця, локальні обчислювальні мережі, серверні сегменти цих систем);

системи електронного документообігу

На (таблиці 1.1) детально зображено направлення захисту інформаціх ресурсів в організації.

Таблиця 1.1

Для захисту інформації з обмеженим доступом, що циркулює в автоматизованій інформаційній системі, використовуються сертифіковані відповідно до встановлених вимог програмно-технічні засоби захисту інформації. Виділяються наступні завдання захисту електронних документів, до яких відносяться: підтвердження авторства документа, контроль його цілісності, конфіденційності, а також забезпечення юридичної сили. З метою забезпечення юридично значимого електронного документообігу кожному документу в системі присвоюється реквізит, що дозволяє ідентифікувати його підписанта, який є повноправним учасником документообігу.

При електронній взаємодії уповноважених користувачів повинна забезпечуватися конфіденційність інформації з обмеженим доступом шляхом

захисту змісту електронних документів. Електронні версії документів повинні передаватися захищеними телекомунікаційними каналами зв'язку. Розмежування прав доступу авторизованих користувачів може бути реалізовано шляхом використання підсистеми розроблюваної СЕД, незалежної підсистеми захисту, що зарекомендувала себе на практиці, або їх адаптації до функціональних можливостей існуючої СЕД.

Вимоги до захисту інформації регламентуються виходячи з категорії конфіденційної інформації та потенційних загроз. У більшості випадків захист даних в електронному вигляді, що зберігаються на серверах організації, реалізується шляхом контрольованого доступу та шифрування конфіденційних документів.

Забезпечення безпечного доступу до інформаційних ресурсів в межах системи документообігу досягається шляхом застосування одно- та багатофакторної автентифікації суб'єкта при вході в систему та розмежування прав користувачів, що здійснюється шляхом присвоєння персонального ідентифікатора кожному учаснику. Наступним кроком у вдосконаленні механізмів захисту системи документообігу є протоколювання операцій, що виконуються корпоративними користувачами, яке дозволяє відслідковувати навмисні спроби несанкціонованого доступу та своєчасно їх припиняти.

Сучасні системи електронного документообігу забезпечують необхідний рівень інформаційної безпеки при організації юридично значимого документообігу, виконуючи встановлені вимоги чинного законодавства у сфері захисту інформації.

Розробка повнофункціональної СЕД повинна бути спрямована на зменшення впливу людського фактору в процесі усунення інцидентів кібербезпеки, а також удосконалення механізмів аудиту роботи користувачів в режимі реального часу з можливістю надання керуючих впливів з метою недопущення несанкціонованого доступу до захищених даних. Це дозволить мінімізувати рівень ризиків, пов'язаних з використанням електронного підпису в СЕД.

Засоби захисту інформації, інтегровані в архітектуру СЕД, передбачають забезпечення збереження та достовірності документів, захищеного персоніфікованого доступу та протоколювання дій користувачів. В основу концепції електронного документообігу покладено ідею автоматизації процесів діловодства шляхом впровадження інформаційної системи, яка сприяє підвищенню виконавської дисципліни працівників за рахунок автоматизованих засобів контролю за роботою з електронними документами та прискоренню проходження документопотоків за оптимальними маршрутами. Безпека автоматизованих систем безпосередньо залежить від їх архітектури та вбудованих програмних засобів захисту інформації, які гарантуватимуть автентичність документів та виключатимуть можливість їх фальсифікації. Всі складові СЕД схильні до впливу загроз, які можуть завдати шкоди її компонентам і діяльності організації в цілому.

Впроваджена система електронного документообігу повинна постійно модернізуватися з подальшим розвитком цифрових технологій у сфері кібербезпеки.

Таким чином, широке поширення процесів діджиталізації призвело до необхідності підвищення рівня захисту корпоративних ресурсів. Нематеріальні активи набувають переважного значення у порівнянні з матеріальними активами організації. Забезпечення комплексної інформаційної безпеки передбачає безперервний моніторинг та миттєве реагування в режимі реального часу на події кібербезпеки протягом усього життєвого циклу зберігання та обробки документної інформації. Такі заходи необхідні для мінімізації ризиків витоку конфіденційних даних та пов'язаних з цим збитків для компанії. Впровадження передових цифрових технологій у багатьох галузях економіки вимагає використання інноваційних підходів для забезпечення повноцінного захисту цінних інформаційних масивів.

Рис. 1.4. Лідери по забезпечення захисту кінцевих точок для бізнесу

Кількість кібератак на бізнес-пристрої зростає. З цієї причини вкрай важливо, щоб ваша організація, чи то компанія зі списку Топ 500, чи то команда з 5 осіб, мала ефективний план кібербезпеки для виявлення і припинення атак. Важливою частиною цього має бути впровадження надійного захисту кінцевих точок на всіх пристроях вашої компанії з порталом управління, який дозволить вам контролювати і оновлювати ваші кінцеві точки з будь-якого місця.

Однак ринок безпеки кінцевих точок надзвичайно переповнений, і існує величезна кількість постачальників з різними технологіями, щоб зупинити загрози від досягнення ваших корпоративних пристроїв. Деякі з них орієнтовані на великі організації, в той час як інші краще підходять для малих і середніх організацій.

Проанулізуємо лідерів по забезпечення захисту кінцевих точок для бізнесу:

ESET Endpoint Security

ESET - провідний постачальник програмного забезпечення для захисту кінцевих точок та антивірусного програмного забезпечення, відомий своїми потужними, але легкими рішеннями для кібербезпеки. ESET Endpoint Security - це

хмарне рішення для захисту кінцевих точок, призначене для захисту організацій будь-якого розміру від відомих загроз і загроз нульового дня, таких як шкідливе програмне забезпечення, програми-вимагачі та безфайлові атаки. Рішення пропонує багаторівневий захист, який адміністратори можуть контролювати за допомогою єдиної централізованої консолі управління. ESET Endpoint Security захищає комп'ютери, мобільні пристрої, файлові сервери та віртуальні середовища. Воно доступне як окремий продукт і як частина більш широкого корпоративного пакету кібербезпеки ESET PROTECT Enterprise, який також включає в себе захист файлових серверів, шифрування дисків, хмарну пісочницю і EDR.

ESET Endpoint Security поєднує в собі технології машинного навчання і краудсорсингову аналітику загроз для виявлення і запобігання цілеспрямованим атакам шкідливих програм і програм-вимагачів. Рішення відстежує всі запущені програми на наявність шкідливого контенту на основі їх відомої поведінки та репутації. Воно також сканує поведінку шкідливих файлових процесів у пам'яті кожної кінцевої точки, щоб виявити та усунути безфайлові загрози. Поєднання технічної та людської розвідки загроз означає, що рішення ESET має відмінні показники виявлення загроз до, під час і після виконання. ESET Endpoint Security також пропонує захист веб-браузерів, запобігаючи завантаженню шкідливих файлів і дозволяючи адміністраторам вносити відомі шкідливі URL-адреси в чорний список, а також створювати списки URL-адрес, які потребують особливого захисту.

Команди безпеки можуть керувати безпекою всіх кінцевих точок ESET, включаючи мобільні пристрої, за допомогою єдиної хмарної консолі управління. Це дозволяє їм мати чітке уявлення про стан безпеки в організації.

ESET Endpoint Security цінується за свою легкість; воно працює так само добре, як і будь-яка надійна система захисту від шкідливого програмного забезпечення, без необхідності в додатковому обладнанні і без уповільнення роботи корпоративних систем. Хмарне рішення є масштабованим та гнучким: ESET Endpoint Security сумісний з операційними системами Windows, Mac, Linux і Android, з вбудованим управлінням мобільними пристроями для iOS і AndroidOS.

Крім того, консоль адміністрування доступна 21 мовою, а локалізована підтримка від ESET - 38 мовами. Це робить ESET Endpoint Security надійним рішенням для організацій з глобальною робочою силою, а також для організацій з великою кількістю пристроїв BYOD у своєму використанні.

Heimdal™ Threat Prevention Endpoint

Компанія Heimdal™ зі штаб-квартирою в Копенгагені є провідним європейським постачальником хмарних рішень з кібербезпеки. Їхній внесок у наш список продуктів для захисту кінцевих точок - це інструмент Threat Prevention Endpoint. На перший погляд, продукт являє собою рішення для захисту DNS, яке поєднує в собі аналіз загроз, машинне навчання і штучний інтелект для забезпечення надійного запобігання загрозам на всіх кінцевих точках у вашій мережі. Він може бути інтегрований з будь-якими іншими рішеннями, які вже існують, і не перериває існуючі робочі процеси. Його мета - надати командам повну видимість і розширений контроль над мережею і підключеними до неї кінцевими точками. Все це досягається за допомогою єдиної чистої і консолідованої інформаційної панелі.

Heimdal™ Threat Prevention Endpoint забезпечує безпеку кінцевих точок, виходячи за рамки антивірусних можливостей. Він забезпечує безпечний перегляд веб-сторінок для всіх користувачів, незалежно від того, чи працюють вони вдома, в офісі або там і там, скануючи трафік в режимі реального часу, блокуючи будь-які підозрілі або шкідливі домени і припиняючи будь-яку зловмисну комунікацію. Це особливо корисно для співробітників, які перебувають у дорозі і можуть підключатися до незахищених або вже заражених мереж, а також для захисту кінцевих користувачів від раптових перенаправлень на інші веб-сторінки під час перегляду.

Продукт використовує можливості пошуку загроз DNS кінцевих точок, які допомагають йому виявляти і обробляти будь-які шкідливі URL-адреси, перш ніж відстежувати загрозу до її джерела. Він також використовує DarkLayer Guard™,

механізм фільтрації трафіку, який працює на вхідному та вихідному трафіку. Ця функція може бути налаштована, і адміністратори можуть встановлювати списки, на які буде посилатися механізм.

Heimdal™ Threat Prevention Endpoint пропонує складне, але зручне і просте рішення для захисту кінцевих точок, пропонуючи новий підхід у вигляді DNS, керованого штучним інтелектом. Можно рекомендувати продукт для малого та середнього бізнесу, який шукає щось нове.

Avast Рішення для малого бізнесу

Компанія Avast є світовим лідером у наданні рішень з кібербезпеки для бізнесу та споживачів. Рішення для малого бізнесу Avast захищають клієнтів від шкідливого програмного забезпечення та програм-вимагачів, а також надають можливості VPN та управління виправленнями. Avast має одну з найбільших у світі мереж виявлення загроз та базу даних загроз, яка захищає понад 440 мільйонів кінцевих точок та 10 000 серверів по всьому світу. Це дозволяє їм збирати та аналізувати величезні обсяги даних про загрози, а також створювати технології машинного навчання для зупинки загроз для кінцевих точок в режимі реального часу.

Avast Small Business Solutions - це повністю хмарне рішення з онлайн-платформою управління, за допомогою якої можна легко налаштовувати захист пристроїв, здійснювати моніторинг кінцевих точок та додавати нові пристрої. Avast - провідний розробник антивірусних рішень, що пропонує розширений захист від програм-вимагачів та крадіжки даних. Avast також забезпечує провідну підтримку клієнтів, яка надається досвідченими технічними інженерами в режимі 24/5. Крім того, Avast також пропонує захист особистих даних за допомогою пароля та веб-камери, призначених для запобігання компрометації облікових записів та пристроїв співробітників.

Рішення Avast для малого бізнесу доступні в трьох рівнях: Essential, Premium і Ultimate. Premium і Ultimate надають додаткові ключові функції безпеки, включаючи вбудовану VPN для шифрування даних і безпечного інтернет-з'єднання при використанні публічних мереж WiFi, захист USB. Ultimate також забезпечує управління виправленнями, що гарантує автоматичне усунення вразливостей при їх появі. Це рішення отримало високу оцінку клієнтів і доступне для Windows, MacOs, IOS, Android та інших операційних систем.

Можно рекомендувати це рішення для малого та середнього бізнесу та підприємств, яким потрібен посилений захист кінцевих пристроїв з функціями VPN, управління виправленнями та захисту від програм-вимагачів.

Bitdefender GravityZone

Bitdefender GravityZone - це універсальна платформа для захисту кінцевих точок, що забезпечує як захист, так і виявлення та реагування на загрози. Bitdefender використовує машинне навчання для моніторингу поведінки та запобігання атакам, що, за їхніми словами, зупиняє загрози, які традиційні технології захисту кінцевих точок та антивірусні технології пропускають. Вони також пропонують розширений контроль над кінцевими точками, з управлінням виправленнями, захистом від веб-загроз і контролем додатків і пристроїв, щоб допомогти організаціям керувати кінцевими пристроями. Bitdefender може бути доставлений через хмару або локально.

Ключовими сильними сторонами Bitdefender є дослідження загроз і простота управління, а також надійний захист від загроз. Антивірус, заснований на поведінкових моделях, може допомогти запобігти атакам на кінцеву точку. Bitdefender також має велику команду дослідників і розробників, яка допомагає тримати руку на пульсі нових і нових загроз. Весь набір продуктів Bitdefender для кінцевих точок також управляється з однієї консолі адміністратора.

Клієнти Bitdefender хвалять сервіс за простоту використання, надійний захист від загроз і легкий клієнт для кінцевих точок. Користувачі припускають, що використання GravityZone в хмарі робить управління кінцевими точками "безпроблемним". Центральне розташування для управління додатком і станціями кінцевих користувачів користується великою популярністю серед користувачів. Однак деякі клієнти вважають, що сервісу не вистачає деяких більш просунутих функцій, які пропонують інші постачальники засобів захисту кінцевих точок. Послуга популярна серед малих і середніх організацій, а також серед деяких корпоративних клієнтів. Можно рекомендувати її організаціям, які потребують надійного захисту кінцевих точок від загроз за допомогою простого в управлінні рішення.

Trend Micro

Trend Micro пропонує повний набір рішень для захисту кінцевих точок. Воно захищає фізичні кінцеві точки, ПК і сервери, комп'ютери Mac, а також кінцеві точки в торгових точках і банкоматах. Рішення Trend Micro поставляється у вигляді єдиного агента, який забезпечує автоматизоване виявлення і реагування, а також централізоване спостереження і контроль. Trend Micro забезпечує надійний захист від шкідливих програм і програм-вимагачів, володіючи розширеними можливостями захисту як від відомих, так і від невідомих загроз.

Рішення Trend Micro захищає широкий спектр кінцевих пристроїв і підходить як для нових кінцевих пристроїв і серверів, так і для застарілих операційних систем для користувачів застарілих пристроїв. Клієнти Trend Micro високо оцінюють

надійний захист від загроз, який забезпечує захист файлів, хостів і серверів, до яких надається спільний доступ, від вірусів, шкідливих програм і програм-вимагачів. Клієнти також відзначають простоту установки і невелику вагу рішення. Trend - це надійне рішення для середніх і великих корпоративних клієнтів. Воно пропонує потужний захист від загроз і доступне по всьому світу завдяки потужній партнерській мережі.

Crowdstrike Falcon

Crowdstrike пропонує комплексний набір опцій захисту кінцевих точок під назвою Falcon. Вони пропонують комплексну, провідну на ринку платформу для захисту кінцевих точок, різні варіанти для підприємств, малих і середніх клієнтів, кожен з яких має унікальні можливості виявлення та реагування на загрози. Crowdstrike є одним з провідних постачальників рішень для захисту кінцевих точок, і компанія швидко зростає. Вони працюють в більш ніж 176 країнах, і їх частка на ринку рішень для кінцевих точок зростає.

Crowdstrike захищає від атак шкідливого програмного забезпечення та забезпечує постійну та всебічну видимість на всіх ваших кінцевих пристроях. Crowdstrike також може виявляти і попереджати адміністраторів про несанкціоновані системи і додатки в режимі реального часу, що дозволяє швидше усунути загрози. У Crowdstrike також працюють досвідчені аналітики з кібербезпеки, які можуть забезпечити кероване виявлення та реагування, а також кероване полювання на загрози. Ключовими перевагами цього сервісу є простота розгортання, потужні можливості виявлення загроз та широкий спектр кінцевих точок, які вони можуть захистити. Рішення повністю хмарне, без локальної версії.

Клієнти Crowdstrike високо оцінюють сервіс, багато з них відзначають потужність виявлення загроз і оповіщення адміністраторів в режимі реального часу. Рішення найбільш підходить для корпоративних клієнтів, хоча Crowdstrike пропонує рішення для малих і середніх організацій. Як хмарне рішення для кінцевих точок, Crowdstrike є хорошим варіантом для організацій, які шукають потужний захист кінцевих точок, що надається як послуга, з гнучкими ціновими опціями і швидким розгортанням.

Trellix Endpoint Security

Trellix Endpoint Security (раніше McAfee Enterprise) забезпечує інтегровану, централізовано керовану платформу захисту кінцевих точок з розширеними можливостями захисту від загроз. Для виявлення загроз Trellix використовує передові можливості виявлення загроз, включаючи машинне навчання та моніторинг крадіжок облікових даних, а також розширені можливості виявлення та реагування (XDR).

Ключовими сильними сторонами платформи Trellix є виявлення та реагування на загрози, які добре інтегруються з Windows. Trellix фокусується на

автоматизації, використовуючи машинне навчання і поведінковий аналіз, щоб дозволити кінцевим точкам швидше взаємодіяти і виявляти загрози. Це означає, що зменшується потреба в ручному виявленні та усуненні загроз, оскільки Trellix може забезпечити автоматичний аналіз, локалізацію та усунення загроз для вашого парку кінцевих точок.

Trellix Endpoint Security підходить для великих клієнтів, які шукають надійне рішення для захисту кінцевих точок з потужним і автоматизованим виявленням загроз і реагуванням на них. Платформа Trellix є відмінним варіантом для організацій, які шукають інтегроване рішення для захисту кінцевих точок, XDR і MDR, що забезпечує безперервний моніторинг загроз і автоматизоване реагування, з потужним захистом на рівні пристроїв.

Microsoft Endpoint Protection

Microsoft Endpoint Protection тісно інтегрована з Windows 10. Microsoft описує її як уніфіковану платформу для захисту пристроїв за допомогою поведінкового антивірусу, пост-інцидентного виявлення, автоматизації та реагування. Microsoft також надає консоль реагування на інциденти, яка забезпечує оповіщення та заходи реагування на інциденти в програмі Defender ATP, а також ATP, Office 365, Azure та Active Directory.

Defender ATP працює безпосередньо з Windows 10, але також доступний в різних середовищах з версією для Mac і Linux. Антивірус Windows Defender - одна з найпопулярніших платформ для захисту кінцевих точок бізнесу, яка є лідером на ринку в цьому сегменті. Однак, в ліцензуванні важко орієнтуватися, і цей паритет функцій не відповідає рівню рішень для захисту кінцевих точок від сторонніх виробників. Це підтверджується незалежними дослідженнями, які показують, що Defender не має високого рейтингу серед конкурентів з точки зору захисту від загроз.

Клієнти в Інтернеті високо оцінюють Microsoft Defender, а деякі з них повідомляють, що після встановлення служби вони побачили "більшу безпеку та ефективність". Таким чином, Windows Defender є хорошим варіантом для користувачів Windows, які шукають рішення для управління своїми кінцевими точками Windows 10, не бажаючи використовувати сторонні засоби захисту кінцевих точок.

SentinelOne

SentinelOne описується як "автономна платформа штучного інтелекту" для захисту від атак на кінцеву точку. За допомогою єдиного агента SentinelOne виявляє, реагує і зупиняє загрози на всіх кінцевих точках. Воно розроблене з урахуванням простоти використання, використовуючи штучний інтелект для автоматичного усунення загроз в режимі реального часу, заощаджуючи час команд IT-безпеки і підвищуючи ефективність їхньої безпеки. Рішення також надає

детальні звіти, що дозволяє адміністраторам краще бачити стан справ у своїх мережах. Платформа SentinelOne швидко розвивалася протягом останніх кількох років. SentinelOne може бути розгорнута в хмарних середовищах і як локальне рішення.

Ключовою особливістю SentinelOne є її високоавтоматизовані можливості захисту кінцевих точок від загроз з акцентом на інноваційні підходи до безпеки. SentinelOne використовує алгоритми штучного інтелекту для захисту від широкого спектру векторів загроз в режимі реального часу. Вони стверджують, що це підвищує ефективність безпеки, усуваючи затримку в хмарі і необхідність втручання людини. SentinelOne також пропонує функцію "Ranger", яка перетворює кожну кінцеву точку на вартового, який полює на шкідливе програмне забезпечення і може впроваджувати динамічні політики. SentinelOne забезпечує високий рівень ефективності роботи агентів.

SentinelOne користується популярністю серед клієнтів, а онлайн-огляди свідчать про високий рівень задоволеності клієнтів. Багато хто хвалить його ефективність захисту від загроз і простоту сервісу. Користувачі також повідомляють, що розгортання дуже просте, з мінімальним впливом на їх виробниче середовище. SentinelOne є хорошим варіантом для організацій, які шукають новий підхід до безпеки кінцевих точок, з більш автоматизованим, спрощеним підходом до безпеки кінцевих точок, без шкоди для сильної функціональності безпеки кінцевих точок.

Sophos Endpoint Protection

Sophos Endpoint Protection має на меті спростити захист кінцевих точок для організацій, полегшуючи захист систем Windows, Mac і Linux. Він забезпечує захист від шкідливого програмного забезпечення та шкідливого веб-трафіку. Вона також дозволяє адміністраторам отримати більший контроль над веб-контентом, пристроями додатків і управлінням даними з комплексним застосуванням політик. Платформа може бути розгорнута як хмарна консоль або встановлена на місці.

У січні 2019 року Sophos придбав DarkBytes, постачальника послуг з криміналістики кінцевих точок. Ця послуга була включена в платформу керованого виявлення та реагування Sophos. У жовтні 2019 року Sophos погодився на придбання Thoma Bravo, яка заявила, що має намір зберегти Sophos як окрему компанію.

Клієнти Sophos високо оцінюють пропоновані функції безпеки, стверджуючи, що вони "зупиняють шкідливе програмне забезпечення нульового дня" і забезпечують розширену функціональність проти програм-вимагачів. Клієнти також хвалять Sophos за простоту використання. Sophos надає одну єдину консоль адміністратора, з якої можна керувати всіма кінцевими точками. Однак, відгуки клієнтів свідчать про те, що деякі клієнти зіткнулися з повільною установкою і оновленням програмного забезпечення. Sophos є хорошим варіантом для розгляду для організацій середнього та великого бізнесу.

Symantec Endpoint Protection

Symantec - ще один з лідерів ринку захисту кінцевих точок, з великою клієнтською базою великих компаній та підприємств. Вони надають повне, інтегроване рішення для кінцевих точок, яке може бути розгорнуте в приміщенні або як хмарне рішення. Symantec Cloud Endpoint Security забезпечує повний захист кінцевих точок, а також хмарне управління виявленням і реагуванням на загрози, яке здійснюється за допомогою єдиного агента. У серпні 2019 року підрозділ корпоративної безпеки Symantec, включаючи Symantec Endpoint Security, був придбаний компанією Broadcom.

Symantec пропонує повнофункціональне рішення для захисту кінцевих точок з потужними можливостями запобігання загрозам, включаючи захист від безфайлових атак, посилену безпеку мобільних додатків, захист користувачів, підключених до хмарних технологій, а також можливість моніторингу та блокування несанкціонованого доступу. Symantec використовує штучний інтелект, щоб полегшити оновлення політик і спростити робочі процеси для команд адміністраторів.

До недавнього часу Symantec була лідером на ринку безпеки кінцевих точок, зараз вона поступається Microsoft, і її частка на ринку продовжує скорочуватися. Придбання Broadcom занепокоїло аналітиків з кібербезпеки та багатьох клієнтів Symantec, які побоюються, що підтримка буде скорочена. Broadcom дала зрозуміти, що зосередиться на зростанні ринку Global 2000, що викликало занепокоєння у менших організацій, які користуються цією послугою. Загальним наслідком цього стало те, що багато клієнтів зараз шукають альтернативи рішенням Symantec Endpoint Security. Інші постачальники використовують цю можливість на свою користь, деякі з них пропонують спеціальні пропозиції для клієнтів Symantec. В цілому, Symantec пропонує комплексне і потужне рішення для захисту кінцевих точок, але придбання Broadcom ставить під сумнів його придатність для малих і середніх організацій.

Висновки до розділу

В роботі проведено дослідження та аналіз проблеми забезпечення захисту кінцевих точок корпоративної інформаційної системи, встановлена сутність завдань їх захисту.

Проаналізовано існуючі технології захисту кінцевих точок корпоративної інформаційної системи.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КІНЦЕВИХ ТОЧОК НА ПРИКЛАДІ SYXSENSE ENDPOINT SECURITY

2.1. Призначення, основні функції та склад програмного комплексу Syxsense Endpoint Security

Сьогоднішній ландшафт загроз є більш непередбачуваним, ніж будь-коли, після COVID-19, подальшого переходу на віддалену та гібридну роботу, а також у зв'язку з тим, що кіберзлочинці використовують все більш витончені методи атак. Кількість атак на кінцеві точки зростає, а вартість витоку даних продовжує збільшуватися - з 3,86 млн доларів до 4,24 млн доларів у 2021 році, згідно зі звітом IBM про вартість витоку даних (Cost of a Data Breach Report).

Кінцеві точки є воротами, які зловмисники використовують для доступу до даних власників компанії; залишаючи їх незахищеними, користувач наражаєте себе на ризик і потенційну атаку, а також на фінансові, репутаційні та юридичні наслідки витоку даних.

Для організацій вкрай важливо прийняти послідовні підходи до захисту кінцевих точок в 2022 році і надалі. Найкращий спосіб для IT-команд досягти цього без додаткового навантаження - це рішення для захисту кінцевих точок, яке забезпечує безперервний моніторинг загроз, виявлення та автоматизацію критично важливих завдань безпеки.

Syxsense створила інноваційну та інтуїтивно зрозумілу технологію, яка бачить і знає все. Захистіть кожну кінцеву точку, в будь-якому місці, всюди в мережі і за її межами, а також в хмарі. Штучний інтелект (ШІ) допомагає командам безпеки прогнозувати і усувати загрози до того, як вони відбудуться, і швидко змусити їх зникнути, коли вони відбудуться.

Штаб-квартира Syxsense знаходиться в Ньюпорт-Біч, штат Каліфорнія, і є зростаючою і динамічною організацією з офісами в чотирьох країнах і 12 партнерами в дев'яти країнах. За останні 10 років Syxsense працювала з більш ніж

500 компаніями, що мають від 100 до 100 000 кінцевих точок, надаючи різноманітні рішення для організацій будь-якого розміру, а також постачальників керованих послуг (MSPs).

6 простих правил від Syxsense для забезпечення захисту кінцевих точок:

Завжди встановлювати оновлення

Керування оновленнями програмного забезпечення, зокрема, виправленнями на кінцевих точках, захищає вашу організацію від відомих загроз. Поява нових типів кінцевих точок, таких як Інтернет речей (IoT), Bring Your Own Device (BYOD) та інших вразливостей операційних систем і програмного забезпечення, вимагає незліченної кількості виправлень. Завжди встановлювати патчі, це можливість випередити зловмисників.

2. Шукати всі кінцеві точки

Думати про мережу всієї компанії - скільки там пристроїв? Чи не вражає їх кількість? Користувачу краще подумати про це, тому що на кінцеві точки припадає переважна більшість порушень безпеки - за оцінками, ця цифра становить близько 70 відсотків. І якщо користувач не знає, що вони у нього є, він не можете їх захистити.

3. Бути в курсі подій

Компанія повинна адаптуватися до зростаючої складності хакерів та їх кібератак. Погані актори ніколи не сплять - вони постійно працюють над вдосконаленням своїх кібератак, постійно розвиваючи ландшафт загроз. Тому організація повинна розгорнути рішення для захисту кінцевих точок, які не відставатимуть від потоку шкідливого програмного забезпечення, який можна очікувати в майбутньому.

4. Будти стійкими

Експерти вважають, що компанії повинні прагнути бути стійкими, припускаючи, що порушення неминучі. Оскільки на кінцеві точки припадає

близько 70 відсотків всіх порушень, здатність знайти і виправити атаку на кінцеву точку, продовжуючи при цьому ефективно управляти своїм бізнесом, є ключем до стійкості. Не можна допустити, щоб загроза або злом кінцевих точок призвели до демобілізації всього бізнесу.

5. Стратегія розвитку

Багато організацій мають непослідовний підхід до безпеки кінцевих точок. Сьогодні компанії повинні управляти безпекою кінцевих точок стратегічно і почати повністю розуміти ризики, пов'язані з усіма кінцевими точками. Якщо цього не зробити, то це може призвести до недосконалості процесів і процедур, в результаті чого кінцеві точки стануть відкритими для атак і порушень.

6. Пріорітетність

В цілому, безпека кінцевих точок та кібербезпека повинні стати пріоритетом у бізнес-планах вашої організації. Безпека кінцевих точок не просто захищає бізнес - вона зберігає репутацію, заспокоює клієнтів компанії та оптимізує бізнес-процеси. Без необхідної розстановки пріоритетів, якої вимагає кібербезпека, система захисту кінцевих точок, швидше за все, зазнає невдачі.

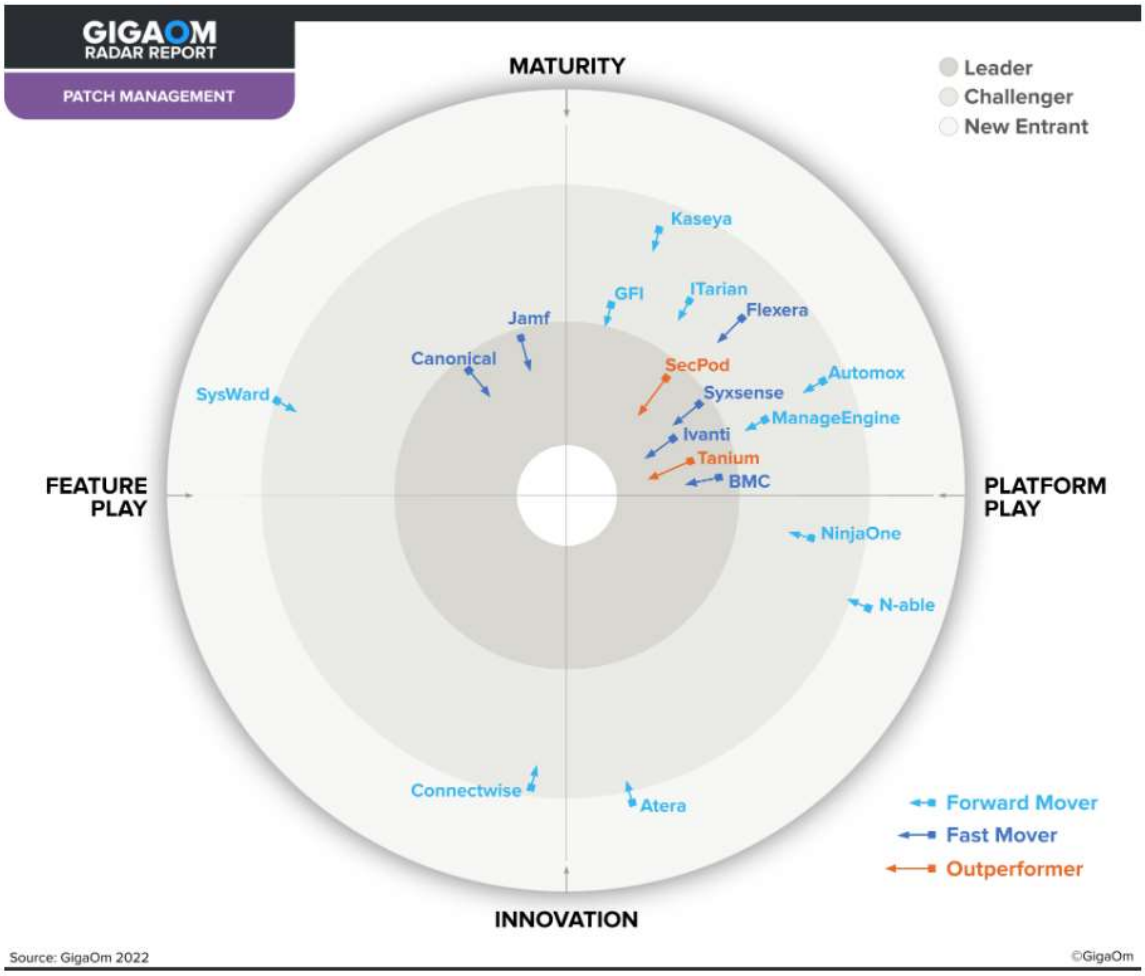


Рис. 2.1. Syxsense названа лідером рейтингу GigaOm Radar Report для рішень з патч менеджменту

Syxsense була названа Fast Mover у звіті GigaOm Radar Report for Patch Management. Цей звіт є одним із серії документів, які допомагають IT-організаціям оцінювати конкуруючі рішення в контексті чітко визначених функцій і критеріїв, а також надає перспективний аналіз, який відображає відносну цінність і прогрес рішень постачальників по декількох осях, заснованих на стратегії і виконанні.

У цьому звіті узагальнено аналіз ключових критеріїв та їх вплив на показники оцінки для створення графіку GigaOm Radar, на якому рішення постачальників зображені у вигляді серії концентричних кілець, причому ті, що розташовані ближче до центру, оцінюються як такі, що мають вищу загальну цінність. Діаграма характеризує кожного постачальника по двох осях - балансуючи між зрілістю та інноваціями, а також між функціоналом та платформою, - а стрілка вказує на

еволюцію кожного рішення протягом наступних 12-18 місяців.

Як Fast Mover в управлінні виправленнями, Syxsense забезпечує повне охоплення настільних комп'ютерів і серверів Windows, macOS і Linux, а також мобільних пристроїв і віддалених систем. Наші сильні сторони полягають в управлінні життєвим циклом, тестуванні патчів, розгортанні патчів, визначенні пріоритетів патчів і великій кількості сторонніх додатків. Syxsense також підтримує API, що дозволяє інтегруватися з іншими системами, такими як ITSM і CMDB. Наше рішення для управління виправленнями розгортається як SaaS-додаток з агентами, встановленими на кінцевих точках вашої організації, і добре підходить для сегментів ринку, включаючи середній ринок, великі підприємства і MSP.

Основні причини при виборі Syxsense Endpoint Security:

Комплексне виявлення вразливостей

Syxsense відстежує середовище і виявляє відсутні оновлення ОС і патчі сторонніх виробників, а також неправильні конфігурації безпеки, які можуть зробити ваші кінцеві точки відкритими для атак. Завдяки точному і своєчасному виявленню користувач точно знає, де і які пристрої представляють серйозний рівень ризику для організації, гарантуючи, що він можете націлити критичні оновлення на потрібні пристрої.

Syxscore

Інструмент оцінки безпеки надає актуальну інформацію про рейтинги серйозності та оцінки CVSS, обізнаність громадськості, контрзаходи та статус озброєності щодо пристроїв у вашому середовищі, а також розбивку пристроїв, які є вразливими.

Усунення вразливостей безпеки

Допомагає виявити та усунути вразливості безпеки та неправильні конфігурації за допомогою єдиного агента з єдиного рішення. Дані в режимі реального часу про зміни поведінки і стану і інтелектуальна автоматизація робочих процесів забезпечують зв'язок між кінцевими точками і консоллю в режимі 24/7. З Syxsense пристрої є самосвідомими і самокерованими, і можуть автоматично ініціювати дії по усуненню несправностей. Не просто знаходьте загрози, а усувайте

їх.

Безпечне рішення

Syxsense є хмарним рішенням і розміщується в Microsoft Azure для забезпечення безпечної передачі даних. Кожен клієнт має приватну базу даних, без змішування даних. Завдяки підтримці двофакторної автентифікації, IP обмежень, єдиного входу в систему, відстеження та сповіщення входу в систему, а також оповіщення про аномальні входи, гарантовано, що дані залишаються такими ж захищеними, як і кінцеві точки.

100% Видимість

Видимість кожної кінцевої точки у середовищі, яка взаємодіє через мережу користувача. Syxsense виявляє настільні комп'ютери, ноутбуки, сервери, віртуальні машини, мобільні пристрої та пристрої IoT, незалежно від того, чи знаходяться вони на місці, в роумінгу, віддалено або в хмарі. Повна видимість кінцевих точок в реальному часі і детальна інформацію про їх стан, безпеку і потенційні ризики.

Реагування в режимі реального часу

Скорочення часу між виявленням і усуненням загроз є невід'ємною частиною безпеки вашого середовища і вашої здатності уникати інцидентів, що завдають шкоди. За допомогою даних в режимі реального часу можливо локалізувати і усунути загрози відразу після їх виявлення - до того, як вони поширяться на решту мережі.

Підтвердження відповідності

Мінімальний тягар документування та демонстрації відповідності під час регуляторних перевірок за допомогою підготовлених і автоматизованих звітів про підтвердження відповідності. Маючи доступ до готових звітів, можливо генерувати докази відповідності без збору великих обсягів даних або створення складних користувацьких звітів. Користувач забезпечуєте дотримання нормативних вимог, захищає дані клієнтів та уникаєте фінансових, юридичних та репутаційних санкцій для бізнесу.

Автоматизація робочих процесів за допомогою Syxsense Cortex

Можливість створення складних послідовних завдань, які працюють

незалежно на кінцевих точках 24/7 за допомогою інтерфейсу перетягування. Syxsense Cortex робить кінцеві точки по-справжньому інтелектуальними з гіперчутливими рецепторами для збору даних про зміни поведінки і стану і більш швидкого запуску процесів карантину і відновлення, гарантуючи, що користувач зможе управляти розширюваними поверхнями атак і швидше виконувати засоби захисту в віддалених, принесених з собою і хмарних середовищах.

Простота впровадження

Користувач може отримати приватну, захищену консоль, яка буде працювати з власними даними пристроїв в реальному часі менш ніж за п'ять хвилин. Робочий легкий і швидкий агент готовий до розгортання на кожному пристрої на вашому підприємстві з підтримкою операційних систем Windows, Mac, Linux, iOS, iPadOS і Android.

Хмарна архітектура

Керування пристроями будь-де, незалежно від того, де вони знаходяться, без витрат на придбання та підтримку локальних рішень. Syxsense побудований на сучасній архітектурі додатків безпосередньо в хмарі для оптимальної стабільності, безпеки та швидкості реагування.

2.2. Основні функції та принципи роботи модуля Syxsense Manage

Патч менеджмент

Тримати поверхню атаки невеликою. Точне виявлення. Наша вдосконалена логіка виявлення сканує мережу та виявляє пристрої з відсутніми оновленнями.

Швидке розгортання. Скорочення часу між виявленням і локалізацією. Виявлення критичної загрози на ранніх стадіях і миттєве розгортання рішення.

Операційна система та сторонні розробники. Вміст виправлень курується щоночі за допомогою синхронізації баз даних NIST і автоматизованого веб-сканера.

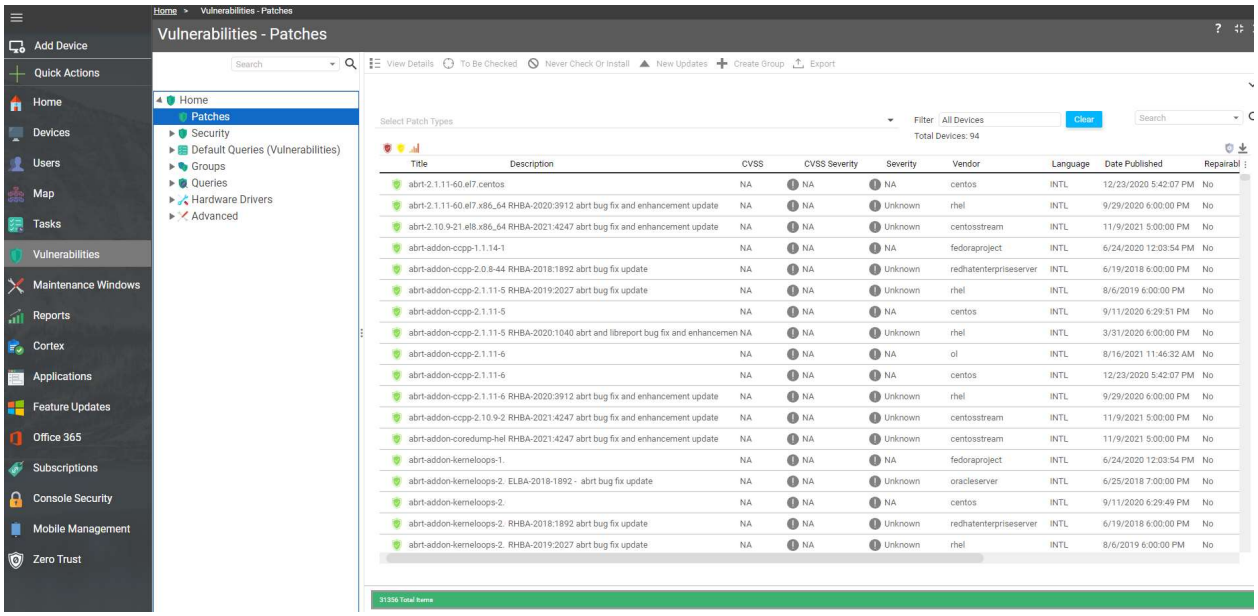


Рис. 2.2. Інтерфейс взаємодії с патчами на які скануються кінцеві точки

Цільове розміщення оновлень

Успіх стратегії безпеки залежить від того, наскільки швидко можливо встановити найважливіші оновлення на найбільш вразливі пристрої. Широкі можливості фільтрів і запитів дають вам повний контроль над визначенням пріоритетів виправлень, в той час як наша сувора логіка виявлення гарантує, що на кожен пристрій будуть встановлені тільки необхідні оновлення. Програмне забезпечення залишається актуальним, розгортання спрощується, а мережа стає безпечною.

Syxscore

Інструмент оцінки безпеки. Syxscore надає оцінки серйозності NIST і постачальників щодо стану безпеки кінцевих точок у вашому середовищі. Це персоналізована оцінка того, які пристрої є вразливими і наскільки важливі оновлення для загального захисту мережі, що дає можливість орієнтуватися на кінцеві точки, які представляють найбільш серйозний рівень ризику.

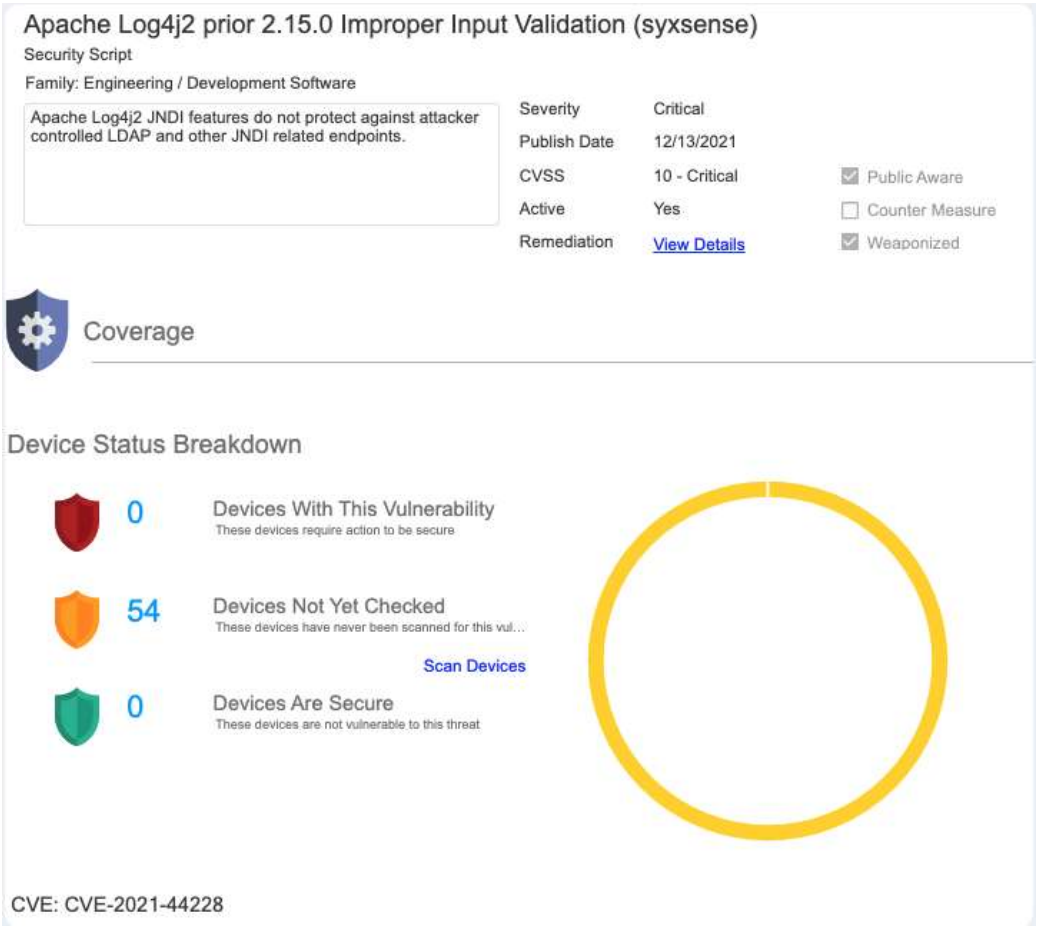


Рис. 2.3. Приклад вигляду описа патча

Заміна патчів

Позбавлення від турбот про застарілі патчі, тому ніколи не доведеться досліджувати, в якому порядку потрібні оновлення. Надається більше, ніж просто статус патча, з автоматичним виключенням застарілих патчів і включенням нових патчів. Якщо користувач розгортає оновлення у всій мережі або на одному пристрої, Syxsense гарантує, що розгортання буде максимально ефективним, заощаджуючи час і пропускну здатність мережі.

Оновлення функцій операційної системи Windows

Керування оновленнями функцій Windows 10 окремо від інших ОС і розгортань сторонніх виробників. За допомогою Syxsense можливо використовувати власні ISO-образи для оновлення пристроїв до підтримуваних версій Windows 10, щоб зменшити навантаження на управління випусками та гарантувати, що користувач не пропустить критичні оновлення.

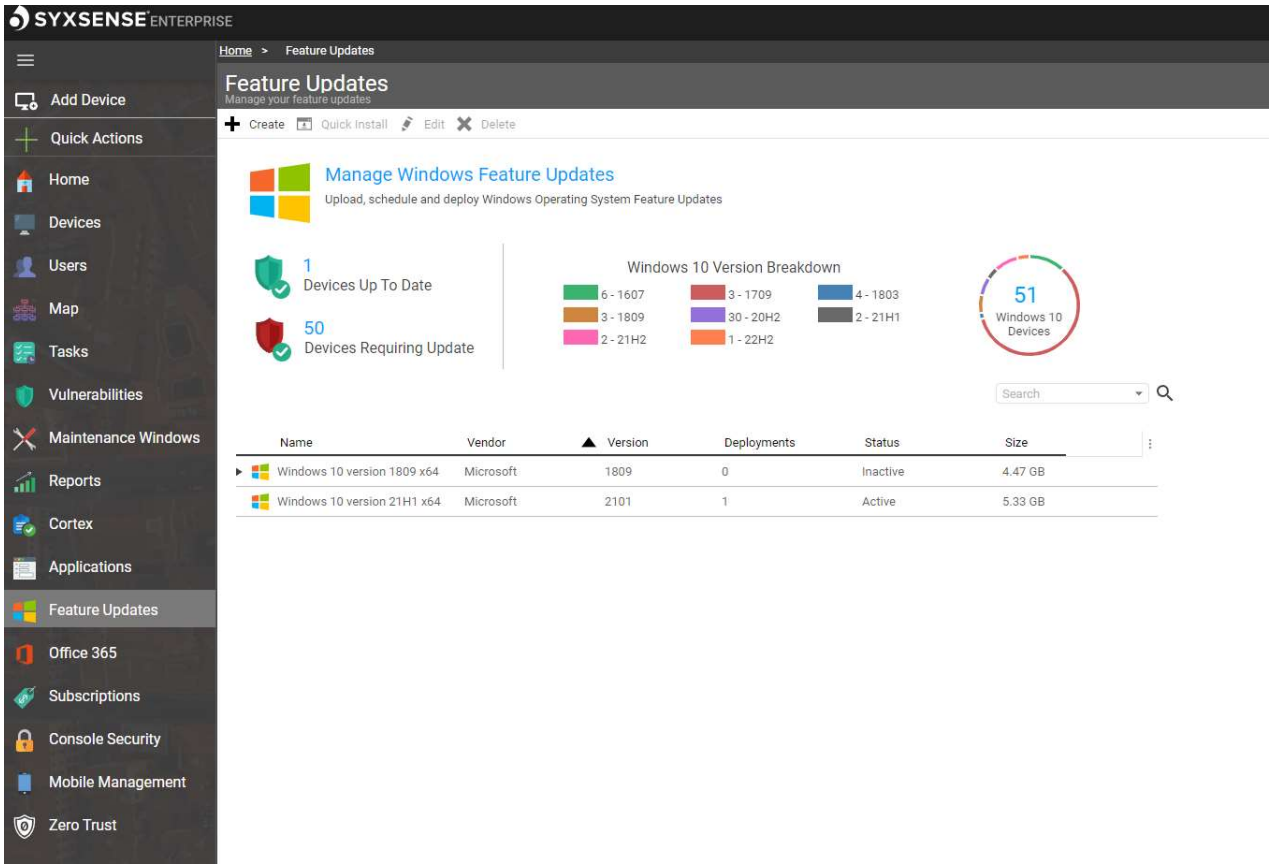


Рис. 2.4. Керування оновленнями для операційної системи Windows

Управління перезавантаженням

За замовчуванням програма пригнічує перезавантаження, щоб ніколи не заважати користувачам працювати в робочий час. Тригери часу та активності дають повний контроль над продуктивністю, повторенням та плануванням кожного завдання перезавантаження, яке обробляється в середовищі.

Дистанційне керування з будь-якого місця, в будь-який час

Віддалений доступ до пристроїв співробітників з будь-якої відстані, незалежно від того, де знаходиться користувач.

Віддалене усунення несправностей. Вирішення будь-яких проблем, великі чи малі. Надання спільного доступу до робочого столу, щоб швидко виявляти проблеми і знаходити рішення за лічені хвилини.

Хмарна платформа. Безпечне хмарне з'єднання, яке дає віддалений доступ до будь-якого пристрою.

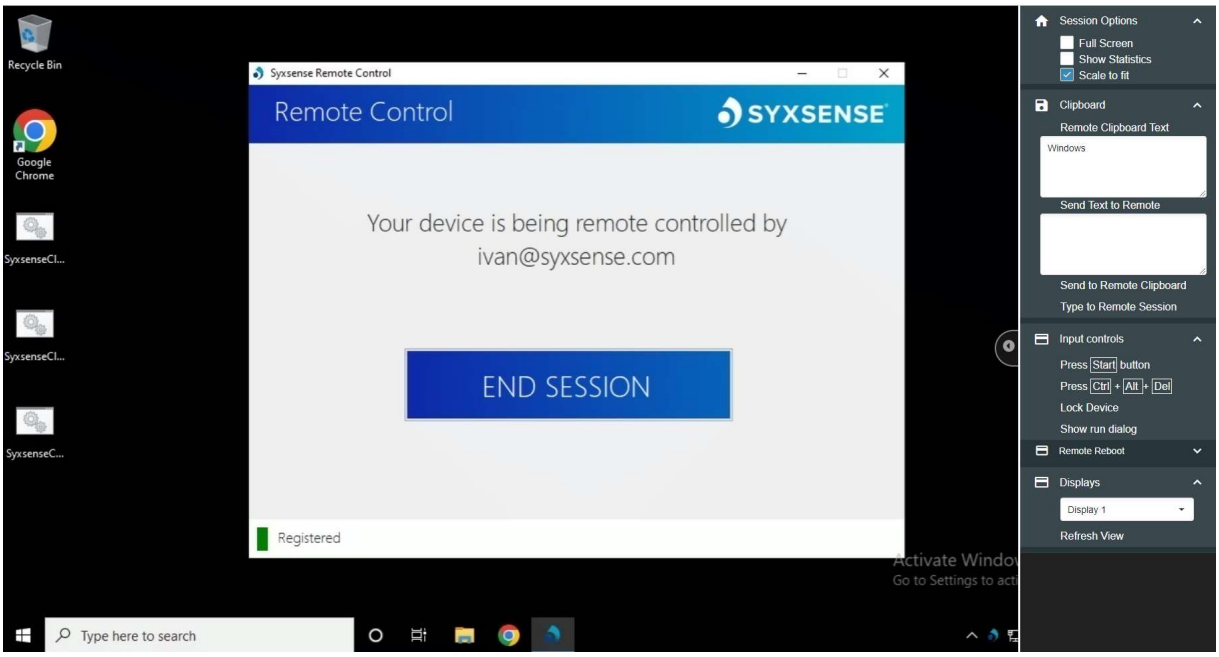


Рис. 2.5. Інтерфейс віддаленого доступу до комп’ютера

Керування через браузер

Усунення несправностей з будь-якої точки світу або просто з іншого офісу. Можливість використовувати будь-який веб-браузер на будь-якому пристрої з підключенням до Інтернету, щоб отримати доступ до пристрою користувача і надати віддалену допомогу. Надати своїм IT-адміністраторам більше часу в робочому дні для швидкого та ефективного вирішення проблем і підтримання продуктивності організації.

Інтеграція інструментів

Консолідація власних інструментів і розширення робочого середовища за допомогою додаткових інтеграцій віддаленого управління і підтримки. Syxsense пропонує інтеграцію з TeamViewer, щоб дає можливість скористатися додатковими функціями, які дозволять запропонувати найвищий рівень підтримки користувачів прямо з консолі Syxsense.

Двостороння передача

Багато інцидентів, пов'язаних з підтримкою, вимагають передачі файлів між пристроями. За допомогою Syxsense є можливість надавати спільний доступ до екрану або просто передавати файли і сценарії через з'єднання, усуваючи зайві

кроки через інші програми або служби обміну файлами. Передача працює в обох напрямках, а безпечне з'єднання захищає ваші файли від зовнішніх загроз, тому можливо вирішувати проблеми швидко і безпечно.

2.3 Основні функції та принципи роботи модуля Syxsense Secure

Cortex Workflows

Інтелектуальні кінцеві точки. Cortex передає дані про зміни поведінки і стану кінцевих точок в режимі реального часу, 24/7.

Використовування автоматизаці. Створення робочих циклів, які пов'язують процеси від початку до кінця, від виявлення загрози до її усунення.

Реагування в один клік. Повний доступ до великої бібліотеки готових робочих процесів для усунення загрози.

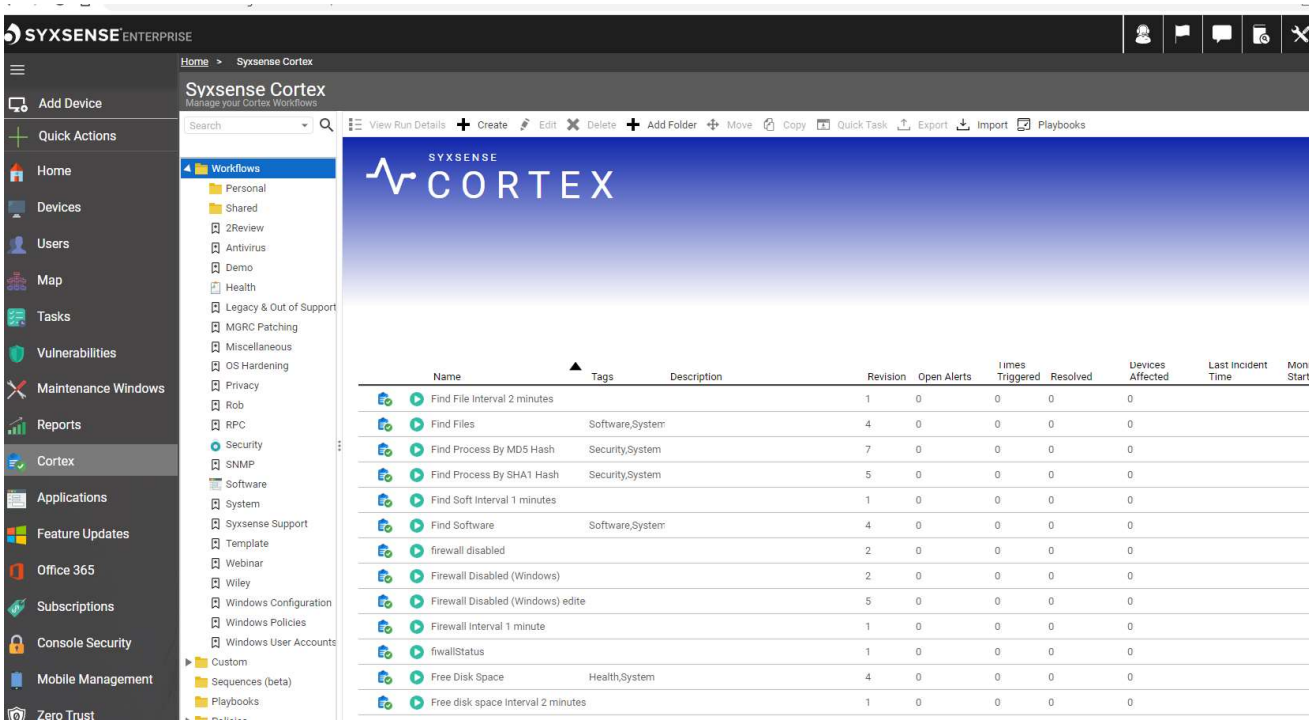


Рис. 2.6. Список робочих процесів Cortex

Гіперчутливі рецептори

Відлік часу до порушення безпеки починається в той момент, коли загроза потрапляє в мережу, тому кожна секунда на рахунку. Точні датчики виявлення

контролюють кінцеві точки 24/7, повідомляють про будь-яку незвичайну активність на консоль Syxsense в режимі реального часу і миттєво виконують засоби захисту при виявленні змін. Cortex забезпечує душевний спокій завдяки швидкому виявленню, втручанню та усуненню загроз безпеці.

Бібліотека робочих процесів

Syxsense зберегли та поділилися критично важливими робочими процесами усунення вразливостей, щоб користувачі могли усунути загрози одним клацанням миші. Не потрібно постійно шукати оновлення або створювати робочі процеси в міру виявлення нових вразливостей - постійне поповнення бібліотеки, щоб вона завжди була актуальною.

Візуальний конструктор робочих процесів

Створення власних робочих процесів Cortex без написання жодного сценарію. Потужний інтерфейс, що не містить коду, надає конструктор процесів за допомогою перетягування для кожної виявленої зміни, втручання та реакції. Користувач може контролювати і управляти своїми пристроями за допомогою спеціальних багатокрокових послідовностей завдань, які захищають від загроз і реагують на них швидше і ефективніше.

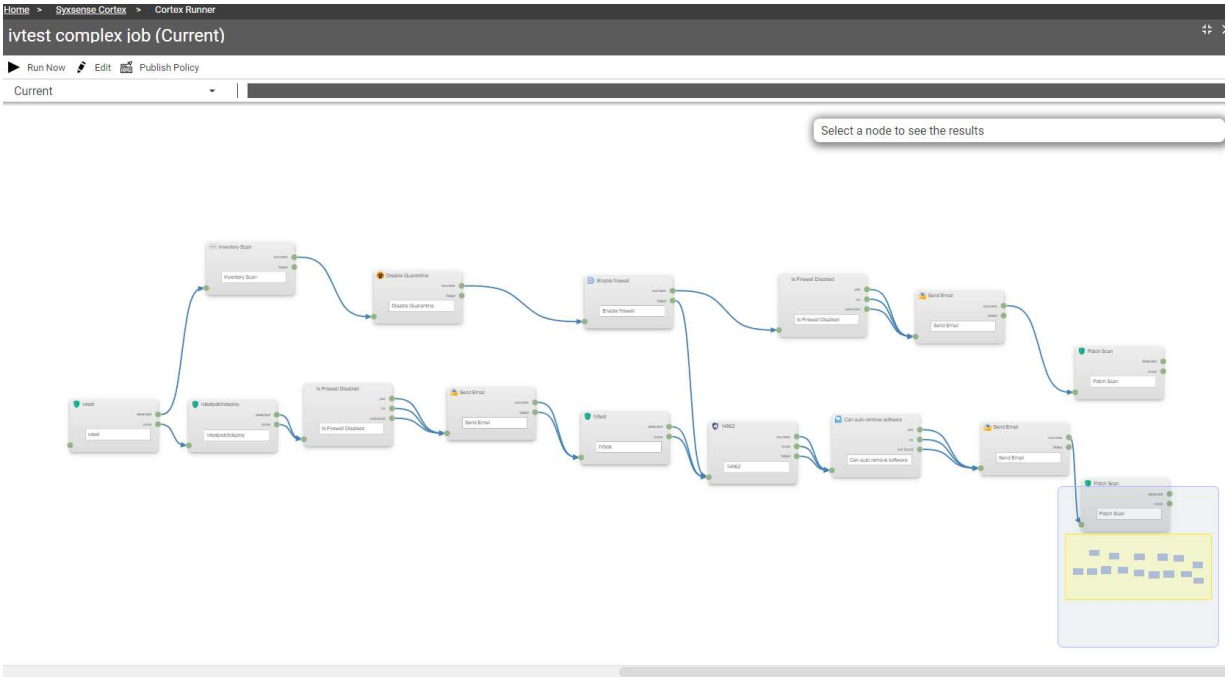


Рис. 2.7. Інтерфейс створення робочого процесу Cortex

СКАНЕР БЕЗПЕКИ

Виявляйє критичні загрози на ранній стадії

Виявляє вразливості. Знаходить слабкі місця та проблеми з неправильною конфігурацією, які піддають конфіденційні дані ризику крадіжки або зміни.

Зниження ризиків. Віднолення контролю за дотриманням вимог безпеки на кожному окремому пристрої, який співробітники організації використовують для роботи.

Покращення виявлення загроз. Виявлення не лише вразливості в ОС і сторонніх програмах. Сканування конфігурації безпеки, такі як відкриті порти, стан антивірусу, відключені брандмауери тощо.

База даних вразливостей

Велика бібліотека вразливостей класифікується по сімействам безпеки і включає в себе ступінь серйозності кожної загрози. Всеосяжний каталог можна легко відфільтрувати для пошуку конкретних типів вразливостей без необхідності сканувати все підряд. Сімейства скриптів безпеки включають: антивірус, криптомайнінг, FTP, брандмауери, сканування портів, VPN, соціальні мережі та багато іншого.

Сповіщення про загрози

Ключем до запобігання кібератак є швидке виявлення та усунення вразливостей безпеки. Syxsense сповіщає вас про загрози в режимі реального часу і негайно поміщає пристрої на карантин, ізолюючи їх від решти вашої мережі. Це зупиняє поширення будь-яких шкідливих процесів, щоб у вас був час усунути загрози, не даючи зловмисникам скористатися вразливістю під час вашої роботи.

Відповідність

Захищання конфіденційних дані. Переконання, що дані клієнтів і компанії отримуються, зберігаються, поширюються та захищаються відповідно до нормативних вимог.

Підтвердження відповідності. Створення звітів про відповідність для аудитів регуляторних органів, оскільки стандарти змінюються і розвиваються.

Уникнення інцидентів. Запобігання фінансовим санкціям, втраті репутації та

клієнтів, а також дорогим судовим позовам за допомогою автоматизованих процесів та звітності.

Стратегія Відповідності

Оскільки стандарти та нормативні акти постійно змінюються та розвиваються для кращого захисту персональних даних, вкрай важливо мати інтегровану та автоматизовану стратегію отримання та захисту даних. Користувач може легко підтримувати державні та регуляторні вимоги щодо захисту конфіденційних даних і створювати заздалегідь підготовлені звіти для аудиторів як доказ дотримання вимог.

Галузеві нормативні акти

Підприємства в таких галузях, як охорона здоров'я, фінансові послуги, роздрібна торгівля та готельний бізнес, серед інших, часто мають більш суворі регуляторні вимоги щодо захисту конфіденційних даних, а також більш високі штрафи і покарання в разі їх недотримання. Syxsense захищає дані за допомогою автоматизованих політик для захисту особистої інформації та генерує звіти про відповідність нормативним стандартам, таким як HIPAA.

Zero Trust

Довіра без кінцевої точки

Контроль. Припустити, що в мережі є зловмисники.

Перевірити. Перевірити стан безпеки користувачів і пристроїв.

Підтвердити. Переоцінка довіри при кожній спробі входу і доступу.

Підхід нульової довіри

Зі збільшенням кількості інцидентів, пов'язаних з безпекою, все більше організацій впроваджують концепцію нульової довіри до кібербезпеки для захисту своїх активів від зловмисників. Наш підхід до нульової довіри базується на мантрі "припускай порушення, ніколи не довіряй, завжди перевіряй" для захисту кожного окремого активу - користувача, програми та пристрою - шляхом інтеграції їх у комплексну стратегію та постійної перевірки для підтвердження довіри.

Стан безпеки

Стан безпеки кінцевих точок складається з багатьох важливих факторів, які

визначають працездатність пристрою, таких як необхідні виправлення для ОС і сторонніх розробників, конфігурації безпеки і програми для шифрування, такі як Bitlocker. Syxsense надає повну інформацію про стан кожної кінцевої точки, що взаємодіє з мережею, щоб ви могли постійно виявляти, контролювати та керувати станом безпеки кожного пристрою, поміщати в карантин пристрої, які не відповідають стандартам безпеки, і автоматично виправляти пристрої з відкритими вразливостями.

Забезпечення оцінки довіри

Syxsense Cortex надає командам можливість створювати складні політики доступу і робочі процеси виправлення для забезпечення відповідності Zero Trust Network Access (ZTNA). Syxsense аутентифікує користувача і пристрій при кожній спробі входу в систему і доступу по активу, щоб встановити ідентичність, стан здоров'я і статус відповідності за допомогою системи аутентифікації Syxsense або за допомогою виклику API до інструменту багатофакторної аутентифікації, такого як Duo, а також автоматично блокує і застосовує виправлення для невідповідних кінцевих точок.

Динамічні запити

Запити надають більший контроль над організацією інвентаризації та застосуванням виправлень. Можливість розставляти пріоритети для груп пристроїв і виправлень на основі умов, які ви адаптуєте до конкретних потреб вашої організації на основі серйозності і ризику, конфігурацій системи і постраждалих процесів або критично важливих систем, які можуть бути найбільш пошкоджені в результаті атаки. За допомогою Syxsense користувач може динамічно запитувати і націлювати своє середовище за допомогою безпечних і ефективних розгортань для захисту кінцевих точок.

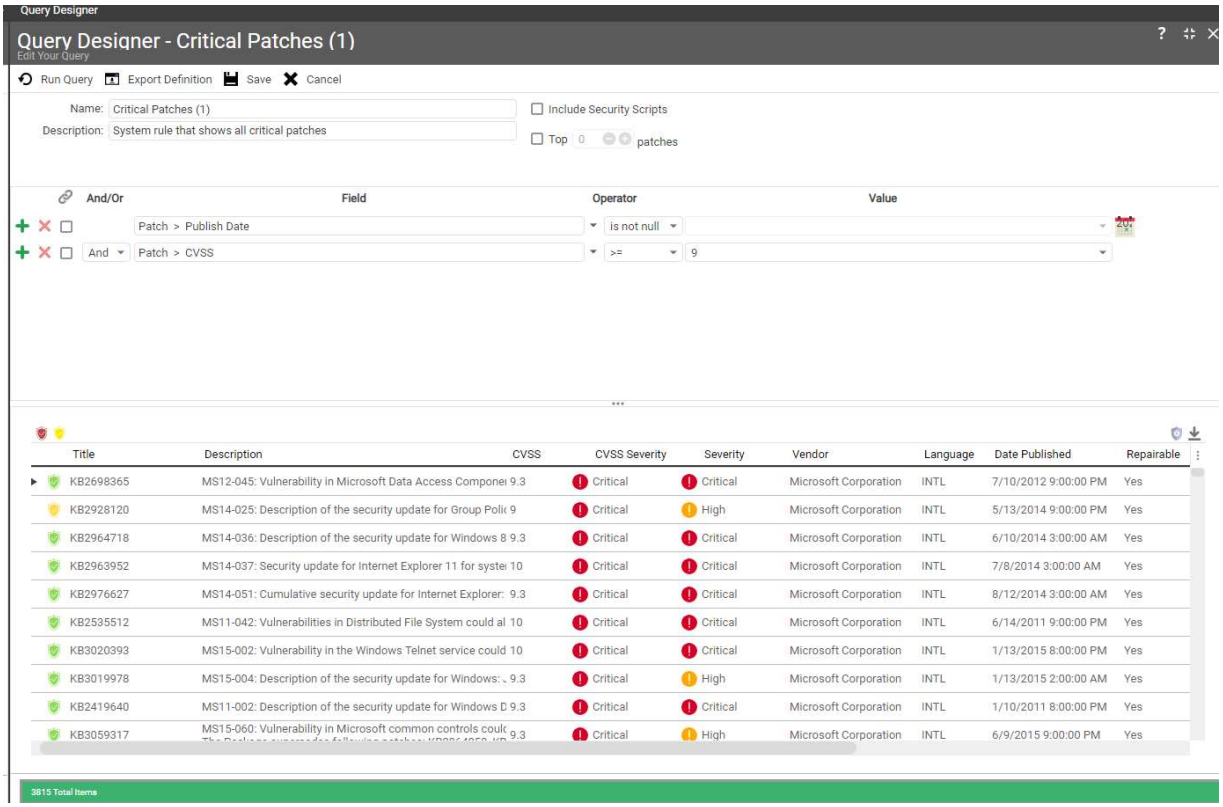


Рис. 2.8. Приклад запиту для пошуку виключно критичних патчів

Завдання та політики

Отримання даних в режимі реального часу про стан кожного пристрою у середовищі під час сканування і розгортання за допомогою запланованих завдань і запущених політик. Політики роблять кінцеві точки по-справжньому інтелектуальними, самостійно відстежуючи зміни поведінки і стану, навіть коли пристрій знаходиться в автономному режимі, і негайно передаючи результати на вашу консоль Syxsense, коли вони з'являються в мережі, усуваючи час між скануванням і запуском завдань по усуненню.

Карантин

Захист своїх кінцевих точок і середовища від виявлених загроз, помістивши пристрої на карантин від решти мережі. Коли консоль Syxsense отримує інформацію про невідому або незвичайну активність, пристрій відключається від зв'язку з корпоративними даними і ресурсами. Період ізоляції дає час для виправлення ситуації, не залишаючи критичні системи вразливими до атаки.

Вікна обслуговування і відключення

Використовувати вікна "Обслуговування" і "Відключення", щоб вказати час, коли зміни повинні і не повинні бути заплановані для управління розгортаннями і захисту пристроїв в критичні робочі години. Syxsense надає опції для глобального відключення, відключення на рівні завдань і відключення на рівні пристроїв. Планування Active Patch Tuesday також доступно для поетапних розгортань з повторюваними вікнами щодо другого вівторка, що полегшує автоматичне розгортання нового контенту.

Керування, налаштування та захист мобільних пристрої

Можливість працювати будь-де. Безпечно дозволяти співробітникам працювати з ресурсами компанії з будь-якого пристрою, включаючи їх власні.

Віддалений захист. Блокуйте, скидайте і очищайте мобільні пристрої з консолі Syxsense незалежно від їх місцезнаходження.

iOS і Android. Підтримка управління мобільними пристроями для iPhone, iPad і Android пристроїв.

Керування програмами телефону

Безшумно встановлення програми та оновлення версій на зареєстровані пристрої у вашій мережі без втручання користувача. Додатки можна вносити до білого, чорного списків або видаляти з пристроїв віддалено з консолі, а також встановлювати обмеження на завантаження, які обмежують доступ користувачів до встановлення додатків.

Мобільна безпека

Користувач не завжди може проконтролювати, чи потрапить пристрій в чужі руки, але є можливість забезпечити дотримання стандартів безпеки на випадок, якщо це станеться. За допомогою MDM в Syxsense користувач встановлює вимоги, яким повинні відповідати користувачі щодо типу і складності паролів і PIN-кодів на пристроях, які взаємодіють з мережею. У разі втрати або крадіжки пристроїв, є можливість заблокувати, скинути і стерти будь-які пристрої віддалено з консолі Syxsense.

Контейнеризація даних

Захист данних компанії за межами екрану блокування. Ізолювання та захист

корпоративних данних на пристроях BYOD і пристроях компанії за допомогою окремих профілів безпеки. Це захищена зона з високим рівнем безпеки, де доступ до даних компанії обмежений, з обмеженою видимістю та додатковим рівнем захищених облікових даних.

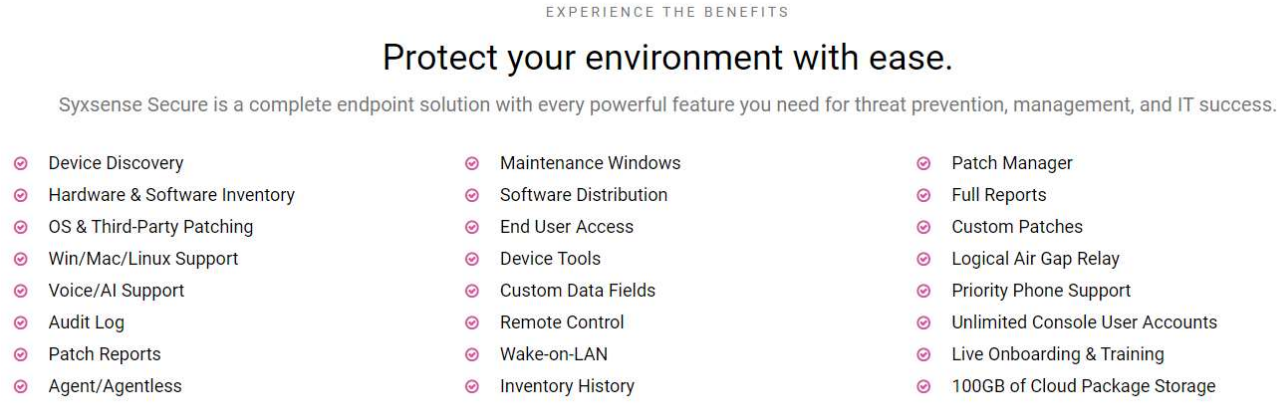


Рис. 2.9. Повний перелік рішень Syxsense Secure який дозволяє забезпечувати захист кінцевих точок

Висновки до розділу

Досліджено призначення та можливості продукту SEP, переваги його використання, а також його підходи до забезпечення захисту на встановленому кінцевому пристрої.

3 РОЗРОБЛЕННЯ ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК НА БАЗІ РІШЕННЯ SYXSENSE ENDPOINT SECURITY

3.1. Порядок розгортання рішення AWS IAM

В даному розділі розглянемо на практиці використання даного програмного комплексу, а також розглянемо принцип роботи *Syxsense Endpoint Security* для платформи Windows OS.

Спочатку, для отримання безкоштовної trial-версії нам необхідно зайти на сайт Syxsense та пройти реєстрацію:

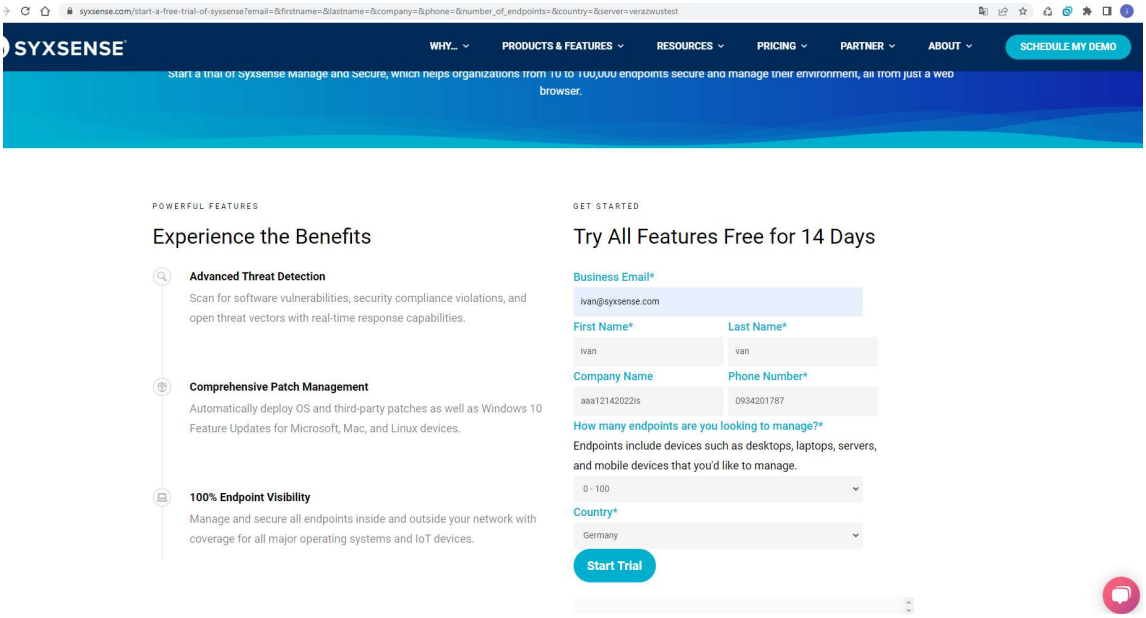


Рис. 3.1 Процес реєстрації на сайті Syxsense

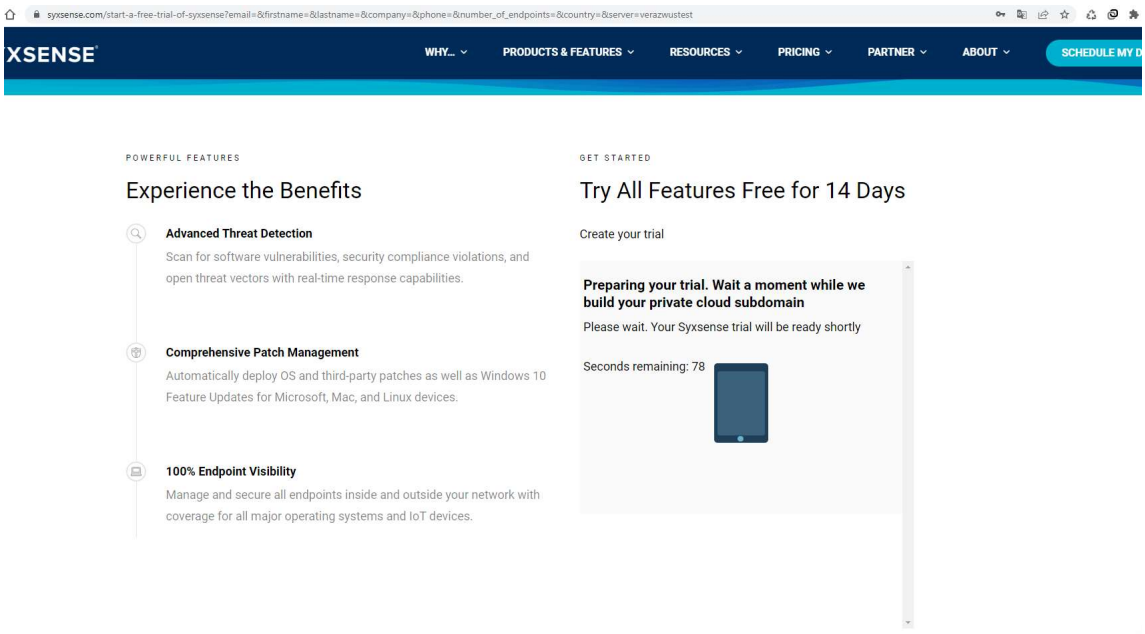


Рис. 3.2. Процес створення сайту консолі

Одним із мінусів було помічено, що у списку країн відсутня Україна, тому треба обирати альтернативу.

Далі після реєстрації на вказану електронну пошту надходить лист з підтвердженням реєстрації:

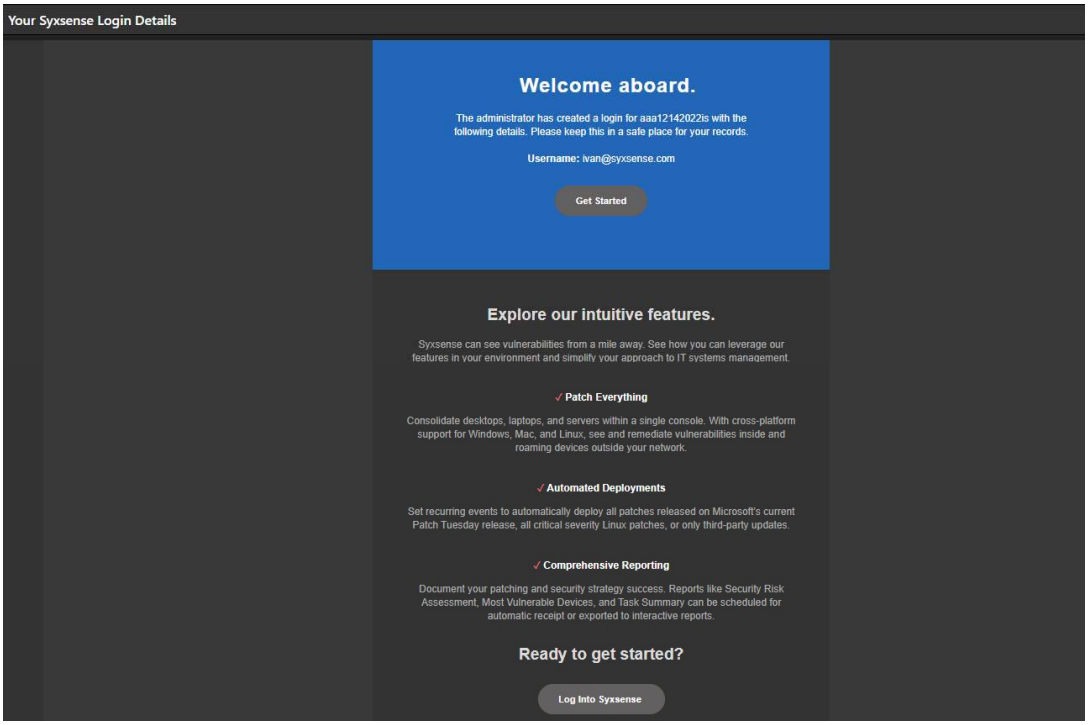


Рис. 3.3. Лист з поштової скриньки в якому міститься посилання на сайт де потрібно скачати агент

Після переходу за посиланням відкривається сторінка сайту, на якій потрібно вибрати операційну систему для якої буде потрібно встановити агент.

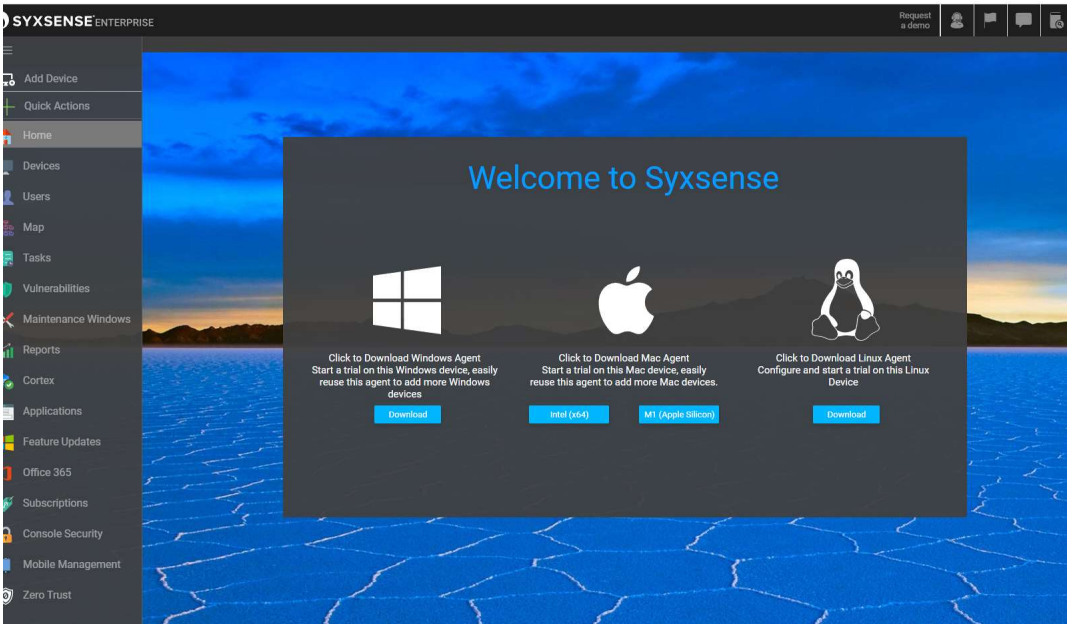
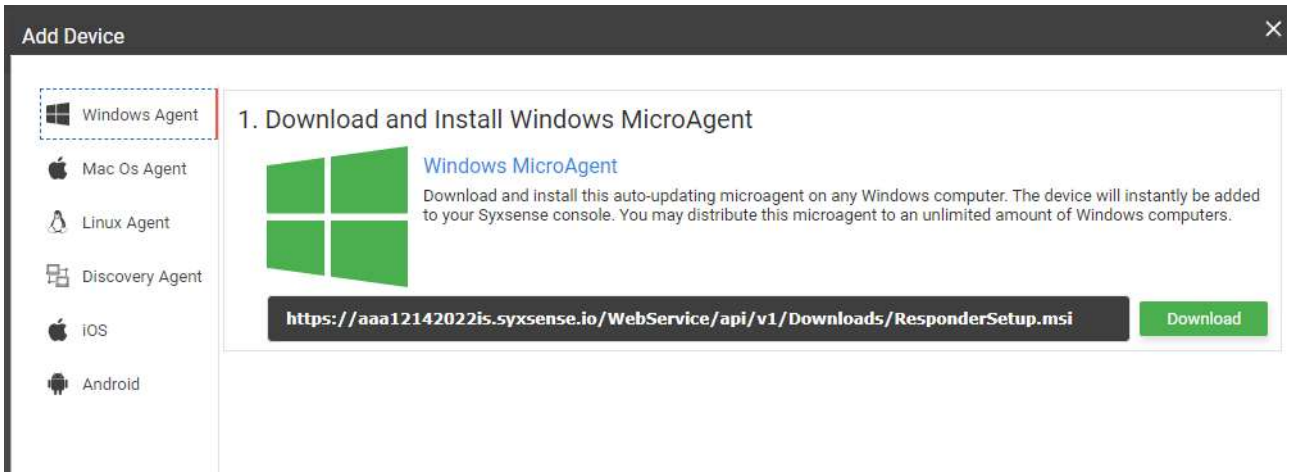
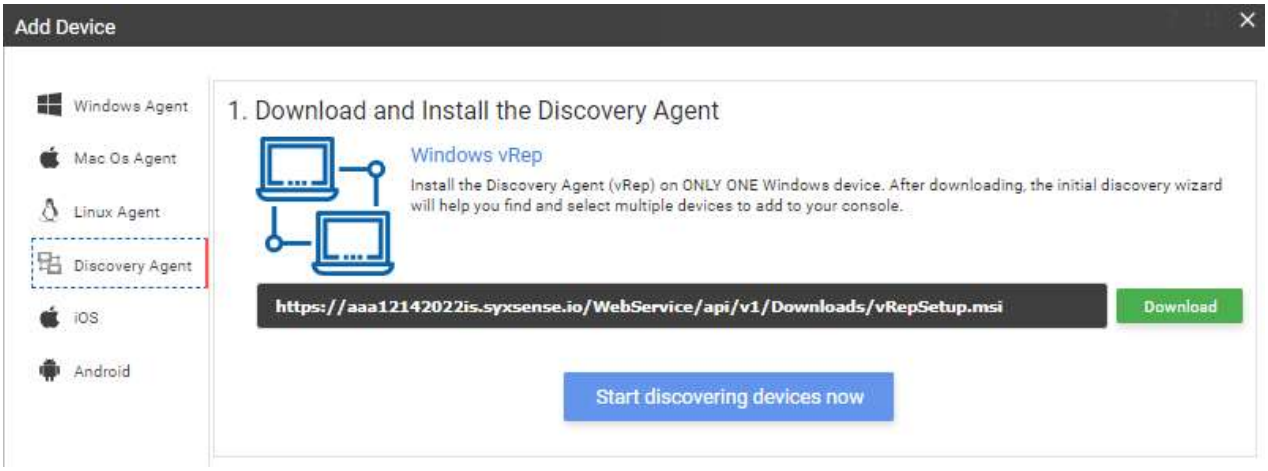
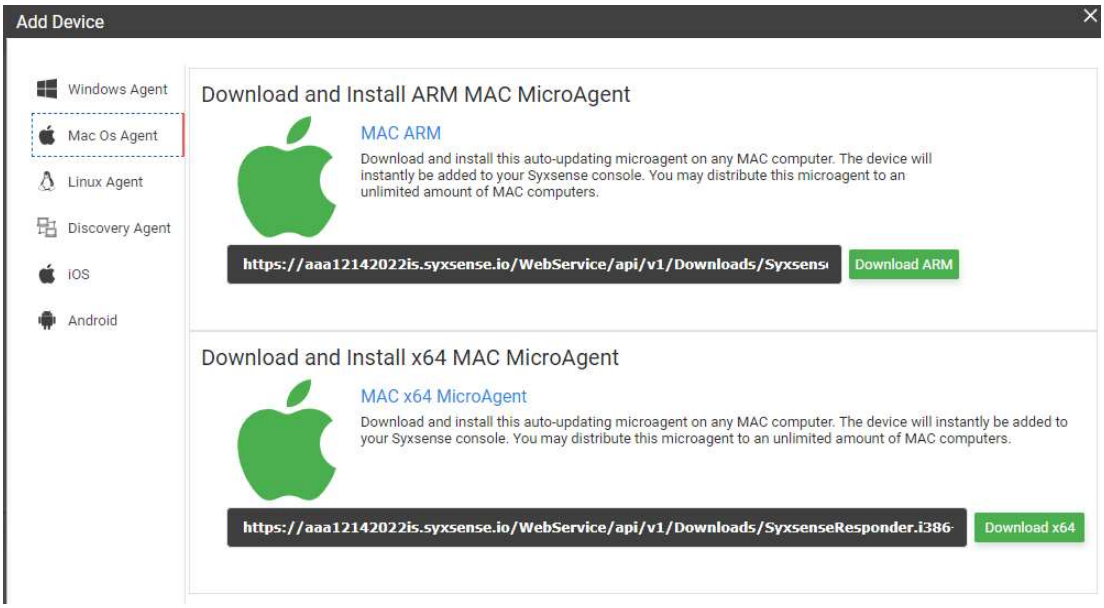
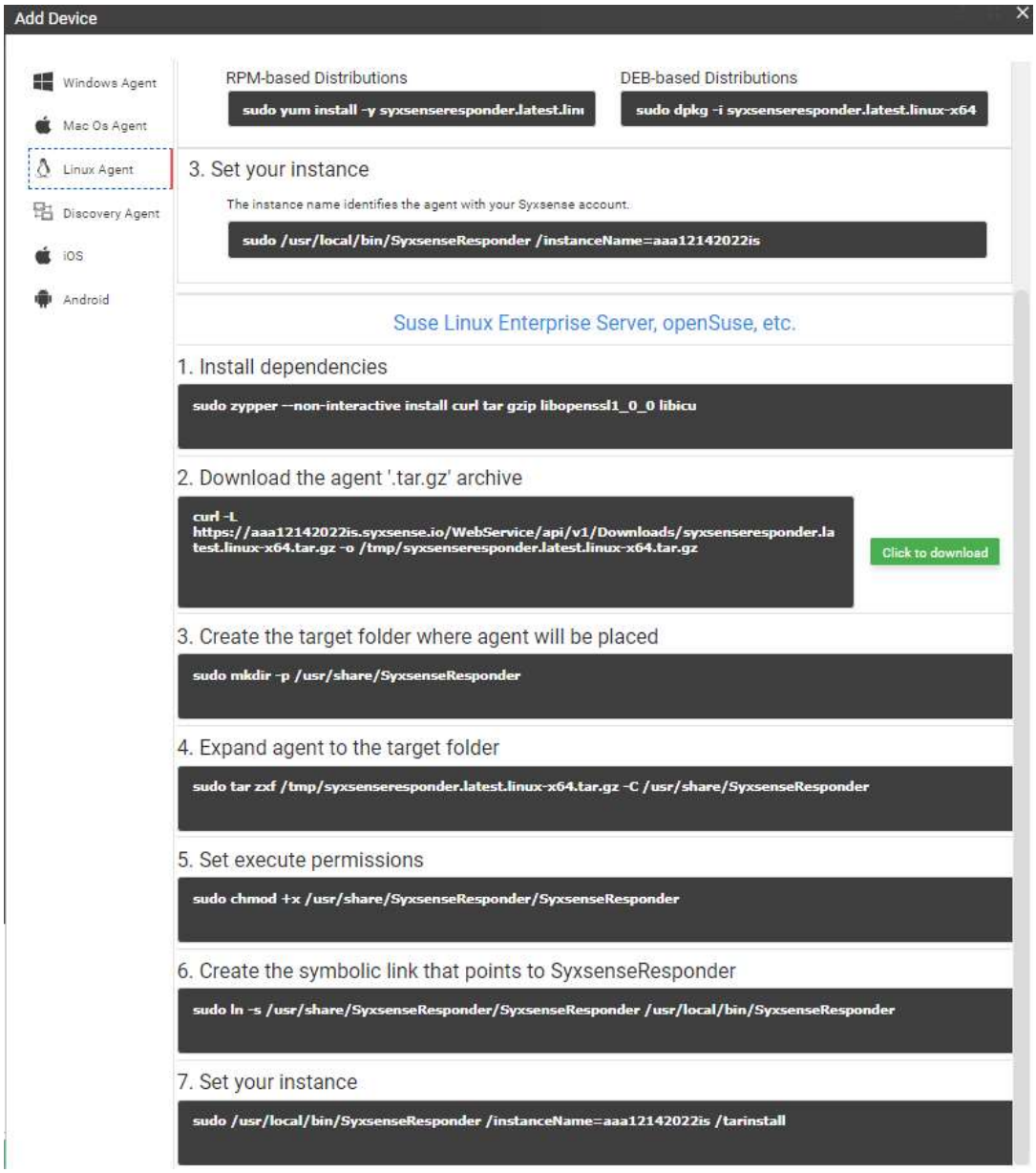


Рис. 3.4. Сторінка вибору операційної системи при перцій взаємодії користувача с сайтом






Add Device
Windows Agent
Mac Os Agent
Linux Agent
Discovery Agent
iOS
Android
Download and Install ARM MAC MicroAgent
MAC ARM
Download and install this auto-updating microagent on any MAC computer. The device will instantly be added to your Syxsense console. You may distribute this microagent to an unlimited amount of MAC computers.
https://aaa12142022is.syxsense.io/WebService/api/v1/Downloads/Syxsens
Download ARM
Download and Install x64 MAC MicroAgent
MAC x64 MicroAgent
Download and install this auto-updating microagent on any MAC computer. The device will instantly be added to your Syxsense console. You may distribute this microagent to an unlimited amount of MAC computers.
https://aaa12142022is.syxsense.io/WebService/api/v1/Downloads/SyxsenseResponder.i386
Download x64


Add Device
Windows Agent
Mac Os Agent
Linux Agent
Discovery Agent
iOS
Android
RPM-based Distributions
sudo yum install -y syxsenseresponder.latest.lin
DEB-based Distributions
sudo dpkg -i syxsenseresponder.latest.linux-x64
3. Set your instance
The instance name identifies the agent with your Syxsense account.
sudo /usr/local/bin/SyxsenseResponder /instanceName=aaa12142022is
Suse Linux Enterprise Server, openSuse, etc.
1. Install dependencies
sudo zypper --non-interactive install curl tar gzip libopenssl1_0_0 libicu
2. Download the agent '.tar.gz' archive
curl -L https://aaa12142022is.syxsense.io/WebService/api/v1/Downloads/syxsenseresponder.latest.linux-x64.tar.gz -o /tmp/syxsenseresponder.latest.linux-x64.tar.gz
Click to download
3. Create the target folder where agent will be placed
sudo mkdir -p /usr/share/SyxsenseResponder
4. Expand agent to the target folder
sudo tar zxf /tmp/syxsenseresponder.latest.linux-x64.tar.gz -C /usr/share/SyxsenseResponder
5. Set execute permissions
sudo chmod +x /usr/share/SyxsenseResponder/SyxsenseResponder
6. Create the symbolic link that points to SyxsenseResponder
sudo ln -s /usr/share/SyxsenseResponder/SyxsenseResponder /usr/local/bin/SyxsenseResponder
7. Set your instance
sudo /usr/local/bin/SyxsenseResponder /instanceName=aaa12142022is /tarinstall

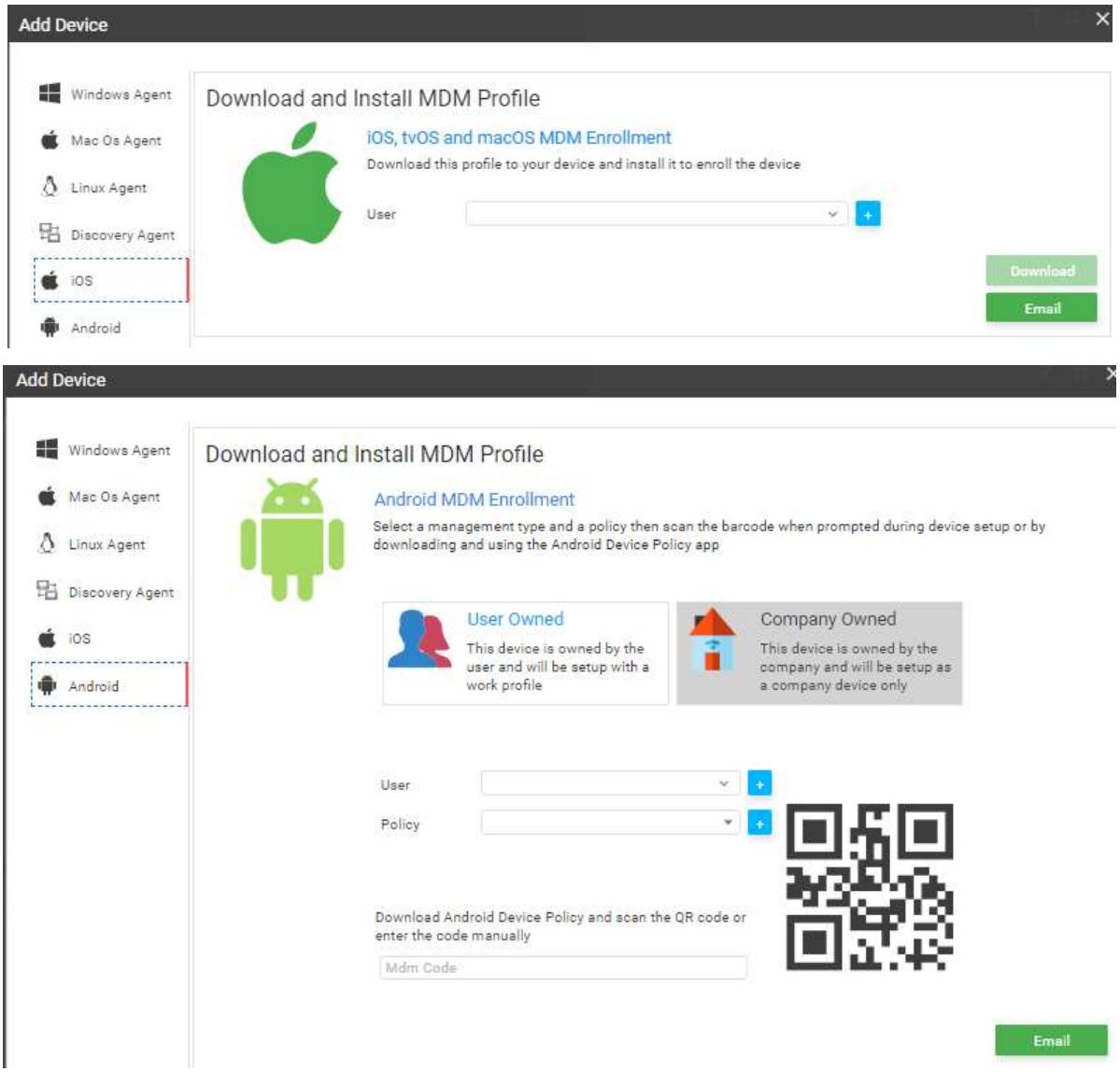


Рис 3.5, 3.6, 3.7, 3.8, 3.9, 3.10 Сторінки для завантаження агентів для різних кінцевих точок

Коли агент завантажиться, то пристрій з’явиться на сайті створеному для компанії у вкладці Devices.

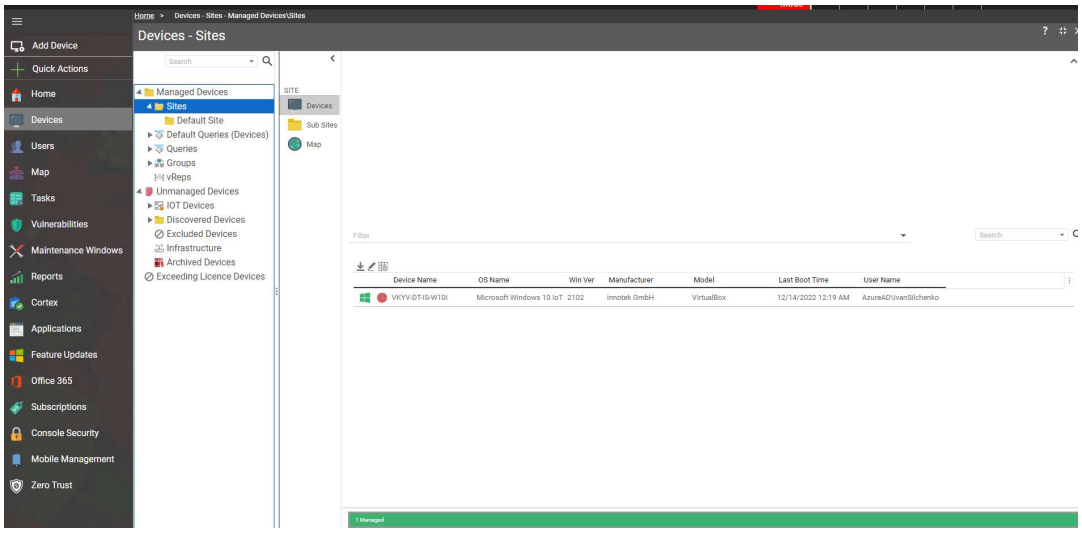


Рис. 3.11. Вкладка Devices відображає пристрої які використовую компанія

Сайти - це діапазони IP-адрес, в межах яких здійснюється пошук пристроїв в процесі виявлення та впровадження. При створенні двох сайтів з діапазонами IP-адрес, що перетинаються, пристрої, що знаходяться в межах перетину, будуть додані в перший сайт, який знаходиться вище на вкладці.

Якщо користувач бажає підключити до мережі конкретні пристрої з відомою IP-адресою, є можливість вказати не діапазон IP-адрес, а одну IP-адресу у відповідному полі.

Перелік усіх сайтів і пристроїв, які належать до цих діапазонів IP-адрес, можно переглянути в розділі "Глобальний перегляд сайтів". Якщо не вказаний конкретний діапазон IP-адрес, можно переглянути всі пристрої, що входять до нього, в папці "Сайт за замовчуванням".

На сторінці "Детальний огляд пристрою" можно переглянути візуалізацію стану "Здоров'я комп'ютера" з повною розбивкою, стану "Безпека комп'ютера", "Поточна активність", а також "Інформація про систему".

Інструменти пристрою дозволяють виконувати різні операції з пристроями, такі як перевірка їх інвентаризації або історії інвентаризації, а також відправка заражених пристроїв на карантин. У цьому розділі можно знайти всю інформацію про загальні відомості про пристрої, інвентаризацію пристроїв і способи її використання для ваших цілей, а також різні інструменти для роботи з пристроями,

які полегшать вашу роботу з пристроями і посилять контроль над ними.

Windows Discovery Agent дає можливість встановити агент на комп'ютери які знаходяться у локальній мережі використовуючи задачу Discovery. Вказуючи IP-адреси пристроїв та дані локального користувача, встановити агент Syxsense Micro agent, зручність полягає у тому що не потрібно інсталювати програму на кожен пристрій але працює ця функція тільки для операційної системи Windows.

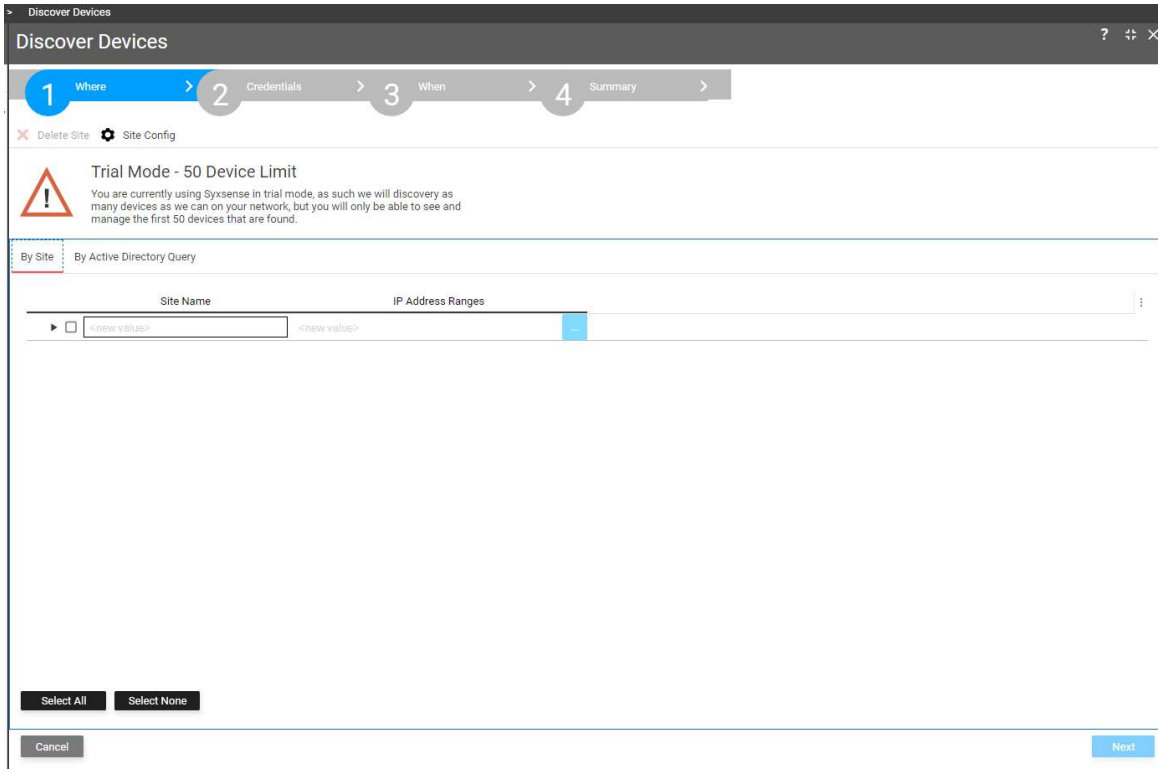


Рис. 3.12. Інтерфейс для створення задачі Discovery

Облікові записи користувачів - це те, що колеги використовують для входу в консоль Syxsense. Рекомендується захистити всі облікові записи користувачів двофакторною автентифікацією, а також увімкнути інші глобальні та індивідуальні налаштування безпеки для забезпечення найвищого рівня захисту.

При створенні нових облікових записів користувачів найкраще відразу призначати їм контекст безпеки.

Контекст безпеки - це унікальна комбінація з 1 Ролі (що можна робити) і 1 Області (до яких пристроїв є доступ). Будь-який користувач може мати кілька контекстів безпеки і перемикатися між різними поданнями (або клієнтами для MSP) у верхньому правому куті консолі. Не потрібно входити і виходити з

системи.

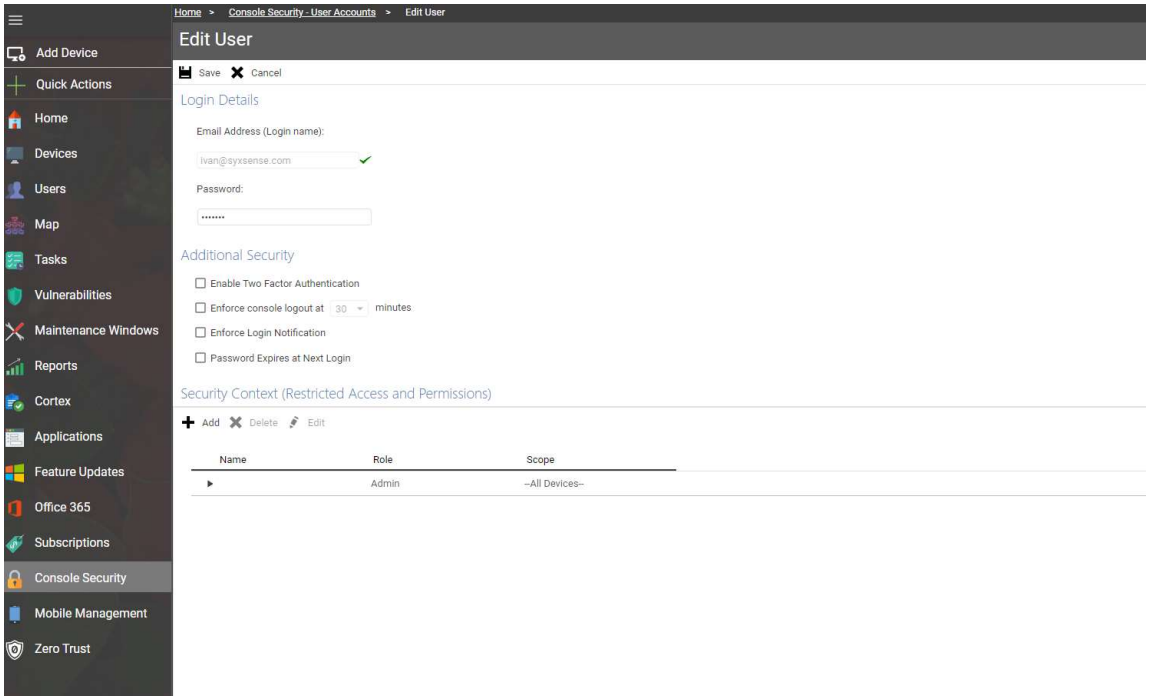


Рис. 3.13. Інтерфейс Console Security

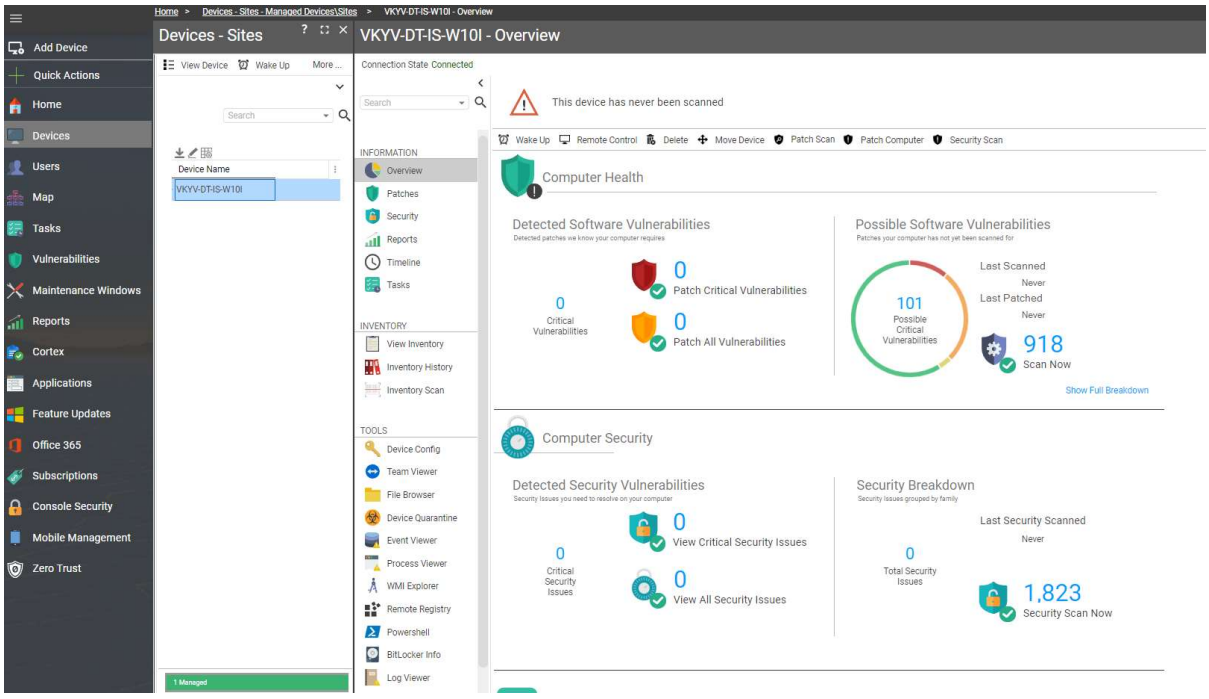


Рис. 3.14. Інтерфейс панелі інструментів пристрою

Панель інструментів

Ці кнопки дозволяють виконувати певні операції на вибраному пристрої.

Переглянути пристрій - Дозволяє заглибитися в деталі пристрою.

Пробудження - надсилання магічного пакету для пробудження пристрою з вимкненого стану. Ця функція вимагає увімкнення Wake-On-Lan в BIOS.

Дистанційне керування - ініціює сеанс дистанційного керування пристроєм за допомогою HTML5 у новій вкладці браузера.

Диспетчер виправлень - Запуск майстра виправлень, де ви можете вибрати, які оновлення розгорнути на пристрої. Перегляд відомостей про виправлення. Перевірте вразливості для отримання інформації про патч.

Видалити/Архівувати - Видаляє пристрій з бази даних або архівує його.

Перемістити пристрій(и) - Дозволяє перемістити пристрій між групами сайтів.

Інвентаризація - Запуск сканування для збору останньої інформації про апаратне та програмне забезпечення.

Видалити агента - Видалення агента з пристрою (доступно тільки для пристрою, підключеного до Інтернету).

Створити групу - створення групи пристроїв.

Створити звіти - створення звітів, що групують різні показники.

Інформація

Огляд - повернення до екрана за замовчуванням.

Стан пристрою (патчі) - Перелік доступних патчів для всіх виявлених вразливостей та історія патчів.

Безпека - Перелік виявлених вразливостей відповідно до завдання сканування безпеки. Ця функція доступна лише для ліцензії Secure.

Звіти - відображає всі звіти. Звіти будуть відфільтровані тільки для цього пристрою.

Часова шкала - Відображає життєвий цикл пристрою. Ця функція доступна лише для ліцензії Secure.

Завдання - Відображає список усіх поточних завдань, які виконує пристрій.

Інвентар

Перегляд інвентаризації - відображення інформації про апаратне та програмне забезпечення з останнього сканування інвентаризації.

Історія інвентаризації - перегляд змін на пристрої між двома різними точками архівування.

Сканування інвентаризації - Запустити сканування для збору найновішої інформації про апаратне та програмне забезпечення.

Інструменти

Примітка: Список доступних інструментів може відрізнятися в залежності від операційної системи пристрою.

Конфігурація пристрою - Дозволяє налаштувати виключення, відбитки пальців пристрою, блокування сайту, дистанційне керування, доступ та години вимкнення.

Team Viewer - Ініціює сеанс дистанційного керування за допомогою програми TeamViewer.

Файловий браузер - досліджує всі локальні диски пристрою.

Карантин пристрою - дозволяє легко помістити пристрій на карантин простим клацанням миші. Ця функція доступна тільки для ліцензії Secure і відображається, тільки якщо пристрій підключено.

Пінг - Дозволяє виконати сканування портів або ICMP на пристрої. Ця функція відображається, тільки якщо пристрій не підключено.

Перегляд подій - пошук та експорт подій Windows, записаних на пристрої.

Перегляд процесів - подібно до диспетчера завдань, відображає всі запущені процеси та служби на пристрої.

Linux Scanner - інструмент автоматизації завдань за допомогою оболонки командного рядка.

WMI Explorer - передача на пристрій настроюються WMI-виписок для розширеного збору інвентаризації.

Віддалений реєстр - зберігає дані про дії, виконані ОС Windows, що служить основою для створення журналу подій.

PowerShell: Розширений. Віддалений термінал PowerShell з поверненням відповіді.

Log Viewer - Аудит активності служби Syxsense.

Після успішного завантаження агента на пристрій та додавання його до консолі, буде створені Patch Scan і Security Patch Scan задачі.

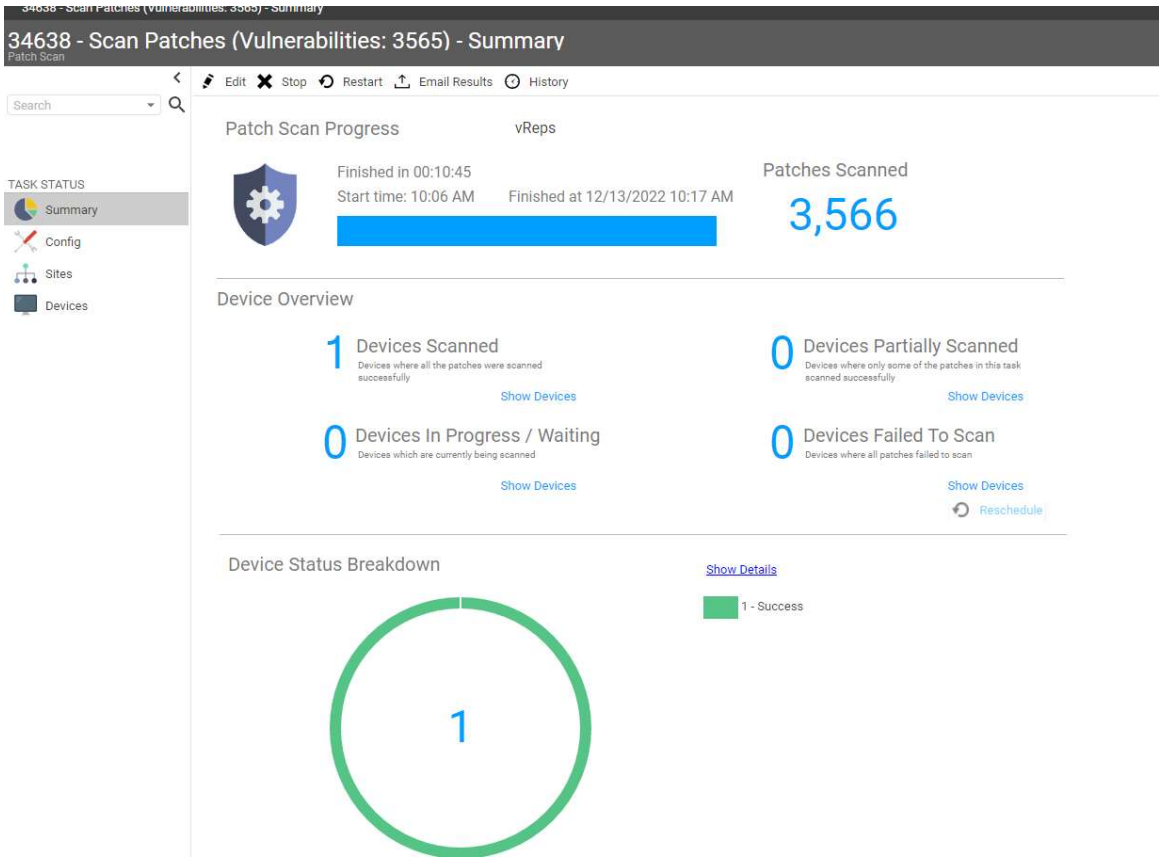


Рис 3.15. Успішно закінчена задача Patch Scan

Програмне забезпечення Syxsense сканує пристрої на предмет необхідності встановлення певних патчів як для операційних систем, так і для стороннього програмного забезпечення, а також перевіряє, чи є на пристроях застарілі або новіші патчі. Воно також оцінює стан пристрою на основі оцінки CVSS, пов'язаної з кожним відсутнім виправленням як для операційної системи, так і для сторонніх програм, щоб була можливість визначити пріоритетність встановлення виправлень відповідно до ризику, якому користувач піддається. Докладні відомості про патчі наведено в Короткому огляді патчів.

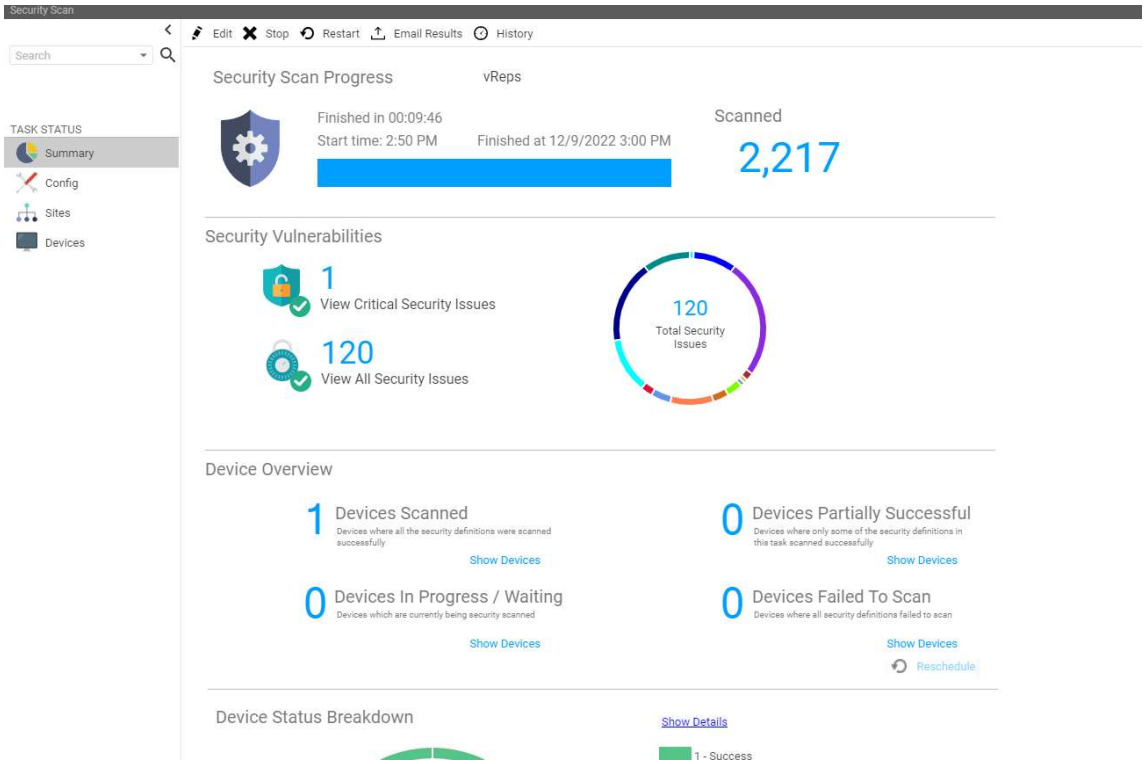


Рис. 3.16. Успішно закінчена задача Security Patch Scan

Security Scan - це потужний інструмент, доступний з ліцензіями Syxsense Secure & Enterprise, який дозволяє планувати регулярне або одноразове сканування вразливостей всіх пристроїв або певних пристроїв.

Ви можете сканувати всі можливі вразливості, створивши завдання Сканування в підрозділі Безпека на вкладці Вразливості або спроектувавши відповідний робочий процес Cortex.

За допомогою Syxsense Secure користувач також може виправити більшість недоліків безпеки відразу після їх виявлення без написання жодного рядка коду.

Після того, як сканування безпеки виявить деякі порушення безпеки, наприклад, небажане програмне забезпечення, включений автозапуск або відключений антивірус, користувач може автоматично виправити їх, використовуючи готові і перевірені робочі процеси вирішення в Syxsense Cortex. Для тих недоліків, які не можуть бути виправлені автоматично, користувач може знайти рекомендоване рішення, натиснувши посилання Переглянути деталі у вкладці зведення на сторінці конкретної вразливості.

Після скану пристрою були виявлені уразливості. В панелі інструментів у

вкладці девайси можно побачити виявлені патчі, які потрібно завантажити.

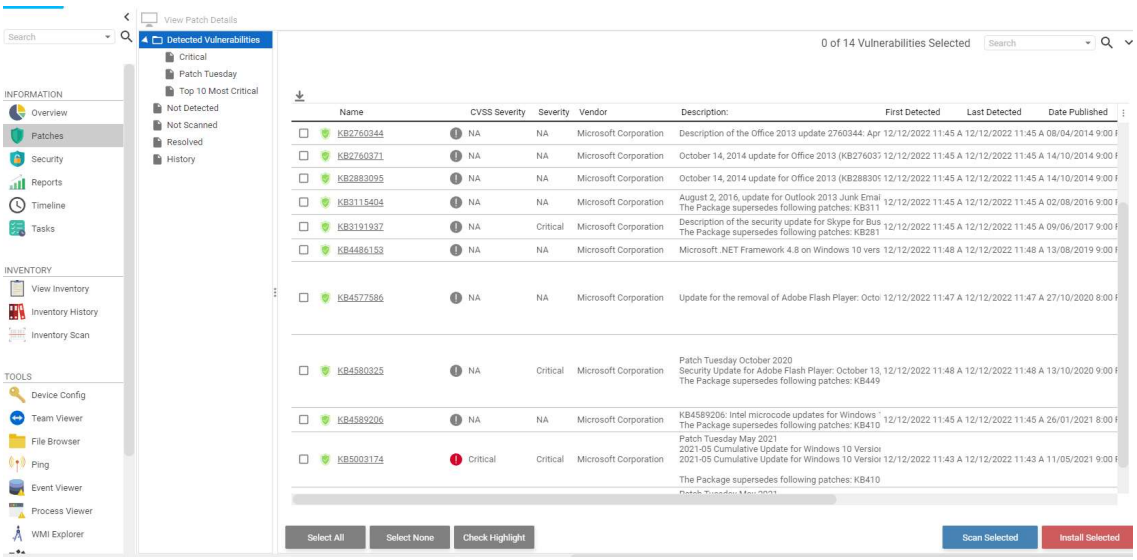


Рис. 3.17. Виявлені уразливості на пристрої після скану

У разі виявлення вразливостей, для забезпечення безпеки кінцевої точки потрібно створити Patch Deploy задачу та вказати виявлені патчі.

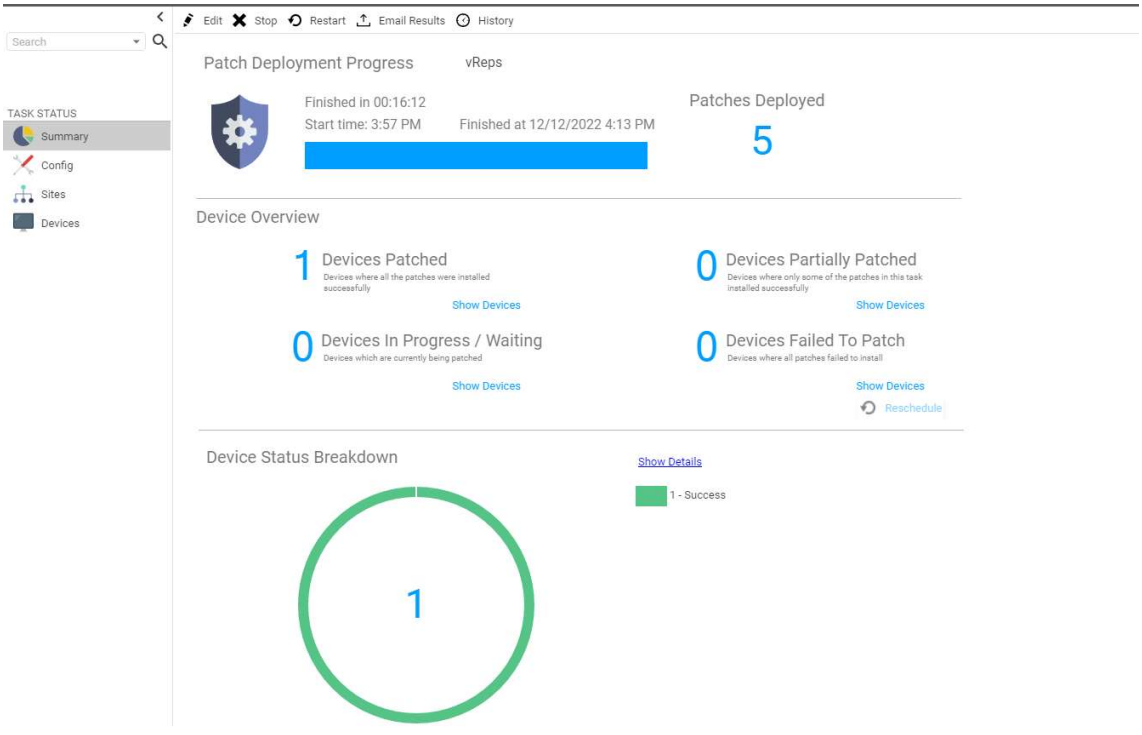


Рис. 3.18. Успішно закінчена задача Patch Deploy

Користувач може організувати виправлення через завдання і через політику. Якщо пристрій увімкнено і необхідно виправити кінцеві точки системи у вікні обслуговування, то необхідно створити завдання "Виправлення" (Patch). У разі

виправлення через політику, навіть якщо пристрій вимкнено, сервер періодично відправляє запити, поки не отримає відповідь від пристрою, після чого починається процес виправлення.

Програмне забезпечення Syxsense надає доступ до найсвіжішого і повного набору патчів, так як рішення має провідну в галузі бібліотеку патчів стороннього програмного забезпечення. Всі патчі проходять попереднє тестування, тому якщо певний патч має критичні помилки або несумісний з іншим програмним забезпеченням, він не буде присутній в консолі, а про більшість таких патчів ви побачите повідомлення. Це дозволяє уникнути відкату поганих патчів, тим самим допомагаючи більш раціонально розподіляти час ваших співробітників.

По закінченню процесу установки виправлень можна створювати різноманітні Звіти за результатами установки виправлень, які дозволяють як оцінити виконану роботу, виявити проблемні пристрої і недоставлені виправлення, так і порівняти зміну рівня захищеності системи в часі, а також спланувати подальші роботи.

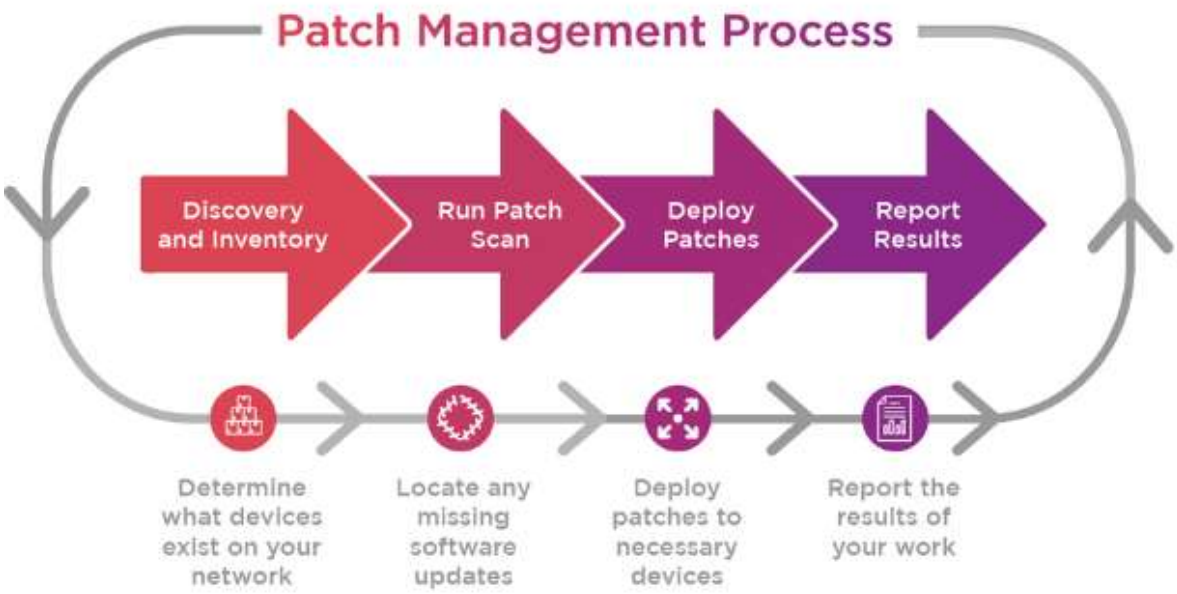


Рис. 3.19. Процес менеджменту патчів

Syxsense Cortex

Щоб вручну виконати всі процеси, необхідні для забезпечення безпеки корпоративної мережі, зазвичай витрачається багато часу. Якщо користувач

автоматизує процеси за допомогою написання скриптів, це займає менше часу, але все одно доведеться писати окремі фрагменти скриптів для всіх завдань.

Syxsense Cortex - це drag-and-drop інтерфейс для інтелектуальної автоматизації робочих процесів IT та безпеки зі складною логікою, який може заощадити вам купу часу.

Завдання - це одноразові запити сервера до пристрою, тому, якщо пристрій знаходиться в автономному режимі, ви можете організувати його у вигляді політики Cortex, щоб гарантувати виконання завдання. В цьому випадку сервер багаторазово пінгує пристрій до тих пір, поки не отримає позитивну відповідь. При отриманні доступу до пристрою на ньому створюється запланована задача і додається в чергу завдань.

Syxsense Cortex - це потужна та інтуїтивно зрозуміла система автоматизації, яка дозволяє створювати власні послідовності завдань в консолі Syxsense.

Обробка Syxsense Cortex використовує дані для запуску дій, включаючи інформацію про кінцеву точку, таку як стан вразливості, розташування в мережі, встановлення програмного забезпечення, запущені процеси та інше. Потім користувальницький інтерфейс перетягування впорядковує такі дії, як виправлення, розгортання програмного забезпечення, сканування безпеки і повне написання сценаріїв (PowerShell, C #, VB) в механізмі IT-процесів "Наступного покоління".

Вимоги до IT та безпеки в режимі 24x7 вимагають, щоб рішення надавалися різними способами і в різний час за запланованим і передбачуваним графіком, під постійним контролем або в непередбачуваному і терміновому порядку. Будь-який з цих варіантів може бути спрямований на необхідні пристрої за запитом, групою, сайтом або організаційною структурою за вибором користувача.

Послідовності Cortex дозволяють створити ланцюжок стандартних або налаштованих робочих процесів в одному завданні для конкретного пристрою.

Дії - це цеглинки, з яких користувач будує свої складні автоматизовані робочі процеси.

Додайти дію задачі до робочого процесу Cortex для виконання простих або

дуже складних функцій, і можливість запуску іншої дії задачі на основі поведінки попередніх дій. З одного кроку робочого процесу можна налаштувати кілька результатів, а також кілька дій, вишикуваних в один наступний крок.

Рис. 3.20. Перевірка, чи потрібне перезавантаження перед виконанням сканування патчів

При роботі с великою кількістю пристроїв клієнтам компаніям зручно мати звіт щодо результатів забезпечення захисту кінцевих точок або для знаходження певної інформації про пристрої в користуванні.

Звіти Syxsense є результатом десятиліть роботи з клієнтами і тому не потрібно буде їх редагувати в більшості випадків, так як вони відображають всю необхідну інформацію і відповідають всім можливим нормативним документам.

У звітах відображається інформація з інвентаризації, яка оновлюється раз на добу у відповідь на запит пристрою до сервера. Є можливість створювати звіти "Аудит", "Інвентаризація" і "Безпека", групуючи різні метрики. Звіти Audit відображають активність консолі, Inventory - стан пристроїв, програмного забезпечення і всього середовища, а Security - вразливості системи та інші проблеми з безпекою. Для вибору необхідного звіту при його створенні можна вказати категорію звіту в випадаючому списку.

Syxsense також дозволяє планувати створення і відправку звітів в потрібному форматі (PDF, CSV або будь-якому іншому) і встановлювати періодичність їх відправки на певну електронну пошту.

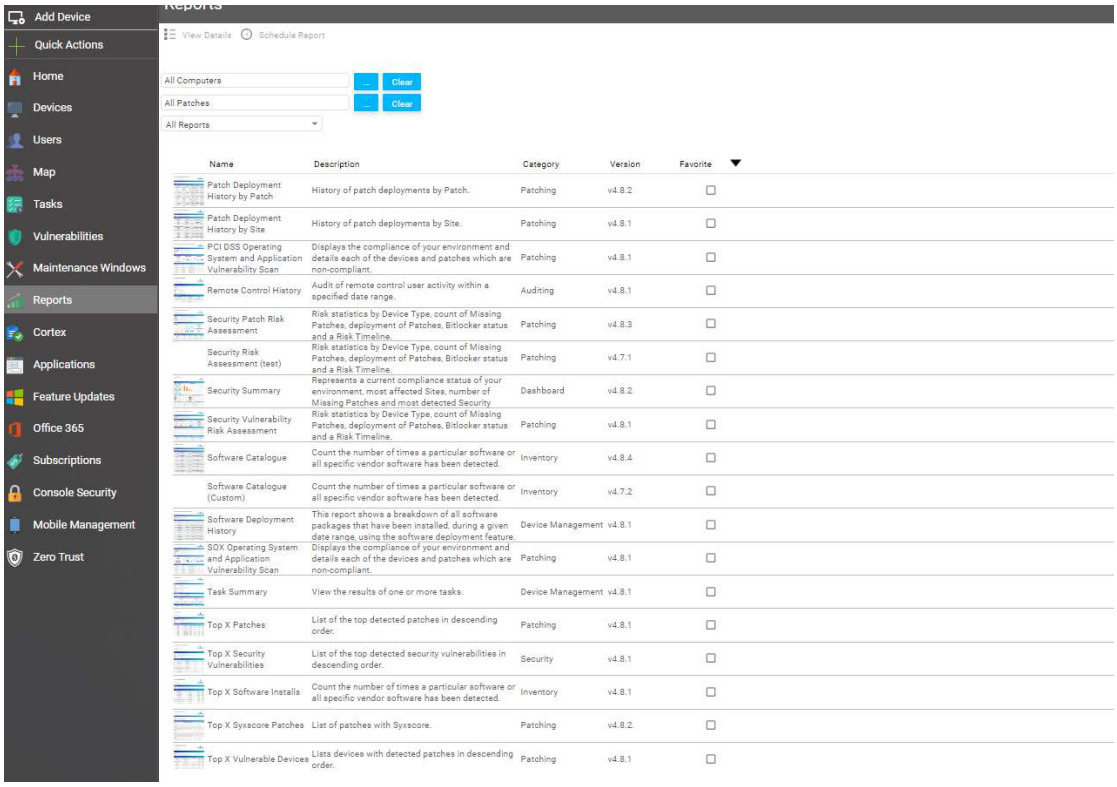


Рис. 3.21. Перелік частини звітів

3.2. Технологія застосування рішення AWS IAM

Незалежно від того, наскільки сильно бізнес захищає свою мережу безпеки та дані, він все одно залишається вразливим, оскільки кіберзлочинці стають все більш досконалими у своїх методах атак. Як наслідок, єдиним рішенням є постійне вдосконалення плану кібербезпеки у мережі, і одним з мережевих рішень для підвищення рівня її безпеки є кінцеві точки.

Просунутий захист кінцевих точок має важливе значення, оскільки кінцеві точки традиційно є ареною кібернетичних битв. Як наслідок, важливо, щоб компанія, як велика, так і мала, мала ефективне налаштування безпеки кінцевих точок.

Необхідність поліпшення безпеки кінцевих точок

Кінцеві точки є основною мішенню для кібератак, оскільки вони є точкою входу до всієї вашої мережі і всіх корпоративних даних. Багато зловмисників націлили свої гарпуни на цю нову, головну ціль, оскільки зламати кінцеву точку

набагато простіше, ніж атакувати мережевий сервер або веб-сайт, за яким пильно стежать.

Будь-який пристрій, що має доступ до мережевих ресурсів компанії або інших конфіденційних даних, є потенційною мішенню для хакерів. До таких пристроїв належать ноутбуки, мобільні телефони/планшети, настільні комп'ютери тощо.

Ось ілюстрація: Хакери можуть отримати доступ до вашої системи, використовуючи застарілий комп'ютер із застарілим програмним забезпеченням або електронну поштову скриньку, яка зазнала фішингової атаки.

За даними IDC, до 70% всіх успішних мережевих атак відбуваються з кінцевих точок. Покращення безпеки кінцевих точок допомагає йти в ногу з обсягом і швидкістю появи нових загроз.

Прийняття стратегії захисту кінцевих точок для поліпшення безпеки кінцевих точок

Проблеми з поточними рішеннями безпеки кінцевих точок в організаціях включають 49% недостатнього захисту від нових атак, 43% високої складності розгортання і експлуатації, а також 27% поганого досвіду роботи користувачів.

Тисячі кінцевих точок у вашій інфраструктурі вразливі до атак зловмисного програмного забезпечення та зниження продуктивності. Прийняття плану посилення безпеки кінцевих точок має вирішальне значення, оскільки одна пошкоджена кінцева точка може завдати серйозної шкоди вашій компанії, наприклад, фінансових втрат або простою. Але не багато організацій застосовують комплексний підхід до захисту своїх кінцевих точок.

Ознаками компетентної програми захисту кінцевих точок є належні операційні практики, такі як вразливість конфігурації та управління виправленнями; однак менш зрілим підприємствам не вистачає ресурсів для модернізації своїх процесів, і вони повинні негайно шукати замінники.

Ось рекомендації щодо поліпшення безпеки кінцевих точок:

Ідентифікування всіх кінцевих точок

Першим кроком до поліпшення безпеки кінцевих точок є ідентифікація,

оцінка та каталогізація всіх кінцевих точок, які знаходяться у вашому бізнесі. Це може бути складним завданням, оскільки багато організацій дозволяють співробітникам приносити свої пристрої на роботу. Пристрої Інтернету речей також є точками доступу для хакерів.

Працювати зі співробітниками і мережевими адміністраторами, щоб ідентифікувати і класифікувати кожну кінцеву точку, підключену до мережі або даних вашої компанії. Отримавши цю інформацію, ви зможете визначити пріоритетність найбільш ризикованих і делікатних кінцевих точок і обмежити доступ до мережі тільки авторизованими пристроями.

Якщо не захистити ці пристрої, це може призвести до прогалин у безпеці ваших кінцевих точок.

Впровадити процес обслуговування кінцевих точок

Якщо система безпеки кінцевих точок у вашій компанії є менш зрілою, впровадьте процес обслуговування кінцевих точок і виберіть рішення, які пропонують хмарні технології та керовані сервіси. І навпаки, якщо система безпеки кінцевих точок у вашій компанії досить розвинена, інвестуйте в поліпшення стандартів конфігурації безпеки кінцевих точок і процесів обслуговування кінцевих точок, а також перейдіть від захисту до виявлення і реагування на загрози.

Впровадити політику використання власних пристроїв (BYOD)

Використання мобільних пристроїв співробітниками - це реальність, яка залишиться тут, тому дуже важливо впроваджувати політику "Приносьте свої пристрої" (Bring-Your-Own-Device, BYOD). Ця політика визначає ступінь підтримки, яку IT-відділ може запропонувати для комп'ютерів, смартфонів та планшетів, що знаходяться у співробітників компанії.

Якщо компанія працює з конфіденційними даними, надайте співробітникам ноутбуки або мобільні телефони з функціями шифрування повідомлень та обмеженими і дозволеними додатками для підвищення рівня безпеки кінцевих точок.

Усувати загрози за допомогою програмного забезпечення для виявлення та реагування на мережеві загрози (NDR)

Навіть найнадійніші брандмауери іноді можуть бути подолані складним шкідливим програмним забезпеченням. Щоб розпізнати загрози та відстежити їх, використовуйте програмне забезпечення NDR (мережеве виявлення та реагування). За допомогою цього програмного забезпечення компанії можуть краще зрозуміти, як сталася атака, і зміцнити свій захист за допомогою повністю відкритого методу.

Використовувати моніторинг кінцевих точок

Тільки половина рівняння включає в себе моніторинг активності та поведінки користувачів. Кожна кінцева точка має унікальну поведінку, якою можуть прямо або віддалено зловживати хакери. Як наслідок, дуже важливо визначити базові дії для самих кінцевих точок.

Команда безпеки може відстежувати, збирати та вивчати поведінку кінцевих точок за допомогою моніторингу кінцевих точок. Він створює базову поведінку, щоб оцінити, чи поводиться вона неналежним чином, і може швидко повідомити вашу службу безпеки, щоб вона розібралася з цим.

Використовувати інформацію про безпеку та інструменти управління подіями

Розробка рішень для управління інформацією та подіями безпеки (SIEM) є важливим аспектом IT-безпеки. Вони здійснюють моніторинг всієї мережі та збирають метрики і дані про будь-яку підозрілу активність для великих корпорацій або підприємств, що працюють з великими обсягами даних.

Для виявлення та запобігання порушенням безпеки та зменшення наслідків будь-якого вторгнення або атаки, інструменти управління інформацією та подіями безпеки (SIEM) допомагають автоматизувати операції та зрозуміти сенс величезних обсягів складних звітних даних.

Дотримуйтися принципу найменших привілеїв

Прийняття принципу найменших привілеїв є одним з найефективніших методів підвищення безпеки кінцевих точок.

Концепція цього принципу передбачає, що суб'єктам надаються тільки ті привілеї, які необхідні для виконання обов'язків або завдань. Це означає, що користувачі не зможуть отримати доступ до служб, які не є необхідними для

виконання їх звичайних завдань.

Дотримуючись принципу найменших привілеїв, IT-активи будуть менш вразливими до внутрішніх загроз. По суті, пристрій буде з меншою ймовірністю скомпрометований меншою кількістю персоналу, який має доступ адміністратора.

Висновки до розділу

Безпека кінцевих точок: Необхідність для сучасного бізнесу. Застосування вищевказаних рекомендацій для поліпшення безпеки кінцевих точок має велике значення для захисту пристроїв і конфіденційних даних компанії. Syxsense Endpoint Security пропонує сучасне рішення для забезпечення захисту кінцевих точок.

ВИСНОВКИ

Отже, підбиваючи *підсумки* з приводу засобів захисту кінцевих точок підприємства, можна зробити такі висновки:

Syxsense Endpoint Security надає фахівцям з інформаційної безпеки всі необхідні інструменти для того, аби позбавити зловмисників переваги першого удару, а саме набір інтелектуальних, взаємодіючих один із одним засобів захисту та платформу для спрощення складних середовищ, високі показники надійності, швидкодії та високої ефективності виявлення загроз, що підтверджені результатами незалежних тестів, дозволяють організаціям захистити своїх користувачів, підвищити продуктивність праці та бути впевненими у захищеності власних корпоративних систем.

Компанія Syxsense, що розвивається дуже швидко на ринку безпеки кінцевих точок, пропонує повний спектр рішень для будь-якого підприємства, незалежно від його розмірів. Скорочення часу для впровадження засобів захисту, підвищений рівень швидкодії та ефективне управління програмним продуктом дозволяють фахівцям з безпеки виявляти набагато більше загроз, роблячи це швидше та з меншими витратами власних ресурсів.

Дане програмне рішення дозволяє контролювати доступ до корпоративної мережі, застосовувати політику щодо кінцевих точок та інтегрувати засоби управління кінцевими точками в існуючі мережеві інфраструктури підприємства. Незалежно від того, як кінцеві точки підключаються до мережі, служба контролю мережевого доступу виявляє та оцінює стан нормативно-правової відповідності кінцевої точки, застосовує необхідні політики доступу до мережі та забезпечує можливості автоматичного виправлення за допомогою технології Syxsense Cortex.

Зважаючи на постійне зростання кіберзагроз підвищеної складності, підприємства не можуть покладатися на рішення, які використовують лише аналіз сигнатур для захисту кінцевих точок. Як вже відомо, інтервал між часом виявлення загрози та часом установки сигнатури на кінцевій точці становить від однієї до

трьох діб. В цей період дані та самі системи залишаються незахищеними. Шляхом інтеграції результатів досліджень і відповідних дій рішення Syxsense може відправити на карантинне зберігання або запобігти проникнення вірусів, троянів, «черв'яків», рекламних, шпигунських та інших потенційно небажаних програм, що займаються крадіжкою конфіденційних даних та знижують продуктивність праці працівників підприємств. Це зайвий раз підкреслює, що правильно підібраний програмний продукт може повністю забезпечити захист усіх кінцевих точок в корпоративній інформаційній системі підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1. Morey J. Haber, Darran Rolls. Identity Attack Vectors. Implementing an Effective Identity and Access Management Solution. Apress Media. 2020. 205 p.

2. Michael Schwartz, Maciej Machulak. Securing the Perimeter. Deploying Identity and Access Management with Free Open Source Software. 2018. 383 p.

3. Michael Wittig, Andreas Wittig, foreword by Ben Whaley. Amazon Web Services in Action, Second Edition. Manning Publications Co. 2019. 530 p.

4. What is an endpoint? [Електронний ресурс] – Режим доступу до ресурсу: https://www.cloudflare.com/learning/security/glossary/what-is-endpoint/.

5. Gartner Magic Quadrant for Endpoint Protection Platforms [Електронний ресурс] // Gartner. – 2019. – Режим доступу до ресурсу: https://www.gartner.com/doc/reprints?id=1-1OEZ6HOU&ct=190822&st=sb&elqTrackId=8bc9582d06cd4faaac82be0cf92483ca&elqaid=5362&elqat=

6. Hu, C., Ferraiolo, D., Kuhn, D., Schnitzer, A., Sandlin, K., Miller, R. and Scarfone, K. (2019), Guide to Attribute Based Access Control (ABAC) Definition and Considerations, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927500 (Accessed November 27, 2021).

7. Endpoint security deployment status [Електронний ресурс] – Режим доступу до ресурсу: https://www.statista.com/statistics/1319760/endpoint-security-deployment-status-worldwide/.

8. Designing a modern IAM program for your business. IBM Security. September 2020. https://www.ibm.com/downloads/cas/9YBEK41O.

9. Robert Snow. 5 Key Predictions for Identity and Access Management and Fraud Detection. January 14, 2021. https://www.gartner.com/smarterwithgartner/5-key-predictions-for-identity-and-access-management-and-fraud-detection.

10. The Forrester Wave: Identity-As-A-Service For Enterprise, Q3 2021 by Sean Ryan with Merritt Maxim, Elsa Pikulik and Peggy Dostie, August 31, 2021. https://reprints2.forrester.com/#/assets/2/108/RES176134/report.

11. Endpoint Device [Електронний ресурс] – Режим доступу до ресурсу: https://www.barracuda.com/glossary/endpoint-device.

12. Road Map To Improve Your Endpoint Security https://quantumpc.com/improve-endpoint-security/

13. Syxsense Documentation, Getting Started https://testteamtest.cloudmanagementsuite.com//Documentation/.

14. The Top 11 Endpoint Security Solutions For Business [Електронний ресурс] – Режим доступу до ресурсу: https://expertinsights.com/insights/the-top-endpoint-security-solutions-for-business/.

15. The Future of Endpoint Management [Електронний ресурс] – Режим доступу до ресурсу: https://www.securityweek.com/future-endpoint-management.

16. Макарова Н.В., Самарханова Е.А. Анализ состояния и тенденции развития рынка корпоративных информационных систем // Компьютерные технологии поддержки бизнес процессов.2014.№3(11). С.9-22.

17. 12 essential features of advanced endpoint security tools https://www.techtarget.com/searchsecurity/feature/12-essential-features-of-advanced-endpoint-security-tools.

18. THE ULTIMATE GUIDE TO ENDPOINT SECURITY -TOP ENDPOINT SECURITY SOLUTIONS https://www.datalinknetworks.net/dln_blog/the-ultimate-guide-to-endpoint-security-top-endpoint-security-solutions-2021.

19. What Is Endpoint Protection and Top 6 EPP Solutions https://www.cynet.com/endpoint-protection/top-6-endpoint-protection-platforms-and-how-to-choose/.

20. The Ultimate Guide to Endpoint Security https://research.aimultiple.com/endpoint-security/.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)