ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захисту кінцевих точок організації на базі Bitdefender GravityZone Business Security»

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

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

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

_____ Владислав ПАХНЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-62
ПАХНЕНКО Владислав
(прізвище, ім'я)

Керівник к.військ.н., доцент ГАХОВ Сергій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
Систем та технологій кібербезпеки
Галина ГАЙДУР
"___" жовтня 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

ПАХНЕНКУ Владиславу Олександровичу
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Технологія захисту кінцевих точок організації на базі Bitdefender GravityZone Business Security»

керівник кваліфікаційної роботи Гахов Сергій Олександрович, к.військ.н., доц.
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» жовтня 2024 року № ___.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 15.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
рішення Bitdefender GravityZone Business Security;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблеми захисту кінцевих точок організації.

2. Аналіз методів та засобів забезпечення безпеки кінцевих точок організації на базі Bitdefender GravityZone Business Security.

3. Технологія забезпечення безпеки кінцевих точок організації на базі Bitdefender GravityZone Business Security.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 01.10.2024 р.

КАЛЕНДАРНИЙ ПЛАН

	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
	Визначення актуальності проблеми забезпечення безпечної роботи гібридних працівників організації.	01.10.2024 р.	
	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	12.10.2024 р.	
	Аналіз методів та засобів забезпечення безпеки кінцевих точок на базі Bitdefender GravityZone Business Security.	27.10.2024 р.	
	Технологія забезпечення безпеки кінцевих точок організації на базі Bitdefender GravityZone Business Security	03.11.2024 р.	
	Розроблення рекомендацій щодо застосування технології забезпечення безпеки кінцевих точок	15.11.2024 р.	
	Оформлення результатів дослідження.	26.11.2024 р.	
	Підготовка доповіді до захисту.	15.12.2024 р.	

Здобувач вищої освіти _____ Владислав ПАХНЕНКО
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Сергій ГАХОВ
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача Пахненко Владислава

на тему: «Технологія захисту кінцевих точок організації на базі Bitdefender GravityZone Business Security»

Актуальність: . У сучасному світі став популярний вислів "Гібридна робота", що являє собою поняття працівників, які працюють як і з офісів організацій так і віддалено з будь якого місця. У випадку з віддаленою роботою це викликає ряд негативних факторів, які впливають на безпеку кінцевих точок в мережі організації. Віддалена робота часто здійснюється через домашні мережі, які зазвичай мають слабший рівень захисту порівняно з корпоративними мережами.

Необхідно зауважити, що впровадження та застосування технології забезпечення захисту кінцевих точок організації є необхідною умовою прояву стійкості бізнес-процесів організацій. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі було встановлено зміст проблеми забезпечення безпеки кінцевих точок організації та визначено мету та завдання даного виду забезпечення, а також його складові частини.
2. Досліджено методи та засоби забезпечення безпеки кінцевих точок організації на базі Bitdefender GravityZone Business Security.
3. Розглянуто зміст технології забезпечення безпеки захисту кінцевих точок організації на базі Bitdefender GravityZone Business Security та рекомендації щодо її застосування.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1. У кваліфікаційній роботі бажано було б провести аналіз умов застосування корпоративних додатків та забезпечення безпеки кінцевих точок на прикладі конкретної організації.
2. Запропонований порядок застосування технології забезпечення безпеки кінцевих точок бажано було б показати на прикладі конкретної організації.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **"добре"**, а здобувач(ка) **ПАХНЕНКО Владислав** – присвоєння кваліфікації магістр з кібербезпеки за освітньою програмою інформаційна та кібернетична безпека.

Рецензент:

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

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 76 сторінок, 40 рисунків, 1 таблиця, 12 джерел.

Об'єкт дослідження – забезпечення захисту кінцевих точок організації.

Предмет дослідження - технологія захисту кінцевих точок організації на базі Bitdefender GravityZone Business Security.

Мета роботи – розробити порядок застосування технології захисту кінцевих точок організації та рекомендації щодо її реалізації.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, огляд рішення Bitdefender GravityZone Business Security, огляд міжнародних стандартів та їх порівняння.

Однією з передових технологій, що є критично важливою для забезпечення надійного кіберзахисту, є розширене виявлення та реагування на загрози (Endpoint Detection and Response, EDR). Ця технологія дозволяє здійснювати безперервний моніторинг активності кінцевих точок, проводити глибокий аналіз подій у реальному часі, ідентифікувати аномалії та запобігати складним загрозам. Особливістю EDR є її здатність до автоматизованого збору даних, які використовуються для кореляції подій і визначення загрозових моделей. Це забезпечує підвищення швидкості та точності реагування на інциденти безпеки, що є важливим у сучасному кіберпросторі. Рішення Bitdefender GravityZone Business Security має передовий EDR, що значно спрощує та покращує захист кінцевих точок організації.

У роботі проаналізовано проблему забезпечення ефективного захисту кінцевих точок організації, визначено її актуальність, мету та завдання. Здійснено комплексний аналіз існуючих технологій кібербезпеки для захисту кінцевих точок. Проведено дослідження методів і засобів забезпечення захисту кінцевих точок організації з використанням платформи Bitdefender GravityZone Business Security. Визначено

функціональне призначення, складові компоненти та ключові переваги зазначеного рішення.

На основі проведених досліджень у роботі запропоновано порядок впровадження Bitdefender GravityZone Business Security для захисту кінцевих точок організації. Розроблено практичні рекомендації для фахівців з кібербезпеки щодо оптимального застосування цього рішення у сучасних умовах.

Галузь використання – кібербезпека інформаційних ресурсів організації.

ЗАХИСТ КІНЦЕВИХ ТОЧОК, EDR, BITDEFENDER GRAVITYZONE BUSINESS SECURITY, КІБЕРБЕЗПЕКА, ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ.

ABSTRACT

Text part of the qualification work: 77 pages, 40 figures, 1 table, 12 sources.

The object of research is to ensure the protection of an organisation's endpoints.

The subject of the research is the technology for protecting the organisation's endpoints based on Bitdefender GravityZone Business Security.

The purpose of the study is to develop a procedure for applying endpoint security technology and recommendations for its implementation.

Research methods : studying the literature on this topic, analysing operational documentation, reviewing the Bitdefender GravityZone Business Security solution, reviewing international standards and comparing them.

One of the advanced technologies that is critical for ensuring reliable cyber defence is Endpoint Detection and Response (EDR). This technology allows for continuous monitoring of endpoint activity, in-depth real-time event analysis, anomaly detection, and prevention of complex threats. EDR's special feature is its ability to automate data collection, which is used to correlate events and identify threat patterns. This ensures faster and more accurate response to security incidents, which is important in today's cyberspace. The Bitdefender GravityZone Business Security solution has an advanced EDR, which greatly simplifies and improves the protection of an organisation's endpoints.

The paper analyses the problem of ensuring effective protection of an organisation's endpoints, defines its relevance, purpose and objectives. A comprehensive analysis of existing cybersecurity technologies for endpoint protection is carried out. A study of methods and means of ensuring the protection of endpoints of an organisation using the Bitdefender GravityZone Business Security platform is carried out. The functional purpose, components and key advantages of this solution are determined.

Based on the research, the paper proposes a procedure for implementing Bitdefender GravityZone Business Security to protect the organisation's endpoints. Practical

recommendations for cybersecurity professionals on the optimal use of this solution in modern conditions have been developed.

Application area - cybersecurity of an organisation's information resources.

ENDPOINT PROTECTION, EDR, BITDEFENDER GRAVITYZONE BUSINESS SECURITY, CYBERSECURITY, INFORMATION RESOURCES OF AN ORGANISATION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

EDR - Endpoint Detection and Response

MDM – Mobile Device Management

ПЗ – програмне забезпечення

MitM – Man-in-the-Middle

Evil Twin – фальшива точка доступа

CVE – Common Vulnerabilities and Exposures

VPN – Virtual Private Network

SIEM – Security Information and Event Management

MDM – Mobile Device Management

ШІ – штучний інтелект

ML – Machine Learning

ВСТУП

Актуальність дослідження. У сучасному світі став популярний вислів “Гібридна робота”, що являє собою поняття працівників, які працюють як і з офісів організацій так і віддалено з будь якого місця. У випадку з віддаленою роботою це викликає ряд негативних факторів, які впливають на безпеку кінцевих точок в мережі організації. Віддалена робота часто здійснюється через домашні мережі, які зазвичай мають слабший рівень захисту порівняно з корпоративними мережами. Це відкриває кінцеві точки для атак, таких як перехоплення даних (Man-in-the-Middle), експлуатація вразливостей у маршрутизаторах тощо. Також потрібно виділити, що якщо організація не використовує рішення для контролю (MDM) кінцевих точок, а також для їх захисту, то кінцева точка буде позбавлена можливості оновлення операційної системи, виправлень безпеки, антивірусного ПЗ та користувацького ПЗ. Такі працівники більш схильні до фішингових атак, що являє собою мету вкрасти облікові дані користувача. Тут також велику роль грає фізичний фактор людини, пристрій може бути забутий в громадському місці, конфіденційна інформація може зберігатися в ненадійних місцях.

Також загрозу становить, якщо пристрій був уражений та через деякий час потрапляє в корпоративну мережу організації. У випадку недосконалої системи захисту це може становити велику загрозу та в кінцевому результаті уразити ще більше кінцевих точок організації.

На даний момент існують рішення та технології, які посилюють захист кінцевих точок в корпоративній мережі організації. Вони дозволяють забезпечити моніторинг активності пристроїв, виявлення аномалій та запобігання можливим загрозам у реальному часі. Такі підходи сприяють зменшенню ризиків компрометації критично важливих даних і підвищенню загального рівня кібербезпеки. Завдяки автоматизації

процесів захисту та розширеним можливостям аналізу організації можуть ефективніше протидіяти як зовнішнім атакам, так і внутрішнім загрозам.

Endpoint Detection and Response (EDR) — це сучасна технологія кібербезпеки, яка забезпечує моніторинг, виявлення та реагування на загрози, спрямовані на кінцеві точки (комп'ютери, сервери, мобільні пристрої). EDR надає глибоку видимість діяльності на кінцевих точках, дозволяючи ідентифікувати аномалії та запобігати атакам у реальному часі. Це є одним із основних компонентів, який використовується у рішенні Bitdefender GravityZone Business Security.

Все, що було сказано попередньо доводить про актуальність вибраної теми у цій кваліфікаційній роботі основним зміст якої становить дослідження технології захисту кінцевих точок організації на базі Bitdefender GravityZone Business Security.

Об'єкт дослідження – забезпечення захисту кінцевих точок організації.

Предмет дослідження - технологія захисту кінцевих точок організації на базі Bitdefender GravityZone Business Security.

Мета роботи – розробити порядок застосування технології захисту кінцевих точок організації та рекомендації щодо її реалізації.

Наукові завдання :

дослідити сутність проблеми захисту кінцевих точок організації;

проаналізувати підходи задля забезпечення захисту кінцевих точок організації;

проаналізувати існуючі рішення щодо забезпечення захисту кінцевих точок організації;

проаналізувати методи та засоби забезпечення захисту кінцевих точок організації на базі Bitdefender GravityZone Business Security;

розкрити порядок реалізації технології щодо захисту кінцевих точок організації.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, огляд рішення Bitdefender GravityZone Business Security, огляд міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано порядок застосування технології захисту кінцевих точок організації, а також розроблено рекомендації фахівцям кібербезпеки щодо її реалізації.

Результати кваліфікаційної роботи апробовані на VII Всеукраїнській студентській конференції «Експериментальні та теоретичні дослідження в контексті сучасної науки», яка відбулася 22 листопада 2024 року у м. Львові.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ

1.1 Дослідження проблеми забезпечення захисту кінцевих точок організації

З появою віддаленого та гібридного типу роботи питання захисту кінцевих точок в мережі організації стало як ніколи важливим. Кінцева точка (endpoint) — це будь-який пристрій, який підключається до мережі організації та взаємодіє з нею. Кінцеві точки включають персональні комп’ютери, ноутбуки, смартфони, планшети, сервери, IoT-пристрої, принтери, а також інші елементи, що забезпечують доступ користувачів до мережевих ресурсів. У контексті кібербезпеки кінцеві точки є важливими об'єктами захисту, оскільки вони часто стають першочерговою ціллю зловмисників через їхню уразливість до атак, таких як фішинг, експлуатація вразливостей у ПЗ, або зараження шкідливими програмами. Вразливість цих точок ставить під загрозу всю корпоративну інформаційну систему та дає кіберзлочинцям багато опцій для взаємодії з незахищенними точками. В першу чергу потрібно виділити місце роботи працівника на кінцевій точці. Зазвичай домашні мережі є більш вразливі ніж відокремлена корпоративна мережа. При невірних налаштуваннях домашньої мережі, зловмисники з легкістю потрапляють в локальну мережу та можуть взаємодіяти з наявними пристроями. Більш небезпечним є якщо співробітник працює в громадському місці з відкритих та повністю незахищених мереж. В наш час є так звані опенспейси, пункти незламності та коворкінги, ці місця є найбільш вразливими та надають кіберзлочинцям великий спектр інструментів для взаємодії з кінцевими точками[1]. Серед них можливо виділити такі:

1. **Атака "Man-in-the-Middle" (MitM)**: Кіберзлочинець може перехоплювати трафік між користувачем і мережею, отримуючи доступ до облікових даних, паролів, або інших конфіденційних даних.
2. **Фальшива точка доступу (Evil Twin)**: Зловмисник створює Wi-Fi мережу з ідентичною або схожою назвою, змушуючи користувачів підключатися до неї.
3. **Використання незашифрованого трафіку**: Якщо мережа або користувачі не використовують шифрування (наприклад, HTTPS), це робить дані вразливими до перехоплення.

Статистичні дані свідчать, що після широкого впровадження віддаленої та гібридної роботи значно зросла кількість виявлених вразливостей в кінцевих точках. За останні роки, кількість зареєстрованих CVE (Common Vulnerabilities and Exposures) зросла на понад 25% (рисунок 1.1).

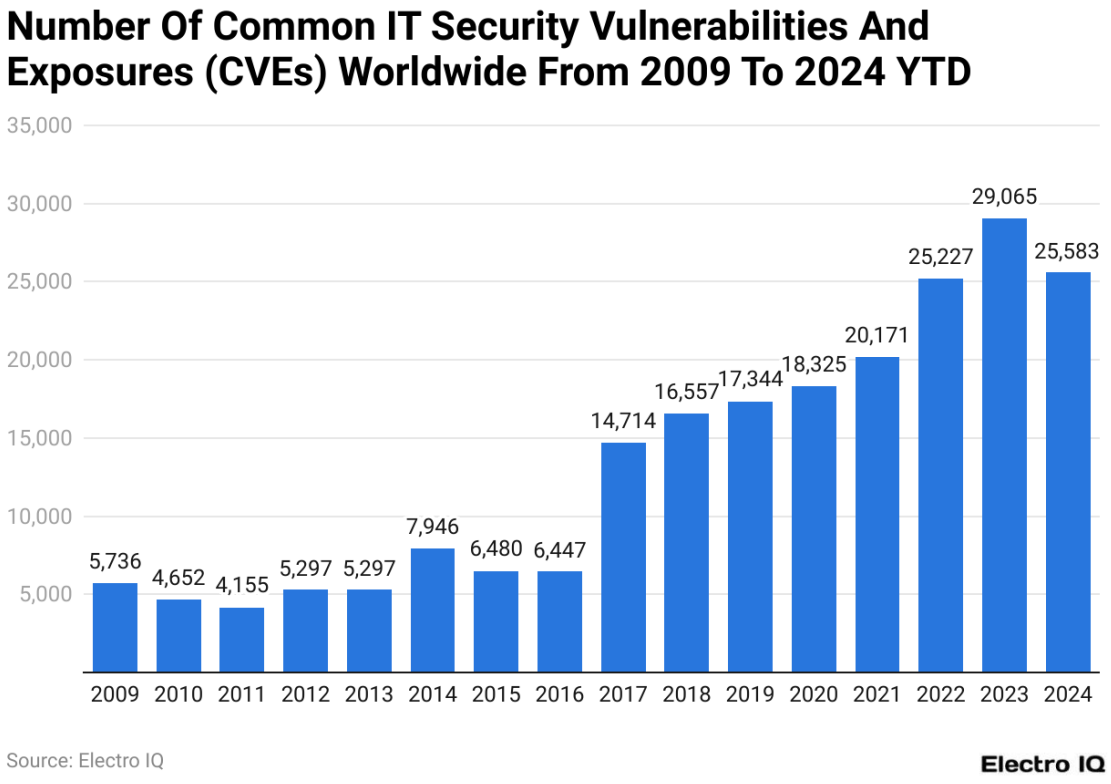

Рис. 1.1 – Кількість наявних IT вразливостей починаючи з 2009 до 2024 року[1]

Ця проблема є глобальною та відноситься не лише до другорядних компаній, а й до гігантів ринку. Великі компанії також стикнулися з проблемою захисту своїх девайсів та кінцевих точок (Рисунок 1.2). Це нагально показує, що усі наявні рішення з захисту кінцевих точок є апробованими та актуальними[1].

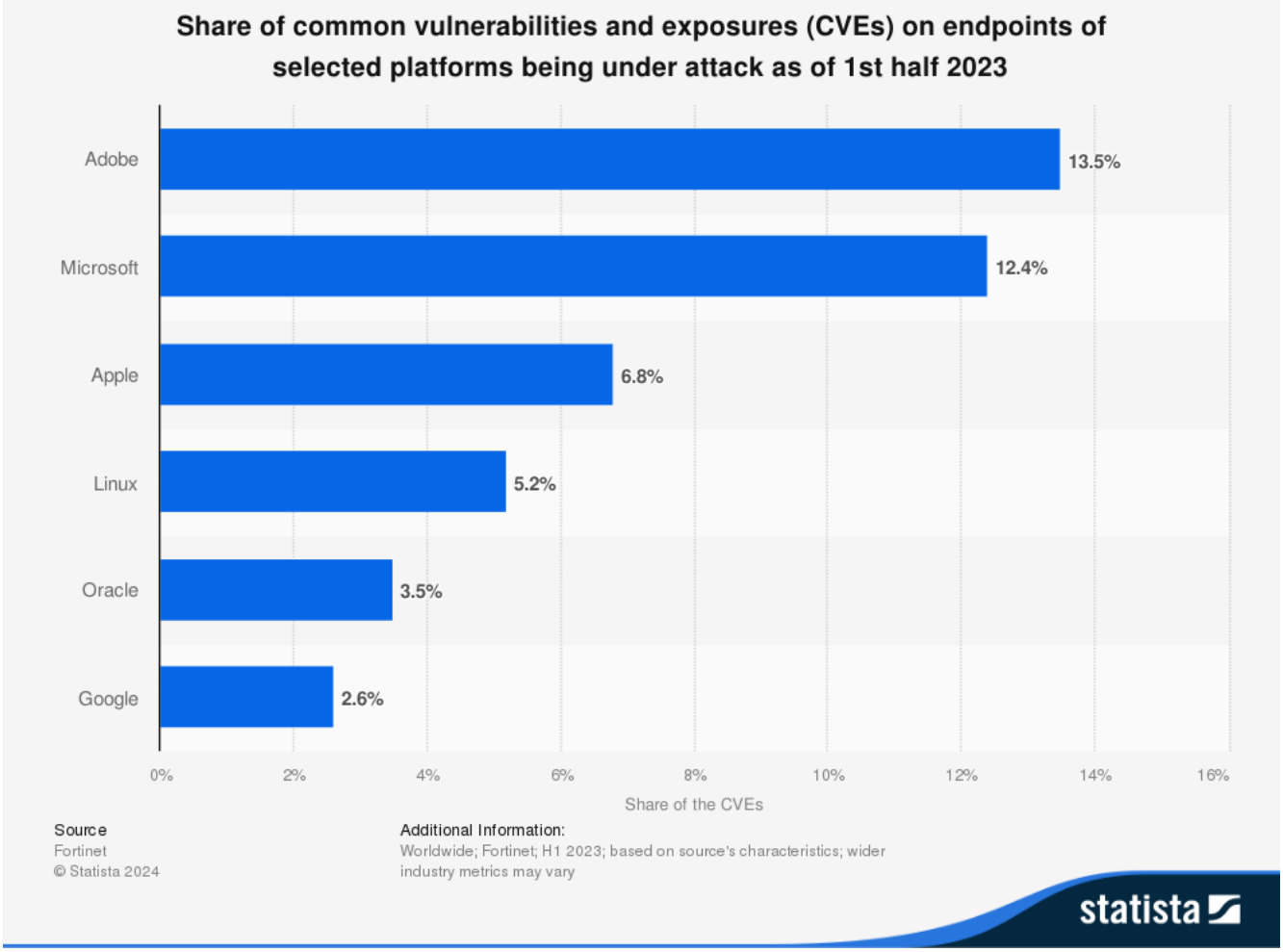

Рис. 1.2 - Процент уражених кінцевих точок відомих компаній[1]

Попередньо ми розглянули 3 типи атак, які найчастіше використовуються при використанні кінцевої точки в незахищеній мережі. Розглянемо їх більш детально, що вони являють собою, та їхню статистику по атакам[2].

Атаки типу «Man in the Middle» використовуються вже давно і в різних контекстах. Наприклад, щоб підслуховувати мережевий трафік, зловмисник може надіслати на інші пристрої оновлення, в якому йдеться про те, що їхній комп'ютер є новим шлюзом за замовчуванням і весь мережевий трафік повинен проходити через

нього. Зловмисник може видати себе за надійний пристрій, встановивши власну точку доступу Wi-Fi поруч з іншими доступними бездротовими мережами, що дозволить йому перехоплювати трафік з будь-якого пристрою, який до неї підключається. При фішингу з використанням облікових даних сервер «Man in the Middle» виступає в ролі проксі-сервера між користувачем і фактичним пунктом призначення. Він показує користувачеві сторінку входу на сайт призначення і передає отримані ім'я користувача та пароль на сайт призначення. Якщо для цього облікового запису ввімкнено багатофакторну автентифікацію (MFA), він покаже користувачеві запит MFA для подальшого введення і перенаправить будь-які відповіді на сайт призначення[3].

Також можемо замітити тенденцію зросту цієї атаки до 2022 року та незначний спад у 2023 (Рисунок 1.3).

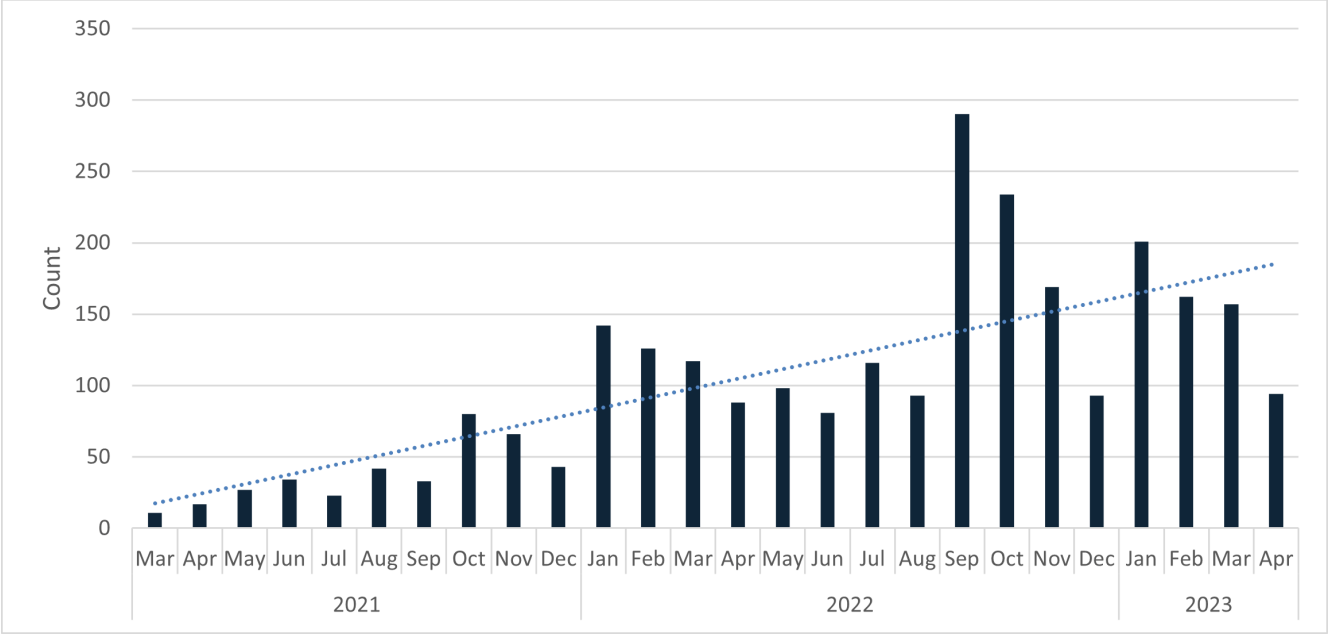

Рис. 1.3 - тенденція використання кібератаки (Man in the Middle)[3]

Атаки «Evit Twin» - це різновид атак типу «людина посередині» (MitM), в яких створюється фальшива мережа Wi-Fi для крадіжки інформації або подальшого проникнення на пристрій, що підключається до неї[4].

Це часто робиться в громадських місцях, де люди, швидше за все, шукають або підключаються до вільно доступного Wi-Fi. Це можуть бути аеропорти, кафе, великі громадські парки тощо, але хакери можуть використовувати цю атаку будь-де,

головним чином тому, що фальшивий Wi-Fi можна легко налаштувати і розгорнути[4].

Також цікаво спостерігати за паттерном трафіку при використанні цих двох атак. Розглянемо паттерн при використанні атаки Evil Twin (Рисунок 1.4).

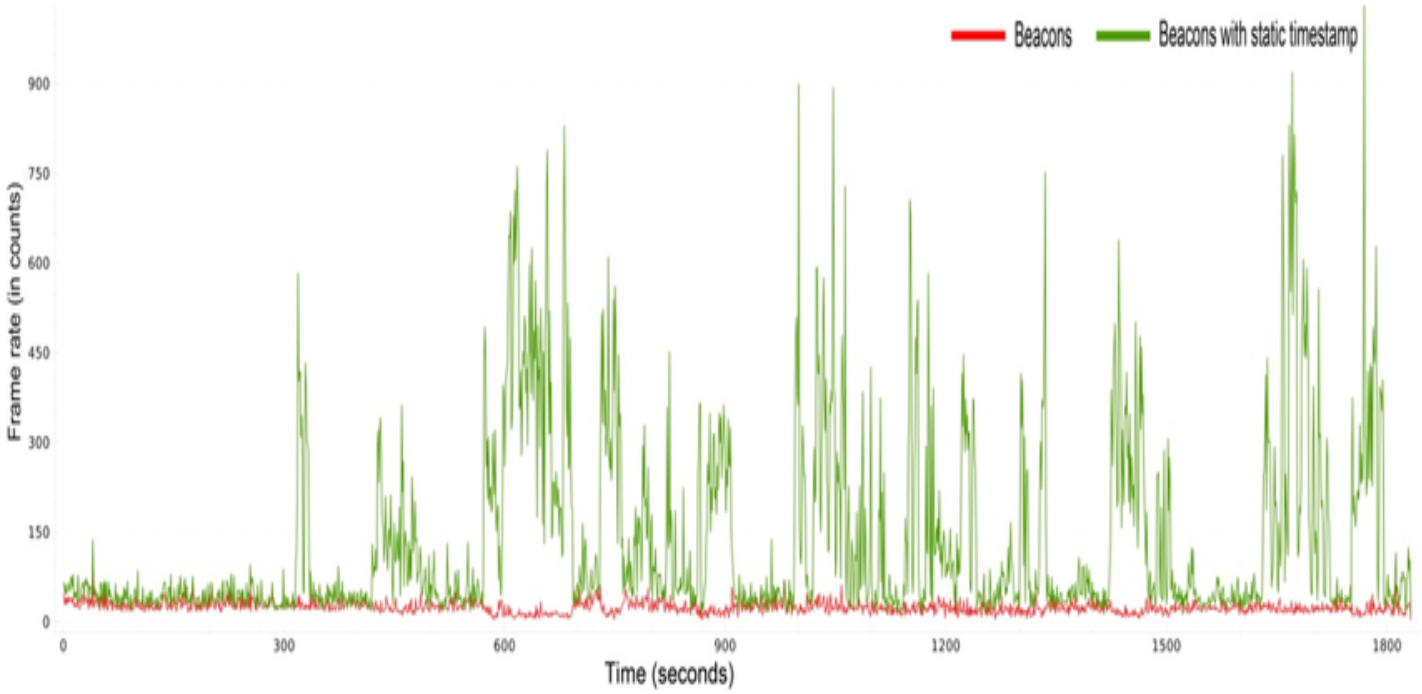

Рис. 1.4 - паттерн мережевого трафіку при активній атаці Evil Twin[5]

Та останнє це використання зловмисниками незахищеного трафіку. Щоб скористатися цією вразливістю, зловмисник повинен мати можливість підслуховувати мережевий трафік жертви. Такий сценарій зазвичай відбувається, коли клієнт взаємодіє з сервером через незахищене з'єднання, наприклад, публічний Wi-Fi, корпоративну або домашню мережу, яка використовується спільно зі скомпрометованим комп'ютером. Звичайних засобів захисту, таких як комутовані мережі, недостатньо, щоб запобігти цьому. Зловмисник, який перебуває у провайдера користувача або в інфраструктурі хостингу додатку, також може здійснити цю атаку. Зауважте, що просунутий зловмисник потенційно може атакувати будь-яке з'єднання, встановлене через основну інфраструктуру Інтернету. Це є проблемою як і мережі з якої відбувається з’єднання так і налаштуваннями безпеки мережі та ресурсів зі сторони управляючої компанії. Тому також потрібно звернути увагу на те, що

використання суміші зашифрованих і незашифрованих комунікацій є неефективним захистом від активних зловмисників, оскільки вони можуть легко видалити посилання на зашифровані ресурси, коли ці посилання передаються через незашифроване з'єднання[6].

Приведемо приклад незашифрованого та шифрованого трафіку різних протоколів при використанні віртуальної машини на базі ОС Windows 10, яка використовувалась 365 днів поспіль (Рисунок 1.5).

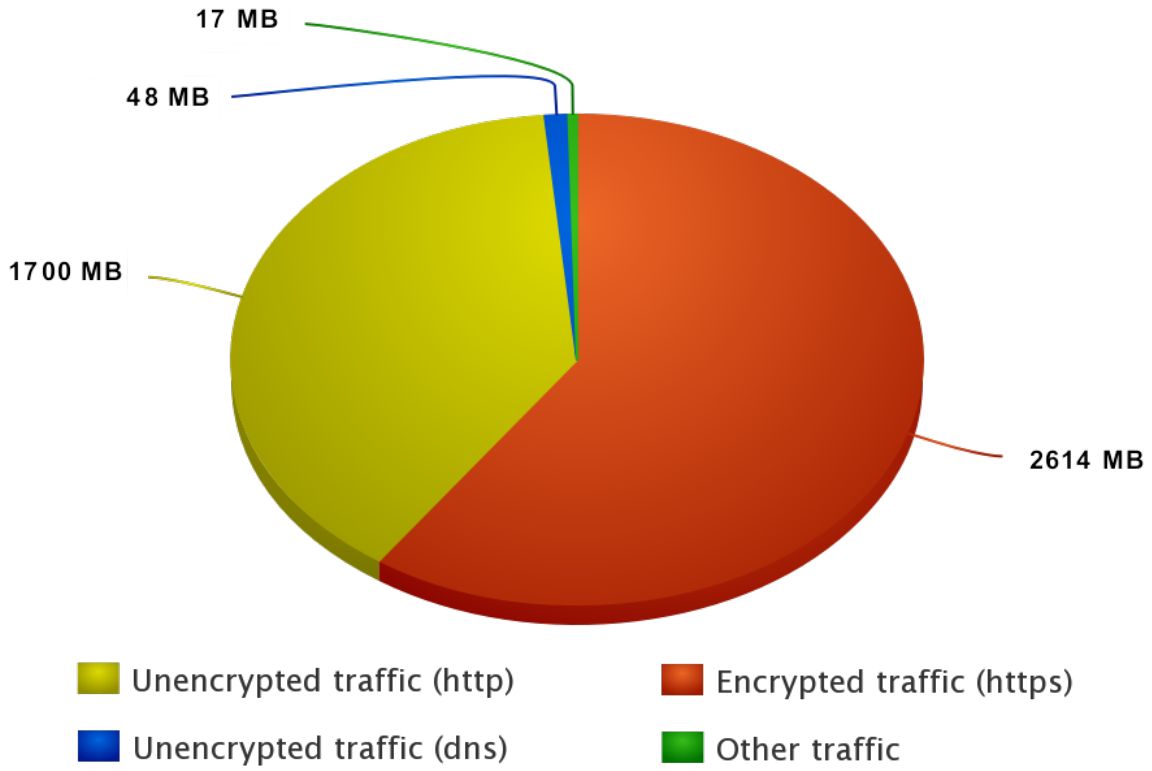

Рис. 1.5 - використання трафіку віртуальною машиною на базі OS Windows 10[4]

На заключення можемо сказати, що станом на 2024 рік з оглядом на статистику можна сказати, що як великі організація так і звичайні користувачі стали трохи менш вразливими після періоду переходу на віддалений та гібридний тип роботи. Тим не менш кіберзлочинці також не зупиняються та використовують нові CVE та відомі

методи проникнення в кінцеву точку тому проблема у винайдені та постійного оновлення вже існуючих рішень для їх захисту є актуальним.

1.2 Аналіз підходів до забезпечення безпеки кінцевих точок організації

На сам перед потрібно розуміти, що в наших умовах не існує повністю ізольованої локальної мережі організації, яка зовсім не мала б виходу у світ. Це пов’язано з поставленими задачами бізнесу, доступами до корпоративних ресурсів, в потребі комунікації всіх співробітників, наявністю як локальних так і хмарних інструментів. Особливу увагу слід приділяти організації безпечного доступу для віддалених працівників, адже їх інтеграція до корпоративної мережі найчастіше здійснюється через VPN (Virtual Private Network). VPN забезпечує зашифроване передавання даних, але сам по собі не гарантує захисту від шкідливих програм чи фішингових атак, які можуть бути спрямовані на кінцеві точки. У цьому контексті ключовим завданням стає забезпечення надійного захисту кінцевих пристроїв, які можуть бути використані як шлюзи для проникнення зловмисників у мережу.

Виходячи з цього маємо розуміти, що підхід до захисту кінцевих точок організації, які найчастіше використовуються для проникнення в систему має бути комплексним. Під цим розуміється, що це має бути набір рішень, порад, вказівок які націлені на виявленні та аналізі різних типів та векторів атак. В цьому плані не можна зосерджуватися на чомусь одному, а в дечому бути як зловмисник та намагатися самому знайти вразливі місця.

Отже визначившись, що захист має відбуватися комплексно, що розуміє під собою використання багаторівневих методів та типів рішень потрібно розібрати, що вони собою являють[4].

Антивірусний захист – являє собою певне сучасне рішення, яке виявляє та нейтралізує відомі типи кібератак. Це агенти, які встановлюються безпосередньо на

кінцеву точку та з заданою періодичністю сканують усі файлові системи, як вбудовані так і дискретні. Це дозволяє постійно тримати кінцеву точку під наглядом та превентивно знешкоджувати зловісне ПЗ. Зазвичай такі рішення є хмарними та напряму пересилають всі діагностичні дані на Dashboard власника та сервери компанії власника наданого ПЗ. Вкрай не рекомендується використовувати безкоштовні антивіруси, оскільки вони самі можуть нести велику загрозу для кінцевої точки. У цій науковій роботі ми розглянемо рішення, яке містить в собі антивірусне ПЗ. Вибір такого рішення має бути зваженим оскільки компанія власник антивірусного ПЗ постійно має оновлювати та актуалізувати базу відомого шкідливого ПЗ та CVE. Окрім сканування системи, антивіруси зазвичай також сканують мережу та завантаження з невідомих джерел.[5]

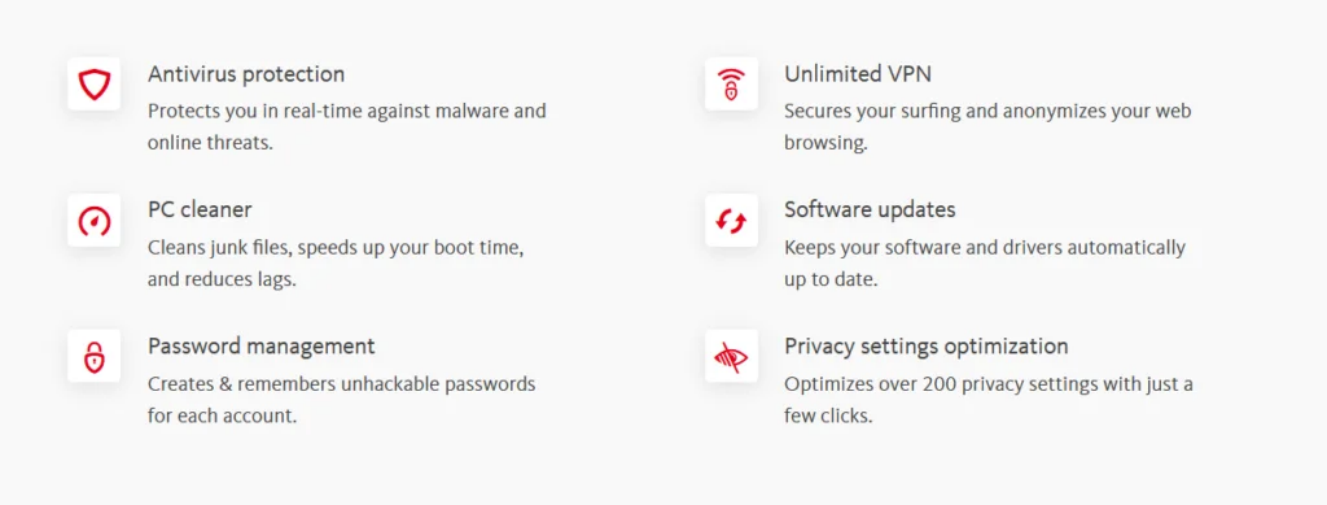

Рис. 1.6 - функції антивірусної програми

Endpoint Detection and Response (EDR). Це системи для моніторингу та аналізу активності кінцевих пристроїв у реальному часі, що дозволяють швидко виявляти аномалії та реагувати на інциденти безпеки. Це рішення в комплексі з антивірусним забезпеченням дозволяє відслідковувати поведінку кінцевої точки, можливу роботу шкідливого ПЗ та витік конфіденційної інформації. Зазвичай при виявленні аномалії в моніторингову систему відправляється звіт та маркується відповідною пріоритетністю в залежності від виставлених налаштувань. Ці дії можуть бути унікальними для кожної компанії, ролі та типу кінцевої точки. Також можливо

налаштувати швидкі дії, які відразу застосовуються до враженої кінцевої точки, що дозволяє мінімізувати ризик втручання у мережу організації. Алгоритм роботи EDR це виявлення, процес коли аномалію було знайдено. Вивчення, процес коли EDR аналізує чи несе загрозу виявлена аномалія. Відповідь, процес коли EDR передає дані про виявлену загрозу на хмарне середовище фахівцю з кібербезпеки. Сповіщення, це процес інформування фахівця з кібербезпеки про виявлену аномалію з відповідним рівнем загрози. Та на кінець після виявлений аналіз, EDR аналізує цю аномалію, прийняті рішення та завдану шкоду [5]

Рис. 1.7 - алгоритм роботи EDR

Як і будь-який великий корпоративний продукт, EDR ґрунтується на кількох ключових принципів, незалежно від розробника. Це як перелік основних правил, яких необхідно дотримуватися, щоб назвати ваш продукт рішенням EDR. Ці принципи також можна інтерпретувати як мінімальні вимоги до програмного продукту, який видає себе за безпекове ПЗ корпоративного масштабу.

Координована відповідь усіх поверхонь атаки. Як зазначалося вище, під час атаки важливо реагувати всіма елементами системи одночасно. Система EDR має надавати цю можливість за замовчуванням або після певного налаштування[6].

Хмарне керування системою. Рішення EDR повинні мати можливість дистанційного керування, аби протидіяти атаці та аналізувати ситуацію з будь-якого

місця та в будь-який час. Як свідчить статистика, більшість кібератак трапляються в неробочий час – коли мало хто стежить за корпоративною мережею.

Найвищий рівень захисту. Навіщо потрібна дорога і складна в налаштуванні система безпеки, якщо вона не може протистояти сучасним загрозам? Це питання риторичне. Захист у рішеннях безпеки кінцевих точок має спиратися на евристичні механізми виявлення та механізми виявлення на базі даних і, можливо, на нейронні мережі. Такі організації, як AV-Comparatives, регулярно тестують доступні рішення і потім публікують власний рейтинг для кожної системи EDR.[7]

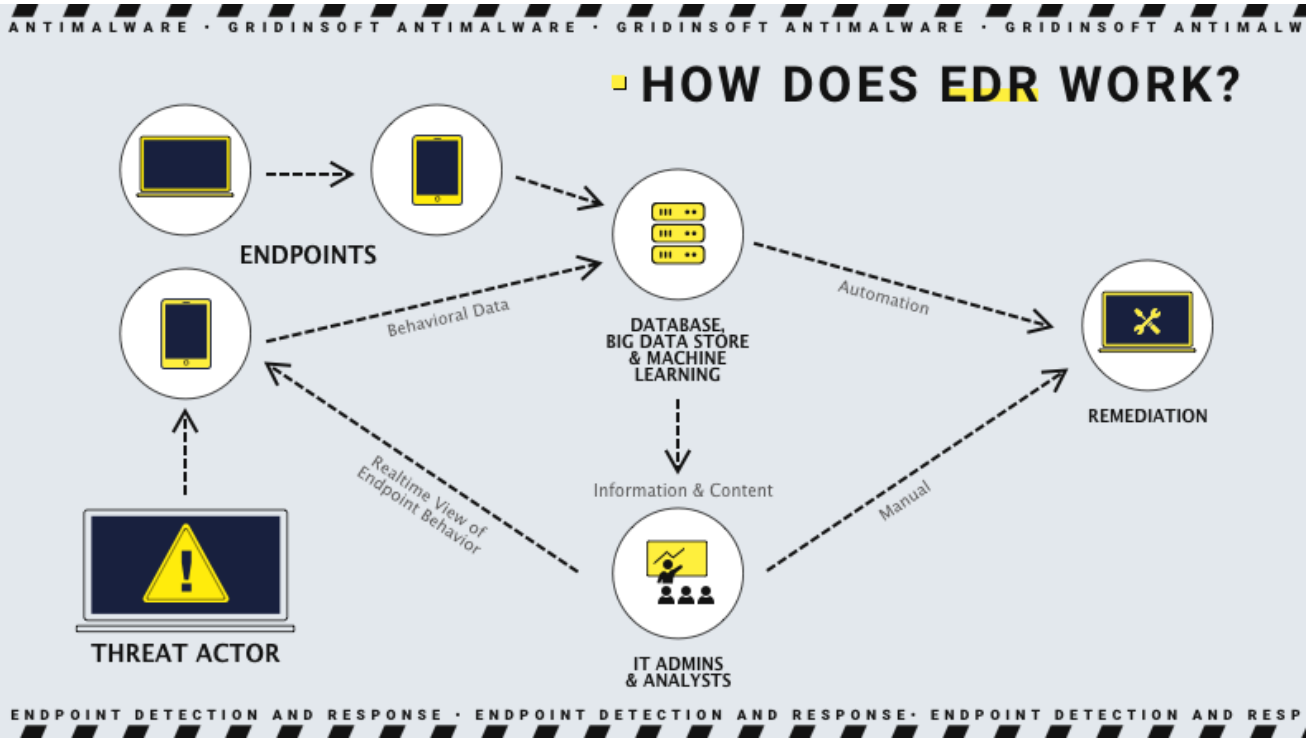

Рис. 1.8 - принцип роботи EDR

Наступне це контроль доступу, що розуміє під собою реалізації. політик доступу на основі ролей, а також обмеження прав користувачів для зменшення можливостей зловмисників використовувати привілейовані облікові записи. Не потрібно нехтувати цим методом захисту, оскільки, якщо зловмисник скомпрометує запис рядового співробітника і у разі не налаштованих ролей він відразу отримає доступ до всієї інформації. У випадку ж налаштованих ролей, доступ до всієї інформації можливо

отримати скомпроментувавши облікові записи лише високопоставлених співробітників або адміністраторів систем захисту[8].

Не менш важливим є шифрування даних. Адміністратори забов’язані проводити шифрування знімних носіїв на кінцевих точках. При випадках крадіжки техніки у більшості випадків рядовий зловмисник не зможе скомпрометувати дані з шифрованого носія, також при форматуванні таких носіїв інформація видаляється повністю і її практично неможливо відновити. У процесі шифрування відкритий текст перетворюється в зашифрований за допомогою криптографічного ключа. Криптографічний ключ — це набір відомих математичних величин, погоджених як відправником, так і одержувачем[6].

Дешифрування, або перетворення зашифрованих даних, виконується будь-якою особою, що має відповідний ключ. Саме тому фахівці з криптографії постійно займаються розробкою більш витончених і складних ключів. У більш безпечному шифруванні використовуються ключі високого рівня складності, тому хакери визнають процес вичерпного дешифрування (також відомого як метод «грубої сили») функціонально неможливим.

Дані можуть бути зашифровані як під час зберігання, так і під час передачі. Двома основними видами шифрування є симетричне шифрування та асиметричне шифрування. (Рисунок 1.9)

У симетричному шифруванні використовується лише один ключ, і всі сторони користуються одним і тим самим секретним ключом.

В асиметричному шифруванні використовується декілька ключів: один ключ для шифрування, а інший для дешифрування. Ключ шифрування називають «відкритим ключем», а ключ дешифрування — «закритим ключем». [7]

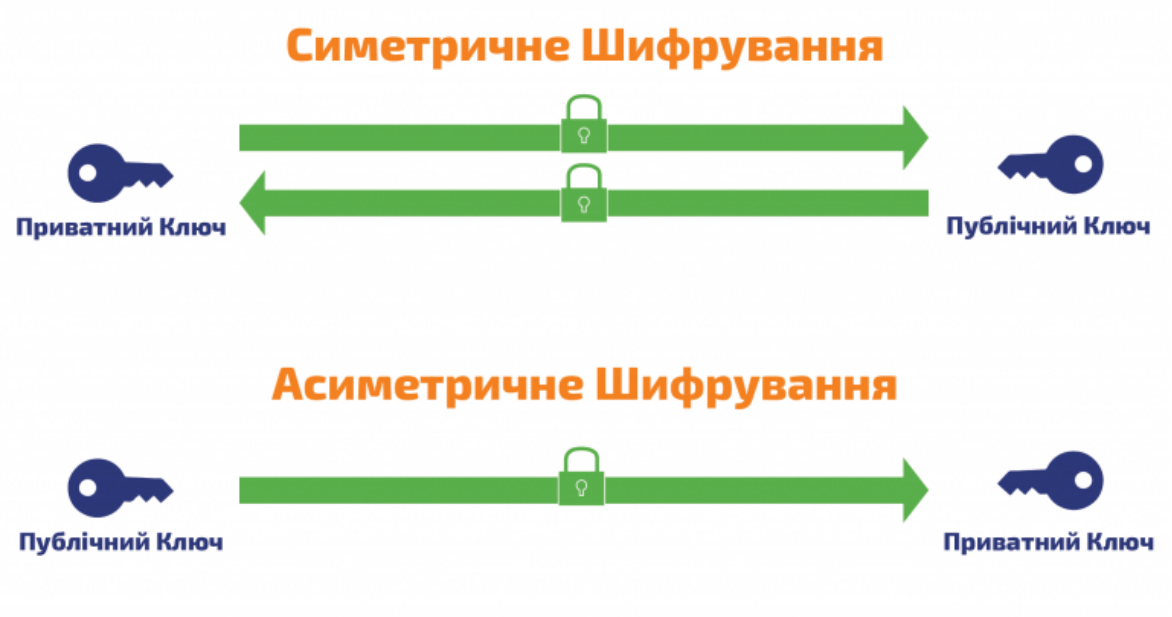

Рис. 1.9 - типи шифрування даних

Не менш важливим є моніторинг та аналітика. Зазвичай такі рішення пропонують SIEM-системи (Security Information and Event Management). Вони дозволяють постійно тримати під наглядом усі наявні кінцеві точки, проводити їх моніторинг та аналізувати поведінку. Ці рішення також дозволяють постійно проводити інвентаризацію кінцевих точок, де зберігається вся потрібна інформація починаючи від серійного номеру пристрою та закінчуючи присвоєним власником та його роллю в організації. В залежності від цих даних можуть бути налаштовані відповідні політики безпеки та доступів для різних груп користувачів та приладів. Потрібно зазначити, що і вищесказані методи захисту також мають свої налаштовані політики та групи доступів, але в залежності від типу рішення це політики, які впливають на різні речі. Що стосується SIEM-систем це зазвичай вже є комплексом рішень, який включає в себе антивірусне ПЗ, EDR, MDM (Mobile Device Management)[8].

Процес SIEM складається з 4 логічних кроків. Збір даних – це частина, де система збирає всю можливу інформацію про події в мережі. Джерелами цієї інформації є комп'ютери в мережі, сервери та мережеві засоби (наприклад, брандмауери, мережеві комутатори тощо). Крім того, SIEM може збирати інформацію

з програмного забезпечення кібербезпеки, якщо воно наявне та налаштоване для обміну даними з інформацією про безпеку та системами керування подіями. На цьому етапі формується набір даних, необхідний для подальшого аналізу[6].

Консолідація даних – це етап аналізу зібраної інформації. Щоб було зручніше як для системи, так і для спеціалістів, SIEM автоматично сортує вхідну інформацію. Потім дані групуються за категоріями та визначається кореляція подій. Цієї інформації вже достатньо, щоб зробити висновки та простежити причинно-наслідкові зв'язки. Останнє надзвичайно важливо, коли йдеться про розслідування інциденту кібербезпеки[5].

Сповіщення про події є найменш складною процедурою, оскільки вона просто передбачає певний спосіб сповіщень про заздалегідь визначені події. Спосіб і випадки надсилання цих сповіщень встановлюються під час розгортання SIEM у захищеній мережі. Ці сповіщення служать маркерами для команди з кібербезпеки про на що їм слід звернути увагу[8].

Політика дій – це список попередньо визначених станів контрольованої території за певних обставин, а також тривоги та сповіщення, які їм відповідають. Аналітики створюють так звані «профілі», які встановлюють, як виглядає та діє середовище в нормальній ситуації, а також під час звичайних інцидентів кібербезпеки. Політики потрібні, щоб SIEM міг визначати, чи система функціонує нормально чи піддається небезпеці.[9]

Рис. 1.10 - принцип роботи SIEM-систем

Application Whitelisting. Це налаштовуваний перелік програмного забезпечення, який є перевіреним та безпечним для запуску. Він дозволяє адміністраторам блокувати відоме шкідливе ПЗ, а також визначати дії при запуску програм не з довіреного списку або програм викачаних з невідомих ресурсів. Це є важливою ланкою, що не дозволить запустити програму з наявним вірусним кодом по причині недбалості співробітника. Здебільшого дана функція присутня навіть в чистих операційних системах, до прикладу ОС Windows з наявним Windows Defender та MacOS з влаштованим Gatekeeper. Але досвідчений користувач в змозі самостійно відключити ці компоненти, тому whitelisting також потрібен в сторонньому вибраному організацією рішенні, що дозволить мінімізувати втручання зі сторони користувача. Принцип роботи простий, при не виявленні окремого додатку в переліку дозволених ПЗ, наявне рішення може або з повідомленням або без примусово завершувати процес виконуваної програми[7].

Для коректного забезпечення захисту кінцевої точки, має бути присутній Patch Management. Він дозволяє постійно тримати програмне забезпечення та операційну систему на останній стабільній версії. Це актуально оскільки власники ПЗ та ОС постійно удосконалюють свої продукти для забезпечення безпеки від виявлених CVE.

На останок потрібно розглянути, постійній бесіди, нагадування зі сторони інформаційної служби безпеки до кінцевих користувачів про інформаційну гігієну. При влаштуванні співробітника потрібно в перший день проводити онбординг про загальноприйняті правила користування технікою організації, як поводити себе та реагувати на різні події. Оскільки треба розуміти, що при наявності навіть найкращого комплексу рішень з безпеки, все одно найбільшою загрозою є кінцевий користувач та його незнання або невміння, як поводити себе в мережі та у різних ситуаціях[9].

У висновку можемо сказати, що на даний момент є безліч рішень для вирішення тих чи інших проблем безпеки кінцевих точок. Потрібно постійно аналізувати та проводити інвентаризацію наявних кінцевих точок. Для найкращого захисту звісно потрібно використовувати повний комплекс захисних мір, та намагатися аналізувати наявну безпеку для її покращення. Було розглянуто одні з найважливіших аспектів захисту, які мають використовуватись у великих організаціях. Але навіть при їх використанні потрібно не нехтувати неуважністю та халатністю з боку кінцевого користувача кінцевої точки[11].

1.3 Аналіз існуючих рішень до забезпечення захисту кінцевих точок організації

Беручи до уваги все, що було описано вище не можна не зрозуміти, що ринок наявних рішень є не малим та в ньому є що запропонувати, як малим так і великим організаціям. Потрібно розуміти, що ціновий сегмент таких рішень залежить від багатьох факторів таких як: функціональність, масштабованість, підтримка хмарних технологій, наявність додаткових інструментів (наприклад, EDR, MDR), кількість кінцевих точок, а також бренд. Умовно ми можемо розділити ці сегменти на три групи: бюджетний сегмент, середній сегмент та преміум-сегмент. (Таблиця 1.1) Цей поділ відбувається виходячи з цінової політики, функцій та можливостей які надає те чи інше рішення.

Таблиця 1. 1.

Сегмент	Опис	Основні характеристики	Приклади рішень	Орієнтовна ціна
Бююжетний	Підходить для малого бізнесу або організацій з обмеженим бюджетом.	Базовий захист: антивірус, фаєрвол, антифішинг, прості інструменти керування.	Avast Business Antivirus ESET Endpoint Protection Standard	$20–40
Середній	Для середніх організацій з потребою у розширеній функціональності.	Інтеграція з SIEM, контроль додатків, виявлення аномалій, хмарне керування, підтримка EDR.	Bitdefender GravityZone Business Security Trend Micro Worry-Free Business Security-Sophos Intercept X	$40–80
Преміум	Для великих корпорацій з високими вимогами до кібербезпеки.	Повний спектр EPP+EDR функцій, захист від APT, інструменти відповідності, використання	CrowdStrike Falcon Symantec Endpoint Protection Microsoft Defender for Endpoint SentinelOne	$80–150+

Сегмент	Опис	Основні характеристики	Приклади рішень	Орієнтовна ціна
		ШІ для аналітики.		

Бюджетний сегмент. Він є ідеальним варіантом для починаючих чи невеликих організацій. Зазвичай з наявних інструментів в них є: фаєрволи, базовий захист від вірусів, антифішинг та прості елементи керування. Цінова політика варіюється в межах 20-40 на рік. Для прикладу ми можемо привести: Avast Business Antivirus, ESET Endpoint Protection Standart[8].

Середній сегмент. Чудово підходить для організацій яким потрібен розширений функціонал, та ті які вже мають в рази більшу кількість кінцевих точок. Загалом по функціоналу, вони мають всі базові можливості та вже дозволяють проводити інтеграції з SIEM-системами задля більш згрупованого контролю кінцевих точок. Такі рішення також вже надають можливість хмарної реалізації, що допомагає тримати систему контроля ізольовано від всієї мережі та дозволяє завжди вчасно отримувати всі актуальні патчі безпеки та функціоналу. В таких рішеннях вже присутня функція EDR. З них можна виділити наступні приклади: Bitdefender GravityZone Business Security, Trend Micro Worry-Free Business Security. Зазвичай ціна варіюється в межах $40-80 за кінцеву точку[8].

Преміум сегмент. Є актуальним для великих організацій де потреби у високотехнологічних засобах з кібербезпеки є вже вимушеною та необіхдною мірою. Основні характеристики це повний спектр EPP+EDR функцій, захист від цільових атак, інструменти для управління відповідністю, використання ШІ для аналітики. Для прикладу можна привести: CrowdStrike Falcon, Symantec Endpoint Protection. Приблизна ціна таких рішень $80-150+ за кінцеву точку на рік.

Потрібно розуміти, що це все варіюється від декількох факторів. Наявність функціоналу є одним з ключовим оскільки треба підбирати план, який буде найбільше

підходити до кінцевої організації. Всі організації мають різну кількість кінцевих точок, різну інфраструктуру та різні потреби.

ExpertInsights вже виділив найкращі рішення з захисту кінцевих точок на 2024 рік[8].

1. ESET Endpoint Security;
2. Heimdal DNS Security Endpoint;
3. Avast Small Business Solutions;
4. ThreatLocker Protect;
5. Bitdefender GravityZone Small Business Security;
6. Check Point Harmony Endpoint;
7. Crowdstrike Falcon Endpoint Protection Pro;
8. Trellix Endpoint Security Suite;
9. Microsoft Defender for Endpoint;
10. SentinelOne Singularity for Endpoint;
11. Broadcom Symantec Endpoint Security.

Рішення для захисту кінцевих точок контролюють усі пристрої та автоматично усувають інциденти безпеки. Вони дозволяють адміністраторам керувати всіма пристроями з єдиної адміністративної консолі та поглиблено досліджувати складні загрози з можливістю виконання заходів з їх усунення[8].

Ринок безпеки кінцевих точок сьогодні надзвичайно переповнений. На ринку представлені десятки постачальників з різними технологіями та підходами, покликаними запобігти проникненню загроз на ваші корпоративні пристрої[8].

Виходячи з усього вищесказаного можна зробити висновок, що станом на 2024 рік, на ринку присутні безліч рішень для забезпечення якісного захисту кінцевих точок організацій. Вони є різних сегментів та містять в собі багатий функціонал, який певні організації можуть використовувати в залежності від своїх потреб та можливостей.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ НА БАЗІ BITDEFENDER GRAVITY ZONE BUSINESS SECURITY

2.1 Призначення та огляд Bitdefender GravityZone Business Security

В цій науковій роботі буде розглянуто рішення для забезпечення безпеки кінцевих точок організації Bitdefender Gravity Zone Business Security(Рисунок 2.1). Саме рішення для бізнес сектору є найбільш наповненим різноцінним функціоналом та забезпечую найбільший захист кінцевих точок, а також здатне керувати великою інфраструктурою.

Рис. 2.1 - Bitdefender GravityZone Business Security

Вибір саме цього рішення був обгрунтований після дослідження теми «Актуальність багаторівневого захисту кінцевих точок для забезпечення кібербезпеки

організацій». Тут описана як і актуальність проблеми так і алгоритми, рішення та технології для сучасного кіберзахисту[10].

Актуальність багаторівневого захисту кінцевих точок для кібербезпеки організації зростає в умовах постійно змінюваного ландшафту кіберзагроз. Кінцеві точки, такі як комп'ютери, мобільні пристрої та сервери, є вразливими місцями, через які можуть бути здійснені атаки на корпоративні мережі. Традиційні методи захисту, включаючи антивірусне програмне забезпечення та брандмауери, часто виявляються недостатніми для протидії новим, більш складним загрозам[10].

Тому перше, що можна виділити це багаторівневий підхід до захисту. Комплексні системи безпеки інтегрують різні технології для забезпечення захисту від різноманітних типів кіберзагроз[10]. Це включає в себе:

- Аналіз поведінки користувачів (UEBA). Ця технологія дозволяє виявляти аномальні дії, що можуть свідчити про інсайдерські загрози або компрометацію облікових записів[10].

- Машинне навчання (ML). Використання ML дозволяє системам адаптуватися до нових загроз, зменшуючи кількість помилкових спрацьовувань і підвищуючи точність виявлення атак[10].

- Інтеграція з SIEM. Системи управління інформацією та подіями безпеки (SIEM) забезпечують централізований моніторинг та аналіз подій безпеки в реальному часі, що дозволяє швидко реагувати на загрози[10].

Наступне це стратегії захисту кінцевих точок. Серед сучасних стратегій для зміцнення захисту кінцевих точок можна виділити:

- Архітектура Zero Trust. Цей підхід передбачає постійну перевірку всіх запитів на доступ до ресурсів, незалежно від їхнього джерела. Це значно знижує ризик несанкціонованого доступу[10].

- Розширене виявлення та реагування (XDR). XDR інтегрує дані з різних джерел для покращення виявлення загроз і реагування на них, що дозволяє швидше реагувати на атаки[10].

- Керування привілеями кінцевих точок (EPM). Ця стратегія базується на принципі найменших привілеїв, що обмежує доступ користувачів до необхідного мінімуму[10].

Також потрібно виділити необхідність дотримання міжнародних стандартів безпеки. А саме те, що дотримання міжнародних стандартів безпеки, таких як ISO/IEC 27001 та ISO/IEC 27002, є невід'ємною частиною ефективної стратегії захисту. Ці стандарти допомагають організаціям створити структуровану систему безпеки відповідно до найкращих міжнародних практик[10].

Виходячи з усього вищесказаного можемо зробити висновок про те, що рішення Bitdefender GravityZone Business Security має багато сучасних технологій та відповідає міжнародним протоколам безпеки.

Це рішення є хмарним, а отже має певні переваги та недоліки. З переваг ми можемо виділити:

- Швидкість розгортання, що мінімізує час який потрібен працівникам з кіберзахисту для початку роботи з рішенням;
- Наступне це дистанційне управління, що дозволяє отримати доступ до управлінської консолі з любої точки світу. Це може бути корисним при великій та розподіленій інфраструктурі компанії;
- Серед іншого це актуалізація та підтримка, що означає що оновлення самого рішення виконує провайдер, а отже фахівці з кіберзахисту використовують постійно актуальні версії продукту;
- Також потрібно зазначити зниження витрат на розгортання, оскільки компанії вже не потрібно витрачатися на сервери та іншу інфраструктуру;
- Не можна не сказати про інтеграцію з іншими хмарними сервісами, це можуть бути як SIEM, MDM, AzureAD та безліч інших рішень, які в сукупності створюють великий «щит» захисту;

- Не потрібно перейматися через збереження великих баз даних з кінцевими точками, оскільки провайдер який надає послугу постійно забезпечує резервне копіювання та швидкий доступ до своїх сервісів.

Із недоліків ми можемо виділити наступне:

- Залежність від інтернет-з’єднання. Адже погана якість або відсутність мережі частково або повністю унеможливлюють керування та моніторинг;
- Конфіденційність. Одне з найголовнішого про що хвилюються великі компанії це саме те, що всі дані зберігаються на серверах провайдера, що ставить під сумнів повну конфіденційність організації та її інфраструктури;
- Обмежений контроль. Все ж таки компанія має більш шаблонний та спрощений функціонал керування своїми пристроями та немає таких великих налаштувань;
- Збільшення витрат при обсягах. Зазвичай ліцензії та договори з провайдерами надаваючими хмарні рішення залежить від кількості кінцевих точок що в свою чергу при різкому рості компанії та збільшенні пристроїв призводить до зростання вартості використання рішення;
- Загроза компрометації. Розуміє під собою те, що якщо провайдер який надає послуги організації сам стає об’єктом кібератаки автоматично ставить під ризик всіх їх клієнтів, що буде мати дуже фатальні наслідки.

Ціль Bitdefender GravityZone Business Security полягає в забезпеченні ефективного, комплексного захисту кінцевих точок (endpoints) в організаціях. Це рішення створене для попередження, виявлення та реагування на кіберзагрози, зберігаючи продуктивність систем і спрощуючи управління інформаційною безпекою. Із основних її цілей можемо виділити наступне:

- Захист кінцевих точок. Забезпечення захисту серверів, ПК, ноутбуків, мобільних пристроїв і віртуальних середовищ від загроз, таких як віруси, руткіти, програми-вимагачі, експлойти та інше;

- Превентивний захист. Використання технологій штучного інтелекту, машинного навчання та поведінкового аналізу для попередження атак ще до їхнього здійснення;
- Інтегроване управління. Надання єдиної консолі для централізованого управління захистом усіх кінцевих точок організації, що спрощує адміністрування;
- Зниження ризиків та підвищення стійкості до атак. Реалізація функцій попередження вторгнень, виявлення аномалій та автоматизованої реакції на інциденти безпеки;
- Економія ресурсів та зниження складності;
- Оптимізація використання системних ресурсів кінцевих точок для збереження їх продуктивності. Скорочення необхідності використання кількох розрізнених рішень завдяки інтегрованому підходу;
- Гнучкість впровадження. Можливість вибору між хмарним розгортанням або локальним сервером для забезпечення відповідності інфраструктури організації[10].

Наступним розглянемо технології які містить в собі Bitdefender Gravity Zone Business Security. Оскільки на даний момент компанія рухається в сучасному напрямку, то перелік технологій також великий. Можемо виділити наступне:

- Штучний інтелект (ШІ) та машинне навчання (ML). Використовуються для прогнозування та виявлення нових загроз. Аналіз великих обсягів даних з різних джерел дозволяє ідентифікувати аномалії та підозрілу поведінку в реальному часі. Моделі постійно самонавчаються, адаптуючись до нових типів атак;
- Аналіз поведінки (Behavioral Analysis). Відстежує дії програм і процесів на кінцевих точках для виявлення шкідливих патернів, які не можуть бути виявлені за допомогою сигнатурного методу. Захищає від атак типу zero-day та експлойтів;
- Захист від програм-вимагачів (Ransomware Mitigation). Використовує спеціалізовані технології для виявлення підозрілих змін у файлах, що характерні для

атак програм-вимагачів. Включає функцію резервного копіювання та відновлення пошкоджених файлів;

- Сигнатурний і евристичний аналіз. Традиційний метод визначення шкідливого програмного забезпечення на основі бази даних сигнатур. Евристичний аналіз дозволяє виявляти невідомі загрози на основі загальних характеристик коду;
- Модуль запобігання вторгненням (HIPS). Моніторить активність системи для виявлення вторгнень, спрямованих на обхід стандартних засобів безпеки. Забезпечує багаторівневий захист від атак на рівні операційної системи;
- Виявлення та реагування на кінцевих точках (EDR). Виявляє складні та багатовекторні атаки, які можуть бути пропущені традиційними засобами. Забезпечує детальний аналіз інцидентів і інструменти для автоматичної або ручної реакції;
- Захист від мережевих атак. Виявляє та блокує загрози на рівні мережевих підключень, включаючи атаки через відомі уразливості. Захищає від технік, таких як brute force, сканування портів або MITM-атаки;
- Захист електронної пошти. Фільтрація спаму, фішингових листів та шкідливих вкладень. Інтеграція з поштовими сервісами для запобігання поширенню загроз через електронну пошту;
- Розширене управління пристроями. Забезпечує контроль доступу до периферійних пристроїв (USB, Bluetooth, принтери). Допомагає уникнути витоку даних через незахищені пристрої;
- Антифішинг та веб-фільтрація. Аналізує веб-сайти в реальному часі, щоб запобігти доступу до фішингових ресурсів або шкідливих веб-сторінок. Контролює веб-трафік і блокує небезпечні ресурси;
- Пісочниця (Sandboxing). Підозрілі файли запускаються в ізольованому середовищі для безпечного аналізу їхньої поведінки. Використовується для виявлення складних і прихованих загроз;

- Захист від атак через експлойти. Виявляє та блокує спроби використання уразливостей у програмному забезпеченні. Запобігає атакам, спрямованим на уразливості браузерів, плагінів, ОС чи додатків;
- Централізоване управління. Єдина консоль управління (GravityZone Control Center) дозволяє керувати політиками безпеки, моніторити стан кінцевих точок і реагувати на інциденти;
- Інтеграція з SIEM і SOAR. Підтримує інтеграцію з платформами для моніторингу та автоматизації безпеки, що дозволяє використовувати дані про загрози в ширшому контексті;
- Оптимізація продуктивності. Ефективне використання системних ресурсів завдяки легкому агенту та хмарним обчисленням. Мінімальний вплив на роботу кінцевих пристроїв[10].

На основі проведеного аналізу можна стверджувати, що Bitdefender GravityZone Business Security є потужним та інноваційним рішенням для забезпечення багаторівневого захисту кінцевих точок організацій. Це рішення інтегрує передові технології, такі як штучний інтелект, машинне навчання, аналіз поведінки та захист від програм-вимагачів, що дозволяє досягти високого рівня кібербезпеки навіть за умов динамічного розвитку кіберзагроз[11].

Серед значних переваг варто відзначити інтегрований підхід до управління безпекою, який спрощує адміністрування завдяки єдиній консолі та можливості централізованого моніторингу. Використання хмарної інфраструктури забезпечує швидке розгортання, доступність з будь-якої точки світу та автоматичну актуалізацію системи. Крім того, Bitdefender GravityZone дозволяє ефективно управляти ризиками, інтегруючись із SIEM і SOAR системами, що створює широку екосистему захисту.

Проте поряд із перевагами існують і недоліки, характерні для хмарних рішень. Серед них – залежність від стабільності інтернет-з’єднання, обмежений контроль над конфіденційністю даних та потенційна загроза компрометації у разі атаки на

інфраструктуру провайдера. Також варто враховувати, що вартість рішення може зростати зі збільшенням кількості кінцевих точок у компанії[12].

Отже, Bitdefender GravityZone Business Security є оптимальним вибором для організацій, які потребують комплексного захисту кінцевих точок, зручності управління та відповідності сучасним стандартам кібербезпеки. Це рішення особливо підходить для великих і розподілених інфраструктур, де необхідно забезпечити надійний і масштабований захист.

2.2 Огляд та знайомство з центром керування Bitdefender GravityZone Business Security

Для огляду даного рішення було проведено перемовини з представниками Bitdefender Gravity Zone Business Security та отримано доступ до Trial Version цього продукту. Дана версія має повний функціонал та призначена для ознайомлення з цим продуктом. На період дії trial version спеціалісти з тех. підтримки завжди готові допомогти з налаштуваннями та навіть у проведенні навчання в цілях ознайомлення. Відразу при оформленні даної версії адміністратор отримує обліковий запис та його зустрічає логін-меню Bitdefender Gravity Zone Business Security центру контролю (Рисунок 2.2).

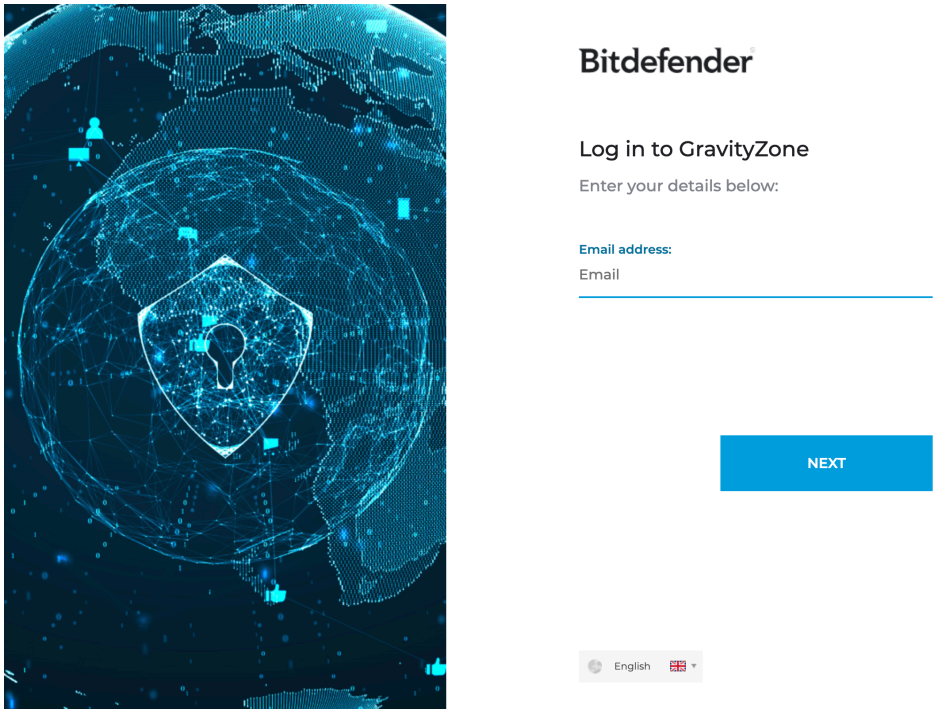

Рис. 2.2 - логін меню Bitdefender Gravity Zone Business Security

Відразу після авторизації, адміністратора зустрічає головне меню в якому міститься корисна інформація, відразу пропонується виконати певні алгоритми дій. Зліва міститься діалогове меню вибору звідки адміністратор може перейти в різні меню для моніторингу або налаштування. У верхньому правому кутку міститься панель в якій можна переглянути сповіщення, перейти в налаштування аккаунту, зв’язатися з тех. підтримкою. Пропонується відразу створити інсталяційний файл агенту Bitdefender Gravity Zone Business Security. Спробувати функції, які тільки розробляються та готуються для впровадження. Можемо відразу бачити різні меню такі, як Monitoring, Threats Xplorer, Network, Risk management, Policies, Reports. Багато з них мають свої під-меню з ще більшою кількістю опцій (Рисунок 2.3).

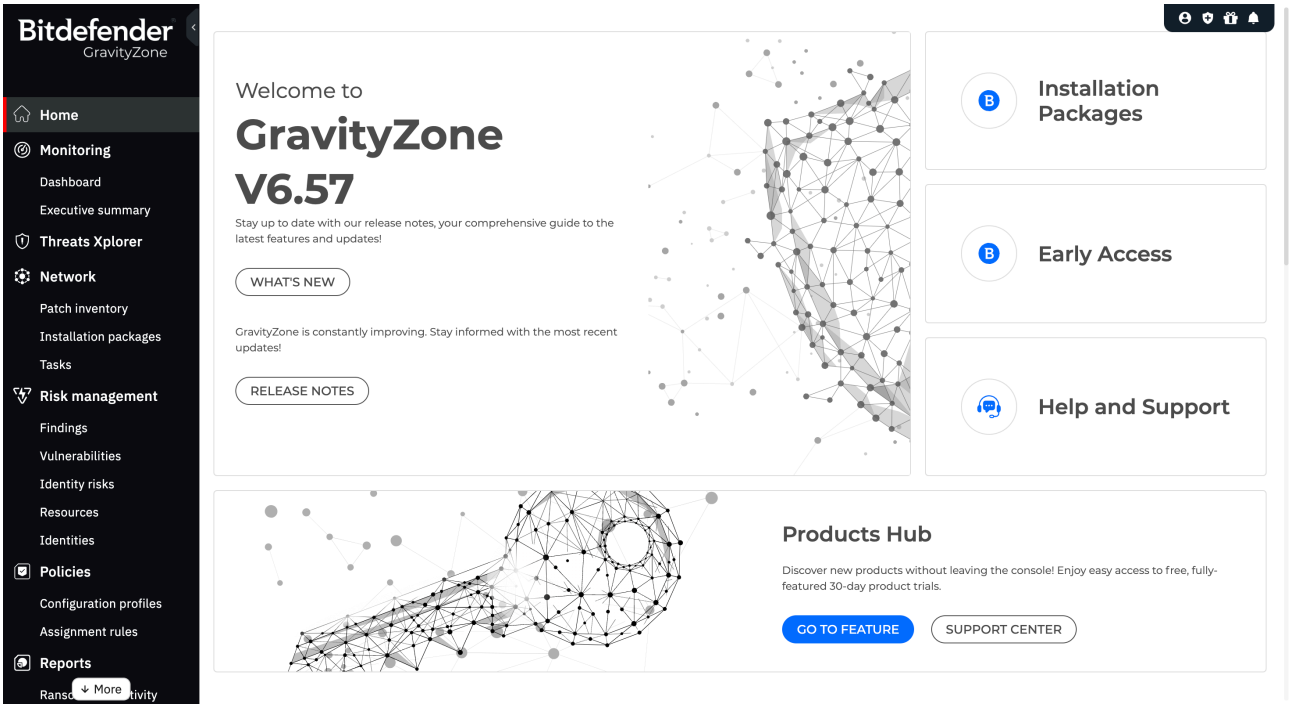

Рис. 2.3 - головне меню Bitdefender Gravity Zone Business Security

Переходячи у вкладку Monitoring, яка є повністю готовою для редактування, адміністратор з вже готовою інфраструктурою може бачити безліч діаграм та списків з корисною інформацією. По стандарту відразу можемо бачити діаграму Security Audit, що дозволяє бачити, які вразливості та типи вразливостей були виявлені, що дозволяє швидко оцінити ситуацію та продумати наступні дії. Після цієї діаграми можна спостерігати Computers- Malware Status, що показує кількість пристроїв, на яких були виявлені вразливості. Тут також відразу присутня опція сканування уражених кінцевих точок. Трохи нижче наступними йдуть дві діаграми, які показують час та кількість заблокованих додатків та веб-ресурсів. Ці ресурси та додатки визначає адміністратор центру керування за допомогою політик безпеки, які застосовуються до потрібних кінцевих точок (Рисунок 2.4).

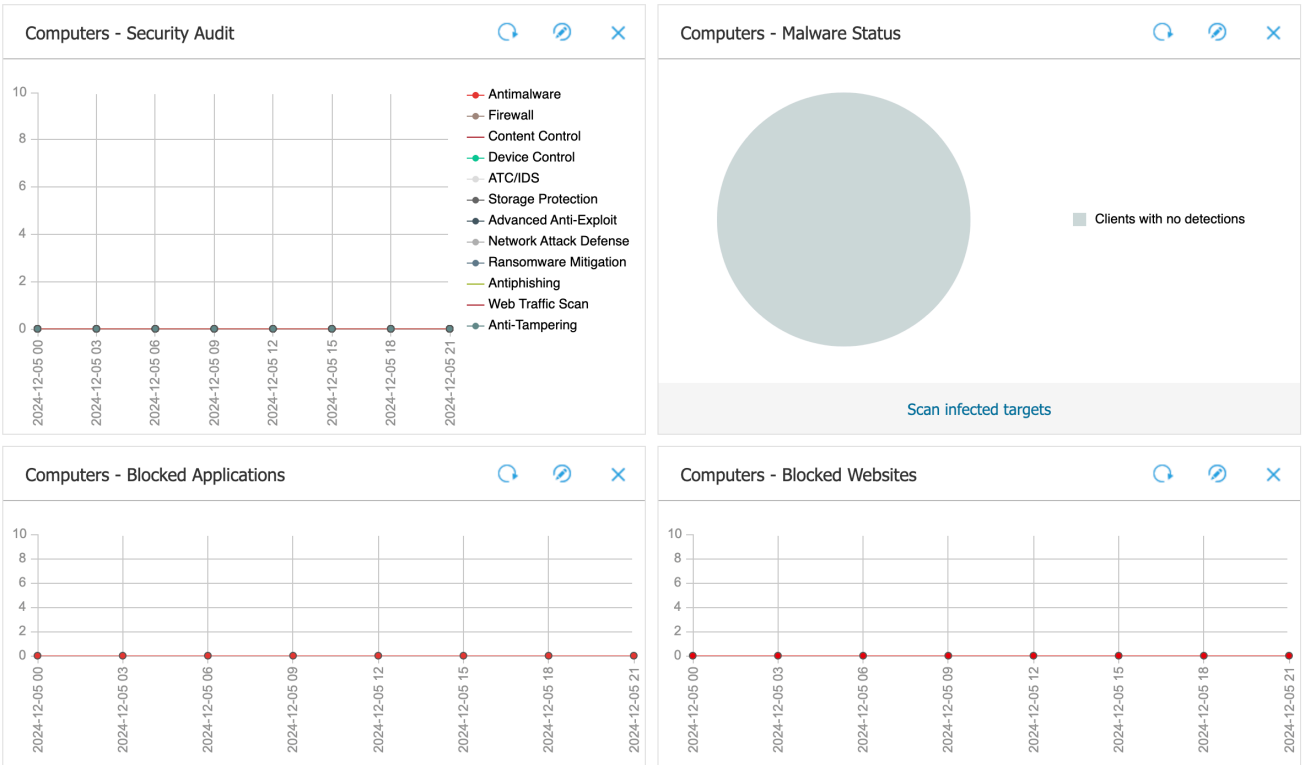

Рис. 2.4 - діаграми Malware Status, Malware Status, Blocked applications and websites

Пролистнувши сторінку до низу можна також спостерігати наступні діаграми:

- Computers – Endpoint Protection Status. Діаграма, яка дозволяє в реальному часі переглянути статус усіх кінцевих точок. Має інформацію, про те чи пристрій онлайн, чи він керується на даний момент, статус оновлення та захисту від загроз (Рисунок 2.5);
- Computers – Update Status. Діаграма, яка більш детально показує демонструє про оновленість кінцевих точок, тобто останньої ОС, версії агенту та додатків (Рисунок 2.5);
- Computer – Policy Appliance. Демонструє на скількох точках було успішно та навпаки невдало примінено налаштовані політики (Рисунок 2.5).

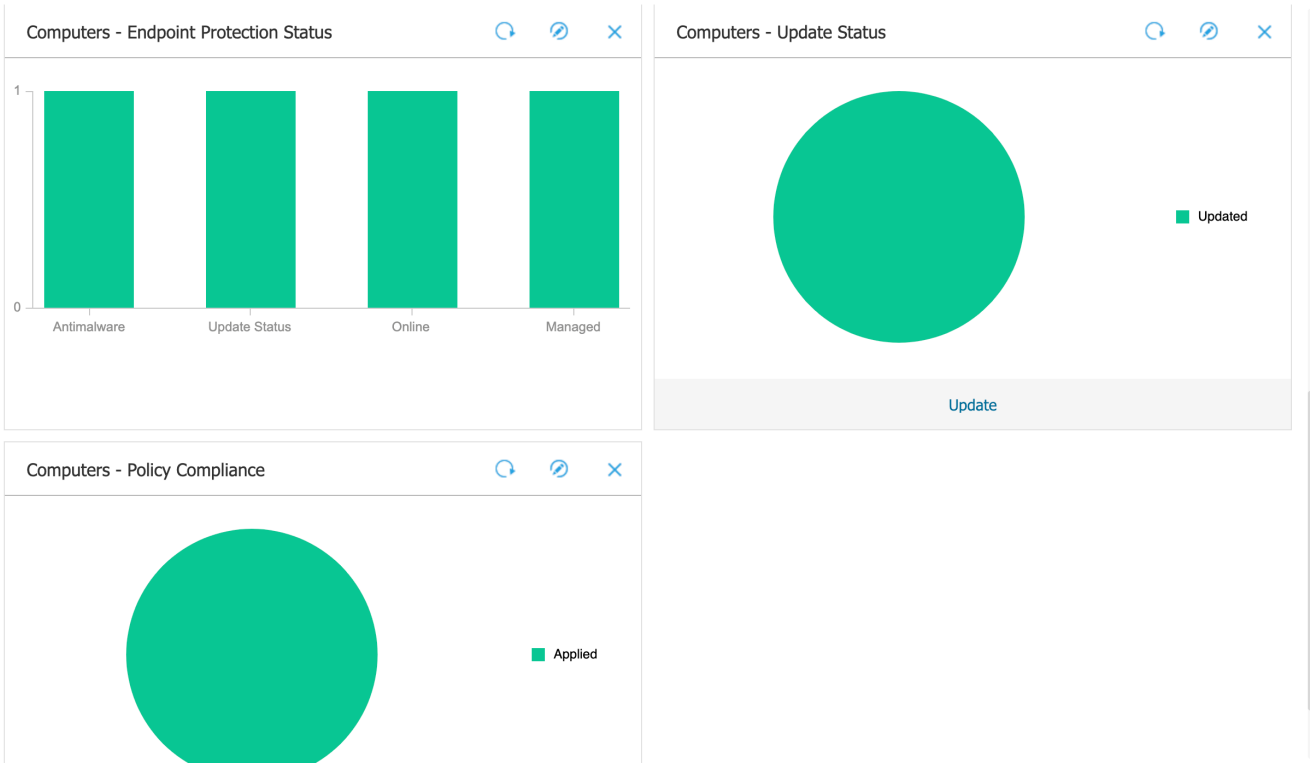

Рис. 2. 5 - діаграми Computer – Policy Appliance, Computer – Update Status та Computers - Endpoint Protection Status

Наступне меню, що використовується також часто фахівцями кібербезпеки це Threat Xplorer. Це оглядач виявлених за весь час вразливостей, який надає повну інформацію за конкретним запитом, та має безліч фільтрів для сортування. Також дозволяє експортувати отриману інформацію в xlsx та XML формати для зручності редагування чи формування звітів. Має опцію пошуку за конкретною датою або проміжком часу, що допомагає в пошуку. Має фільтр для пошуку за типом вразливостей, що в свою чергу також допомагає у формуванні звітів по знайденим вразливостям конкретного типу. Звісно відразу наявний статус рішення яке було прийнято, це можуть бути знешкодженні, ізольовані або дозволені події виявлені агентом на конкретній кінцевій точці. При відкритті додаткового меню, адміністратор має змогу також додати й інші поля для виводу та сортуванню інформації, зокрема інформацію про назву кінцевої точки, обліковий запис користувача, IP адресу, тип кінцевої точки, назву вразливості, якщо вона є (Рисунок 2.6).

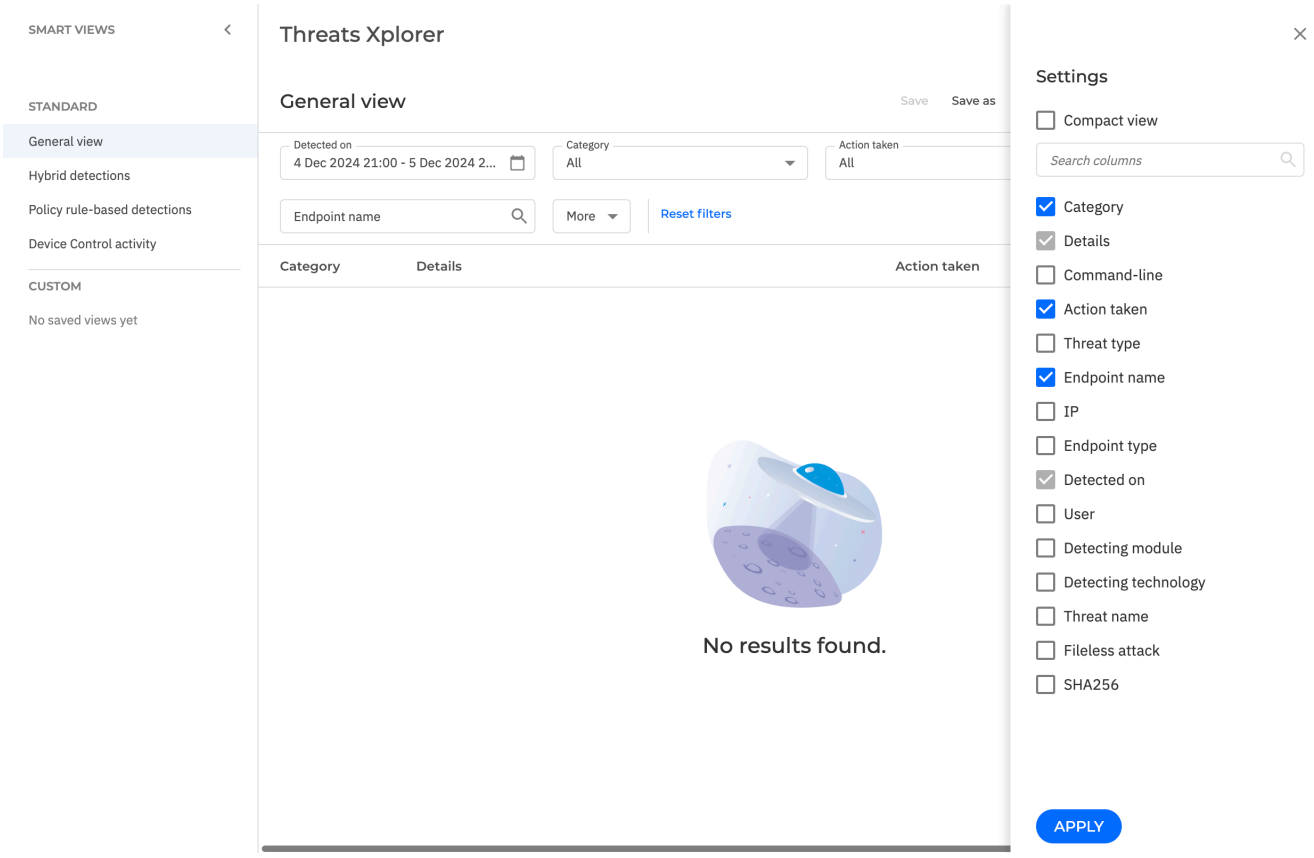

Рис. 2.6 - меню Threat Xplorer

Не менш важливою є наступна вкладка функцій, а саме Network. Вона детально демонструє весь парк кінцевих точок наявних в інфраструктурі організації. Саме тут є можливість налаштувати групи пристроїв в залежності від відділів, призначення, позицій та інших бажаних критеріїв користувачів та кінцевих точок. При наявності знайдених вразливостей можна також спостерігати, які саме пристрої були уражені, або в яких є певні не вирішені питання. На верхній панелі містяться корисні функції, які дозволяють адміністратору, зробити швидкий звіт про вибрані кінцеві точки, поставити завдання в чергу на опрацювання, застосувати створені політики, або заблокувати чи стерти кінцеву точку (Рисунок 2.7).

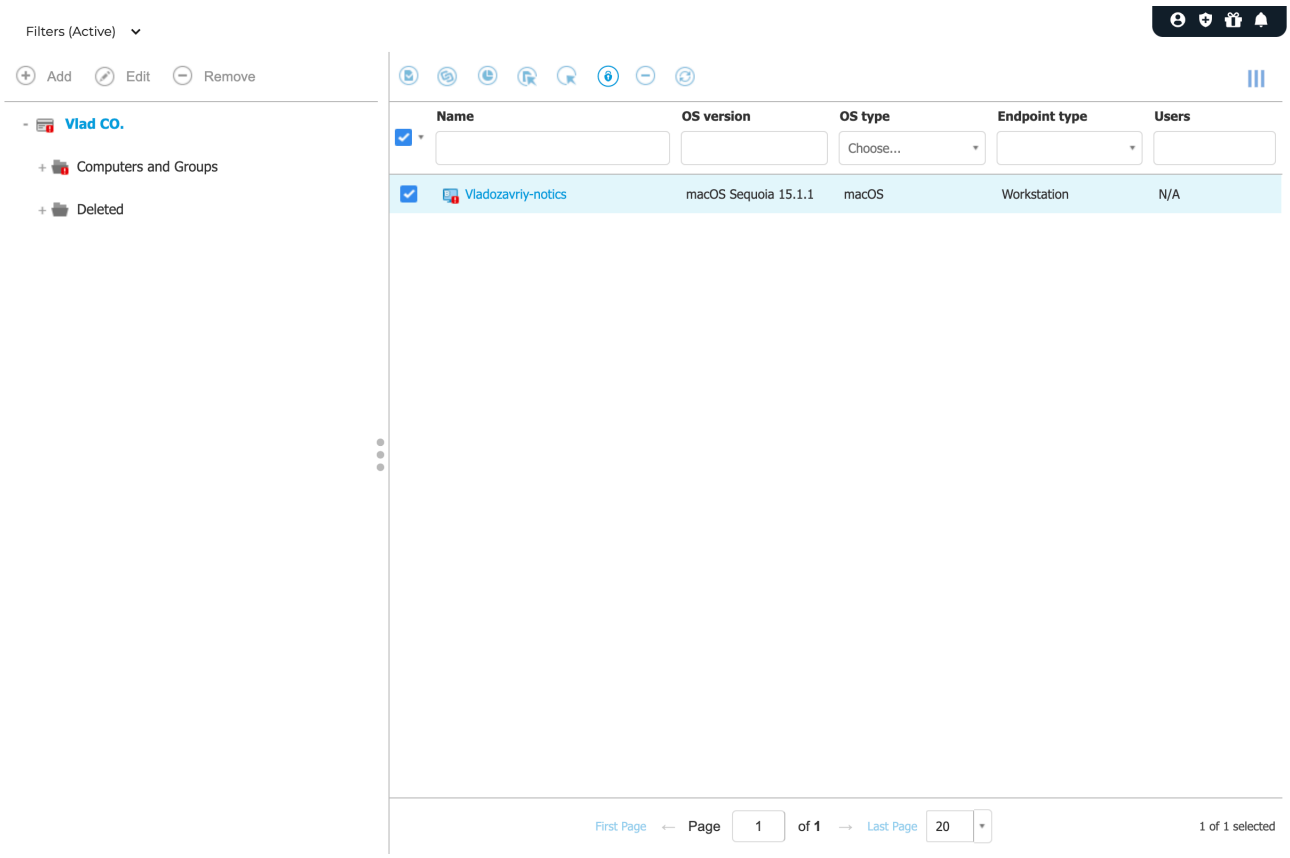

Рис. 2.7 - панель функцій Network

Наступна вкладка функцій під назвою Risk management має також велику користь, та є так званим центром прийняття рішень, оскільки повністю аналізує створену інфраструктуру, кінцеві точки та знайдені в них вразливості. Все це сукупно показує загальний фактор вразливості мережі та кінцевих точок, демонструє це все у відсотках. Містить корисні діаграми, які дозволяють бачити кількість знайдених вразливостей за певний проміжок часу, демонструє степінь вразливості по конкретним групам, додатки, веб-сайти та інше (Рисунок 2.8).

Містить в собі безліч підфункцій, корисна є вкладка Findings де можна бачити знайдені вразливості як самостійно так і в цілому спільнотою фахівців кз кібербезпеки та провайдером рішення (Рисунок 2.9). Та схожі вкладки де можна переглянути актуальні проблеми з кібербезпеки, ризики ідентифікації і т. д.

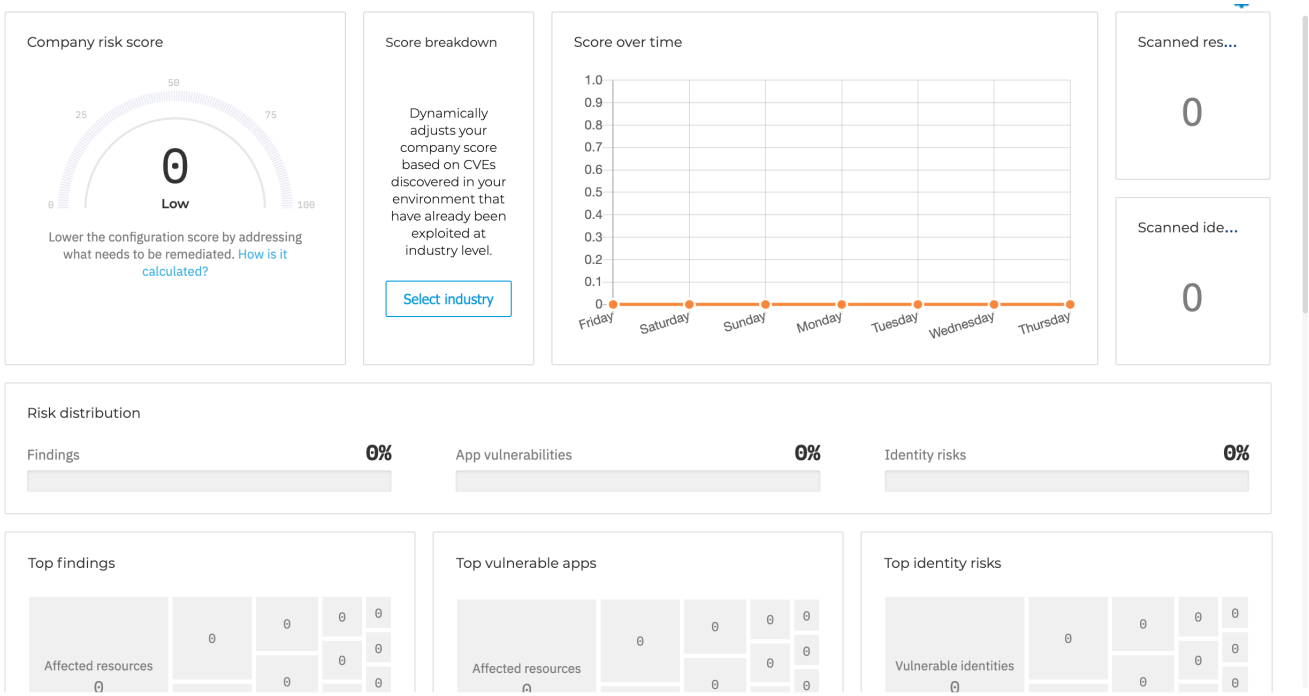

Рис. 2.8 - панель функцій Risk Management

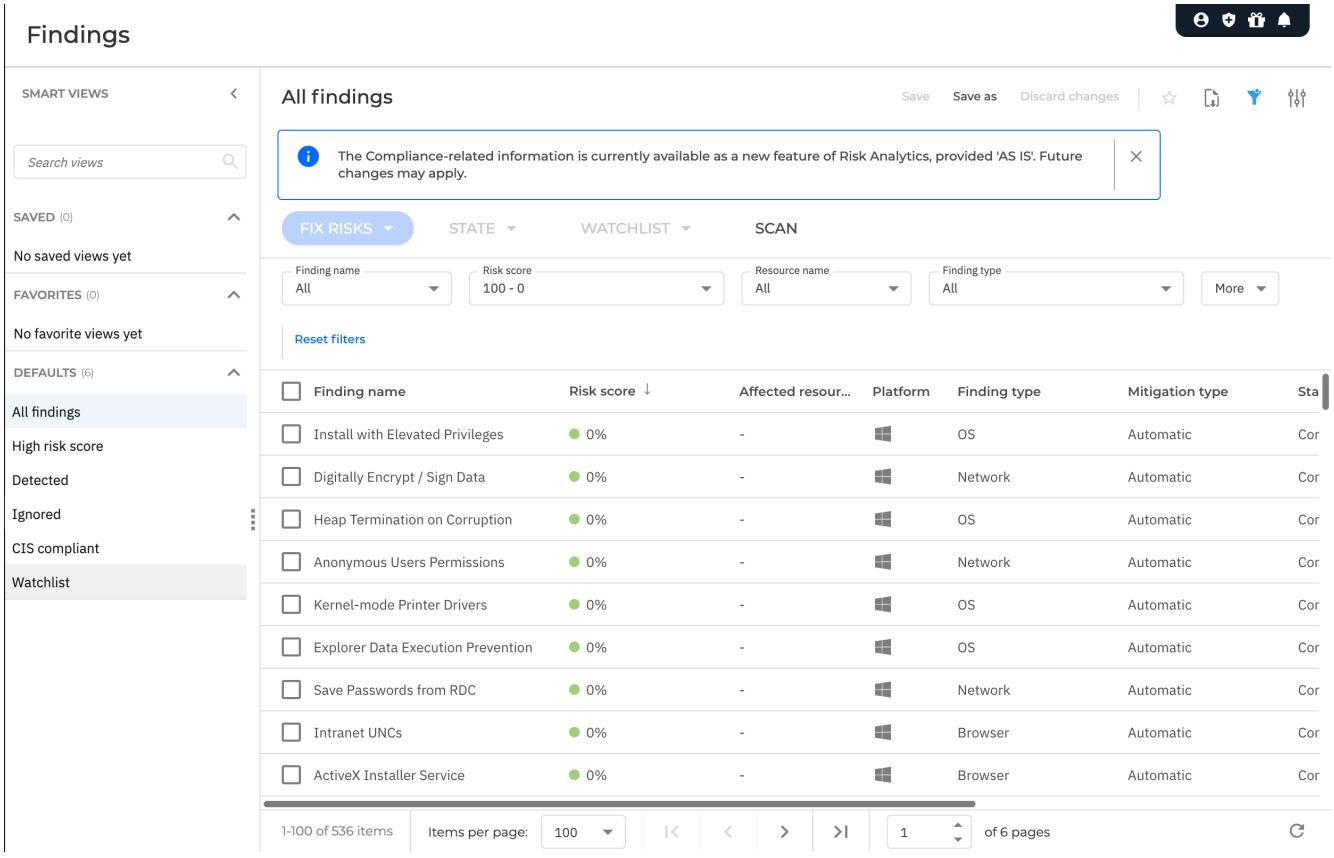

Рис. 2.9 - панель функцій Findings

Наступною та однією з найважливіших панелей меню є Policies. Ця група функцій дозволяє налаштувати групові політики, обмеження веб-сайтів, програм та іншого на всіх або конкретних кінцевих точках. Це є одна з найбільш доцільним опцій для влаштування якісної безпеки кінцевих точок в мережі організації. Меню є максимально зручним в якому є можливість створення, видалення або редагування політик (Рисунок 2.10).

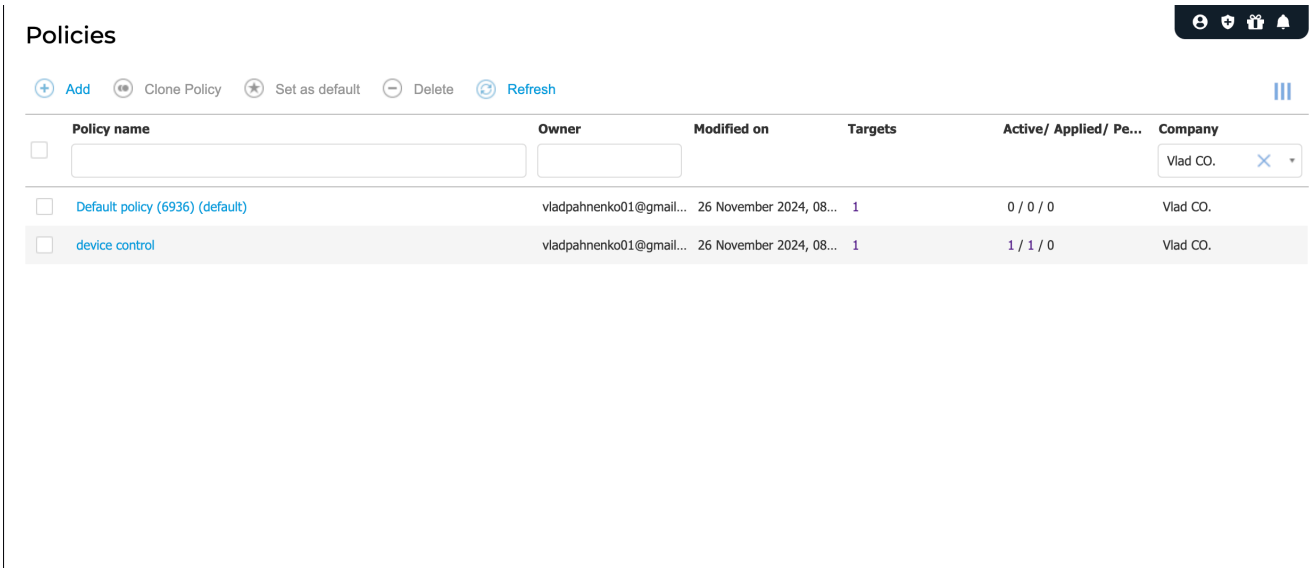

Рис. 2.10 - меню функцій Policies

При створенні нової політики ми маємо обширну панель з великою кількістю опцій, які дозволяють налаштувати дуже детально захист кінцевих точок. Зазвичай все не обмежується однією політикою, а їх кількість варіюється від типів кінцевих точок, департаментів та посад співробітників організації. Для налаштовування представлено функції антивірусного захисту, що дозволяє відслідковувати на кінцевій точці вразливості, експлойти та інші загрози для пристрою; велике меню для налаштування фаєрволу та захисту в інтернеті, що дозволяє блокувати вихід у всесвітню мережу Інтернет та відслідковувати діяльність кінцевої точки в браузерах. Контроль пристроїв дозволяє також сканувати знімні носії, Bluetooth та інші під'єднуванні пристрої задля вбереження кінцевої точки від можливих загроз. Важливим також є примусове шифрування кінцевої точки, що навіть при фізичній втраті кінцевої точки дозволяє вберегти конфіденційну інформацію. Звісно треба

розуміти, що ці функції можливо застосувати лише при встановленосу агенті Bitdefender на кінцевій точці (Рисунок 2.11).

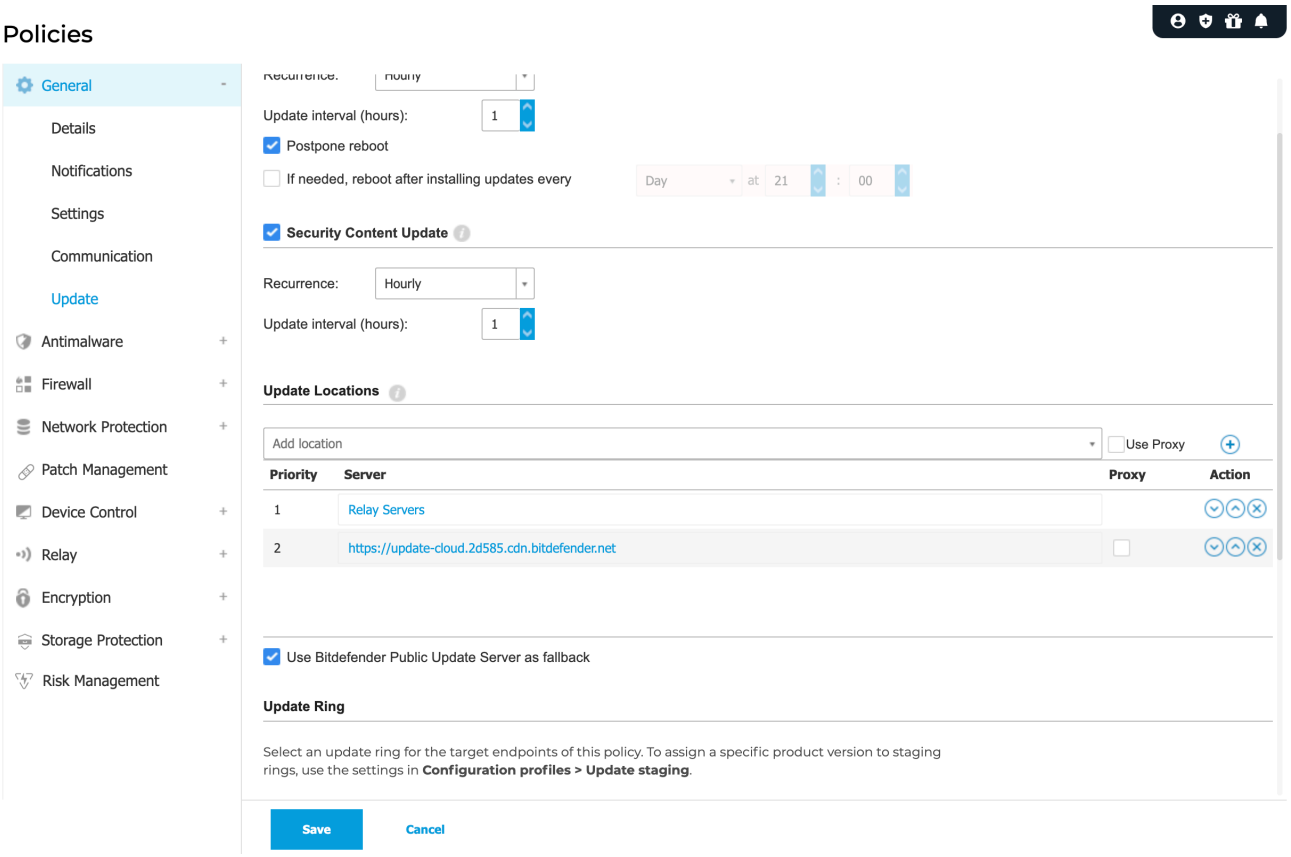

Рис. 2.11 - меню налаштування нової політики

Серед усього іншого присутні меню Reports, Quarantine, Accounts, Email security, Mobile security та Configuration (Рисунок 2.12). Про них можливо сказати наступне:

- Reports. В цій групі меню, можливо створити та переглянути з подальшим збереженням звітів про безпеку в залежності стандартів;
- Quarantine. Група меню, яка демонструє знайдені вразливості та шкідливі програми, які потрапили в карантин та потребують більш детального огляду зі сторони фахівця з кібербезпеки;
- Accounts. Група меню в якій створюються інші облікові записи адміністраторів, які можуть мати лише певні функції;

- Email Security. Група меню, яка дозволяє налаштувати захист корпоративних поштових адресів компанії, шляхом відстеження потенційно вразливих листів та дій користувача;
- Mobile Security. Група меню, яка контролює кінцеві точки у вигляді мобільних пристроїв;
- Configuration. Меню, яке дозволяє створити налаштування саме центру керування Bitdefender GravityZone Business Security.

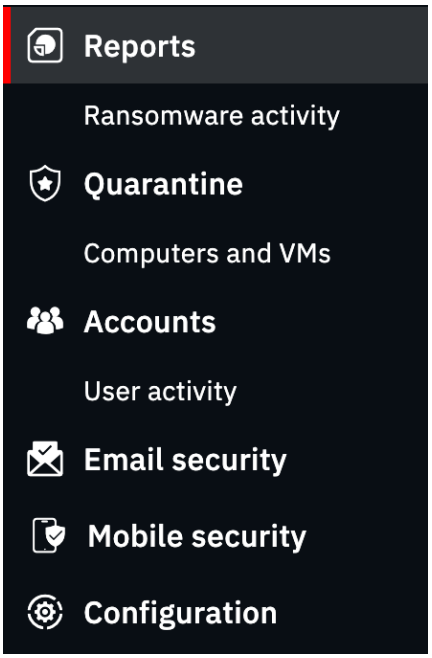

Рис. 2.12 - інші групи меню Bitdefender GravityZone Business Security

У висновку можна сказати наступне, що після огляду на функціонал та інтерфейс рішення з безпеки кінцевих точок організації Bitdefender GravityZone Business Security має великий функціонал та багатогранність в налаштування чудового захисту. Подання інформації для адміністратора відбувається у зручному поданні. Налаштування не потребують великих зусиль та фахівець з кібербезпеки, який в перше працює з цим рішенням зможе розібратися в короткі терміни. Оглянуто чудове поєднання технологій з захисту кінцевих точок. Оглянуто великий набір статистичних можливостей, що дозволяє фахівцям з кібербезпеки завжди опрацьовувати актуальну інформацію.

2.3 Дослідження можливостей використання рішення Bitdefender GravityZone Business Security

Bitdefender GravityZone Business Security має великий спектр послуг, технологій та функцій, що допоможе адміністратору в зоні кібербезпеки вести централізований та контрольований захист кінцевих точок в інформаційній системі організації.

Bitdefender GravityZone Business Security є мультиплатформеним, що дозволяє налаштовувати різні за типом кінцеві точки та за використовуваною ОС на ній. Рішення підтримує наступні ОС: Windows, MacOS, Linux та мобільні пристрої на базі ОС Android та IOS. Це дозволяє адміністраторам працювати за одним шаблоном для різних пристроїв та не робити виключень, які можуть призвести до можливих загроз.

Розгортання Bitdefender GravityZone Business Security відбувається шляхом встановлення спеціального агента на кінцеву точку, або встановлення додатку на мобільний пристрій. В центрі керування фахівець з кібербезпеки може створити відповідний інсталятор агента. Є варіант вже зібраного інсталятора з усіма компонентами, або спрощений варіант де актуальний агент викачується безпосередньо на кінцевій точці (Рисунок 2.13). Варіант розгортання вручну це коли системний адміністратор при налаштуванні кінцевої точки встановлює агент Bitdefender GravityZone Business Security за відповідною вказівкою служби безпеки. Більш легким та автоматизованим варіантом є суміжне використання рішень MDM, що дозволяє розгортати агент в режимі Pre-Enroll, тобто без фізичного втручання адміністраторів, а лише при наявному інтернет з’єднанні.

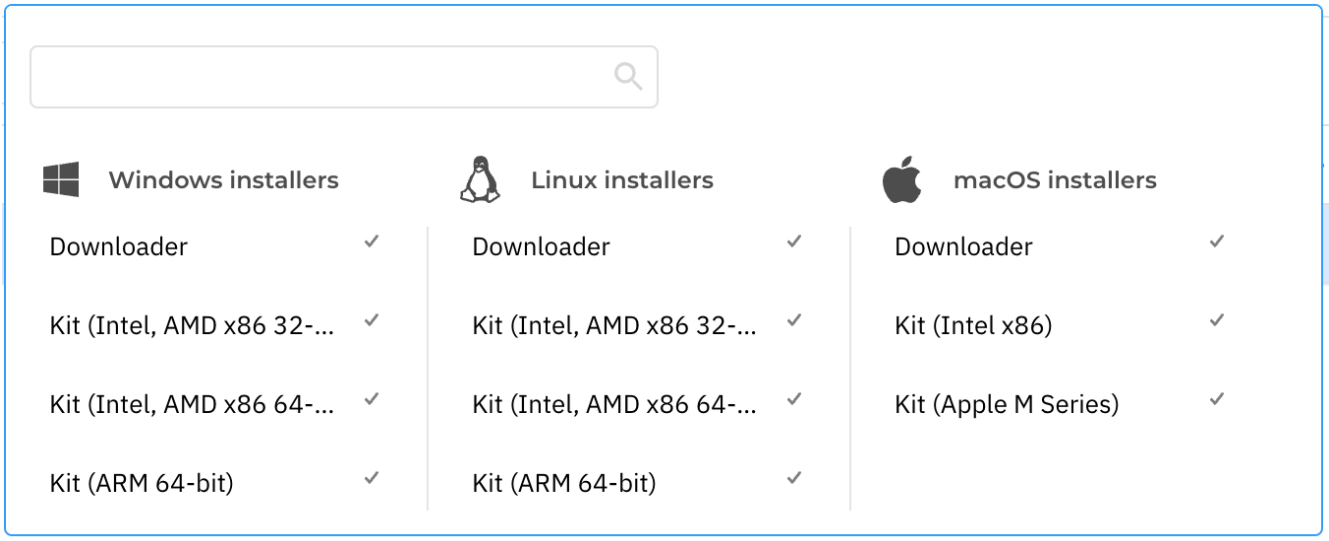

Рис. 2.13 - типи інсталяційних файлів агентів Bitdefender GravityZone Business Security

Великим плюсом є те, що агент Bitdefender GravityZone Business Security можна розгорнути на внутрішніх серверах організації, що дозволить тримати великі проміжні вузли також під наглядом, є зручним варіантом для контролю контролерів домену, MDM серверів, файлових станцій та іншого. Розгортання відбувається такими ж методами, як і на звичайну кінцеву точку, тому це не має викликати складності у реалізації.

Перевагою є гнучкість ліцензування, а отже малому та середньому бізнесу не потрібно платити за весь пакет послуг, а лиш за те, що дійсно корисно в даному випадку.

Рішення Bitdefender GravityZone Business Security є комплексним рішенням, а тому його реалізація вже надає безліч переваг та можливостей використання, але також потрібно враховувати гнучкість даної системи, що дозволяє інтегровувати його з іншими рішеннями безпеки таких як: MDM, SIEM-системи, AD, AzureAD (EntraID) та безліччю іншого. В першу чергу це значно підвищує рівень захищенності кінцевих точок.

При використанні даного рішення потрібно звернути увагу на нові технології, такі як EDR. EDR (виявлення та реагування на загрози в кінцевих точках) є

технологією кібербезпеки, яка спеціалізується на моніторингу та захисті кінцевих пристроїв у мережі. Ця система постійно відстежує активність на кінцевих точках, таких як комп'ютери, ноутбуки, мобільні пристрої та віртуальні машини, для виявлення загроз і реагування на них.Основні функції EDR:

- Моніторинг у реальному часі. EDR забезпечує безперервний моніторинг кінцевих точок на предмет підозрілої активності, що дозволяє швидко виявляти загрози, які можуть уникнути традиційних антивірусних рішень;

- Виявлення аномалій. Системи EDR використовують алгоритми машинного навчання та аналітику поведінки для виявлення незвичних шаблонів активності, що може свідчити про кібератаку або компрометацію;

- Автоматичне реагування. При виявленні загрози EDR може автоматично виконувати дії, такі як ізоляція заражених систем або блокування шкідливих процесів, щоб запобігти подальшому поширенню атаки;

- Аналіз інцидентів. EDR збирає та зберігає дані про всі події на кінцевих точках, що дозволяє командам безпеки проводити глибокий аналіз інцидентів і визначати причини атак;

- Управління вразливостями. Системи EDR допомагають виявляти вразливості в програмному забезпеченні та конфігураціях кінцевих точок, що може бути використано зловмисниками для атак.

Переваги використання EDR. EDR надає централізовану видимість всіх кінцевих пристроїв у мережі, що дозволяє командам безпеки швидше реагувати на загрози. Завдяки автоматизації процесів реагування на загрози, команди безпеки можуть значно скоротити час, необхідний для усунення інцидентів. EDR ефективно бореться з сучасними загрозами, такими як безфайлові атаки та шкідливе програмне забезпечення з вимогою викупу, які можуть уникнути традиційних антивірусних рішень.

Мультишарновий захист, Bitdefender GravityZone забезпечує захист на рівнях від мережі до кінцевих точок. Завдяки використанню передових технологій, таких як

штучний інтелект, визначення поведінки та машинне навчання, система обірає потенційні загрози до того, як вони поставлять ризик системі[12].

У висновку можна сказати, що Bitdefender GravityZone Business Security має великі можливості до застосування в інформаційній системі організації. Це обумовлено легкою розгорткою, як самого центру керування так і самих агентів на кінцеві точки. Можливостей додає наявність великої кількості нових технологій захисту зокрема EDR. Не менш важливим, є те, що центр керування Bitdefender GravityZone Business Security є максимально легким до сприйняття через легкий інтерфейс. Було оглянуто його зовнішній вигляд та структурованість. Перевагою є інтеграція з іншими системами безпеки такими як MDM, SIEM-системами, AD та AzureAD (EntraID). Це все разом обумовлює актуальність та моживості використання цього рішення для захисту кінцевих точок організації.

3 ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ НА БАЗІ BITDEFENDER GRAVITYZONE BUSINESS SECURITY

3.1 Приклад розгортання агенту та взаємодії з кінцевою точкою на базі пристрою з ОС MacOs

Для першого прикладу ми будемо використовувати кінцеву точку у вигляді ноутбуку з операційною системою MacOS. Алгоритм роботи буде складатися з початкового створення інсталяційного файлу агенту Bitdefender GravityZone Business Security. Потім наступним етапом буде встановлення цього агенту на кінцеву точку та подальша діагностика та маніпуляції з кінцевою точкою. Основна відмінність між іншими кінцевими точками з іншою ОС це те, що MacOs без використання MDM рішень, потребує надання всіх потрібних доступів для роботи інакше захист не буде відбуватися.

Першочергово фахівець з кібербезпеки має увійти в центр керування Bitdefender GravityZone Business Security та перейти за вкладаками Network – Installation Packages. В даному меню фахівець вибирає або вже створений інсталяційний файл, або створює його за допомогою однойменної кнопки Create. Наступним етапом адміністратору пропонується дати назву пакету, створити опис та вибрати функції та технології, які буде мати кінцевий агент (Рисунок 3.1). Дуже зручним є те, що інтерфейс відразу демонструє, які функції працюють на конкретній ОС. Іншою відмінністю є те, що у порівнянні з ОС Windows агент для MacOs немає меню SuperUser, що дозволило б адміністратору тимчасово безпосередньо зайти в налаштування агенту та проводити певні маніпуляції. Ми створимо агент з функціями Antimalware, Advanced Threat Control, Network protection, що включає в себе: Content Control, Antiphishing, Web

Traffic Scan. Також додамо Device Control, для перевірки пристроїв, які під'єднуються до кінцевої точки. Encryption та Patch Management також будуть обов'язковими пунктами (Рисунок 3.2).

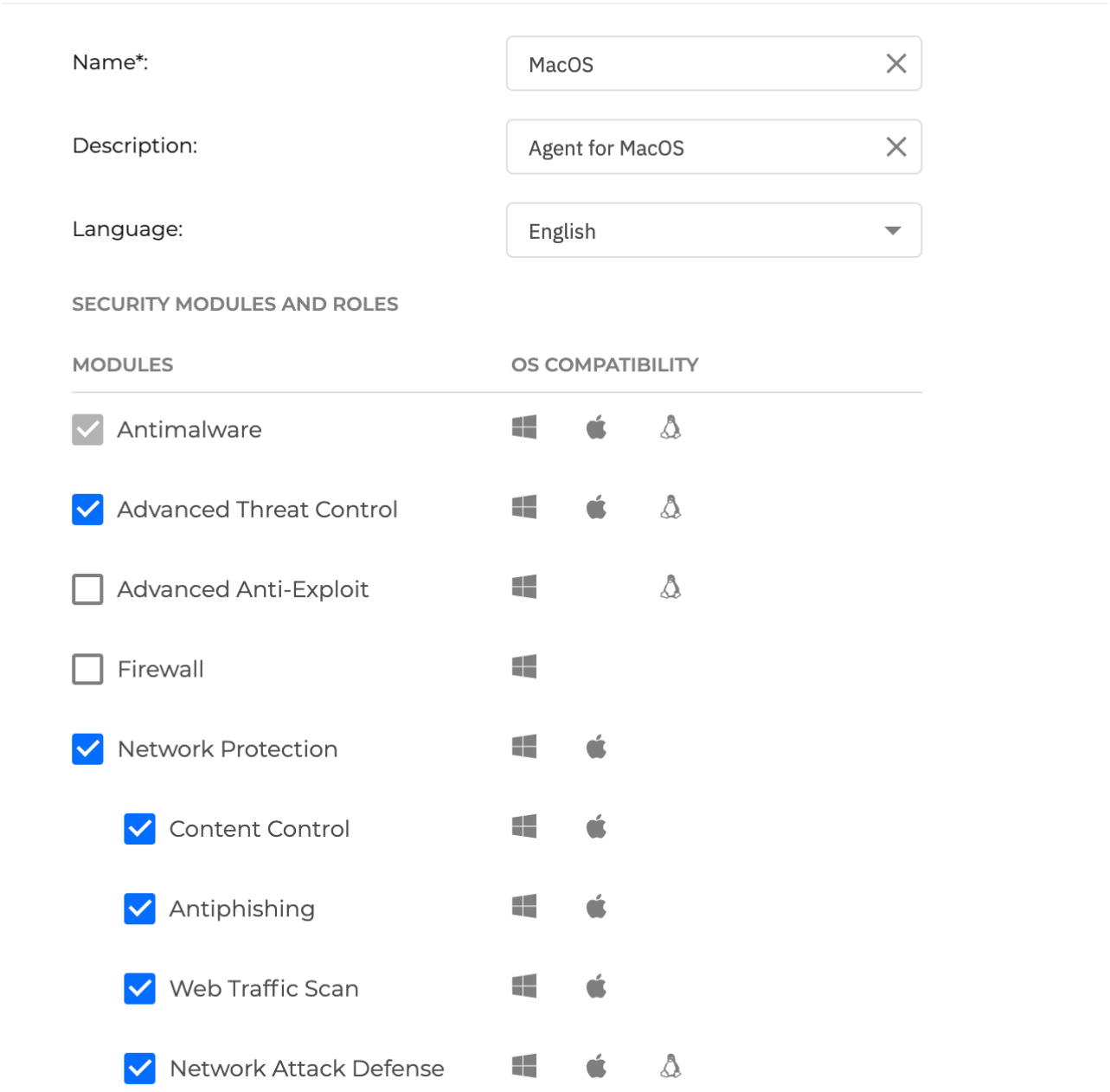

Рис. 3.1 - вибір налаштувань при створенні агенту Bitdefender GravityZone Business Security

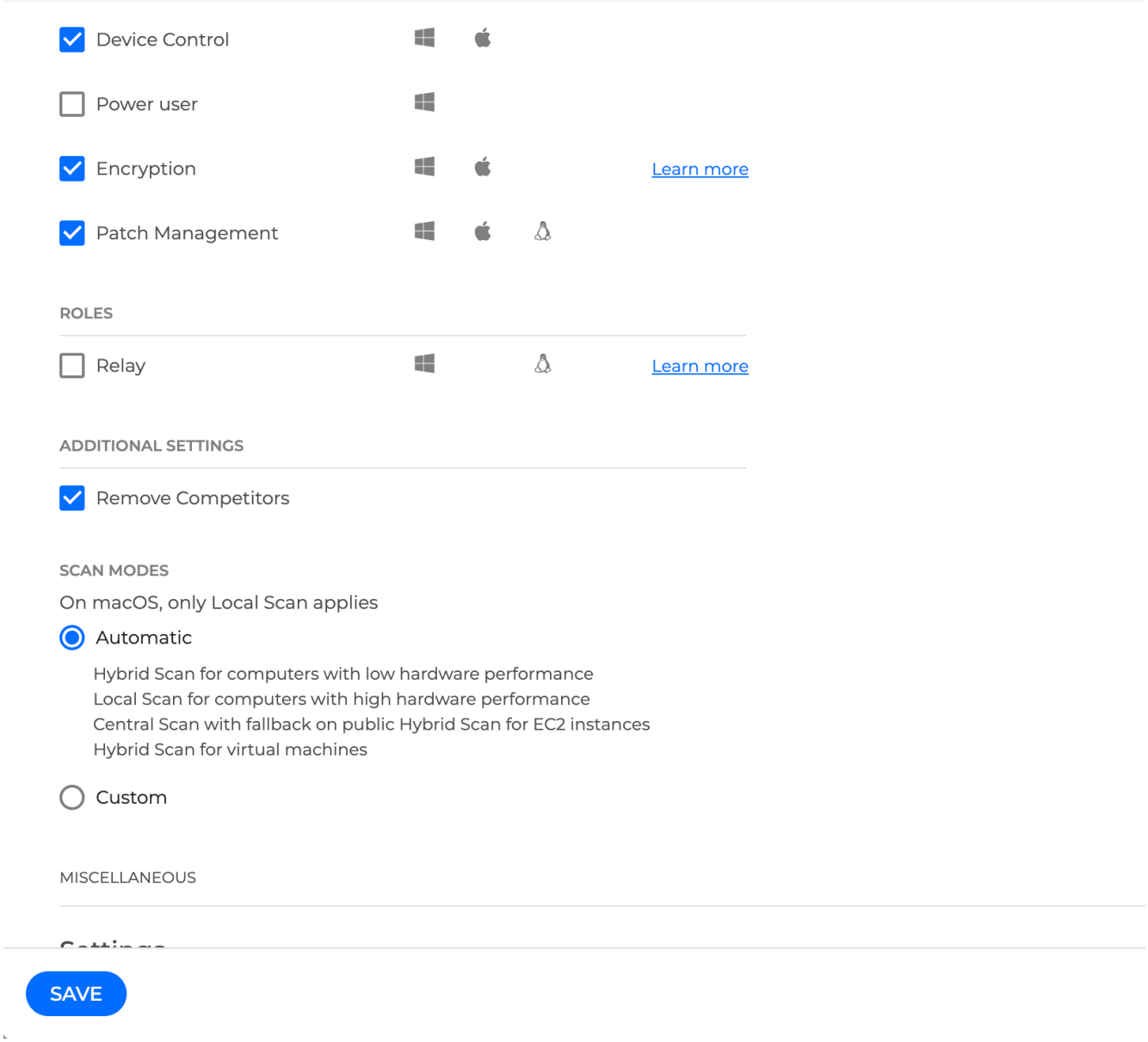

Рис. 3.2 - додаткові налаштування при створенні інсталяційного файлу агенту

Після вибору всіх налаштувань адміністратор натискає кнопку Save та отримує кінцевий результат, який буде відображатись в панелі інсталяційних файлів.

При виборі потрібного інсталяційного файлу, стають активними меню вибору методу встановлення агенту. У випадку з MacOS є три варіанти (Рисунок 3.3):

- Downloader. Самий зручний та легкий спосіб, але потребує інтернет-з’єднання на кінцевій точці для встановлення. Створює інсталятор, який в процесі інсталяції сам викачує актуальний агент;

- Kit (Intel x86). Цей інсталятор йде вже повністю зібраним та дозволяє інсталювати агент на кінцеву точку, яка на момент інсталяції немає інтернет-з’єднання. Треба взяти до уваги, що саме цей інсталятор використовується MacBook до 2019 року, оскільки в той час вони використовували процесори Intel;
- Kit (Apple M Series). Цей інсталятор йде вже повністю зібраним та дозволяє інсталювати агент на кінцеву точку, яка на момент інсталяції немає інтернет-з’єднання. Цей інсталятор призначений вже для нових MacBook, які використовують власні процесори з іншою архітектурою Apple Silicon M.

В нашому випадку використовується кінцева точка на базі процесору Apple Silicon M3, а отже доступними є варіанти Downloader та Kit (Apple M Series). Так як кінцева точка має активне інтернет-з’єднання будемо використовувати інсталятор Downloader.

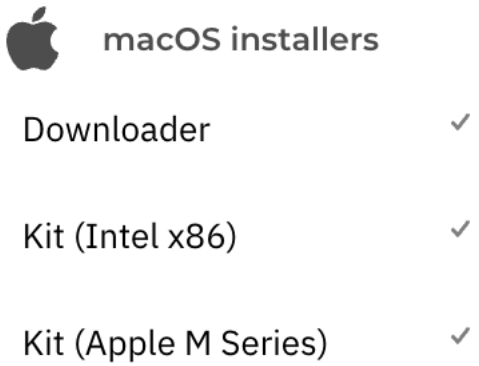

Рис. 3.3 - типи інсталяційних файлів агенту для пристроїв на базі MacOS

Після скачування інсталяційного файлу агенту та відкриття його на кінцевій точці, файл відразу починає скачувати актуальну версію агенту (Рисунок 3.4). Після цього якщо не використовується MDM рішення паралельно агент запросить пароль адміністратора для надання всіх доступів, а також вручну потрібно буде надати дозволи для передачі даних через інтернет-з’єднання. Загалом при стабільному

інтернет-з’єднанні інсталяція не займає більше однієї хвилини, хоча це також залежить від системних характеристик кінцевої точки.

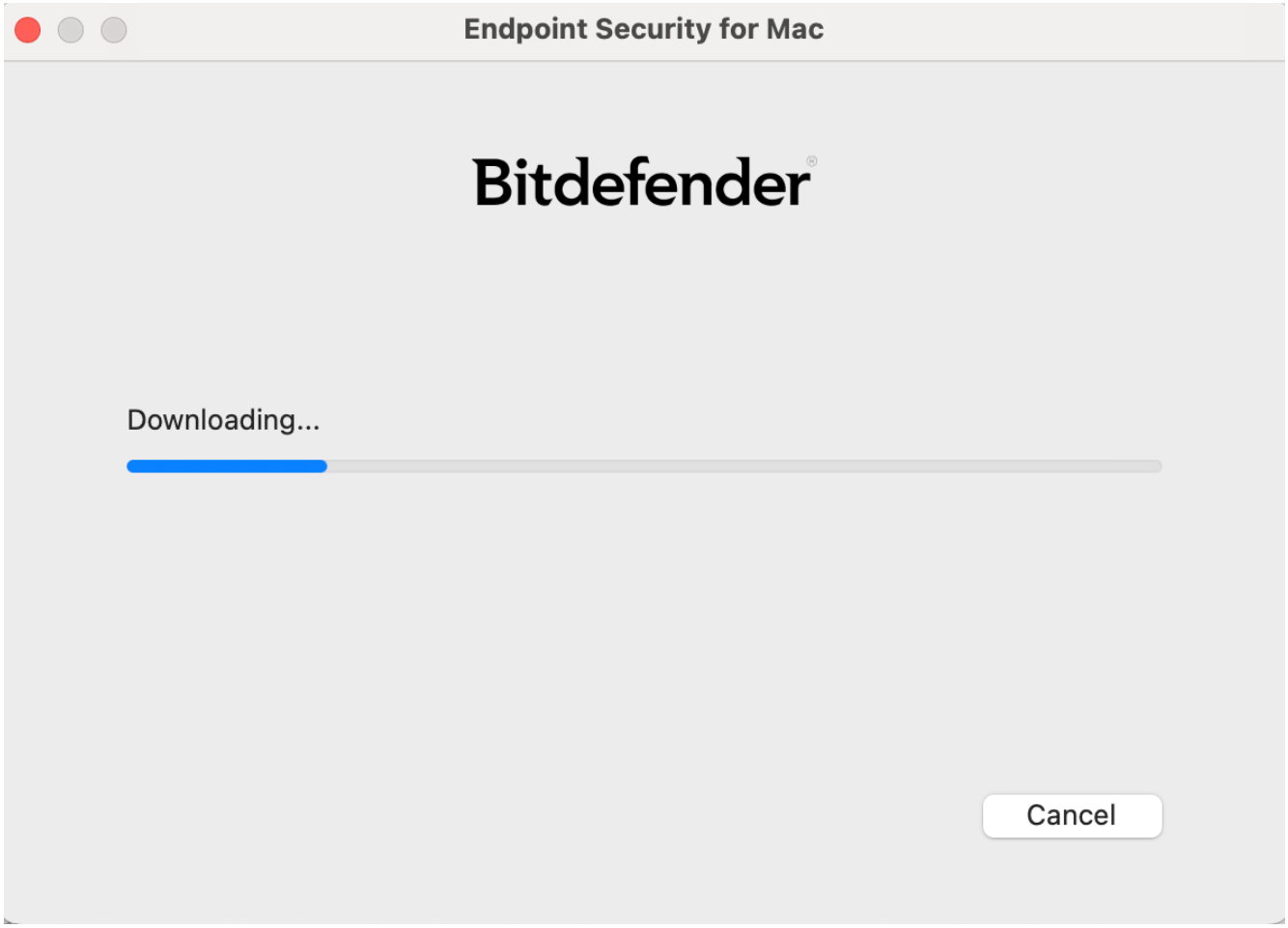

Рис. 3.4 - викачування актуальної версії агенту Bitdefender GravityZone Business Security за допомогою Downloader

Після успішного інсталювання агент з’являється в системному треї де має лише два варіанти відображення, якщо кінцева точка у безпеці або коли є активності, які потребують уваги користувача або адміністратора. При натисканні на нього відкривається Dashboard агенту Bitdefender GravityZone Business Security, в якому можна спостерігати за коректною роботою всіх попередньо вибраних функцій та технологій (Рисунок 3.5).

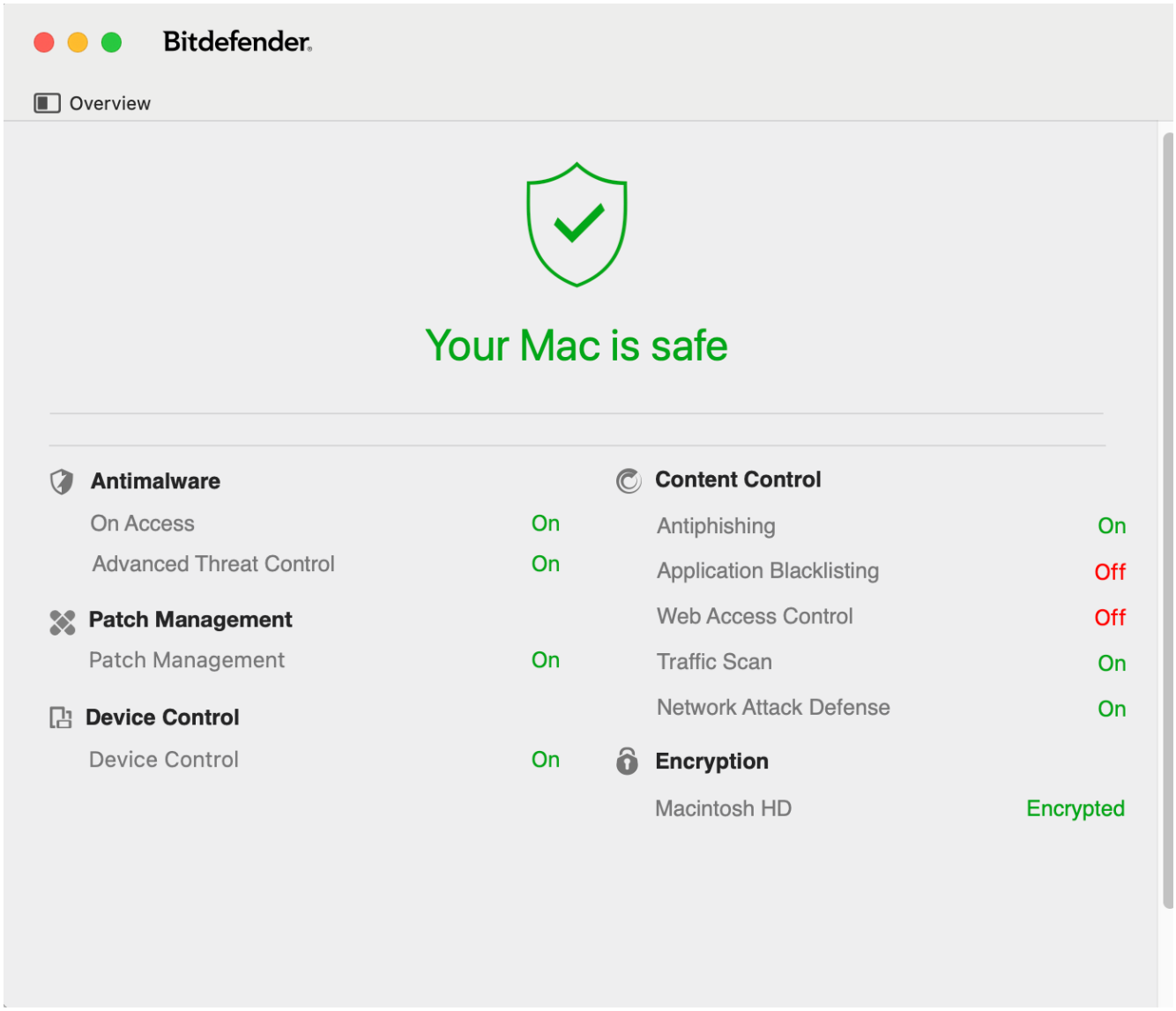

Рис. 3.5 - Dashboard агенту Bitdefender GravityZone Business Security для MacOS

Після коректного встановлення агенту та його подальшого оновлення в центрі керування Bitdefender GravityZone Business Security у вкладці меню Network девайс починає відображатися з локальною назвою ноутбука. Можна або швидко призначити для нього певні попередньо налаштовані політики, або відкрити повний огляд кінцевої точки, де ми можемо бачити її ім'я, IP-адресу, версію OS, інфраструктуру, групу пристроїв, статус та останній час коли вона була онлайн (Рисунок 3.6). Також присутні додаткові вкладки в яких можна переглянути призначені політики, степінь захисту, роботу над помилками, файли відгуки про сканування на кінцевій точці та активних користувачів, це може бути корисно, якщо кінцева точка знаходиться в AD.

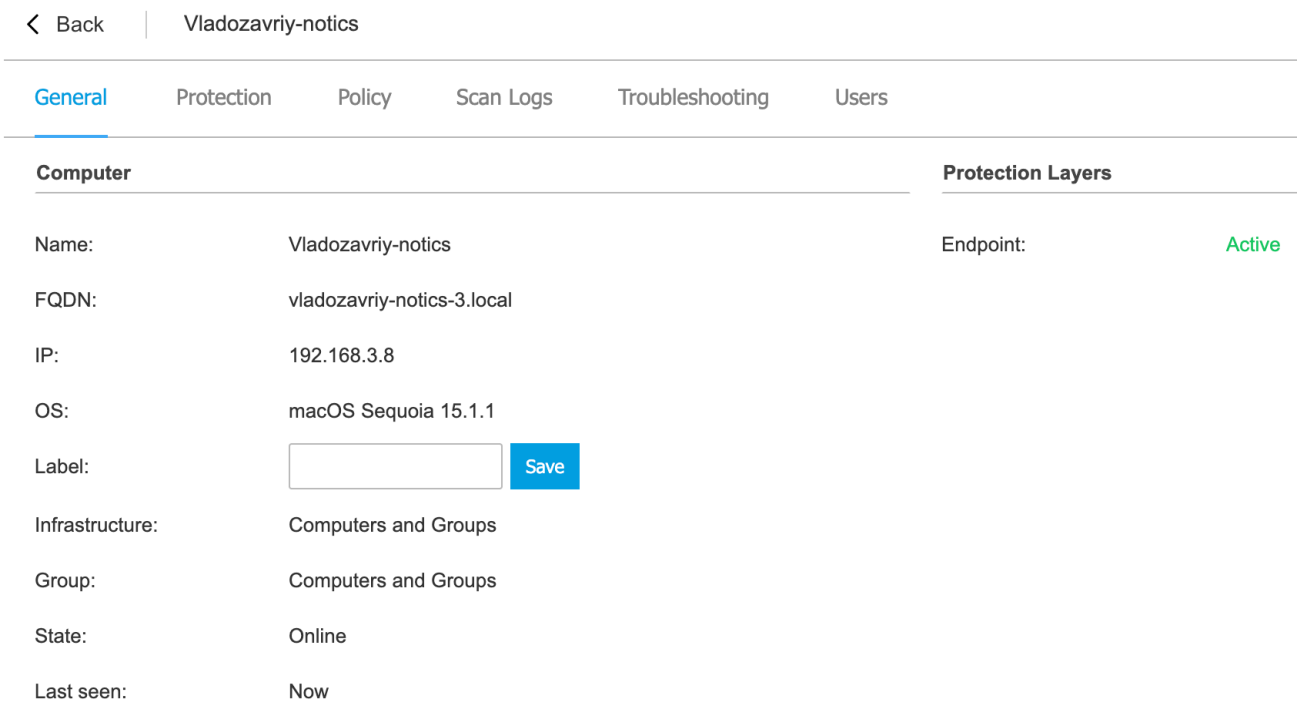

Рис. 3.6 - огляд стану кінцевої точки в центрі керування Bitdefender GravityZone Business Security

Доцільним є після налаштування відразу додати певні політики на кінцеву точку для збільшення степеню її захисту. Але для початку саму політику потрібно створити, це відбувається безпосередньо через центр керування у відповідній вкладці Policies. Тут адміністратор може спостерігати за вже наявними політиками або скористувавшись кнопкою Add та розпочати створення нової політики. В самому діалоговому вікні при створенні нової політики можна увімкнути функції та технології, які з певних причин не були додані відразу при створенні інсталяційного файлу, але також і увімкнути планові сканування, увімкнути Patch Management та інше (Рисунок 3.7). У випадку з Patch Management ми налаштовуємо опцію, яка буде примусово оновлювати встановлений софт на кінцевій точці, адже розробники ПЗ постійно випускають виправлення безпеки, що зменшує ризики використання шкідливого ПЗ та втручання в інформаційну мережу компанії. Risk management налаштовує обов’язкові сканування системи з тією періодичністю, яку фахівець з кібербезпеки вважає потрібною.

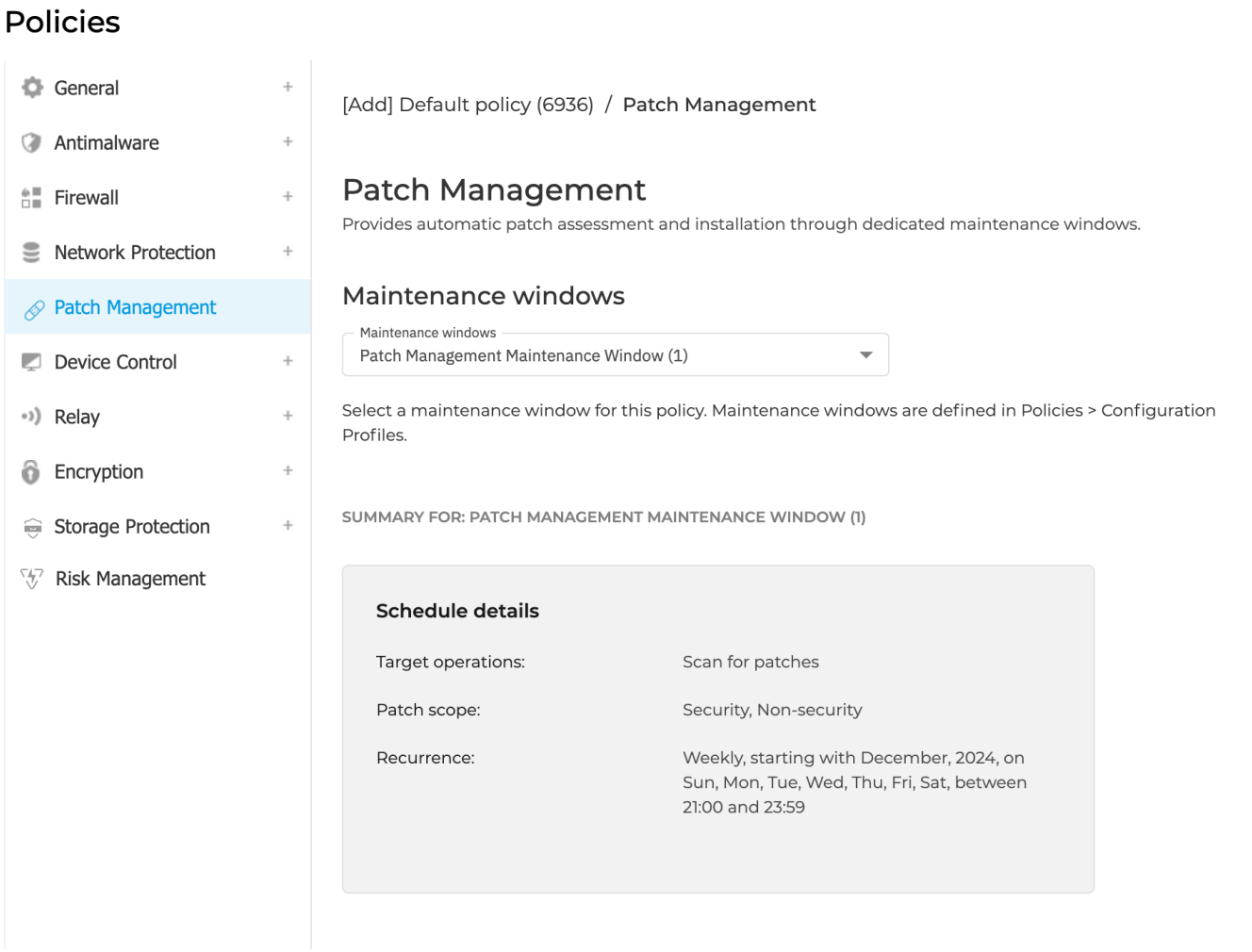

Рис. 3.7 - створення політики для агенту Bitdefender GravityZone Business Security

Після успішного створення політики, адміністратора має повернутись у вкладку меню Network, де відбувається огляд всіх кінцевих точок. Адміністратор має вибрати кінцеву точку або групу кінцевих точок та за допомогою швидкої кнопки перейти до меню вибору потрібної політики додати її в чергу на виконання (Рисунок 3.8).

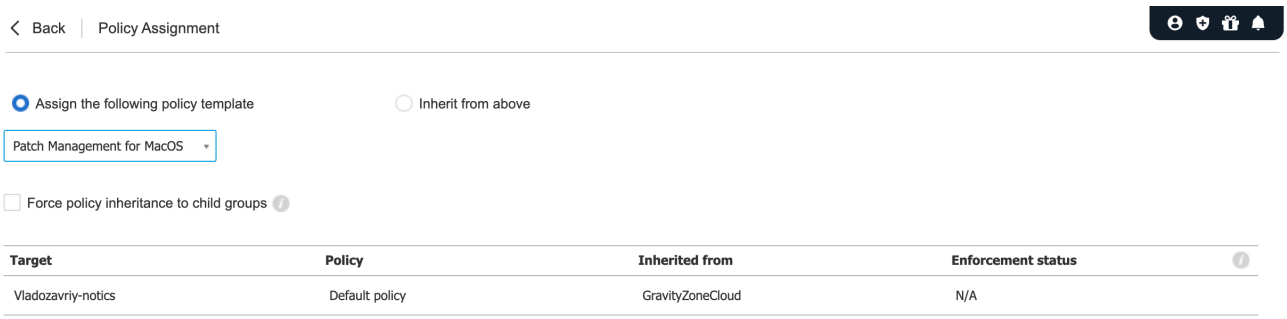

Рис. 3.8 - призначення політики на конкретну кінцеву точку

Після вдалого застосування кінцевої політики на кінцеву точку можна спостерігати у центрі керування, при повному огляді кінцевої точки назначені політики. Також можна на самій кінцевій точці при огляді Dashboard на агенті спостерігати, як клієнт отримав оновлення політик від серверу та успішно застосував їх і політика відразу почала діяти (Рисунок 3.9).

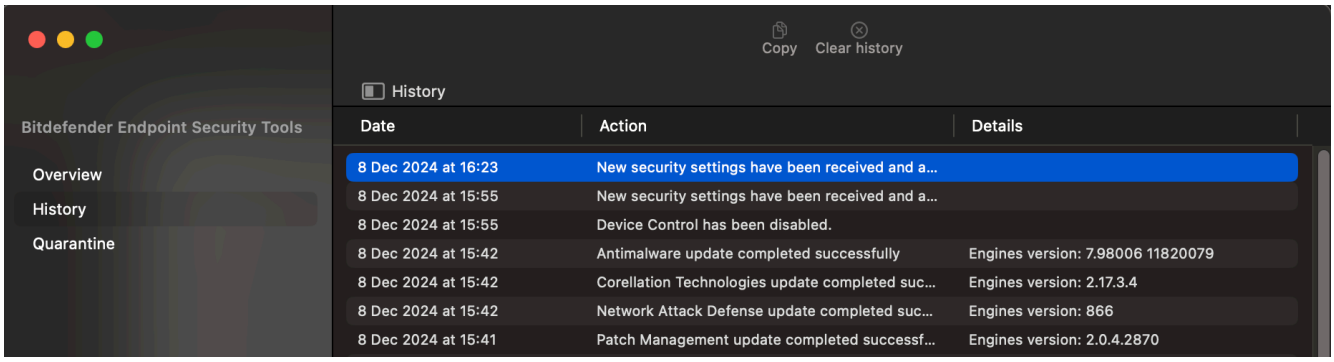

Рис. 3.9 - успішне примінення політики безпеки на кінцевій точці на базі ОС MacOS

З плином часу після успішних сканувань, застосувань нових політик фахівець з кібербезпеки буде отримувати все більш детальні звіти та спостерігати за життя кінцевої точки. Функція EDR буде в свою чергу відслідковувати підозрілу активність як і зі сторони кінцевої точки так і зі сторони користувача. Всі діаграми та статистики будуть заповнюватись відповідно до знайдених вразливостей та їх знешкодження.

За декілька днів кінцева точка не була вражена шкідливим ПЗ, отже і рахунок загрози компанії залишається на рівні 0% (Рисунок 3.10).

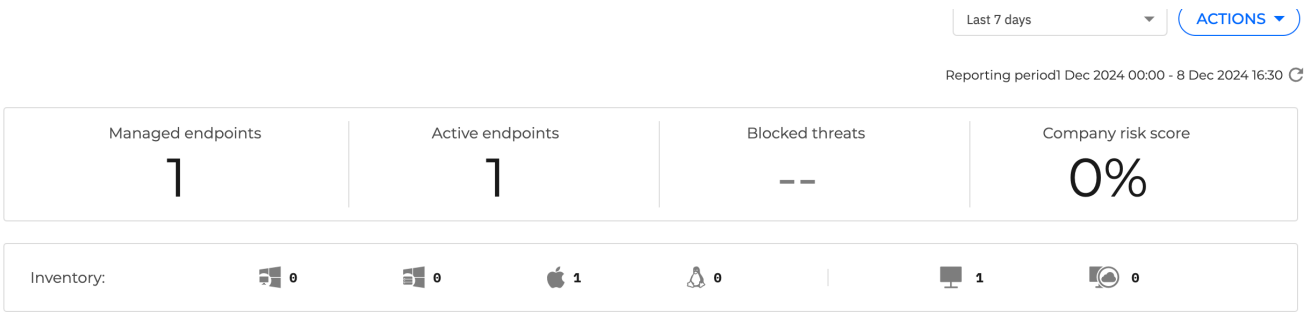

Рис. 3.10 - огляд рахунку загрози інформаційної системи компанії

У висновку можна сказати, що функціонал Bitdefender GravityZone Business Security підходить чудово. Було розглянуто етап створення інсталяційного файлу для пристрою на базі ОС MacOS. Було розглянуто його інсталяцію на кінцеву точку. Було створено та налаштовано політику безпеки, яка запланує автоматичні сканування системи на вразливості та включає Patch Management задля оновлення всього ПЗ до актуальної версії. В цілому результат є задовільним.

3.2 Приклад розгортання агенту та взаємодії з кінцевою точкою на базі пристрою з ОС Windows 10

ОС Windows є однією з найрозповсюдженних ОС в організаціях. Вона є досить рідною та зрозумілою для більшості кінцевих користувачів та зручна для адміністрування фахівцям з кібербезпеки.

У випадку з рішенням Bitdefender GravityZone Business Security, його агент має найбільший парк функцій та технологій для цієї ОС, оскільки вона була перша підтримувана ОС в історії з моменту започаткування Bitdefender. Для огляду можливостей агенту Bitdefender GravityZone Business Security ми візьмемо тестовий девайс на базі ОС Windows 11. У випадку як і з MacOS, якщо в інформаційній системі компанії паралельно не використовуються рішення MDM, то інсталяція відбувається в ручному режимі напряму через фахівця з кібербезпеки або системного адміністратора.

Для ОС Windows ми створимо окремий інсталяційний файл, оскільки дана ОС підтримує більшу кількість функцій та технологій. Зокрема ми додамо функції Firewall, Advanced Anti-Exploit, Power User та Relay (Рисунок 3.11).

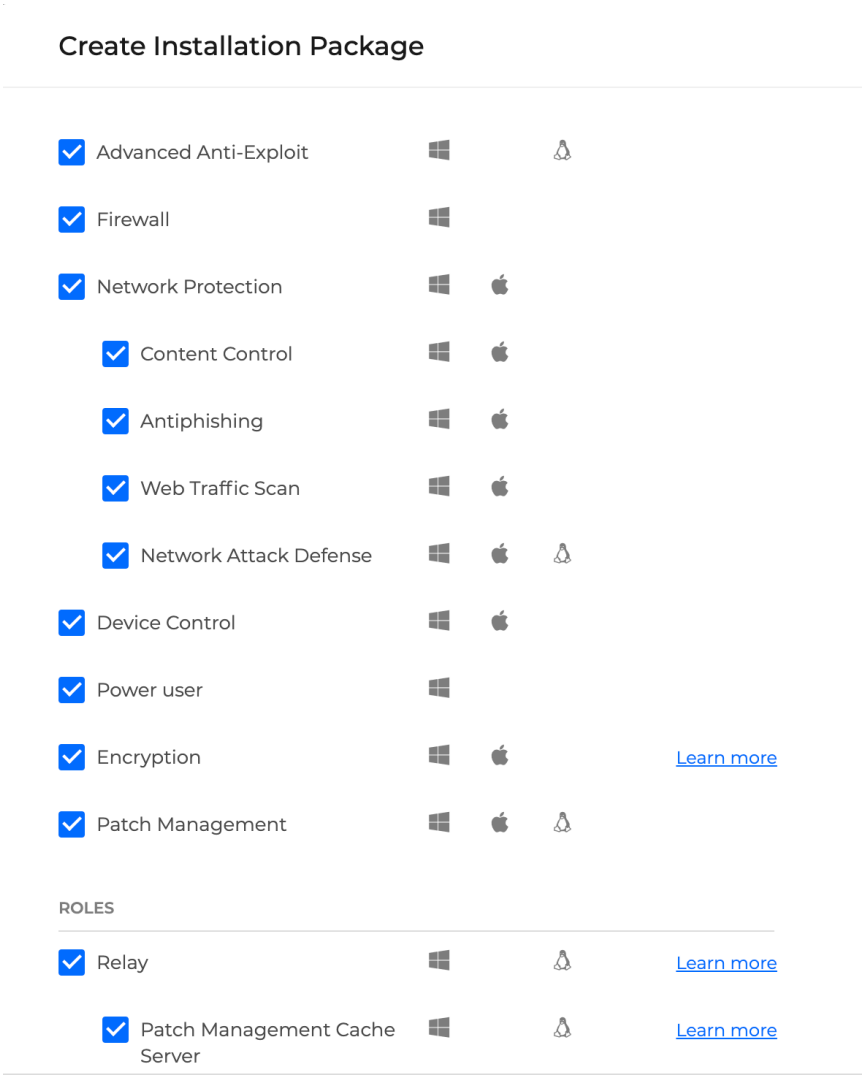

Рис. 3.11 - створення інсталяційного файлу агенту для ОС Windows 11

Після успішного створення інсталятора з базовими функціями на відміну від MacOS має 4 типи інсталяційних файлів (Рисунок 3.12):

- Downloader. Виконує таку саму функцію як і на MacOS. Потрібно стабільне інтернет-з’єднання;
- Kit (Intel, AMD x86, 32 bit). Повністю зібраний пакет агенту призначений для кінцевих точок на базі процесорів Intel та AMD з 32 бітною ОС;

- Kit (Intel, AMD x86, 64 bit). Повністю зібраний пакет агенту призначений для кінцевих точок на базі процесорів Intel та AMD з 64 бітною ОС;
- Kit (ARM 64 bit). Повністю зібраний пакет агенту призначений для кінцевих точок на базі мобільних ARM процесорів з 64 бітною ОС.

Рис. 3.12 - типи інсталяційних файлів агенту для кінцевих точок на базі ОС Windows

Так само будемо використовувати інсталятор типу Downloader, який викачає актуальну версію інсталятора на кінцеву точку. На відміну від MacOS адміністратору достатньо лише його запустити на кінцевій точці після чого більше втручання адміністратора не потребується. Після успішного інсталювання агенту Bitdefender GravityZone Business Security значок агенту з’являється в треї пристрою, а сам девайс починає відображатись в меню Network у центрі керування Bitdefender GravityZone Business Security. Можна оглянути детально щойно додану кінцеву точку в якій ми знову ж таки побачимо її актуальну інформацію, назву пристрою, IP-адресу, призначені політики та іншу корисну інформацію (Рисунок 3.13).

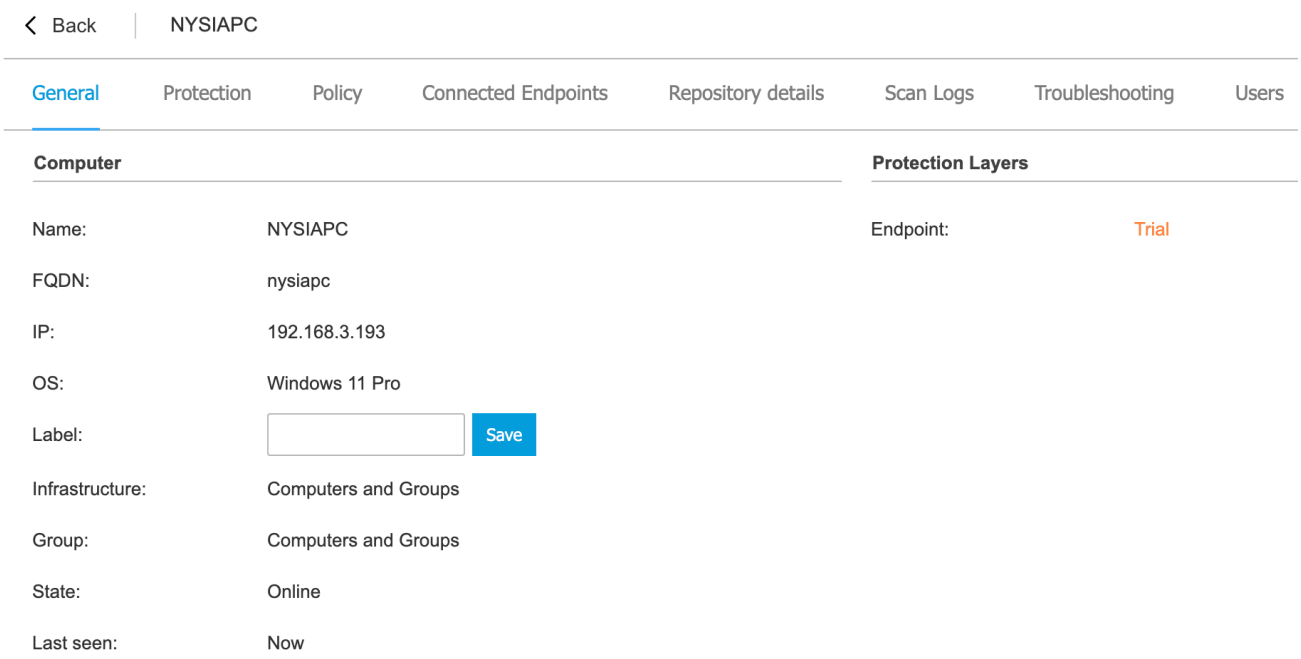

Рис. 3.13 - огляд щойно доданої кінцевої точки на базі ОС Windows 11

Звісно для створення більш міцного захисту для групи кінцевих точок на базі ОС Windows потрібно створити та застосувати розширені політики безпеки, які будуть більш розгорнуто керувати кінцевою точкою.

В нашому випадку ми також застосуємо політику, яка додає спеціальний пароль для видалення агенту Bitdefender GravityZone Business Security та для введення PowerUser паролю, для локального тимчасового призупинення захисту або для внесення локальних змін у фаєрвол чи принцип захисту кінцевої точки (Рисунок 3.14). Відбувається це таким самим чином, як і з кінцевими точками на базі ОС MacOS. Фахівцю з кібербезпеки потрібно перейти у вкладку функцій Policies, де він натискає кнопку Add та потрапляє в діалогове вікно створення нової політики. Окрім всіх попередніх політик, які були створенні для пристроїв на базі ОС MacOS, а саме Patch Management та Storage Protection ми додаємо пароль для видалення агенту Bitdefender GravityZone Business Security та для PowerUser для локального адміністрування.

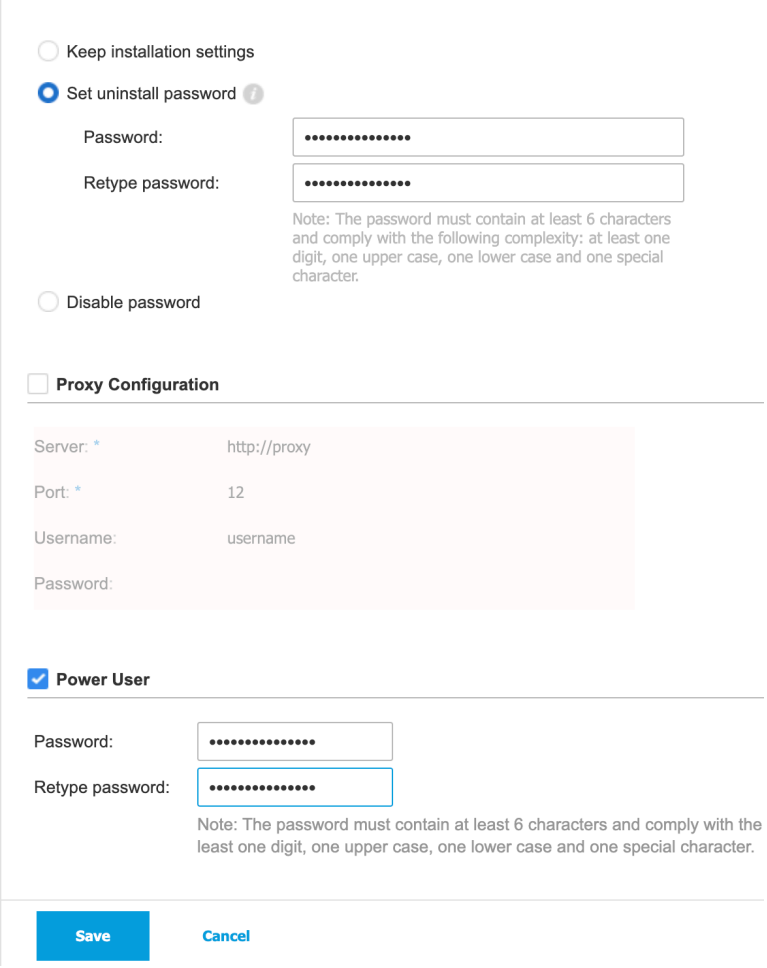

Рис. 3.14 - створення паролів PowerUser та видалення агенту Bitdefender GravityZone Business Security

Після успішного створення політики адміністратор має повернутися у вкладку Network для вибору конкретної або групи кінцевих точок для примінення цієї політики. Відбувається шляхом швидкої опціїї Assign a polici, після чого завдання становить в чергу. Майже відразу в логах агенту кінцевої точки ми можемо спостерігати запис про те, що нові політики безпеки були успішно застосовані та приступили до роботи.

Іноді фахівцям з безпеки або системних адміністраторам потрібен доступ до налаштувань агенту саме на кінцевій точці. Відбувається це з причин дебагу або коли системному адміністратору потрібно вимкнути тимчасово захист для встановлення певних програм або додавання їх у білий список чи навпаки у правила фаєрволу.

Зазвичай такі зміни застосовуються лише до конкретної кінцевої точки і такі правила зберігаються лише локально на ній.

Потрапити в меню PowerUser можна двома шляхами. Найшвидший це через праву кнопку на значку агенту в треї та вибору опції PowerUser. Після цих маніпуляцій адміністратор отримує вікно командної строки в яку може вводити різного типу команди, наприклад вимкнення захисту в реальному часі, фаєрволу та іншого (Рисунок 3.15). Після вибору потрібної опції та введених атрибутів адміністратор обов'язково має ввести пароль PowerUser, який був заданий фахівцем кібербезпеки у конкретній політиці.

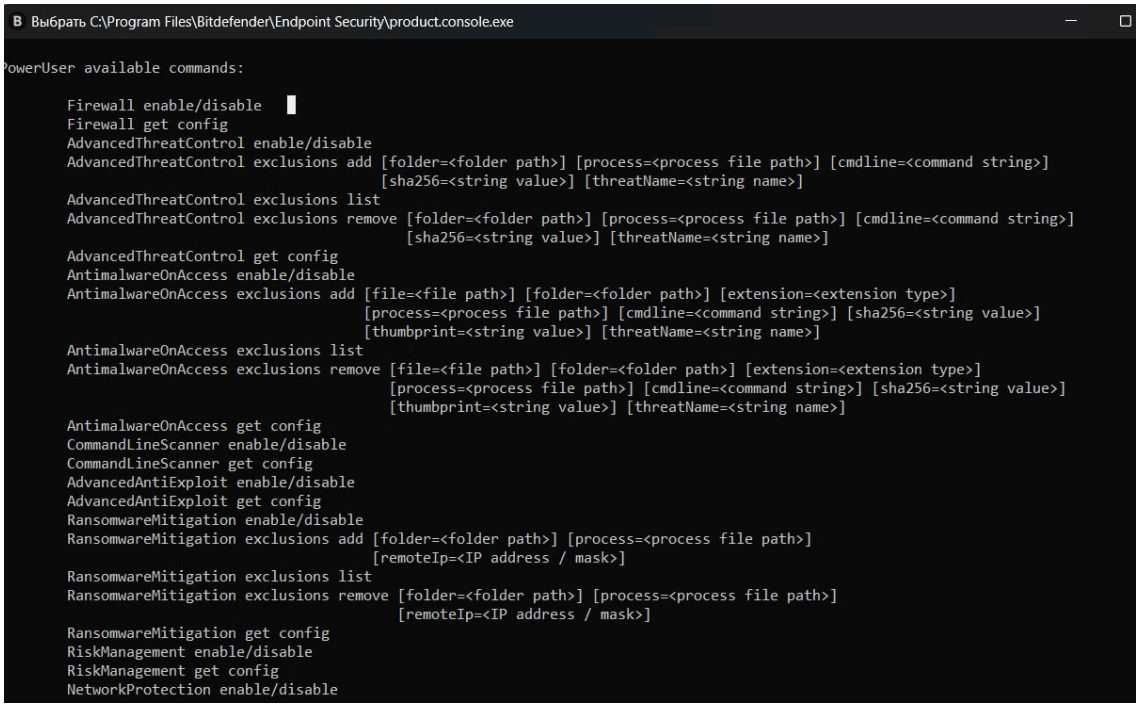

Рис. 3.15 - меню PowerUser у командній строці на кінцевій точці на базі ОС Windows

Існує інший спосіб потрапляння до цих налаштувань, який був основним до 2024 року. В локальному агенті Bitdefender GravityZone Business Security на кінцевих точках на базі ОС Windows також є користувацький інтерфейс, який спрощує взаємодію з агентом. Раніше потрапляння до нього відбувалося безпосередньо через кнопку PowerUser у треї, але з новими введеннями компанії Bitdefender, це меню було перенесено в окремий виконуваний файл, який зберігається у місці дислокації самого агенту. Зазвичай це C:\ProgramFiles\Bitdefender\EndpointSecurity\EPPConsole.exe. При

відкриванні цього виконуваного файлу користувача у вигляді адміністратору запросить відразу ввести пароль PowerUser наданий фахівцем з кібербезпеки, після чого адміністратор потрапляє в меню керування агентом, яке майже не відрізняється від меню налаштування політик в центрі керування Bitdefender GravityZone Business Security (Рисунок 3.16).

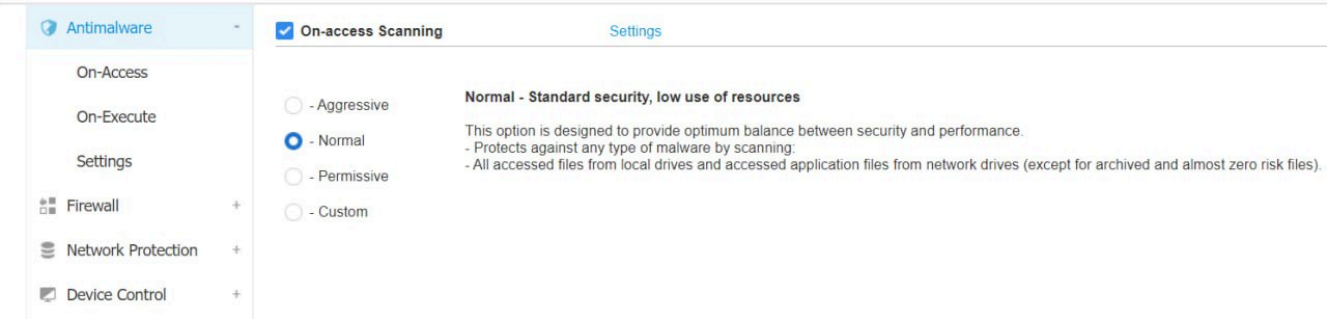

Рис. 3.16 - меню керування агенту через користувацький інтерфейс на кінцевій точці на базі ОС Windows

Після вдалого налаштування кінцевої точки та політик для неї починає відбуватись безпосередньо процес контролю кінцевої точки та реагування на знайдені вразливості.

Для огляду можемо бачити в центрі загального рахунку вразливості, що наша нова точка додалась та те, що вразливостей не було виявлено (Рисунок 3.17). загалом також бачимо, що загальний рахунок вразливості на даний момент складає 0%, що при великих масштабах звісно не буде таким.

Рис. 3.17 - загальний рахунок вразливості організації після додавання другої кінцевої точки

Потрібно розуміти, що це лише базові функції, які мають бути застосовані у найшвидші терміни для створення чудової екосистеми захисту кінцевих точок. Окрім цього центр керування Bitdefender GravityZone Business Security має безліч інших груп

меню, які дозволяють досконаліше керувати захистом кінцевих точок. Невідомі вразливості будуть потрапляти в карантин звідти фахівець з безпеки зможе прийняти рішення чи це дійсно шкідливе ПЗ чи лише програма, яка немає нормально підписаного сертифікату розробника. Фахівці з кібербезпеки можуть блокувати несприятливе ПЗ та доступ до певних ресурсів, що дозволяє превентивно зашкодити встановленню шкідливого ПЗ. Вагомою є функція Device Control, яка не дозволить кінцеве під'єднання стороннього обладнання без попереднього сканування. Звісно за весь час роботи активно працює технологія EDR, яка використовуючи машинне навчання та відстеження аномальної активності кінцевої точки та користувача самостійно приймає певні заходи для забезпечення захисту.

У висновку можна сказати, що захист кінцевої точки на базі ОС Windows відбувається на рівні з MacOS та навіть має певні додаткові можливості яких немає на іншій ОС. Було розглянуто процес створення інсталяційного файлу для кінцевих точок на базі ОС Windows. Було переглянуто варіативність інсталяції. Розглянуто повне створення нової політики для пристроїв на базі ОС Windows та налаштування PowerUser доступу локально на кінцевій точці. Паралельно оглянули типи PowerUser консолей та для чого вони потрібні. Розібрано взаємодію кінцвої точки з центром керування Bitdefender GravityZone Business Security. Загалом результат дослідження задовільний.

3.3 Створення рекомендацій щодо забезпечення захисту кінцевих точок на базі рішення Bitdefender GravityZone Business Security для фахівців з кібербезпеки

Ключовим фактором для забезпечення захисту кінцевих точок є правильний підхід і правильні рішення для виявлення потенційних загроз. Головним є аналіз поведінки користувачів, розуміти принцип та режим роботи в організації (в офісі, віддалено чи гібридна). Аналізуючи користувачів можна виявити коли він поводиться підозріло або його дії є поза типовою поведінкою.

Перш ніж впроваджувати будь які системи захисту кінцевих точок, потрібно оцінити вже наявні системи та потреби організації. Потрібно інвентаризувати всі кінцеві точки в організації та вже впроваджені системи контролю, що також допоможе в майбутньому виявляти загрози інформаційній системі. Необхідно визначити всю кількість користувачів кінцевих точок, як і в самій організації так і віддалених працівників. Варто знати, яка кінцева точка належить якому користувачу. Оскільки під управлінням одного користувача може бути декілька пристроїв, це узгоджується та залежить від посади та потреб співробітника.

Потрібно сформувати звіт вже виявлених загроз кінцевим точкам та виставити пріоритет серед них, для розуміння найважливішого в даний момент. Потрібно враховувати багато факторів, це може бути, як і втрата пристрою користувачем так і втрата конфіденційної інформації. Також важливим є виявити, які облікові записи користувачів були компрометовані.

При можливості також потрібно зібрати всі можливі журнали з усіх кінцевих точок.

Не потрібно відразу братися за всі виявлені загрози. Потрібно поступово починаючи з першої виявленої загрози та виставляти пріоритетність.

З розвитком штучного інтелекту в останні роки IT-фахівець може залучити його для виконання цієї роботи. Але потрібно розуміти, що в таких випадках більш ефективнішим буде звичайне дотримання правил при перевірці. Наприклад, що IT-фахівець з досвідом знає, що співробітник працює більшу частину часу з офісу, а в останні дні почав розсилати інформацію організації через відкриту мережу в ресторані.

На основі цих даних потрібно вибрати та впровадити рішення з захисту кінцевих точок. Це перший крок до повного захисту всіх пристроїв організації. Це дозволить відслідковувати їх дії, проводити постійні сканування системи та забороняти користувачам робити дії, які не потрібні їм для виконання робочих обов’язків. Наприклад, на телефоні водія, який має лише спілкуватися з диспетчером

за допомогою стільникового зв’язку, не потрібно додавати обліковий запис організації, для протидії витоку інформації.

Вивчаючи рішення з захисту кінцевих точок, необхідно звернути увагу на потреби організації та на особливості рішення, а саме: автоматизація процесу, огляд загроз, відгуки користувачів.

Автоматизація процесу – це дозволить адміністраторам підготовлювати пристрої без зайвих складностей, користуючись вже готовими темплейтами. Налаштувати графіки сканування систем, для постійного відслідковування появи шкідливого ПЗ. Налаштувати систему сповіщень, яка буде доносити до адміністратора інформацію про порушення політик безпеки, компрометований обліковий запис або про підозрілі дії зі сторони користувача.

Огляд загроз – інструмент, який на базі звітів безпеки, дозволяє оцінити ризики пов’язані з цією вразливістю, виставити пріоритетність та прийняти відповідні дії.

Відгуки користувачів – перед впровадженням рішення необхідно ознайомитися з відгуками від інших організацій. Які є складності після впровадження рішення, яким вразливостям рішення допомогло запобігти.

Зрештою, вибір найкращого рішення захисту кінцевих точок в організації залежить від сукупності пріоритетів та проблем, які наявні в організації. Потрібно також розуміти, що для ефективної протидії загрозам потрібен комплекс рішень, а не лише одне. Мають бути як і програмні рішення, які були описані вище так і не меншу частину займає виховна робота. Вона розуміє під собою бесіди та навчання з робочим персоналом, пояснювання ризиків і що до цього може призвести, а також, які конкретні наслідки можуть спіткати співробітника.

Окрім цього також треба постійно проводити аудит систем та інвентаризацію наявних кінцевих точок. Це дозволить завжди розуміти порядок діл та дозволить запобігти багатьом вразливостям завчасно. Але все ж таки потрібно розуміти, що людський фактор завжди був найбільш великою загрозою будь якій організації, незалежно від того, які рішення були прийняті для їх запобігання

ВИСНОВКИ

В роботі проведено дослідження шляхів та аналіз загроз щодо використання рішень захисту кінцевих точок організації.

Проаналізовано роль та місце кінцевих точок в сучасній інформаційній системі організацій. Були проаналізовані сутність проблем із зовнішньої вразливості кінцевих точок, а також сутність проблеми захисту цих кінцевих точок. Було розглянуто та приведено статистику, яка показує актуальність цієї проблеми у сучасному світі.

Досліджено існуючі методи захисту кінцевих точок та порівняно їх з рішенням Bitdefender GravityZone Business Security. Більш детально було досліджено саме рішення Bitdefender GravityZone Business Security, а саме його функціонал, які саме проблеми воно може вирішити. Розглянуто переваги та недоліки цього рішення. Дослідження проводилися практично, що допомогло одразу побачити весь функціонал, та виявити проблеми з якими може спіткнутися фахівець з кібербезпеки в організації.

Окрім цього, наведено способи застосування цього рішення, яке призначення для захисту кінцевих точок, що допомогло відслідкувати дії, які відбувались на кінцевих точках, переглянути існуючі вразливості систем. Було показано сам процес інсталяції рішення та його налаштування для комфортної та продуктивної роботи. Розглянуто можливості інтеграції з існуючими рішеннями та програмними комплексами розміщеними в інформаційній системі організації. Великим плюсом є можливість інтеграції AD та Azure AD(EntraID) в систему захисту кінцевих точок, що відразу дає можливість експортувати вже готову структуру організації та слідкувати за скомпрометованістю облікових записів.

Приведено результати експерименту із застосування агентів в комплексі Bitdefender GravityZone Business Security. В процесі експерименту використовувалися

реальні пристрої, що допомогло перевірити функціонал та відпрацювання всіх налаштувань. Крім цього було розглянуто можливості сканування систем та протидій виявленим загрозам. У результаті експерименту було встановлено важливість використання рішень захисту кінцевих точок в інформаційних системах організацій та потенційну автоматизацію цього процесу.

Розроблено рекомендації щодо застосування рішень з захисту кінцевих точок організації. Надано, як і програмні рекомендації щодо збору інформації, журналів, а також виявлення вже наявних вразливостей, так і виховні роботи, які безпосередньо спрямовані на людський фактор.

Таким чином, розглянуті методи та засоби захисту кінцевих точок, а також рекомендації щодо їх вибору та впровадження допоможуть забезпечити повний захист кінцевих точок організації та забезпечити їх безпеку перед виявленими загрозами.

ПЕРЕЛІК ПОСИЛАНЬ

1.Share of common vulnerabilities and exposures (CVEs) on endpoints of selected platforms being under attack as of 1st half 2023. URL: https://www.statista.com/statistics/1450556/cves-endpoints-attacked-selected-platforms/ (дата звернення 08.11.2024).

2. Common IT Security Vulnerabilities Exposed Worldwide. URL: https://electroiq.com/stats/home-security-camera-statistics/ (дата звернення 08.11.2024).

3. Man-in-the-Middle (MitM) attacks reaching inboxes increase 35% since 2022. URL: https://cofense.com/blog/cofense-intelligence-strategic-analysis-2/ (дата звернення 08.11.2024).

4. Evil Twin Attack: What it is, How to Detect & Prevent it. URL: https://www.varonis.com/blog/evil-twin-attack (дата звернення 08.11.2024).

5. Unencrypted communications. URL: https://portswigger.net/kb/issues/01000200_unencrypted-communications (дата звернення 08.11.2024).

6. Популярне антивірусне програмне забезпечення для вашої безпеки в Інтернеті. URL: https://www.websiterating.com/uk/blog/online-security/best-antivirus-software/ (дата звернення 08.11.2024).

7. Що таке Endpoint Detection and Response (EDR). URL: https://gridinsoft.ua/edr (дата звернення 08.11.2024).

8. The Top 11 Endpoint Security Solutions For Business. URL: https://expertinsights.com/insights/the-top-endpoint-security-solutions-for-business/ (дата звернення 09.11.2024).

9.Молодіжна наукова ліга. URL: https://archive.liga.science/index.php/conference-proceedings/issue/view/ukr-22.11.2024?utm_source=eSputnik-

promo&utm_medium=email&utm_campaign=MNL_Konferenc%D1%96ja_%7C_Status_:_opubl%D1%96kovano&utm_content=2782780369&etm_term=aWlkPTZkNTAzMDNiLWMxODgtNDBhZS1iY2Y5LWUwZGJiYTJiNTM5MSZjaWQ9Mjc4Mjc4MDM2OQ== (дата звернення 06.12.2024).

10. Bitdefender GravityZone Business Security. URL: https://bitdefender.ua/for-business/business-security/ (дата звернення 10.11.2024).

11. Bitdefender GravityZone for Enterprize. URL: https://www.fortsoft.com.ua/ua/catalog/zashchita-informatsii/bitdefender-gravityzone-business-security-for-servers.html (дата звернення: 10.11.2024).

12. Основні тенденції у кібербезпеці на 2024 рік: які виклики стоять перед бізнесом. URL: https://www.issp.ua/post/main-cybersecurity-trends-in-2024 (дата звернення: 13.11.2024).