ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ КОРПОРАТИВНИХ КІНЦЕВИХ ТОЧОК ВІД НОВІТНІХ ЗАГРОЗ НА БАЗІ РІШЕННЯ BITDEFENDER GRAVITYZONE ELITE»

Виконала студентка 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Ліщук І.В.
(прізвище та ініціали)
Керівник Гахов С.О.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"___"_____ 2021 року

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

Ліщук Інні Володимирівні
(прізвище, ім'я, по батькові)

1. Тема магістерської роботи: «Технологія захисту корпоративних кінцевих точок від новітніх загроз на базі рішення Bitdefender GravityZone Elite»

керівник магістерської роботи Гахов Сергій Олександрович, к.військ.н., доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «___» _____ 2021 року №____.

2. Строк подання студентом магістерської роботи 15.12.2021 р.

3. Вихідні дані до магістерської роботи
корпоративна інформаційна система;
програмні комплекси управління захистом кінцевих точок;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність проблеми захисту кінцевих точок корпоративної інформаційної системи.
2. Призначення, можливості та функції програмного забезпечення для захисту кінцевих точок.
3. Методи та засоби управління захистом кінцевих точок.
4. Варіант технології управління захистом кінцевих точок корпоративної інформаційної системи.
5. Перелік графічного матеріалу

1. Тема магістерської роботи.
2. Об’єкт, предмет, мета та наукові завдання дослідження.
3.
4.
5.
6.
7.
8.
9.
10.

6. Дата видачі завдання 27.09.2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми захисту кінцевих точок корпоративних інформаційних систем.	27.09.2021 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	07.10 2021 р.	
3.	Аналіз методів та засобів захисту кінцевих точок.	23.10.2021 р.	
4.	Розроблення варіанту топології системи управління захистом кінцевих точок корпоративної інформаційної системи.	10.112021 р.	
5.	Розроблення рекомендацій щодо застосування технології управління захистом кінцевих точок корпоративної інформаційної системи.	01.12.2021 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	15.12.2021 р.	
7.	Підготовка доповіді до захисту.	15.12.2021 р.	

Студент Ліщук І.В.
(підпис) прізвище та ініціали

Керівник магістерської роботи Гахов С.О.
(підпис) прізвище та ініціали

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Ліщук І.В. до захисту магістерської роботи
(прізвище та ініціали)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Технологія захисту корпоративних кінцевих точок від новітніх загроз на базі рішення Bitdefender GravityZone Elite».

Магістерська робота і рецензія додаються.

Директор інституту _____ _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Ліщук І.В. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2020 року по 2022 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту _____ Журенко О.В.
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студентка ***Ліщук І.В.*** обрала тему роботи, метою якої було дослідити методи та засоби управління захистом кінцевих точок корпоративної інформаційної системи на базі рішення Bitdefender GravityZone Elite, а також розробити варіант технології управління захистом кінцевих точок корпоративної інформаційної системи. Перелік використаних джерел свідчить про вміння магістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Ліщук І.В. показала відмінну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконувала сумлінно, акуратно та вчасно за планом.
Все це дозволяє оцінити виконану магістерську роботу студентки Ліщук Інни Володимирівни на оцінку «відмінно» та присвоїти йому кваліфікацію 2149.2 професіонал з організації інформаційної безпеки, викладач закладу вищої освіти.

Керівник магістерської роботи _____ Гахов С.О.
(підпис) (прізвище та ініціали)
“____” _____ 2021 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студентка Ліщук І.В.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина магістерської роботи: 75 сторінок, 40 рисунків, 28 джерел.

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

Предмет дослідження – технологія управління захистом кінцевих точок корпоративної інформаційної системи.

Мета роботи – розробити варіант технології застосування системи управління захистом кінцевих точок корпоративної інформаційної системи та рекомендації щодо її реалізації на підприємстві.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу управління захистом кінцевих точок корпоративної інформаційної системи.

В роботі проведено аналіз проблеми забезпечення кібербезпеки корпоративної інформаційної системи та досліджено існуючі технології управління захистом кінцевих точок корпоративної інформаційної системи.

Проаналізовано методи та засоби управління захистом кінцевих точок на прикладі рішення Bitdefender GravityZone Elite. Визначено призначення, можливості, основні функції, компоненти та склад програмного комплексу Bitdefender GravityZone Elite. Визначено призначення, основні функції та принципи роботи модуля «Policy» для управління захистом кінцевих точок.

На основі досліджень проведених в роботі розроблено варіант технології застосування системи управління захистом кінцевих точок корпоративної інформаційної системи та рекомендації щодо її реалізації на підприємстві.

Галузь використання – кібербезпека корпоративної інформаційної системи.

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, ЗАХИСТ КІНЦЕВИХ ТОЧОК, МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК, ТЕХНОЛОГІЯ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК

ABSTRACT

Master's thesis: 75 pages, 40 figures, 28 sources.

Object of research – the process of ensuring the protection of endpoints of the corporate information system.

Subject of research – the technology for managing the protection of endpoints of the corporate information system.

The aim of research – to develop a variant of the technology of application of the endpoint protection management system of the corporate information system and recommendations for its implementation at the enterprise.

Research methods – elaboration of literature on the topic, analysis of operational documentation, international standards and their comparison, modeling of the process of managing the protection of the endpoints of the corporate information system.

The paper analyzes the problem of cybersecurity of the corporate information system and examines the existing technologies for managing the protection of endpoints of the corporate information system.

Methods and tools for managing endpoint protection on the example of Bitdefender GravityZone Elite solution are analyzed. The purpose, capabilities, main functions, components and composition of the Bitdefender GravityZone Elite software package have been determined. The purpose, main functions and principles of operation of the module «Policy» for management of protection of endpoints are defined.

Based on the research conducted in the work, a variant of the technology of application of the management system of endpoint protection of the corporate information system and recommendations for its implementation at the enterprise have been developed.

Field of use – cybersecurity of corporate information system.

CORPORATE INFORMATION SYSTEM, CYBER SECURITY, ENDPOINT PROTECTION, METHODS AND MEANS OF MANAGEMENT OF ENDPOINT PROTECTION FOR TECHNICS

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АРМ – автоматизоване робоче місце

КІС – корпоративна інформаційна система

ПЗ – програмне забезпечення

AD – Active Directory

ATC – Advanced Threat Control

AV – Antivirus

BEC – Business Email Compromise

BYOD – Bring Your Own Device

CLI – Command Line Interface

CRM – Customer Relationship Management

DDoS – Distributed Denial of Service

EDR – Endpoint Detection and Response

ERP – Enterprise Resources Planning

ICS – Industrial Control System

IDS – Intrusion Detection System

MFA – Multi-Factor Authentication

NGAV – Next Generation Antivirus

NGEPP – Next Generation Endpoint Protection

OU – Organizational Unit

POP3 – Post Office Protocol Version 3

PUA – Potentially Unwanted Application

RAT – Remote Access Trojan

SCM – Supply Chain Management

SIEM – Security Information and Event Management

SMTP – Simple Mail Transfer Protocol

ВСТУП

Комп'ютерні та інформаційні технології сьогодні охопили усі галузі економіки. Для будь-якої сучасної компанії інформація стає одним із головних ресурсів, збереження та правильне розпорядження яким має ключове значення для розвитку бізнесу та зниження рівня різноманітних ризиків. Актуальною проблемою для підприємства стає забезпечення інформаційної безпеки [1].

Коли йдеться про захищеність IT-інфраструктури, мається на увазі безпека інформаційних систем, з яких вона складається. Але коли йдеться про захищеність організації – це насамперед захищеність бізнесу, його безперервність, стійкість до впливу зовнішніх чинників, підтримка рівня репутації та затребуваності. Сьогодні робота будь-якої організації може зупинитися не лише через економічні чинники. Кібератака – одна з потенційних причин зниження темпів розвитку бізнесу та неможливості досягнення стратегічних цілей.

Для захисту кінцевих точок від загроз, розроблені спеціальні програми – антивіруси. Сучасні антивірусні програми є багатофункціональними продуктами, що поєднують у собі як превентивні, профілактичні засоби, так і засоби лікування вірусів і відновлення даних. У сучасних умовах антивірусний захист став дуже актуальним через щорічне збільшення кількості вірусних атак та кіберзлочинів [2].

Згідно з дослідженням Ponemon Institute у 2020 році , за попередні 12 місяців 68% організацій зазнали однієї або кількох атак на кінцеві точки, які успішно зламали дані та/або їх IT-інфраструктуру. Відповідно до звіту компанії Accenture за 2021 рік, 82% компаній збільшили витрати на кібербезпеку, але кількість зломів, включаючи несанкціонований доступ до даних, додатків, сервісів, мереж або пристроїв, зріс на 31% порівняно з 2020 роком [3].

Затребуваність та складність захисту кінцевих точок посилюється тим, що саме вони все частіше вибираються первинними цілями атак зловмисників, тому багатьом організаціям дедалі гостріше стає питання перегляду стратегії захисту

кінцевих точок, оскільки вони є найважливішими елементами інфраструктури, що потребують підвищеної уваги до питань безпеки [4].

Вищесказане визначає актуальність теми даної магістерської роботи, основний зміст якої становить дослідження технології захисту корпоративних кінцевих точок від новітніх загроз, а також розробка методів та засобів для забезпечення їхньої безпеки на базі рішення Bitdefender GravityZone Elite.

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

Предмет дослідження: технологія управління захистом кінцевих точок корпоративної інформаційної системи.

Мета роботи: розробити варіант технології управління захистом кінцевих точок корпоративної інформаційної системи та рекомендації щодо її застосування на підприємстві.

Наукові завдання:

проаналізувати актуальність проблеми захисту кінцевих точок корпоративної інформаційної системи;

дослідити призначення, можливості та функції програмного забезпечення для захисту кінцевих точок;

дослідити методи та засоби управління захистом кінцевих точок.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

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

Інформаційні та телекомунікаційні технології та системи міцно увійшли в життя більшості підприємств і організацій. Сьогодні корпоративні інформаційні системи в інфраструктурі бізнесу відіграють величезну роль у зниженні витрат підприємств за рахунок оптимізації внутрішніх процесів, автоматизації бізнес-процесів та надання інформації керівникам усіх рівнів. Впливаючи на внутрішні процеси в компаніях, вони змінили і процеси їх взаємодії із зовнішнім середовищем, ставши маркетинговим інструментом і механізмом управління для отримання оптимальних результатів господарської діяльності.

Корпоративна інформаційна система (КІС) – це інформаційна система, яка підтримує автоматизацію функцій управління і надає інформацію для поглиблення знань та прийняття управлінських рішень. В ній реалізована сучасна управлінська ідеологія, яка поєднує бізнес-стратегію підприємства і прогресивні інформаційні технології [5].

Сучасні підприємства являють собою складні динамічні системи. Вони розвиваються в часі і включають велику кількість елементів, що реалізують різні виробничі та управлінські функції. Такі економічні об'єкти мають багаторівневу структуру, а також великі зовнішні та внутрішні інформаційні зв'язки. У теперішній час компанії починають розуміти всю важливість і необхідність комплексного підходу до автоматизації інформаційних процесів.

Головне завдання КІС – ефективне управління всіма ресурсами підприємства (матеріально-технічними, фінансовими, технологічними та інтелектуальними) для отримання максимального прибутку та задоволення матеріальних та професійних потреб усіх працівників підприємства.

Основне призначення КІС – своєчасне надання несуперечливої, достовірної та структурованої інформації для прийняття управлінських рішень.

КІС надає можливість вирішення таких глобальних задач [6]:

зробити прозорим для керівництва використання вкладених у бізнес капіталів;

надати повну інформацію для економічної доцільності стратегічного планування;

професійно керувати витратами, наочно і своєчасно показувати, за рахунок чого можна мінімізувати витрати;

реалізувати оперативне управління підприємством згідно вибраних ключових показників (собівартість продукції, структура витрат, рівень прибутковості тощо);

забезпечити гарантовану прибутковість підприємства за рахунок оптимізації і прискорення ряду процесів (строків виконання нових замовлень , перерозподілу ресурсів тощо).

Отже, КІС охоплює всі бізнес-функції і всі управлінські процеси корпорації. В умовах великих підприємств і корпорацій вона може бути більш ефективна, оскільки забезпечує взаємодію масових і добре організованих процесів швидкодіючими засобами сучасних інформаційних і телекомунікаційних технологій високого науково-технічного рівня.

Але на власному досвіді багато розробників усвідомили, що ефективність автоматизації в першу чергу залежить від того, наскільки широко вона охоплює комплекси розрахунків, проведених в управлінні. Тому останнім часом, стала дуже популярною ідея побудови КІС не тільки на великих, територіально-росподілених інформаційних системах, але і в будь-яких підприємствах, незалежно від їх масштабу і форми власності. Організація, маючи сьогодні одну мережу з локальним сервером і десятком комп'ютерів, завтра може розширитися і представляти із себе саморегулюючу систему, здатну гнучко і оперативно перебудовувати принципи свого функціонування, маючи в своєму активі інтеграцію великого числа програмних продуктів [7].

Основними особливостями КІС є:

комплексність охоплення функцій управління;

підвищена впорядкованість ділових процесів;

масовість операцій;

ефективність використання комп'ютерно-телекомунікаційного устаткування і програмного забезпечення;

можливість локальної установки та впровадження окремих частин системи;

можливість розвитку системи після її впровадження.

Єдність інформаційної системи управління підприємством полягає в тому, що дані, отримані або введені на будь-якому рівні системи, повинні бути доступні всім її компонентам (принцип одноразового введення).

КІС за своїм складом є сукупністю різних програмно-апаратних платформ, універсальних і спеціалізованих додатків різних розробників, інтегрованих в єдину інформаційно-однорідну систему, яка найкраще вирішує унікальне завдання кожного конкретного підприємства. Тобто, КІС – людино-машинна система та інструмент підтримки інтелектуальної діяльності людини, яка під її впливом має:

накопичувати певний досвід та формалізовані знання;

постійно вдосконалюватись та розвиватися;

швидко адаптуватися до умов зовнішнього середовища та нових потреб підприємства.

На сьогоднішній день корпоративні інформаційні системи є невід’ємною складовою конкурентного функціонування сучасного підприємства. Зручність використання, майже не обмежений функціонал, невисока вартість розгортання – це основні переваги даного типу систем.

Першим і основним елементом інформаційної системи управління підприємством є система управління бізнес процесами підприємства – це система класу ERP (Enterprise Resources Planning – Планування ресурсів підприємства). Основним призначенням ERP систем є автоматизація процесів планування, обліку і управління за основними напрямками діяльності підприємств [8].

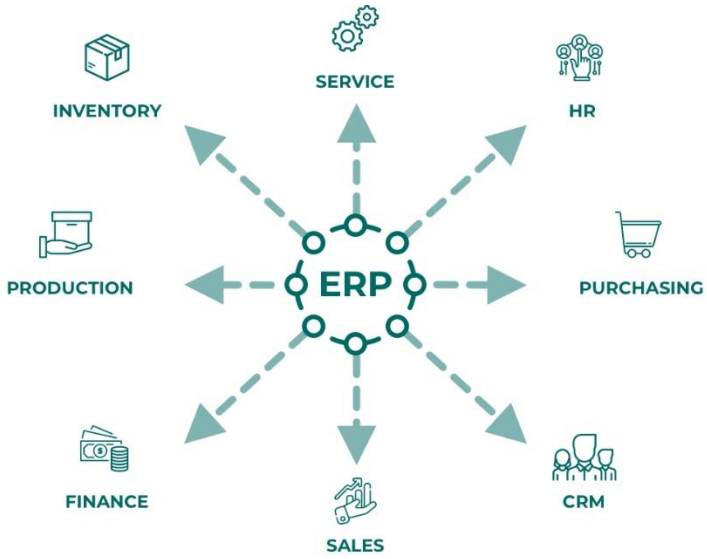


Рис. 1.1. Структура ERP-системи [8]

В загальних рисах можна розглядати як інтегровану сукупність наступних основних підсистем:

управління сервісним обслуговуванням;

управління персоналом;

управління закупками;

управління взаємодією з клієнтами;

управління продажами;

управління фінансами;

управління виробництвом;

управління матеріальними потоками.

Спільна робота підприємства та його партнерів реалізується за рахунок переходу від закритої архітектури традиційних ERP-систем до відкритої компонентної Web-архітектури. В якості підсистем використовуються CRM (Customer Relationship Management – управління відносинами з клієнтами) і SCM (Supply Chain Management – управління ланцюгами поставок).

Як зазначалося вище, основним принципом ERP є центральний збір даних для широкого розповсюдження. ERP-системи структурують та оптимізують, щоб усі користувачі – від генерального директора до робітника компанії могли створювати, зберігати та використовувати ті самі дані, отримані за допомогою

загальних процесів. За допомогою захищеного та централізованого сховища даних можна розраховувати, що дані є правильними, актуальними та повними.

Цілісність даних гарантується для кожного завдання, що виконується в організації, від квартальної фінансової звітності до єдиного звіту про заборгованість, не покладаючись на електронні таблиці, схильні до помилок.

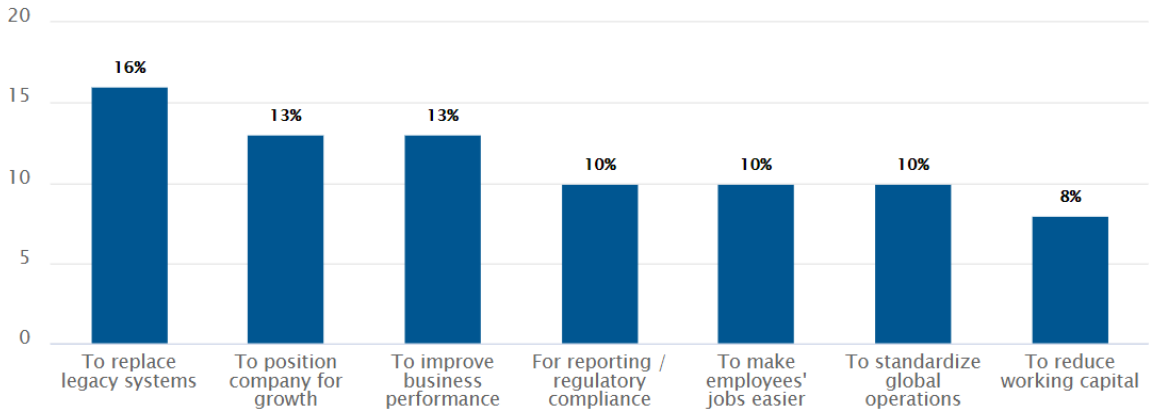


Рис. 1.2. Причини впровадження ERP за даними 2020 року компанії Panorama Consulting Solutions [9]

Як показано на рис. 1.2, основною причиною, чому компанії вибирають ERP-системи є заміна застарілих систем, далі йдуть амбіції організації до зростання та покращення до результативності бізнесу. На одному рівні йдуть такі причини як: звітування, відповідність до законодавства, щоб зробити роботу працівників легше та стандартизація глобальних операцій. І, наостанок, щоб зменшити оборотний капітал [9].

Функціональність інформаційної системи визначається характером діяльності та видом бізнесу компанії, організаційною та юридичною структурою, географічним розташуванням філій тощо.

Однак можна виділити базову функціональність КІС, яка необхідна для інформаційної підтримки та автоматизації бізнес-процесів будь-якої компанії:

інформаційна підтримка та автоматизація процесів бухгалтерського обліку, розрахунку заробітної плати, а також формування внутрішньої та зовнішньої

фінансової та податкової звітності, що регламентується внутрішніми корпоративними стандартами та зовнішнім законодавством.

підтримка розподіленого електронного документообігу підприємства (створення документа, підтримка процедури узгодження документа, постановка документа на облік, зберігання електронної версії документа, захист від несанкціонованого доступу, архівування).

інформаційна підтримка організаційно-функціональної структури, діловодства та кадрового документообігу.

підтримка та ведення нормативно-довідкової інформації [9].

Автоматизація діяльності великих підприємств є досить складним завданням і вимагає, як правило, індивідуального підходу, що враховує особливості організації. Інформаційні системи для таких підприємств досить різноманітні, однак будуються з використанням загальних принципів обробки та зберігання облікових даних.

Отже, основною метою КІС має стати автоматизація всього підприємства, щоб отримати замкнуту, саморегулювану систему, яка здатна гнучко і оперативно перебудовувати принципи свого функціонування у разі реструктуризації. Внаслідок впровадження КІС збільшуються обсяги продажу, знижується собівартість, зменшуються складські запаси, скорочуються терміни виконання замовлень, покращується взаємодія з постачальниками, адже підвищення внутрішньої керованості, гнучкості та стійкості до зовнішніх впливів підвищує ефективність підприємства, її конкурентоспроможність, а, зрештою – прибутковість.

1.2 Аналіз проблеми забезпечення захисту кінцевих точок корпоративної інформаційної системи

Безпека кінцевої точки, також відома як захист кінцевої точки, – це підхід до безпеки мережі, що складається з набору процесів, які ідентифікують, запобігають і реагують на відомі та невідомі загрози. Ці загрози можуть виникати через різні

кінцеві точки, які підключаються до бізнес-мережі IT, які діють як шлюзи для потенційних експлойтів або вторгнень у мережу. Загрози можуть бути засновані на зловмисному програмному забезпеченні або не на його основі, наприклад, крадіжка даних або фізичне пошкодження компонентів обладнання тощо [10].

Але з кожним роком все більш гострою проблемою для багатьох організацій з різних сфер діяльності стає ймовірність зіткнення з цілеспрямованими атаками, які все частіше застосовують поєднання поширених загроз, уразливостей нульового дня, унікальних схем без використання шкідливого програмного забезпечення, безфайлових методів та ін.

Платформа захисту кінцевих точок є важливою частиною кібербезпеки підприємства з ряду причин. Перш за все, у сучасному діловому світі дані часто є найціннішим активом компанії, і втрата цих даних або доступу до них може поставити весь бізнес під загрозу. Підприємствам довелося боротися не тільки зі зростанням кількості кінцевих точок, але й зі зростанням кількості типів кінцевих точок. Ці фактори самі по собі ускладнюють безпеку кінцевих точок підприємства, але до них додається віддалена робота та політика BYOD, що робить безпеку периметра все більш недостатньою та створює вразливості [11].

Врешті-решт, кінцеві точки, включаючи робочі станції, ноутбуки, сервери та смартфони є критично важливими об'єктами контролю, оскільки вони залишаються для зловмисників, у більшості випадків, досить простими та популярними точками проникнення, що підвищує значущість контролю за ними [3].

Інформація, що обробляється в корпоративних мережах, особливо вразлива. Суттєвого підвищення можливості несанкціонованого використання або модифікації даних, або зараження КІС різноманітним шкідливим ПЗ в даний час сприяють:

збільшення обсягів оброблюваної, переданої і збереженої в комп'ютерах інформації;

зосередження в базах даних інформації різного рівня важливості і конфіденційності;

розширення доступу кола користувачів до інформації, що зберігається в базах даних, і до ресурсів обчислювальної мережі;

збільшення числа віддалених робочих місць (враховуючи реалії сьогодення, більшість робітників працюють вдома, що зменшує рівень забезпечення безпеки компаній);

широке використання глобальної мережі Інтернет і різних каналів зв'язку;

автоматизація обміну інформацією між комп'ютерами користувачів тощо.

Кібератаки можуть впливати на інформаційний простір комп'ютера, де знаходяться відомості, зберігаються матеріали фізичного або віртуального пристрою. Атака, як правило, вражає носій даних, спеціально призначений для їх зберігання, обробки та передачі особистої інформації користувача.

Техніки нападу кіберзлочинців зазнали значних змін. Зловмисники стали більш агресивними у своїх підходах до проведення атак і більш досконалими в організації всіх етапів процесу. Дедалі частіше з'являються новини про черговий гучний інцидент. Компаніям доводиться визнавати факт спрямованої на них кібератаки та підраховувати прямі та непрямі збитки.

Згідно з дослідженням Ponemon Institute у 2020 році виявлено, що 68% IT-фахівців виявили, що частота атак на кінцеві точки зросла порівняно з роком раніше.

8 листопада 2021 року компанія Accenture повідомила, що випустила звіт «State of Cybersecurity Resilience 2021». Дослідження відповідає питанням: наскільки ефективні заходи вживають компанії захисту корпоративних мереж. Команда Accenture Research опитала 4744 керівників компаній з річним прибутком не менше 1 млрд доларів у 23 галузях та 18 країнах світу [3].

Більше 55% великих компаній недостатньо ефективно попереджають кібератаки, а також надто повільно виявляють та усувають уразливості, йдеться у дослідженні Accenture.

У середньому на одну компанію припало 270 інцидентів, що на 31% більше ніж у попередньому році [12].

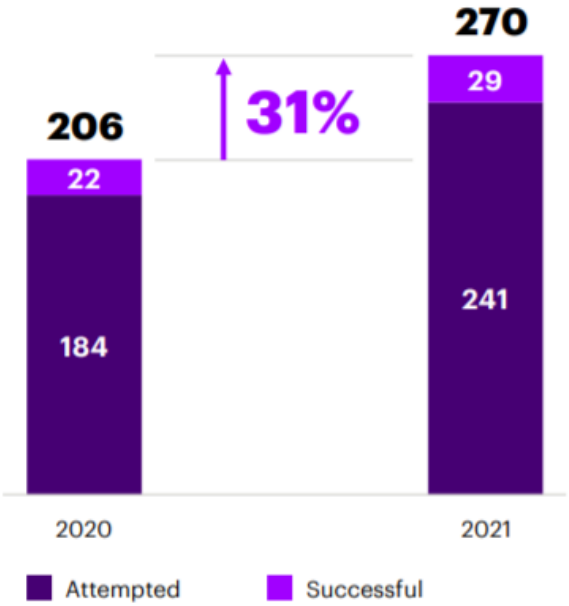


Рис. 1.3. Середній приріст атак на компаній за результатом звіту «State of Cybersecurity Resilience 2021» [12]

Кіберзлочинці процвітають завдяки «зривам» – все, від землетрусів до революцій, можна використати для реалізації будь-яких кібератак, оскільки люди відволікаються, а кібербезпека є останнім, про що вони думають. І, звичайно, останнім часом не було нічого більш руйнівного та відволікаючого, ніж пандемія Covid-19.

2020 рік, безсумнівно, був одним із найбільш значущих і трансформаційна в останній пам'яті: глобальна пандемія, економічні потрясіння, що впливають на життя мільйонів людей, і соціальні і політичні заворушення. Відгуки цих подій дуже сильно вплинули на бізнес.

IBM Security X-Force використав дані мільярдів кінцевих точок клієнтів і загальнодоступних джерел у період із січня по грудень 2020 року, щоб проаналізувати типи атак, вектори зараження, глобальні та галузеві порівняння заради щорічного звіту «X-Force Threat Intelligence Index 2021» [13]. Нижче наведено деякі з основних висновків, представлених в індексі розвідки загроз X-Force.

Сканування та використання вразливостей вийшли на перше місце як найпоширеніший початковий вектор атаки, який використовується суб'єктами загрози – у 35% усіх інцидентів. Для порівняння, сканування та експлойт виступали використовувалися лише для 30% атак минулого року.

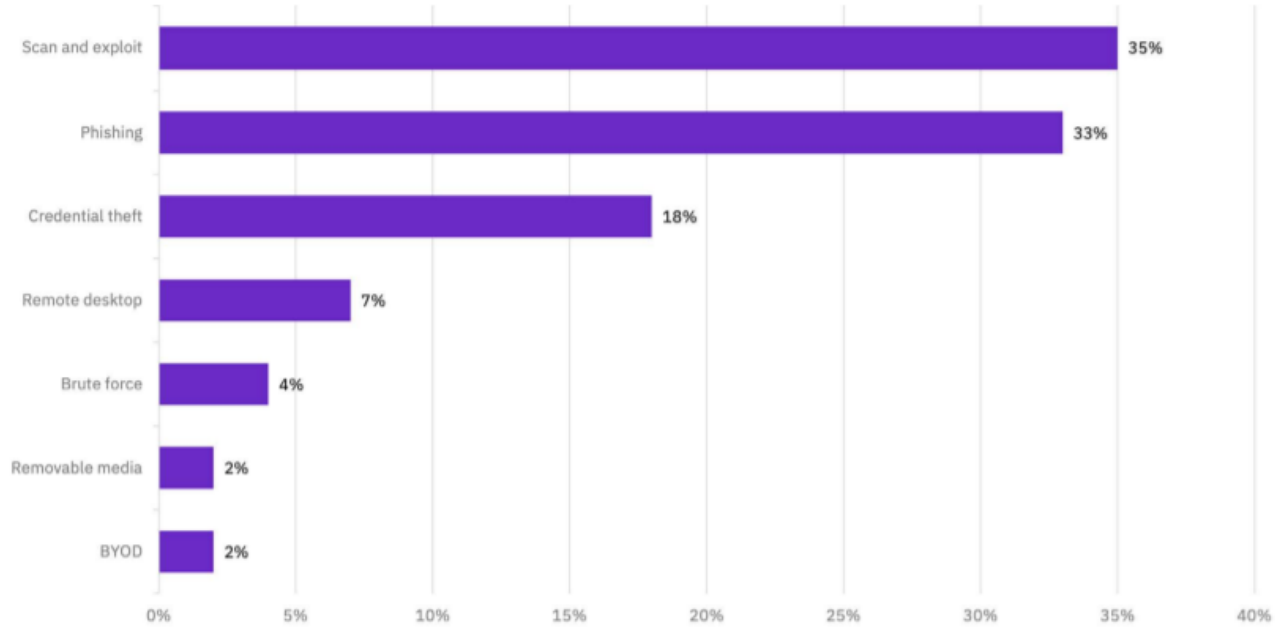


Рис. 1.4. Головні вектори для початку атаки [13]

Атаки сканування та використання зазвичай вимагають мало ресурсів і можуть бути автоматизовані та масштабовані для націлювання на широкий спектр жертв, що може пояснити, чому цей вектор отримав такий великий обсяг у 2020 році.

Фішинг був другим найбільш часто використовуваним, який застосовувався в 33% атак – трохи більше, ніж у 31% минулого року, – що свідчить про те, що зловмисники змінюють методи та захисні механізми проти фішингу.

У середині 2020 року X-Force розкрила глобальну фішингову кампанію, яка охопила понад 100 високопоставлених керівників на керівних посадах та закупівлях для оперативної групи, яка придбала засоби індивідуального захисту у боротьбі з COVID-19.

На крадіжку облікових даних припадало лише 18% атак, що значно скоротилося з 29% минулого року, що свідчить про те, що учасники загроз

використовують методи сканування та використання замість крадіжки облікових даних у 2020 році, швидше за все, через більший рівень успішності сканування.

З переходом компаній на режим віддаленої роботи, відповідно початок атаки відбувався на віддалений доступ – 7%, спроби зламати пароль перебором становили 4%, атаки на з'ємні носії та на власні пристрої BYOD зайняли по 2%.

Рис. 1.5. Загальні висновки IBM «X-Force Threat Intelligence Index 2021» [13]

Найбільш атакованою у 2020 році була Європа, зазнавши 31% атак, зафіксованих X-Force, за нею йдуть Північна Америка (27%) та Азія (25%).

Програми-вимагачі були головним типом атак у Європі в 2020 році, становивши 21% атак. Європа також зазнала великої кількості атак на доступ до серверів – 14% усіх атак на континенті в 2020 році. Крадіжка облікових даних, компроміс ділової електронної пошти (BEC), трояни віддаленого доступу (RAT), шахрайство та DDoS також вплинули на європейські організації в меншій мірі.

За результатами досліджень, серед тенденцій, які були відстеженні, програми-вимагачі (ransomware) продовжують розвиватися і стають першим типом загрози, що становить 23% подій безпеки, на які X-Force реагував у 2020 році.

За консервативними підрахунками X-Force, лише учасники програм-вимагачів Sodinokibi (також відомі як REvil) отримали щонайменше 123 мільйони доларів прибутку в 2020 році і вкрали близько 21,6 Тб даних.

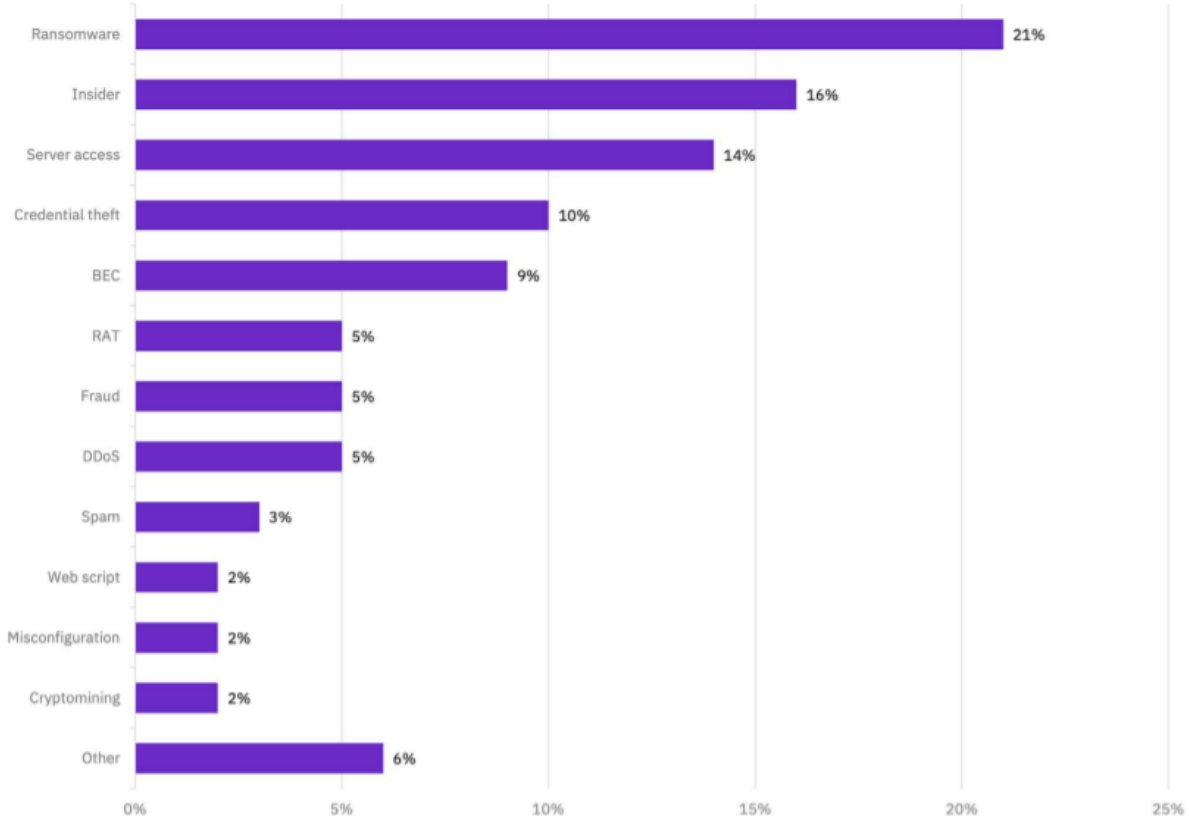


Рис. 1.6. Найпопулярніші типи атак у Європі за 2020 рік [13]

Промислові підприємства були другою за кількістю нападів галуззю, піднявшись з восьмого місця в 2019 році і поступившись лише фінансовим послугам. Уразливості, пов'язані з промисловими системами контролю (ICS), виявлені в 2020 році, були на 49% більше, ніж у 2019 році.

Sector	2020 rank	2019 rank	Change
Finance and insurance	1	1	-
Manufacturing	2	8	6
Energy	3	9	6
Retail	4	2	-2
Professional services	5	5	-
Government	6	6	-
Healthcare	7	10	3
Media	8	4	-4
Transportation	9	3	-6
Education	10	7	-3

Рис.1.7. ТОП-10 галузей за обсягом атак [13]

Рис 1.8. зображує найбільші атаки на кожну галузь за даними X-Force.

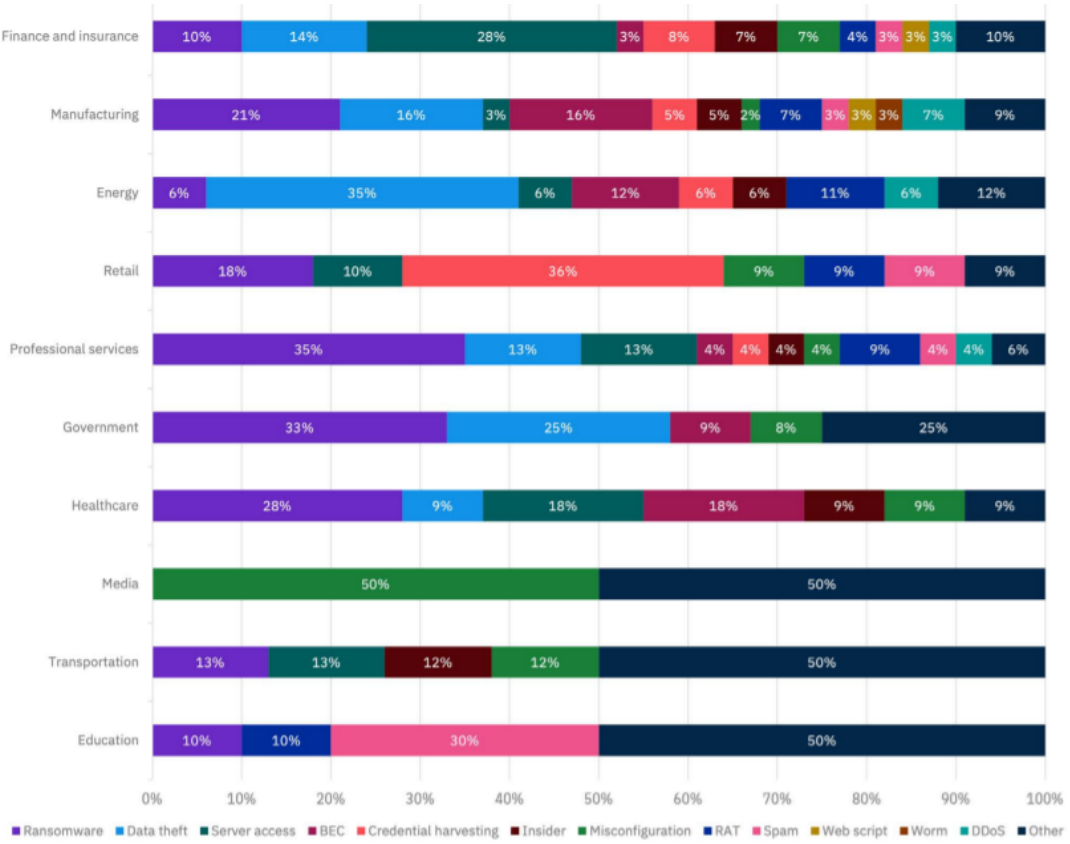


Рис. 1.8. Типи атак у відсотковому відношенні за галузями [13]

Побудова корпоративної системи інформаційної безпеки починається із забезпечення комплексного захисту кінцевих точок від усіх перелічених вище загроз. Ландшафт сучасних інформаційних загроз потребує багаторівневого підходу до захисту.

1.3 Аналіз існуючих технологій управління захистом кінцевих точок корпоративної інформаційної системи

Думка про те, що кожна система надійна настільки, наскільки надійний найслабший її елемент, особливо правильна і актуальна, коли йдеться про захист корпоративної мережі, найуразливішими елементами якої є кінцеві точки. І про це знають не лише фахівці з кібербезпеки, а й хакери, які використовують все більш витончені методи, атакуючи кінцеві точки [14].

З цієї причини надзвичайно важливо, щоб організація, не залежно від її розміру, мала ефективний план кібербезпеки для виявлення та припинення атак. Важливою частиною цього має бути впровадження надійної безпеки кінцевих точок на всіх пристроях компанії. Сучасні системи захисту кінцевих точок розроблені для швидкого виявлення, аналізу, блокування та стримування атак, що відбуваються.

Існує безліч традиційних рішень для безпеки комп'ютерних пристроїв, але вони вже не завжди успішно справляються з величезною кількістю атак, складними вірусами, атаками високого рівня. Традиційне антивірусне програмне забезпечення, хоча іноді й ефективне, але не відстежує та не перевіряє потенційний вірус, оскільки використовує методи виявлення на основі сигнатур, від яких суб’єкти загроз вже давно навчилися уникати. Антивіруси, побудовані на принципі реактивного захисту вважаються застарілими, оскільки обсяг і складність кібератак неухильно зростає, тому постає потреба в більш просунутих рішеннях безпеки кінцевих точок.

Це зумовило виникнення антивірусів класу Next Generation Endpoint Protection (NGEPP). Продукти NGEPP захищають кінцеві точки шляхом зупинення загроз наступного покоління. Програми класу NGEPP здатні не лише виявляти шкідливі програми, наявні на комп'ютері, а й шкідливі дії та найскладніші методи атак зараження кінцевих точок, які використовуються зловмисниками.

Next Generation Antivirus (NGAV) використовує комбінацію сучасних технологій, включаючи машинне навчання та штучний інтелект, щоб ефективніше виявляти та видаляти загрози, щоб створити прогнозну аналітику, яка ідентифікує зловмисне програмне забезпечення та шкідливу поведінку, перш ніж вони зможуть зашкодити кінцевим точкам та корпоративній інформаційній системі вцілому [15]. Також використовує алгоритми, які досліджують процеси, дані, використання додатків, мережеву активність і поведінку кінцевого користувача, щоб зрозуміти нетипову діяльність, яку потім можна оцінити.

Це відрізняється від традиційного AV тим, що за допомогою AV програмісти зазвичай ідентифікують атаку вже після того, як вона вразила КІС, і потім лише

усувають її та розробляють виправлення для користувачів через оновлення своєї платформи.

Ключова відмінність полягає в тому, що *проактивний захист* – працює на випередження, тоді як традиційний – *на виправлення помилок* [16].

Сучасні зловмисники точно знають, де знайти прогалини та слабкі місця в безпеці периметра мережі організації – і вони проникають в них способами, які легко обходять традиційне антивірусне програмне забезпечення.

Рішення захисту кінцевих точок наступного покоління вміють відслідковувати пам'ять і зупиняти програми зі шкідливим кодом, що прослизнули повз інші засоби захисту. Продукти захисту кінцевих точок наступного покоління добре захищають конфіденційну інформацію компанії, інтелектуальну власність, персональні дані клієнтів за допомогою інструментів шифрування інформації. При цьому працівники мають простий та зручний доступ до даних організації, темп роботи не знижується [3].

Але все ж таки головний недолік проактивного захисту – так звані помилкові спрацьовування, часті блокування незараженого програмного забезпечення. Мінус реактивного захисту – неможливість захиститися від нових загроз. У сучасному антивірусному ПЗ використовується і проактивний, і реактивний захист.

У звіті Gartner від 2021 року «Magic Quadrant for Endpoint Protection Platforms» зазначено: «Захист кінцевих точок розвивається, вирішуючи більшість завдань адаптивної архітектури безпеки Gartner, включаючи посилення захисту, дослідження, виявлення інцидентів та реагування на них. Керівники, що керують ризиками та безпекою, повинні переконатися, що їхній виробник рішень для захисту кінцевих точок еволюціонує досить швидко, щоб долати сучасні загрози» [17].

Цей квадрант оцінює інновації, які дозволяють організаціям захищати свої корпоративні кінцеві точки від атак і злому. Розвиток технологій і практик у цій сфері обумовлений двома тенденціями: зростанням і ускладненням атак на кінцеві точки та раптовим сплеском віддаленої роботи [18].

Рис. 1.8. «Magic Quadrant for Endpoint Protection Platforms» за 2021 рік [18]

Таким чином, загальна кількість постачальників, що з'явились у магічному квадранті на 2021 рік, становить 19: Bitdefender, BlackBerry (Cylance), Broadcom (Symantec), Check Point Software Technologies, Cisco, CrowdStrike, Cybereason, ESET, FireEye, Fortinet, F-Secure, Kaspersky, McAfee, Microsoft, Panda Security, SentinelOne, Sophos, Trend Micro і VMware Carbon Black.

Квадрант, як зазвичай ділиться на чотири категорії:

Нішеві гравці (Niche Players), за визначенням Gartner, забезпечують основні необхідні можливості, але часто обмежуються обслуговуванням певним географічним або розміром клієнтів [19]. Нішеві гравці можуть бути орієнтовані на невеликі сегменти ринку та часто демонструють на них більш високу ефективність, ніж лідери.

Візіонери (Visionaries) інвестують кошти в передові технології, які ляжуть в основу наступного покоління продукту та дозволять покупцям отримувати доступ

до покращеного управління кінцевими точками та їх безпекою. Вендори з цієї групи можуть впливати на розвиток галузі, але не можуть впливати на лідерів та претендентів на лідерство.

Претенденти (Challengers) мають якісні продукти, які задовольняють основним вимогам ринку та мають високий рівень продажів, популярності та частку ринку, що дозволяє їм перевершувати нішевих гравців. Претенденти забезпечують собі прибуток шляхом конкуренції лише на рівні базових функцій, але не на рівні досконаліших можливостей.

Лідери (Leaders) демонструють стабільний прогрес та зусилля за всіма показниками, за якими проводиться оцінка. Їх дії піднімають рівень конкуренції над ринком, можуть змінити курс розвитку всієї індустрії. Як правило, ці постачальники є налагодженими підприємствами з великою базою клієнтів та міцними позиціями на ринку [18].

Нішовими гравцями цього року є FireEye, Bitdefender, F-Secure, Blackberry (Cylance), Fortinet, Check Point Software та Panda Security [19]. Вони успішно зосереджуються на невеликому сегменті, не перевершують інновацій та не перевершують інших. В даній роботі ця категорія буде відігравати ключову роль, адже цільовим продуктом для дослідження був обраний продукт для захисту кінцевих точок саме від компанії Bitdefender.

Але, перед тим, як перейти до безпосереднього опису та дослідження вибраного продукту, необхідно детальніше проаналізувати існуючі технології управління захистом кінцевих точок, які містяться у різних категоріях, для повного розуміння ринку.

Ринок справді переповнений, і існує величезна різноманітність постачальників з різними технологіями, щоб запобігти загрозам в КІС, тому нижче наведено короткий опис найбільш популярних продуктів в сегмент.

ESET Endpoint Security.

ESET Endpoint Security – це хмарне рішення для захисту кінцевих точок, розроблене для захисту організації будь-якого розміру. Рішення пропонує

багаторівневий захист, яким адміністратори можуть керувати за допомогою єдиної централізованої консолі керування. ESET Endpoint Security захищає комп'ютери, мобільні пристрої, файлові сервери та віртуальні середовища. Він доступний як окремий продукт і як частина більш широкого пакета корпоративної кібербезпеки, ESET PROTECT Enterprise, який також включає безпеку файлового сервера, шифрування диска, хмарну пісочницю та EDR.

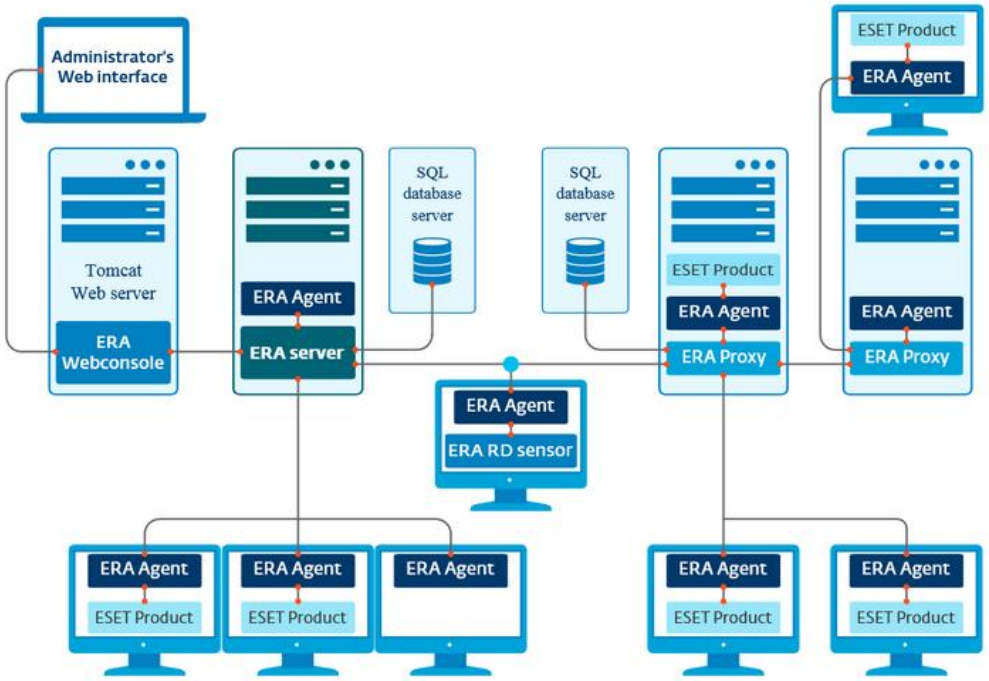


Рис.1.10. Структура програмного рішення ESET Endpoint Security [20]

ESET Endpoint Security також пропонує захист веб-переглядача, запобігаючи завантаженню шкідливих файлів. Хмарне рішення є масштабованим, а також гнучким: ESET Endpoint Security сумісна з операційними системами Windows, Mac, Linux і Android, а також має вбудоване керування мобільними пристроями для iOS і AndroidOS.

McAfee Enterprise.

McAfee Enterprise надає інтегровану, централізовано керовану платформу захисту кінцевих точок із розширеним захистом від загроз. Ключовими сильними сторонами платформи McAfee є виявлення загроз і реагування на них,

які добре інтегруються з Windows. McAfee зосереджена на автоматизації, використовує машинне навчання та поведінковий аналіз, щоб кінцеві точки могли швидше спілкуватися та виявляти загрози. Це означає, що зменшується потреба у ручному виявленні та виправленні, оскільки McAfee може забезпечити автоматичний аналіз, стримування та усунення загроз для кінцевої точки.

McAfee Enterprise підходить для великих клієнтів, які будуть шукати потужне рішення EDR. Клієнти McAfee хвалять службу за простоту використання для кінцевих користувачів. Однак деякі припускають, що сам клієнт займає занадто багато місця на пристроях. Антивірусна безпека кінцевої точки McAfee популярна серед організацій середнього розміру.

Symantec Endpoint Security.

Symantec є ще одним із лідерів ринку захисту кінцевих точок із великою базою клієнтів. Він забезпечує повне інтегроване рішення для кінцевої точки, яке можна розгорнути локально або як хмарне рішення.

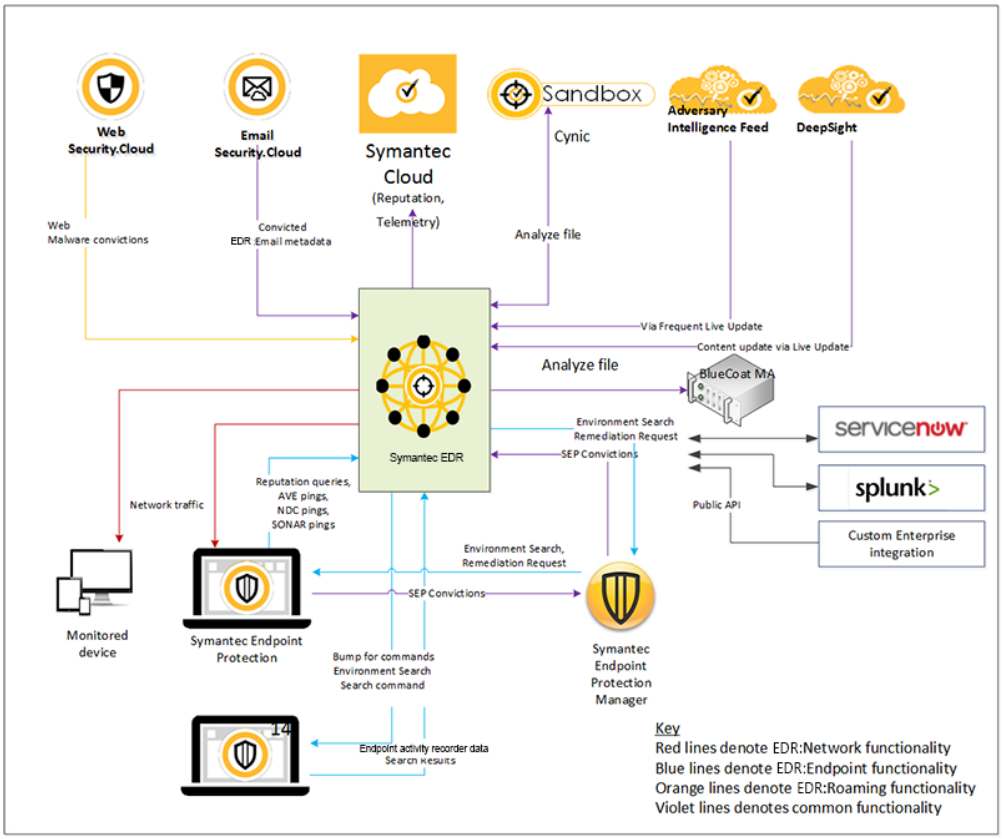


Рис.1.11. Структура програмного рішення Symantec Endpoint Security [22]

Symantec пропонує повнофункціональне рішення захисту кінцевих точок із потужними можливостями запобігання загрозам, включаючи захист від безфайлових атак, покращений захист мобільних додатків, захист для користувачів, підключених до хмари, а також можливість моніторингу та блокування несанкціонованого доступу. Symantec використовує штучний інтелект, щоб полегшити оновлення політики та спростити робочі процеси для команд адміністраторів.

Bitdefender GravityZone.

Bitdefender GravityZone – це платформа захисту кінцевих точок «все в одному», яка забезпечує як захист, так і виявлення загроз і реагування. Bitdefender використовує машинне навчання для моніторингу поведінки та запобігання атак, що, як вони стверджують, зупиняє загрози, які традиційний захист кінцевої точки упустили б. Вони також пропонують розширений контроль кінцевих точок, захистом від веб-загроз та засобами керування програмами та пристроями. Bitdefender може розгортатися в хмарі або локально.

Ключовими сильними сторонами Bitdefender є дослідження загроз і простота керування, а також потужний захист від загроз. Антивірус на основі поведінки може допомогти запобігти атакам на кінцеву точку. У Bitdefender також є велика команда досліджень і розробок, яка допомагає тримати його в курсі нових та нових загроз. Увесь пакет кінцевих точок Bitdefender також керується з однієї консолі адміністратора.

Bitdefender GravityZone простий у використанні, забезпечує надійний захист від загроз і є легким клієнтом для кінцевої точки. Продукт популярний серед малих і середніх організацій, а також серед деяких корпоративних клієнтів [22]. Як зазначено вище, саме цей продукт антивірусного захисту для кінцевих точок є об’єктом дослідження даної роботи, тому він буде детальніше розглянутий нижче.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК НА БАЗІ BITDEFENDER GRAVITYZONE ELITE

2.1 Призначення, можливості та функції Bitdefender GravityZone Elite

Різноманітність кінцевих точок, розвиток BYOD і використання зовнішніх пристроїв зберігання даних створили постійно мінливий периметр безпеки для сучасних організацій, який майже неможливо визначити. Кінцеві точки є поширеною точкою входу для зловмисного програмного забезпечення та інших атак, оскільки вони є легкою точкою доступу для проникнення в мережі, компрометації чи крадіжки конфіденційних даних.

Отже, без належного захисту кінцевої точки підприємство втрачає контроль над конфіденційними даними в момент їх копіювання на зовнішній пристрій або в момент отримання доступу до мережі через незахищену кінцеву точку, що є неприйнятним для будь-якої компанії [23].

Щоб ефективно захиститись від високотехнологічних кібератак, які обходять традиційні засоби захисту кінцевих точок, необхідний багаторівневий підхід захисту, що включає додаткові рівні несигнатурних технологій на базі поведінкового аналізу, машинного навчання та вбудованої пісочниці.

Розробивши GravityZone Endpoint Security, Bitdefender запустив нову адаптивну архітектуру наступного покоління, яка забезпечує найкраще виявлення загроз, запобігання атакам, виправленню модифікованих об'єктів, ефективний моніторинг та оповіщення про події безпеки кінцевого пристрою на єдиній модульній платформі.

Bitdefender GravityZone Elite – це максимальний захист для виявлення загроз, реагування на них та їх усунення на всіх етапах. GravityZone Elite надає багаторівневу архітектуру нового покоління, яка забезпечує запобігання, виявлення, усунення і візуалізацію загроз на єдиній модульній платформі, надає ефективний захист від складних кібератак, які легко обходять традиційні

інструменти безпеки кінцевих точок. GravityZone Elite – це багаторівневий підхід до захисту, машинне навчання, поведінковий аналіз, захист від експлойтів і вбудоване ізольоване програмне середовище.

Рішення GravityZone було розроблено спеціально для надання послуг із захисту бізнесу для фізичних кінцевих пристроїв (в тому числі мобільних), віртуальних машин в приватних і загальнодоступних хмарах, а також поштових серверів Exchange.

GravityZone це продукт з єдиною консоллю управління доступною в хмарі, що надається Bitdefender, або організований в якості віртуального пристрою встановленого локально в компанії, що забезпечує єдину точку для розгортання, дотримання і управління політиками безпеки для будь-якої кількості кінцевих точок, будь-якого типу, в будь-якому місці.

GravityZone забезпечує основні рівні захисту [24]:

1. Захист від шкідливого ПЗ.
2. Розширений контроль загроз (Advanced Threat Control).
3. Виявлення гіпервізора.
4. Брандмауер.
5. Контроль контенту.
6. Контроль пристроїв.
7. Повне шифрування диска.
8. Безпека для поштових серверів Microsoft Exchange.
9. Контроль додатків.
10. Sandbox Analyzer.
11. Безпека для мобільних пристроїв.

Захист від шкідливого ПЗ.

Рівень захисту від шкідливого ПЗ заснований на скануванні сигнатур і евристичному аналізі (B-HAVE, ATC) проти: вірусів, хробаків, троянів, програм-шпигунів, рекламного ПЗ, кейлоггерів, руткітів і інших типів шкідливих програм.

Технологія сканування Bitdefender на наявність шкідливого ПЗ заснована на наступних технологіях:

По-перше, використовується традиційний метод сканування, коли відсканований вміст порівнюється з базою даних сигнатур. У базі даних сигнатур містяться записи байт-кодів, характерні для відомих загроз, які регулярно оновлюються у Bitdefender. Цей метод сканування є ефективним проти відомих загроз, які були досліджені і задокументовані. Проте, незалежно від того, наскільки оперативно база даних оновлює записи, завжди є вікно між тим, коли нова загроза виявлена і коли випущено виправлення.

Проти нових, незареєстрованих загроз, захист здійснює другий шар Bitdefender, використовуючи евристичний двигун B-HAVE, на основі поведінкових характеристик. B-HAVE запускає підозрілі шкідливі програми у віртуальному середовищі, щоб перевірити їх вплив на систему і упевнитися, що вони не представляють ніякої загрози. Якщо загроза виявлена, запобігає запуск програми.

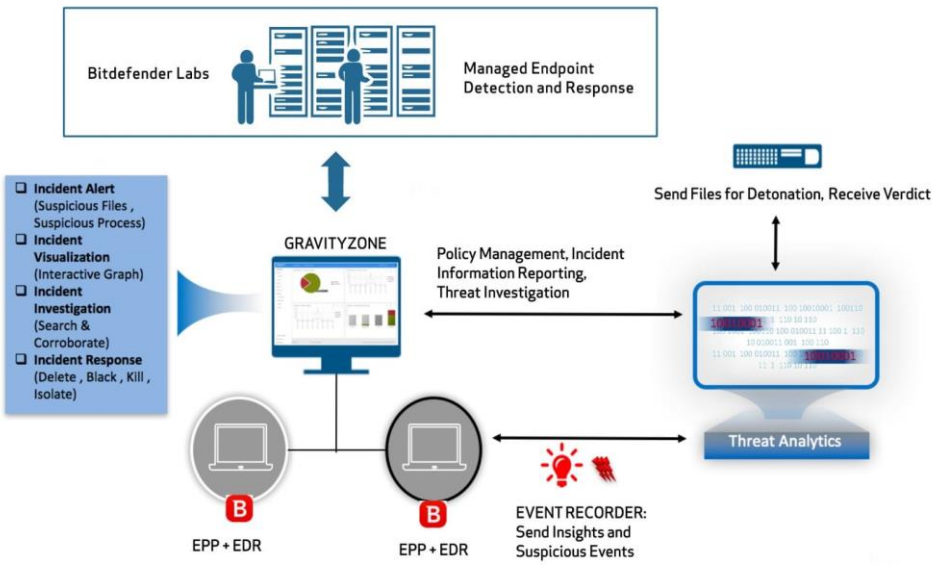


Рис. 2.1. Технологія виявлення та аналізу загроз [24]

Розширений контроль загроз (Advanced Threat Control).

Для загроз, які не перехоплюються навіть евристикою, наявний ще один шар захисту у вигляді Advanced Threat Control (ATC). ATC постійно відстежує запущені процеси і оцінює підозрілу поведінку, таку як: спроби замаскувати тип процесу, виконання коду в пам'яті процесу, реплікацію, переміщення файлів,

приховуваність в списку процесів і т.д. Кожна підозріла поведінка підвищує рейтинг окремого процесу. Коли досягається поріг, включається сигнал тривоги.

Виявлення гіпервізора.

Bitdefender HyperDetect – додатковий рівень безпеки, розроблений спеціально для виявлення просунутих атак і підозрілої активності ще до виконання шкідливих процесів. HyperDetect містить моделі машинного навчання і технології виявлення прихованих атак проти загроз, таких як:

атаки нульового дня;

приховане шкідливе ПЗ;

безфайлові атаки (зловживання PowerShell, інструментарієм управління Windows і т. д.);

крадіжка облікових даних;

цільові кібератаки;

спеціалізоване шкідливе ПЗ;

атаки на основі сценаріїв;

експлойти;

інструменти злому;

підозрілий мережевий трафік;

потенційно небажані програми (PUA);

вимагачі тощо.

Брандмауер.

Брандмауер контролює доступ додатків до мережі і до Інтернету. Доступ дозволяється автоматично, грунтуючись на базі даних відомих, легітимних додатків. Крім того, брандмауер може захистити систему від сканування портів, обмежувати використання загального доступу до Інтернет і попередити, коли нові кінцеві точки підключаються по Wi-Fi.

Контроль контенту.

Модуль контролю контенту допомагає забезпечити дотримання політики компанії щодо дозволеного трафіку, веб-доступу, захисту даних і контролю додатків. Адміністратори можуть задавати параметри сканування трафіку і

виключення, складати графік доступу до мережі Інтернет, блокувати/дозволяти певні веб-адреси або категорії, налаштовувати правила захисту даних і встановлювати дозволи для використання певних програм.

Контроль пристроїв.

Модуль контролю пристроїв дозволяє запобігти витоку конфіденційних даних і проникнення шкідливого ПЗ через зовнішні пристрої, що підключаються до кінцевих точок. Даний модуль працює за допомогою правил і виключень, прописаних в політиках та застосовується для широкого спектру пристроїв (таких, як USB флеш-накопичувачі, пристрої Bluetooth, CD/DVD-плеєри, і т.д.).

Повне шифрування диска.

Даний рівень захисту дозволяє здійснювати шифрування всього диска на машині, керуючи BitLocker для Windows (FileVault і diskutil для macOS). Є можливість шифрувати і дешифрувати томи одним клацанням миші, тому що GravityZone обробляє весь процес з мінімальним втручанням з боку користувачів. Крім того, GravityZone зберігає ключі відновлення, необхідні для розблокування томів, на той випадок, якщо користувач забув свій пароль.

Безпека для поштових серверів Microsoft Exchange.

Bitdefender забезпечує захист Security for Exchange від шкідливих програм, спаму, фішингу, наявна фільтрація контента і вмісту листів, агент Bitdefender повністю інтегрований з серверами Microsoft Exchange, для забезпечення безпечного середовища обміну повідомленнями та підвищення продуктивності. Використовуючи визнані технології захисту від шкідливих програм і спаму, програма захищає користувачів Exchange від новітніх, найскладніших шкідливих програм і від спроб вкрасти конфіденційні і цінні дані користувачів.

Контроль додатків.

Модуль контролюя додатками запобігає активність шкідливих програм, атаки «нульового дня» і підвищує безпеку, не впливаючи на продуктивність. Управління додатками забезпечує гнучке дотримання політик для додатків з «білого» списку, який ідентифікує, запобігає установку і виконання будь-яких небажаних, ненадійних або шкідливих додатків.

Sandbox Analyzer.

Bitdefender Sandbox Analyzer забезпечує потужний рівень захисту від просунутих загроз шляхом автоматичного і глибокого аналізу підозрілих файлів, які не підписані антивірусним движком Bitdefender.

У «пісочниці» використовується великий набір технологій Bitdefender для виконання корисних навантажень в ізольованому віртуальному середовищі, розміщеної в Bitdefender або розгорнутої локально.

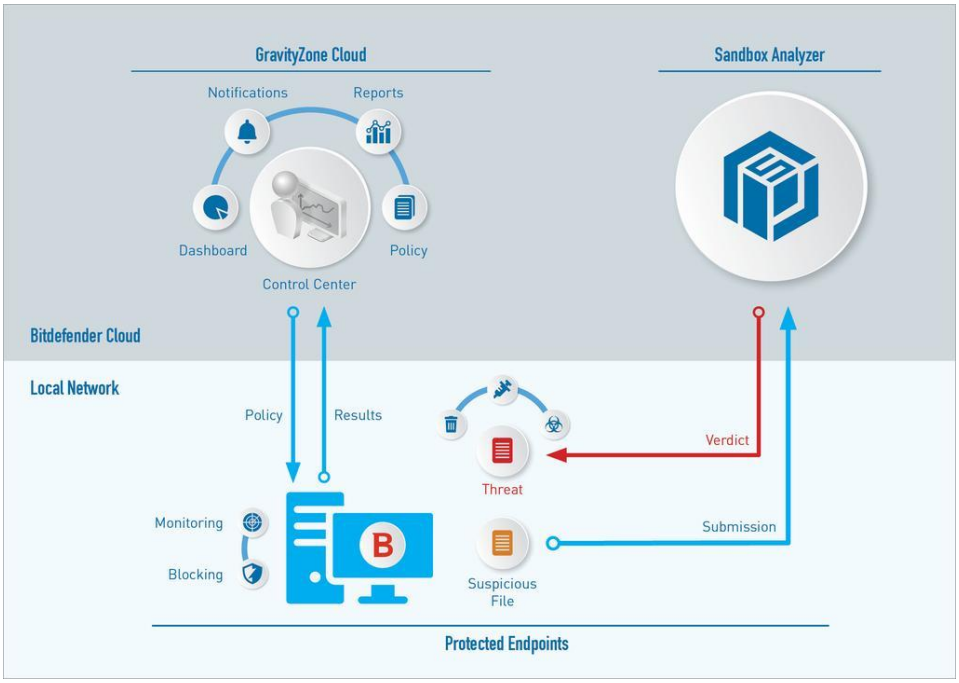


Рис. 2.2. Алгоритм роботи Sandbox Analyzer [24]

Безпека для мобільних пристроїв.

Уніфікує управління безпекою всього підприємства і контроль iPhone, iPad і Android пристроїв, забезпечуючи надійність програмного забезпечення і надання оновлень через онлайн-магазини Apple або Android. Рішення було розроблено для можливості управління особистими пристроями, послідовно просуваючи політику використання будь-яких портативних пристроїв. Функції безпеки включають блокування екрану, місце розташування пристрою, віддалену очистку і профілі безпеки.

На пристроях Android рівень безпеки розширено скануванням в режимі реального часу і шифруванням знімних носіїв. В результаті, мобільні пристрої

знаходяться під контролем і важлива для бізнесу інформація, що знаходиться на них, захищена.

2.2 Компоненти та архітектура рішення Bitdefender GravityZone Elite

Використання звичайного антивірусного програмного забезпечення є неприйнятним у зв'язку з масштабом мережі організації, тому рекомендується використовувати засоби антивірусного захисту з мережевим центром управління. Це дозволяє адміністратору зі свого робочого місця централізовано керувати всіма компонентами, що входять до системи антивірусної безпеки організації, відстежувати антивірусну ситуацію в мережі.

Унікальна архітектура GravityZone дозволяє з легкістю масштабувати рішення та захистити будь-яку кількість систем. GravityZone може бути налаштована на використання кількох віртуальних пристроїв та безліч екземплярів конкретних ролей (бази даних, комунікаційного сервера, балансувальника, сервера оновлень, інцидент-сервера та веб-консолі), щоб забезпечити надійність та масштабованість.

Рішення безпеки Bitdefender керуються в GravityZone з єдиної точки управління – веб-консолі Control Center, яка забезпечує легше управління та доступ до повних налаштувань безпеки, глобальних загроз безпеки, а також повний контроль над усіма модулями безпеки, що захищають віртуальні або фізичні настільні комп'ютери та сервери. Працюючи на архітектурі Gravity, Control Center здатна задовольнити потреби навіть найбільших організацій.

Поставляючись як віртуальний контейнер, GravityZone може бути імпортована на будь-яку платформу віртуалізації, включаючи VMware, Citrix, Microsoft Hyper-V, Nutanix Prism, Microsoft Azure. Інтеграція з VMware vCenter, Citrix XenServer, Microsoft Active Directory, Nutanix Prism Element та Microsoft Azure спрощує розгортання захисту як для фізичних, так і для віртуальних машин [25].

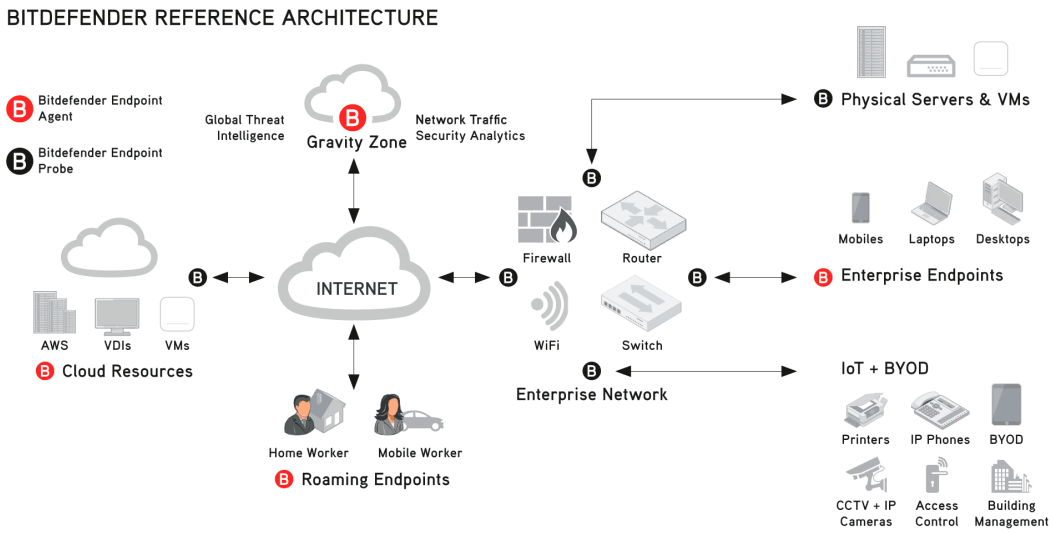


Рис. 2.3. Топологія системи управління кінцевими точками [25]

Як видно з рис 1.1. Bitdefender GravityZone Elite захищає наступні типи кінцевих точок: мобільні пристрої, ноутбуки, комп'ютери, сервери, віртуальні машини тощо.

Локальне рішення GravityZone постачається як налаштований віртуальний пристрій на базі Linux Ubuntu, вбудований у образ віртуальної машини, який можна легко встановити та налаштувати через CLI. Віртуальний пристрій доступний у кількох варіантах, сумісних із основними платформами віртуалізації (OVA, XVA, VHD, OVF, RAW).

Продукти захисту кінцевих точок Bitdefender зручні у застосуванні, багатофункціональні, добре вписуються у загальну стратегію забезпечення безпеки КІС.

Bitdefender GravityZone складається з наступних ролей:

База даних GravityZone. Центральна логіка архітектури GravityZone. Bitdefender використовує нереляційну базу даних MongoDB, яку легко масштабувати та реплікувати.

Сервер оновлень. Відіграє важливу роль у оновленні рішення GravityZone та кінцевих агентів шляхом реплікації та публікації необхідних пакетів або інсталяційних файлів.

Веб-консоль (GravityZone Control Center). Рішення безпеки Bitdefender управляються з єдиної точки, веб-консолі ControlCenter. Це спрощує управління та доступ до загальної системи безпеки, забезпечує контроль над усіма модулями безпеки, що захищають віртуальні та фізичні комп'ютери, сервери та мобільні пристрої від глобальних загроз.

Security Server. Спеціалізована віртульна машина, яка дедублікує та централізує більшу частину функціональностей захисту від шкідливих програм, діючи як сервер сканування.

Сервер інцидентів. Віртуальна машина, яка виступає як колектор шкідливих файлів і відтворює їхній алгоритм дій в тестовому середовищі, тобто діє як пісочниця.

Комунікаційний сервер. Сполучна ланка між агентами безпеки та базами даних, щоб передавати політики для захисту кінцевих точок, а також генерувати звіти від агентів безпеки.

Балансувальник. Використовуються в зв’язці з комунікаційними серверами (від двох і більше) для того, щоб збалансовувати навантаження між ними. Балансувальники ролей дозволяють довести, що розгортання GravityZone захистить навіть найбільші корпоративні мережі, без зповільнення роботи.

Кожен екземпляр ролі може бути встановлений як на одному сервері, так і на різних. Щоб Bitdefender захищав повністю всю мережу, необхідно встановити відповідних агентів безпеки GravityZone на усіх мережевих кінцевих точках.

GravityZone забезпечує захист фізичних та віртуальних Windows, Mac та Linux машин за допомогою Bitdefender Endpoint Security Tools – інтелектуального агента, який адаптується до типу кінцевої точки. Bitdefender Endpoint Security Tools може бути розгорнутий на будь-якій машині, як фізичній так і віртуальній, забезпечуючи гнучку систему сканування та є ідеальним вибором для змішаних середовищ (фізичних, віртуальних та хмарних).

Bitdefender Endpoint Security Tools використовує єдиний шаблон політики для фізичних та віртуальних пристроїв.

Ролі кінцевих точок [25]:

Привілейований користувач

Ретранслятор

Сервер кешування патчів

Exchange Protection

Привілейований користувач. Адміністратори Центру управління (Control Center) можуть надавати права привілейованих користувачів звичайним користувачам кінцевих пристроїв за допомогою політики безпеки. Модуль привілейованих користувачів дозволяє надавати адміністраторські права рівню користувачів, які дозволять отримувати доступ та змінювати налаштування безпеки, використовуючи локальну консоль.

Ретранслятор. Агенти кінцевих точок з роллю Bitdefender Endpoint Security Tools Relay виступають як проксі-сервер та сервер оновлень для інших кінцевих точок у мережі. Агенти кінцевих пристроїв з участю ретранслятора особливо необхідні організаціях із ізольованими мережами, де весь трафік проходить через єдину точку доступу.

У компаніях з великими розподіленими мережами, агент-ретранслятор допомагає знизити використання смуги пропускання. Після того, як агент Bitdefender Endpoint Security Tools Relay встановлений у мережі, інші кінцеві точки можуть бути налаштовані за допомогою політик так, щоб з'єднання з Control Center відбувалося через окремого агента ретрансляції.

Сервер кешування патчів. Кінцеві точки з участю ретранслятора також можуть бути сервером кешування виправлень. При включенні цієї ролі ретранслятори служать для зберігання виправлень програмного забезпечення, що завантажуються з веб-сайтів постачальників, та для їх поширення на кінцеві точки мережі.

Щоразу, коли підключена кінцева точка має програмне забезпечення з відсутніми виправленнями, вона бере їх з сервера, а не з веб-сайту постачальника, таким чином оптимізуючи трафік, що генерується, і зменшуючи навантаження на пропускну здатність мережі.

Exchange Protection. Bitdefender Endpoint Security Tools з роллю захисника Exchange може бути встановлений на сервері Microsoft Exchange з метою захисту користувачів Exchange від загроз, які передаються електронною поштою.

2.3 Призначення та можливості модуля «Policy»

Після встановлення, захист Bitdefender може бути налаштований та керуватися з Control Center за допомогою політик безпеки. Політика визначає параметри безпеки, які застосовуються до певних об'єктів мережевого вмісту (комп'ютери, віртуальні машини або мобільні пристрої).

Є можливість створити стільки політик, скільки потрібно на основі вимог безпеки для кожного типу керованого об'єкта мережі.

Політики мають такі характеристики:

створюються на сторінці Політики та призначаються мережевим об'єктам у розділі Мережа;

можуть успадковувати деякі параметри модулів інших політик;

можна налаштувати призначення політик для кінцевих точок таким чином, що політика зможе застосовуватися лише за певних умов – наприклад, на підставі розташування або користувача (таким чином, кінцева точка може мати більше призначених політик);

кінцеві точки можуть мати одну активну політику одночасно;

можна призначити політику окремим кінцевим точкам або групам кінцевих точок, при призначенні політики також повинні бути визначені параметри

спадкування політики (за замовчуванням кожна кінцева точка успадковує політику батьківської групи);

політики надсилаються об'єктам мережі відразу після їх створення або модифікації, налаштування будуть застосовані до об'єктів мережі менш ніж за хвилину (за умови, що вони є онлайн);

політика застосовується лише до встановлених модулів захисту;

параметри політики можна налаштувати як під час її створення так і за необхідності в будь-який зручний час.

Призначення локальної політики може відбуватися двома способами:

1. Призначення на основі пристрою – означає ручний вибір кінцевих точок, яким ви призначите політику. Ці політики також відомі як політики пристроїв. За замовчуванням, кожна кінцева точка або група кінцевих точок успадковує політику батьківської групи. Якщо змінити політику батьківської групи, то дана зміна буде застосована до всіх нащадків цієї групи, крім тих, які мають примусову політику.

2. Призначення на основі правил – політика призначається керованій кінцевій точці, мережеві налаштування якої відповідають заданим умовам існуючого правила присвоєння. Дозволяє застосовувати окремі налаштування для компонентів політик, наприклад, прописати суворіші правила фаєрволу, коли користувачі підключаються до мережі Інтернет поза межами компанії або є можливість включити керування веб-доступом для користувачів, які не входять до групи адміністраторів тощо.

Правила призначення політик мають наступні характеристики:

політика, що застосовується, перезапише встановлену на кінцевій точці політику пристрою;

якщо жодне з правил призначення не застосовується, буде призначено політику пристрою за замовчуванням;

правила впорядковані та обробляються за пріоритетами, 1 має найвищий пріоритет, є можливість мати кілька правил для одного об'єкта, у цьому випадку застосовуватиметься перше правило, яке відповідає активним налаштуванням з'єднання на певній кінцевій точці.

Кожна політика містить наступні розділи:

основні;

захист від шкідливого ПЗ;

Sandbox Analyzer;

брандмауер;

захист мережі;

контроль програм;

контроль пристроїв;

ретранслятор;

захист Exchange;

шифрування.

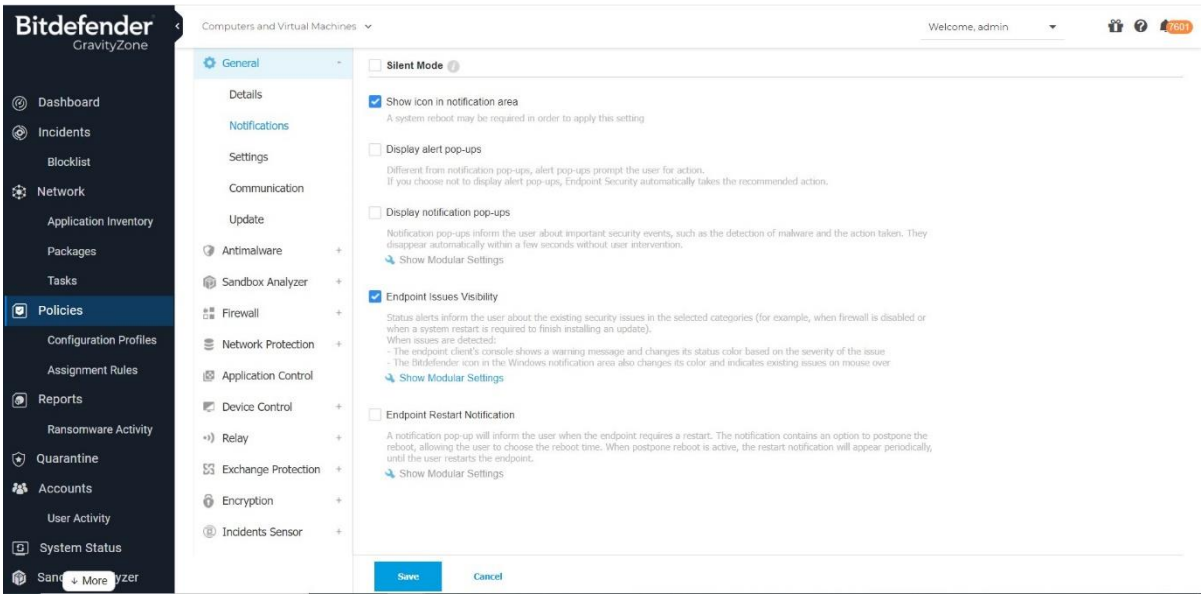


Рис. 2.4. Структура модуля «Політики»

У розділі *«Основні»* можна змінити наступні налаштування:

Парольного захисту – щоб запобігти деінсталяції агента з комп'ютерів користувачами з правами адміністратора, необхідно встановити пароль. Який має бути заданий до процесу установки шляхом налаштування інсталяційного пакета.

Проксі-з’єдання – якщо мережа знаходиться за проксі-сервером, необхідно встановити параметри проксі, які дозволять кінцевим пристроям з'єднуватися з компонентами рішення GravityZone.

Привілейованого користувача – надання адміністраторських прав для рівня кінцевих пристроїв, що дозволяє користувачам кінцевих пристроїв мати доступ та модифікувати налаштування політик через локальну консоль. Модуль привілейованого користувача спеціально розроблений для усунення неполадок, що дозволяє адміністратору мережі легко переглядати та змінювати параметри політик на локальному комп'ютері.

Параметрів зв’язку – можна призначити одну або кілька машин-ретрансляторів для потрібних кінцевих точок, а також прописати один або кілька серверів комунікації. Доступні кінцеві точки-ретранслятори, які виступають як комунікаційні сервери, також будуть враховані.

Оновлень – дуже важлива деталь, яка дозволяє протидіяти актуальним загрозам. Bitdefender публікує всі оновлення продукту та механізмів захисту через сервери Bitdefender в Інтернеті. Усі оновлення зашифровані та мають цифровий підпис, щоб їх не можна було підробити. Коли доступне нове оновлення, агент безпеки Bitdefender перевіряє цифровий підпис оновлень для автентифікації та вміст пакета для забезпечення цілісності. Потім кожен файл оновлень аналізується, і його версія перевіряється на відповідність встановленої. Нові файли завантажуються локально і перевіряються на відповідність хешу MD5, щоб переконатися, що вони не змінені.

Важливою функцією, яка присутня у даному розділі є *наслідування* – можливість встановити розділи, які будуть успадковувати параметри інших політик. Якщо вихідна політика видаляється, то спадкові точки та налаштування розділів повертаються до дочірніх налаштувань. Успадковані розділи не можуть додатково успадковуватись іншими політиками [25].

Модуль *захисту від шкідливого ПЗ* протидіє усім типам шкідливих загроз (вірусів, вірусів-троянів, шпигунських та рекламних програм, руткітів та ін.).

У разі виявлення вірусу або інших шкідливих програм, агент безпеки Bitdefender спробує автоматично видалити шкідливий код із зараженого файлу та відтворити вихідний файл. Ця операція називається «лікування». Файли, які не вдається вилікувати, переміщуються до папки карантину для виключення

поширення вірусу. Вірус, ізольований у карантині, не може заподіяти жодної шкоди, тому що його не можна запустити або відкрити для читання.

Модуль захисту від шкідливого ПЗ містить в наступні підрозділи:

Сканування при доступі (On-Access) – запобігає проникненню в систему нових загроз шкідливих програм шляхом сканування локальних та мережевих файлів, якщо вони доступні (відкриті, переміщені, скопійовані або виконуються), завантажувальних секторів та потенційно небажаних програм (PUA). Також тут є налаштування для програм-вимагачів – блокування процесу шифрування, навіть якщо комп'ютер заражений.

Сканування під час виконання (On-Execute) – налаштування захисту від шкідливих процесів, коли вони виконуються.

Охоплює такі захисні шари:

Розширений контроль загроз (Advanced Threat Control) – це технологія проактивного виявлення, яка використовує розширені евристичні методи виявлення нових потенційних загроз у режимі реального часу. Advanced Threat Control безперервно відстежує програми, запущені на комп'ютері, для пошуку ознак шкідливих дій. Для всіх вищезгаданих дій надається певний бал і для кожного процесу підраховується загальний рейтинг. Якщо бал процесу досяг заданого порогового значення, він вважається шкідливим.

Advanced Threat Control автоматично намагатиметься вилікувати виявлений файл. Якщо лікування не вдалося, Advanced Threat Control видалить цей файл.

Перед виконанням дій з лікування копія файлу відправляється в карантин, тому є можливість пізніше відновити даний файл у разі помилкового спрацьовування.

Захист від безфайлових атак – виявляє та блокує шкідливі безфайлові програми при їх попередньому виконанні, у тому числі завершує роботу PowerShell, що запускає шкідливий командний рядок, блокує шкідливий трафік, аналізує буфер пам'яті до впровадження коду та блокує процес впровадження коду.

Пом'якшення наслідків програм-вимагачів – захист від програм-вимагачів використовує технології виявлення та виправлення, щоб захистити дані, незалежно

від того, чи є програма-вимагач відомою чи новою, GravityZone виявляє аномальні спроби шифрування та блокує процес. Після цього він відновлює файли з резервних копій у їхнє вихідне розташування.

Сканування на запит (On-Demand) – додавання та налаштування завдання перевірки захисту від шкідливого ПЗ, які регулярно працюватимуть на певних кінцевих точках, відповідно до встановленого графіка. Сканування здійснюється у фоновому режимі, незалежно від того, увійшов користувач у систему чи ні.

Рекомендується планувати повне сканування системи щотижня на всіх кінцевих точках. Регулярне сканування кінцевих точок є важливою мірою безпеки, яка може допомогти виявити та блокувати шкідливі програми, які могли обійти функції захисту в реальному часі.

Також можна налаштувати регулярне сканування зовнішніх з’ємних носіїв під час їх підключення до кінцевої точки.

Виявлення гіпервізора (HyperDetect) додає додатковий рівень безпеки до існуючих технологій сканування (сканування при доступі, при виконанні, на вимогу) для боротьби з новим поколінням кіберзагроз, включаючи віруси для атак на об'єкти критичної інфраструктури. Hyper Detect розширює модулі захисту від шкідливих програм та контенту за допомогою потужних евристичних програм на основі штучного інтелекту та машинного навчання. Завдяки своїй здатності прогнозувати цілеспрямовані атаки та виявляти найскладніші шкідливі програми на етапі попереднього виконання, HyperDetect виявляє загрози набагато швидше, ніж технології, що базуються на сигнатурі або поведінковому режимі.

Advanced Anti-Exploit – технологія, заснована на машинному навчанні, для виявлення експлойтів у реальному часі, включаючи безфайлові атаки.

Сервери безпеки (Security Servers) – можна призначити один або кілька Security Server цільовим кінцевим точкам і встановити пріоритет, за яким кінцеві точки будуть вибирати Security Server для надсилання запитів сканування.

Sandbox Analyzer забезпечує потужний рівень захисту від розширених загроз, виконуючи автоматичний всебічний аналіз підозрілих файлів, які ще не підписані механізмами захисту від шкідливих програм Bitdefender.

Можна налаштувати подачу файлів через:

датчик кінцевої точки;

датчик мережі;

датчик ICAP.

В підрозділі Sandbox Manager можна налаштувати кількість днів, протягом яких будуть зберігатися об'єкти звіти у сховищі даних.

Брандмауер служить для захисту кінцевих точок від спроб встановлення несанкціонованих вхідних та вихідних з'єднань. Функціональність брандмауера ґрунтується на мережевих профілях. Профілі ґрунтуються на рівнях довіри, які мають бути визначені для кожної мережі.

Брандмауер виявляє кожне нове підключення, порівнює інформацію адаптера з інформацією профілів і застосовує відповідні налаштування. Брандмауер можна увімкнути або вимкнути, але якщо вибрати останнє, комп'ютери будуть вразливі до мережних та Інтернет-атак.

Захист мережі використовується, щоб налаштувати параметри фільтрації вмісту для користувачів, включаючи перегляд веб-сторінок, а також виявлення методів мережевих атак, які намагаються отримати доступ до певних кінцевих точок.

Налаштування об'єднані в наступні розділи:

Контроль контенту. Керування веб-доступом дозволяє дозволити або заборонити веб-доступ користувачам або програмам у певні інтервали часу.

Веб-сторінки, заблоковані модулем керування веб-доступом, не відображатимуться у браузері. Замість цього буде відображатися веб-сторінка за замовчуванням, яка повідомляє користувачеві про те, що веб-сторінка була заблокована модулем контролю контенту.

Також наявний веб-фільтр за категоріями – це динамічна фільтрація доступу до сайтів на основі їх вмісту. Можна використовувати дозволяти або блокувати доступ для цілих веб-категорій (таких як ігри, контент для дорослих, онлайн мережі тощо).

Веб-захист – захист від фішингу автоматично блокує відомі фішингові веб-сторінки, щоб користувачі випадково не розкрили приватну або конфіденційну інформацію інтернет-шахраям.

Сканування веб-трафіку може дещо уповільнити роботу в Інтернеті, проте воно дозволяє блокувати шкідливі програми, які проникають у ваш комп'ютер з Інтернету, включаючи приховані завантаження.

Якщо веб-сторінка містить або розповсюджує шкідливі програми, вона автоматично блокується. При цьому буде відображено спеціальну сторінку попередження, яка інформує користувача про те, що запитувана веб-сторінка небезпечна.

Вхідні повідомлення електронної пошти (POP3) та веб-трафік перевіряються в режимі реального часу, щоб запобігти проникненню шкідливого програмного забезпечення в кінцеву точку. Вихідні листи (SMTP) перевіряються для запобігання зараженню шкідливими програмами інших кінцевих точок.

Network Attack Defense надає рівень безпеки, заснований на технології Bitdefender, яка застосовує дії проти мережевих атак, призначених для отримання доступу до кінцевих точок, за допомогою спеціальних методів, таких як: атаки методом перебору, мережеві експлойти та програми для крадіжки паролів.

Контроль додатків додає ще один рівень захисту від усіх видів шкідливих загроз (вимагачів, атак нульового дня, експлойтів, троянів, шпигунських програм, руткітів, рекламного ПЗ і т. д.) за рахунок блокування запуску неавторизованих додатків та процесів.

Управління програмами зменшує поверхню атаки, яку шкідливі програми можуть використовувати для впливу на кінцеву точку, запобігає установці та виконанню будь-яких небажаних, ненадійних або шкідливих додатків.

Управління програмами забезпечує гнучке дотримання політик, які дозволяють формувати «білий» та «чорний» список програм і керувати дозволами на їх оновлення. Також є можливість дозволяти або забороняти окремий процес для відповідних програм.

Керування пристроями дозволяє запобігти витоку даних і проникненню шкідливого ПЗ через зовнішні пристрої, що підключаються до кінцевих точок, застосовуючи правила блокувань і виключень, для широкого спектру типів пристроїв (Bluetooth, CD-ROM Drive, модеми, принтери, мережеві адаптери, адаптери безпровідних мереж, внутрішні та зовнішні пристрої збереження інформації).

У розділі *«Ретранслятора»* можна задати налаштування зв'язку (проксі-серверу) та оновлень для кінцевих точок з роллю ретранслятора.

За замовчуванням оновлення для агентів-ретрансляторів розміщуються на локальному сервері оновлень GravityZone, але можна вказати інші джерела – IP-адресу або ім'я одного або декількох серверів оновлень у мережі, а потім налаштувати пріоритети їх використання кнопками вгору та вниз. Якщо перше джерело оновлень недоступне, буде використано наступне у списку і так далі.

Захист Exchange, встановлений на поштовому сервері, дозволяє також фільтрувати повідомлення, що містять вкладення, або якщо вміст листів вважається небезпечним, відповідно до політик безпеки вашої компанії.

Налаштування Security for Exchange організовані в наступних розділах:

Основні. У цьому розділі можна створювати та керувати групами облікових записів електронної пошти, визначати термін зберігання об'єктів у карантині та блокувати певних відправників. Є можливість створювати групи користувачів (IT-відділ, відділ продажів або менеджери компанії), для яких можуть застосовуватися різні політики сканування та фільтрації.

Захист від шкідливого ПЗ. Bitdefender Endpoint Security Tools інтегрується із поштовими транспортними агентами для сканування всього поштового трафіку, та якщо потрібно, інформує користувачів про вжиті заходи, додаючи текст до тіла електронного листа. За замовчуванням увімкнено сканування транспортного рівня.

Антиспам. Модуль антиспаму пропонує кілька захисних шарів проти спаму та фішингу, використовуючи комбінації різних фільтрів та механізмів, щоб визначити чи є листи спамом чи ні. Електронна пошта перевіряється на

відповідність правилам фільтрації спаму на основі груп відправників та одержувачів у порядку пріоритету.

Контроль контенту. Підрозділ керування контентом ісунє для посилення захисту електронної пошти, відфільтрувавши весь поштовий трафік, несумісний із політикою компанії (небажаний або потенційно небезпечний).

Для загального контролю вмісту електронної пошти, модуль включає два варіанти фільтрації електронної пошти:

Фільтрування контенту – дозволяє фільтрувати поштовий трафік на основі символьних рядків, які були визначені раніше. Ці рядки порівнюються з темою листа або текстовим вмістом електронного листа. Потім поштове повідомлення обробляється відповідно до дій, заданих цим правилом.

Фільтрування вкладень – може знайти вкладення з певними шаблонами імен або певного типу (наприклад, блокувати потенційно небезпечні вкладення, такі як .vbs або .exe файли).

Модуль Encryption керує повним шифруванням диска на кінцевих точках, використовуючи BitLocker у Windows та FileVault та утиліту командного рядка diskutil у macOS, відповідно [25].

При такому підході GravityZone може забезпечити захист даних у разі втрати або крадіжки, а також мінімальний вплив на продуктивність кінцевих точок завдяки вбудованим засобам шифрування.

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ BITDEFENDER GRAVITYZONE ELITE

3.1 Розроблення технології застосування системи управління захистом кінцевих точок корпоративної інформаційної системи на базі Bitdefender GravityZone Elite

Комп'ютерні віруси небезпідставно вважаються однією з найсерйозніших загроз у сфері інформаційної безпеки. Підтверджується це шкодою, яку несуть компанії внаслідок впливу вірусних атак.

Bitdefender Endpoint Elite захищає підприємство від усього спектру складних кіберзагроз зі швидкістю, точністю, низькими адміністративними витратами та мінімальним впливом на систему. Рішення усуває необхідність запускати кілька рішень безпеки кінцевих точок на одній машині, поєднуючи запобіжні засоби контролю, багатоетапні методи виявлення загроз та автоматичне реагування.

З цих причин, саме Bitdefender GravityZone Elite був обраний для впровадження системи антивірусного захисту у «Компанії», до складу якої входить 10 підприємств (далі Група компаній).

Для управління антивірусною безпекою в організації на базі рішення Bitdefender GravityZone Elite необхідно слідувати алгоритму дій, який містить 9 процесів:

розробка політики антивірусної безпеки (не залежно від будь-якої системи антивірусного захисту);

інвентаризація, визначення кількості кінцевих точок та необхідних агентів для закупівлі ліцензій;

підготовка інфраструктури, розгортання Bitdefender GravityZone Elite;

синхронізація користувачів за допомогою Active Directory;

налаштування: створення політик та їх поділ на цільові групи;

підготовка до встановлення агентів на кінцеві точки, створення інсталяційних пакетів;

встановлення агентів на кінцеві точки;

управління користувачами системи антивірусної безпеки;

щоденний моніторинг кінцевих точок та подій.

Розробка політики антивірусної безпеки (не залежно від будь-якої системи антивірусного захисту).

Політика антивірусної безпеки – це високорівневий документ, який прописує стандарт організації у цій галузі, описує принципи та порядок функціонування системи антивірусної безпеки, визначає відповідальність кожного з учасників системи, визначає об'єкти, що підлягають захисту. Керуючими даними для процесу розробки політики антивірусної безпеки є документ «Політика інформаційної безпеки». Розробку політики антивірусної безпеки здійснює адміністратор інформаційної безпеки або інша відповідальна за це особа. Вхідними даними для цього процесу є можливі програмні та мережеві загрози безпеці актуальні для організації, а також структура організації.

Вихідними даними є розроблена та затверджена політика антивірусної безпеки, яка має регламентувати всі процеси, пов'язані з антивірусною безпекою організації [26].

Інвентаризація, визначення кількості кінцевих точок та необхідних агентів для закупівлі ліцензій.

Згідно інформації, яка була подана IT-адміністраторами з кожного підприємства окремо, кількість користувачів, які підключаються до корпоративної інформаційної системи по Групі компаній ‑ 3120, кількість кінцевих точок (серверів, ноутбуків, комп’ютерів, віртуальних машин, промислових машин), які необхідно покрити антивірусним захистом ‑ 3470.

Підготовка інфраструктури, розгортання Bitdefender GravityZone Elite.

Вимоги до обладнання віртуального пристрою GravityZone варіюються залежно від мережі та вибраної архітектури установки. Для мереж до 3000 кінцевих точок можна обирати встановлення всіх ролей GravityZone на одному пристрої, у той час як для великих мереж, як в даному випадку, необхідно розподілити ролі між кількома пристроями. Така структура була обрана з розразрахунку на те, що компанія постійно розвивається та машстабується.

Структура взаємодії кінцевих точок та компонентів GravityZone розроблена у наступному вигляді:

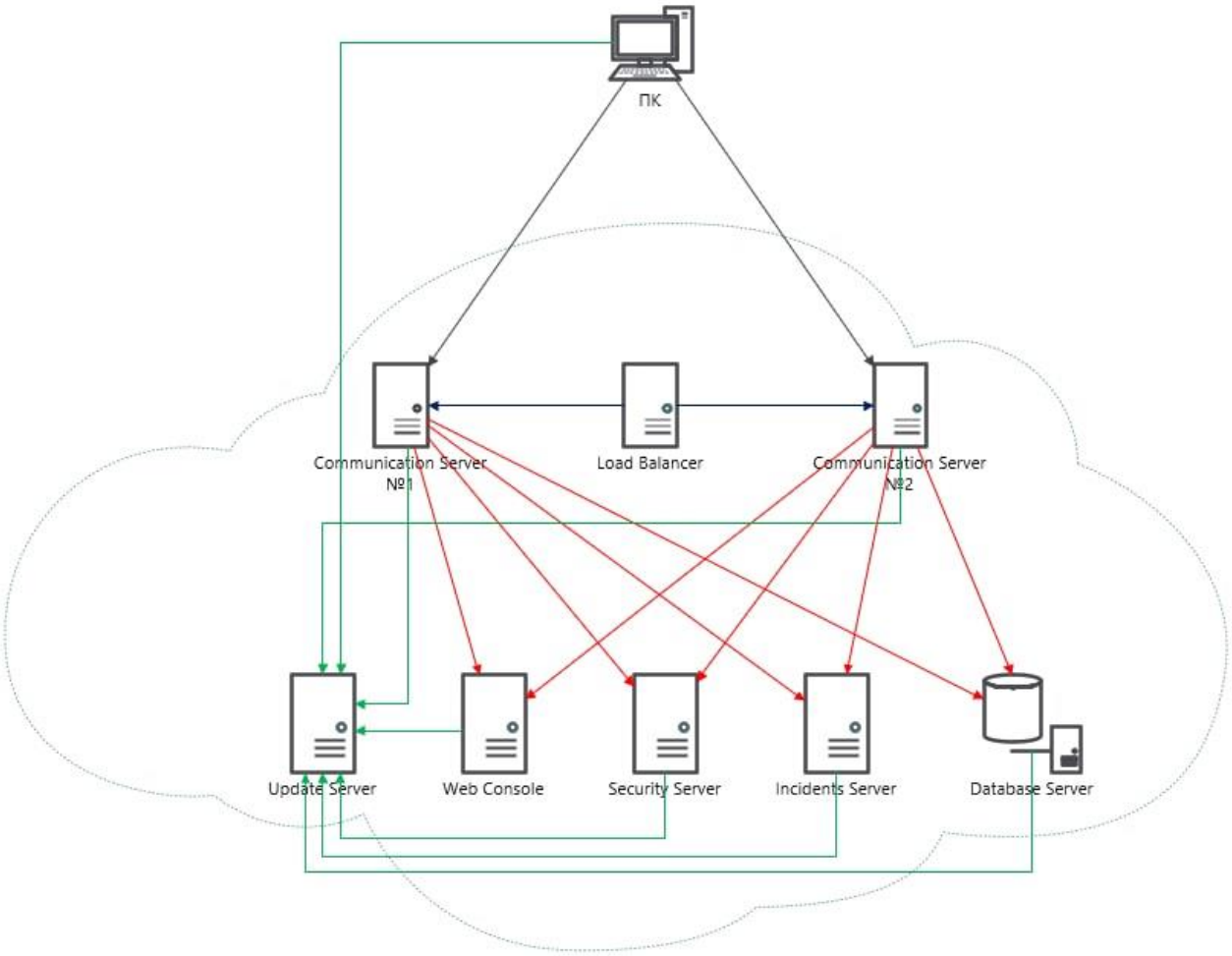


Рис. 3.1. Структура взаємодії кінцевої точки та елементів GravityZone

Група компаній користується послугою хмарної інфрастуктури контрагента та арендує ресурси для компонентів GravityZone.

В хмарі було розгонуто 8 серверів з наступними ролями:

2 комунікаційних сервера;

балансувальник, який діє у зв’язці з комунікаційними серверами;

сервер оновлень;

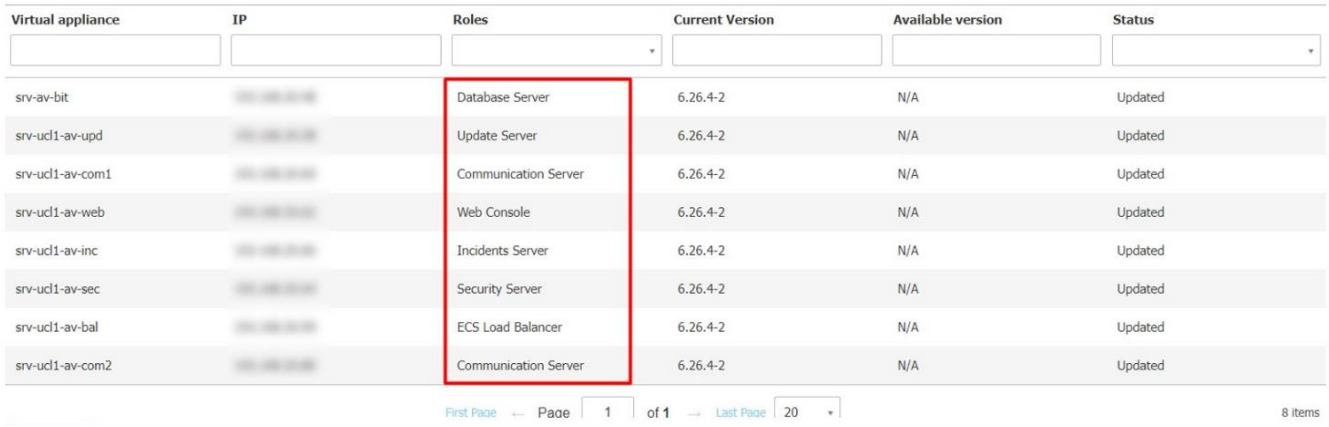
веб-консоль (Control Center);

сервер безпеки, відповідальний за сканування;

сервер інцидентів (пісочниця);

база даних GravityZone.

Усі сервери, окрім веб-консолі не мають GUI, лише CLI. Перелік та статус розгорнутих компонентів можна переглянути у веб-консолі на вкладці «Update».



Virtual appliance	IP	Roles	Current Version	Available version	Status
srv-av-bit	[redacted]	Database Server	6.26.4-2	N/A	Updated
srv-ucl1-av-upd	[redacted]	Update Server	6.26.4-2	N/A	Updated
srv-ucl1-av-com1	[redacted]	Communication Server	6.26.4-2	N/A	Updated
srv-ucl1-av-web	[redacted]	Web Console	6.26.4-2	N/A	Updated
srv-ucl1-av-inc	[redacted]	Incidents Server	6.26.4-2	N/A	Updated
srv-ucl1-av-sec	[redacted]	Security Server	6.26.4-2	N/A	Updated
srv-ucl1-av-bal	[redacted]	ECS Load Balancer	6.26.4-2	N/A	Updated
srv-ucl1-av-com2	[redacted]	Communication Server	6.26.4-2	N/A	Updated

First Page ← Page 1 of 1 → Last Page 20 8 items

Рис. 3.2. Активні компоненти GravityZone

Кожна кінцева точка та елемент GravityZone мають прямий зв’язок із сервером оновлень для того, щоб вчасно отримувати усі необхідні інсталяційні пакети, оновлення, виправлення тощо. У компанії не передбачалося призначення жодного Relay, тому оновлення кінцева точка має отримувати лише з локального Update серверу, або, як альтернавне рішення (для точок, які мають доступ до мережі Інтернет) – безпосередньо з публічних Update-серверів Bitdefender.

Також усі кінцеві точки мають пряме з’єднання (в обхід проксі-серверу) з двома комунікаційними серверами, де перший йде як основний, а другий – як альтернативний. Вони використовуються для того, щоб маршрутизувати запити кінцевих точок до інших серверів. Якщо сервер з пріоритетом «один» буде

неступний, або занадто завантажений, з'єднання з іншими серварами GravityZone буде відбуватися через другий пріоритет. Цей процес відбувається за рахунок розгорнутого балансувальника, який врівноважує навантаження на комунікаційні сервери. При цьому в налаштуваннях «Communication» не взується балансувальник, лише комунікаційні сервери.

Рис. 3.3. Налаштування серверів комунікації

Синхронізація користувачів за допомогою Active Directory.

Control Center інтегрується з існуючими системами керування та моніторингу, щоб спростити автоматичне застосування захисту до некерованих робочих станцій або серверів, що знаходяться у службі каталогів Microsoft Active Directory, або які були виявлені в мережі.

Завдяки інтеграції з Active Directory можна імпортувати в Control Center дані, спрощуючи розгортання захисту, управління, моніторинг та звітність. Крім того, користувачам, зареєстрованим у службі каталогів, можуть бути призначені різні ролі через Control Center.

Для того, щоб додати домен, необхідно зазначити його назву, і дані облікового запису адміністратора. Токож є можливість вибрати усі необхідні домен-контроллери зі списку, який автоматично підтягується в систему після перевірки акаунту адміністратора.

Імпорт можна організувати таким чином: зберегти структуру AD, але ігнорувати пусті підрозділи – Organizational Unit (OUs); повністю ігнорувати структуру AD та перемістити усі дані до однієї узагальненої папки «Custom groups»; зберегти структуру AD та завантажити лише вибрані OUs.

Був обраний перший варіант, оскільки AD якісно структуризована, та поділена за підприємствами та категоріями (сервери, ноутбуки, комп'ютери, віртуальні та промислові машини).

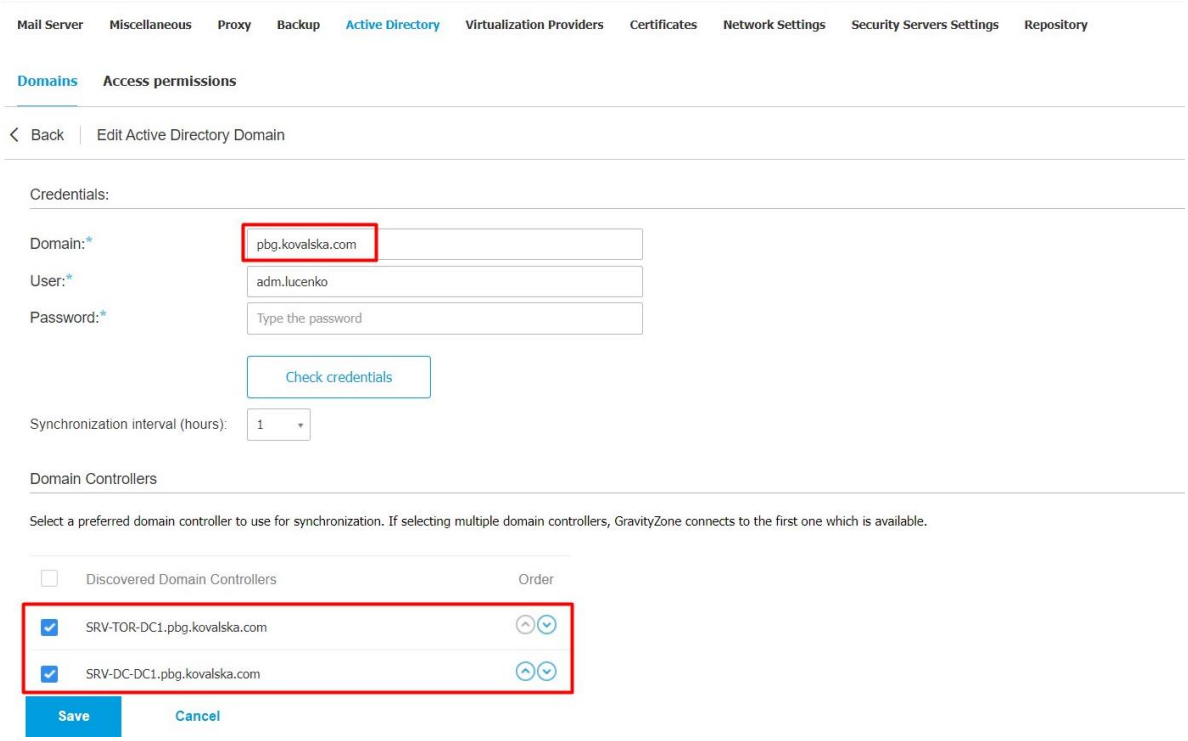


Рис.3.4. Імпорт даних з Active Directory

Після завершення імпорту в розділі «Network» відображаються папки та кінцеві точки, які містяться у них.

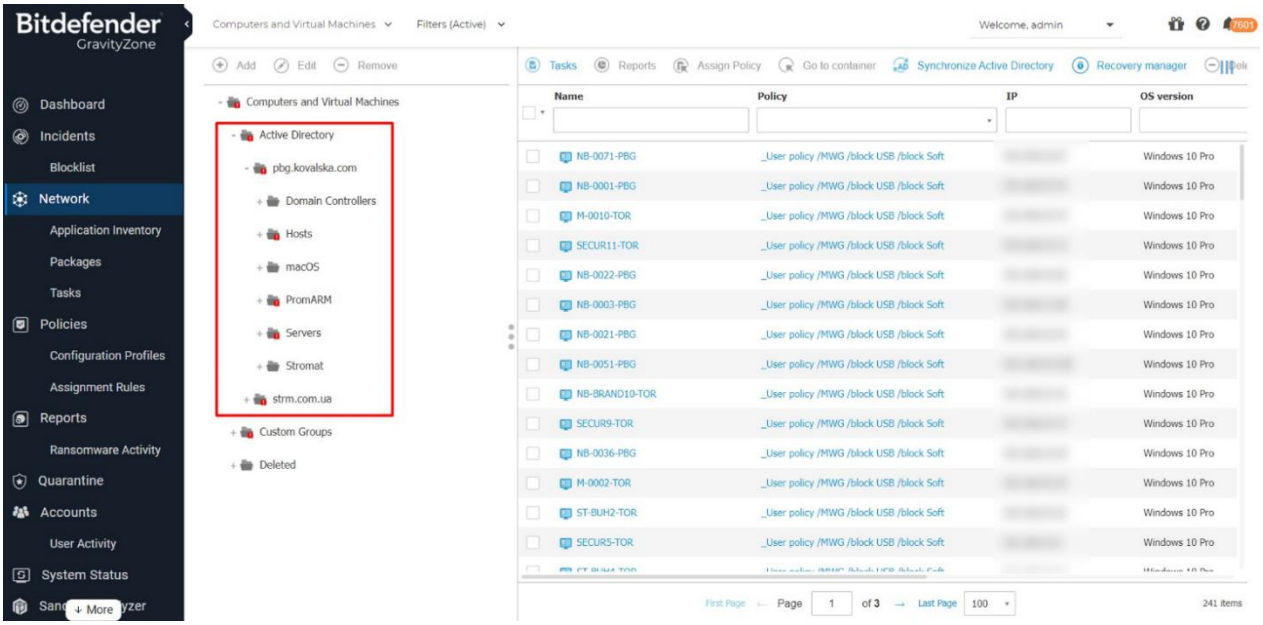


Рис. 3.5. Структура AD в консолі Control Center

Налаштування: створення політик та їх поділ на цільові групи.

Налаштування компонентів системи антивірусної безпеки здійснюється після розгортання системи адміністратором за допомогою мережевого центру керування. Метою процесу є забезпечення функціонування компонентів системи відповідно до політики антивірусної безпеки.

Для того, щоб політики могли ефективно керувати кінцевими точками, їх було поділено на такі цільові групи: користувачі, сервери, промислові машини та поштові сервери.

В свою чергу політики для групи користувачів матимуть також різні варіації. Наприклад, для окремих хостів не будуть блокуватися з'ємні пристрої або програми, для когось – дозволені хмарні сховища або відключене сканування SSL-сертифікатів веб-ресурсів тощо. Політик можна створювати скільки завгодно, відповідно до потреб Компанії або адміністратора системи.

Для кожної з цільових груп налаштування будуть відрізнятися. Перша і основна політика – створена для користувачів.

Як зазначалося вище, політика містить власні розділи та підрозділи, в яких і відбувається налаштування.

У розділі «General» налаштовані сповіщення показувати іконку Bitdefender в зоні сповіщень, а також сигналізувати, коли агентом виявлені будь-які проблеми на кінцевій точці. Всі інші спливаючі повідомлення були заборонені для того, щоб не перенавантажувати користувача зайвою інформацією. Також в цьому розділі був встановлений пароль на видалення агента, прописані сервери комунікацій та локація розташування (локальний сервер оновлень).

У розділі «Antimalware» ключовим налаштуванням є сканування, які діляться на три типи [25]:

При доступі – сканування локальних та мережевих файлів (окрім архівів), якщо вони доступні (відкриті, переміщені, скопійовані або виконуються), а також сканування на наявність процесу шифрування даних. Першочергова дія для знайдених інфікованих файлів – лікування, альтернативна – переміщення до

карантину. Для підозрілих файлів: основна дія – переміщення до карантину, альтернативна – заборона доступу до файлу.

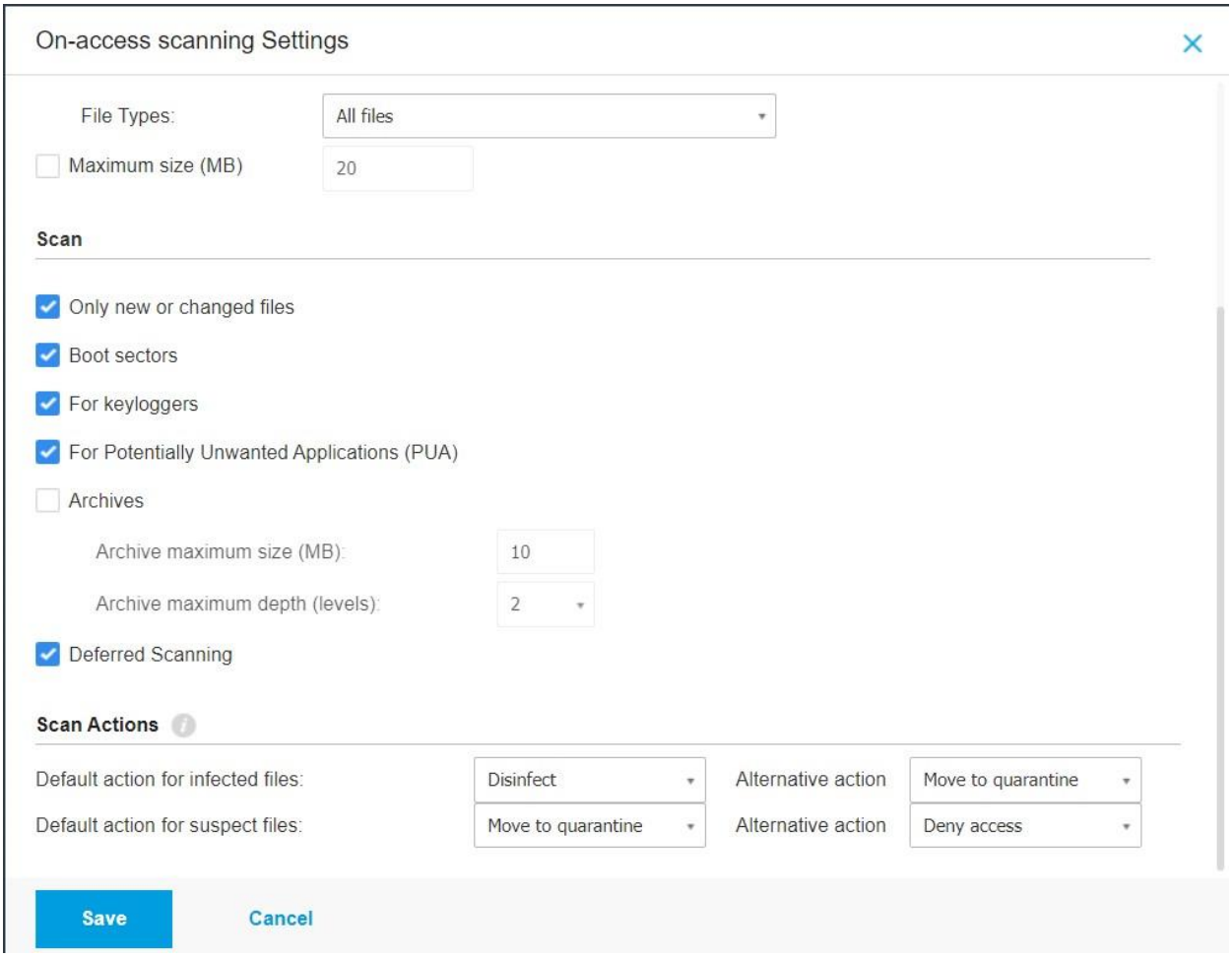


Рис. 3.6. Створення правила сканування при доступі

При виконанні – захист від шкідливих процесів, коли вони виконуються. Увімкнений АТС, який використовує евристичні методи виявлення загроз у режимі реального часу. При виявленні ознак шкідливих дій процесу він відразу заблокує його. Bitdefender Advanced Threat Control – це технологія проактивного виявлення, яка використовує розширені евристичні методи виявлення нових потенційних загроз у режимі реального часу.

Також увімкнений захист від безфайлових атак і пом’якшення наслідків від програм-вимагачів (шифрувальників) для того, щоб в разі шифрування даних, система заблокувала цей процес та відновила дані з резервних копій.

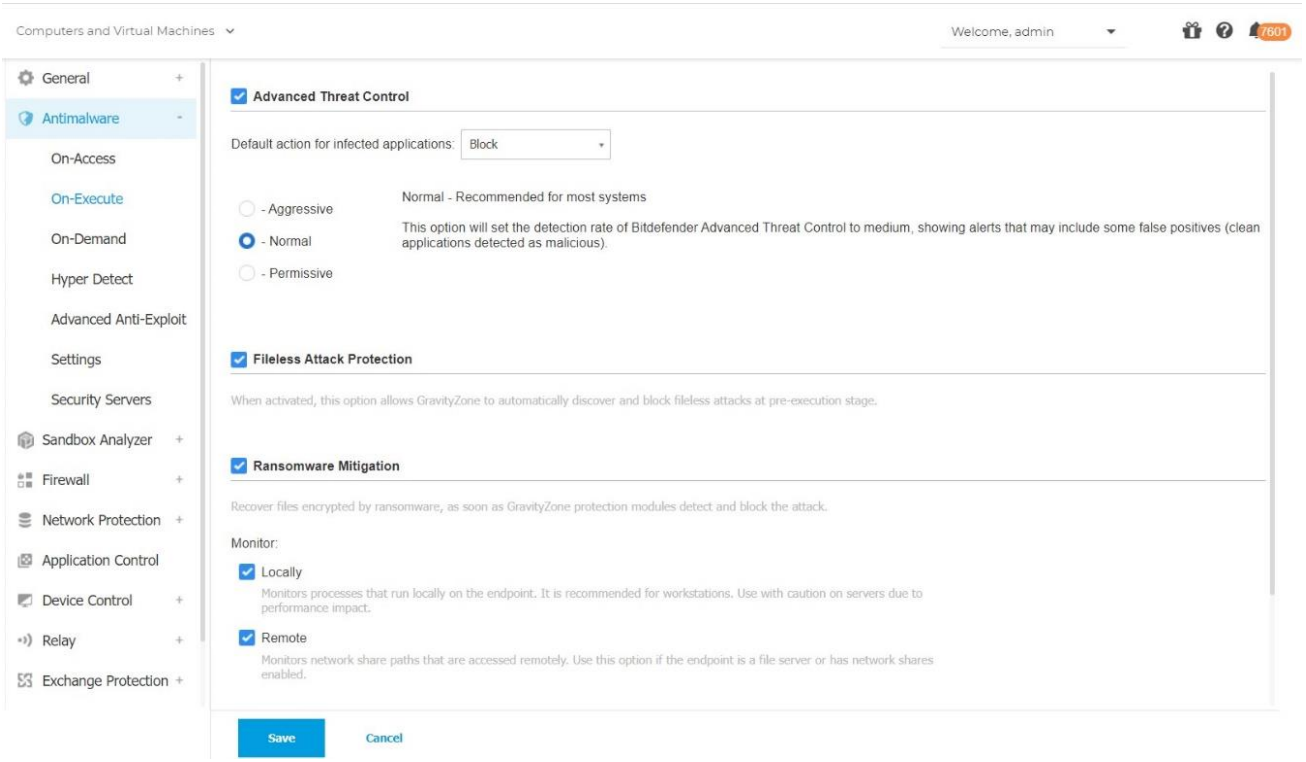


Рис. 3.7. Налаштування сканування при виконанні

На запит – завдання перевірки захисту у фоновому режимі від шкідливого ПЗ відповідно до встановленого графіка.

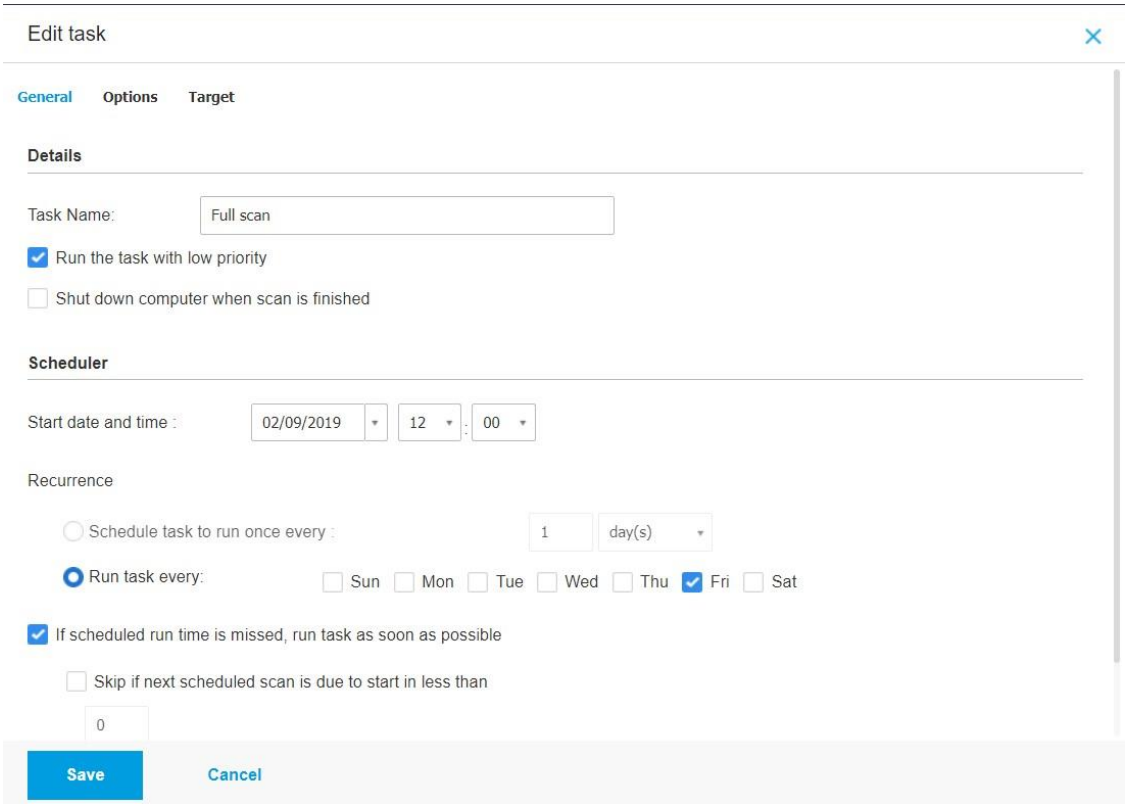


Рис. 3.8. Створення правила сканування на запит

Наявні такі типи завдань сканування:

Швидке сканування (Quick Scan) – використовує хмарне сканування для виявлення шкідливих програм, запущених у системі. Швидке сканування займає, як правило, менше хвилини та використовує лише незначну частину системних ресурсів, на відміну від процесу стандартного антивірусного сканування.

Повне сканування (Full Scan) – перевіряє всі кінцеві точки на усі типи шкідливих програм (віруси, програми-шпигуни, рекламне ПЗ, руткіти та інші).

Сканування користувача (Custom Scan) – дозволяє вибрати розташування об'єктів для сканування та налаштувати параметри сканування.

Мережеве сканування (Network Scan) – це тип сканування, який може бути призначений одній керованій кінцевій точці для сканування мережних дисків, задавши певні налаштування і вказавши певні області, які будуть перевірятися. В даному випадку було налаштоване лише повне сканування, яке проводиться раз на тиждень, за неможливості виконання – в будь-який найближчий момент.

Обов’язково увімкнений HyperDetect, оскільки від надає додатковий рівень захисту завдяки потужним евристичним програмам на основі штучного інтелекту та машинному навчанню. Усі підозрілі файли переміщує до карантину, а шкідливий трафік блокує.

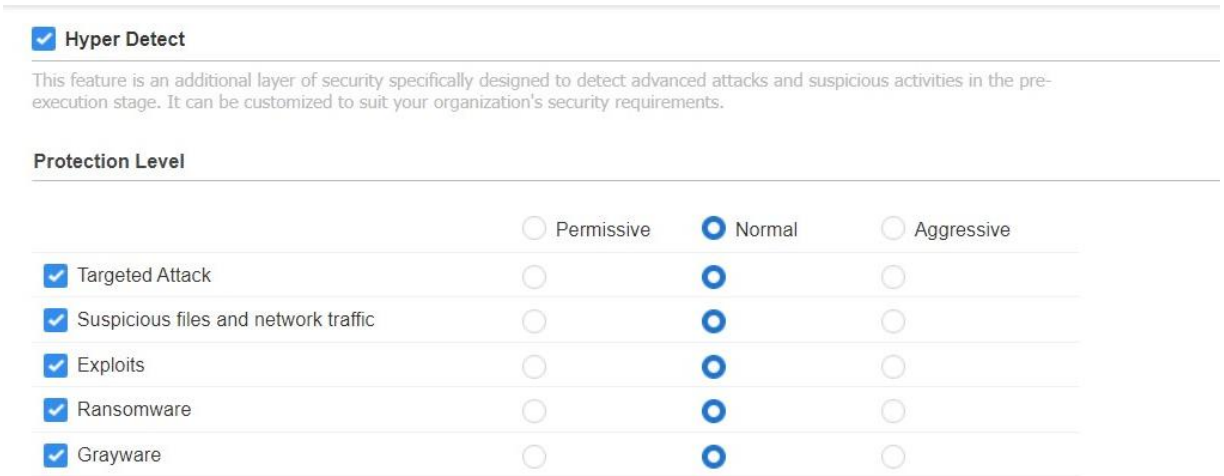


Рис. 3.9. Рівні захисту HyperDetect

Також увімкнена технологія Advanced Anti-Exploit для захисту від експлойтів, що спрямовані на відомі та невідомі вразливості у програмах як в ОС Windows, так і в ОС Linux.

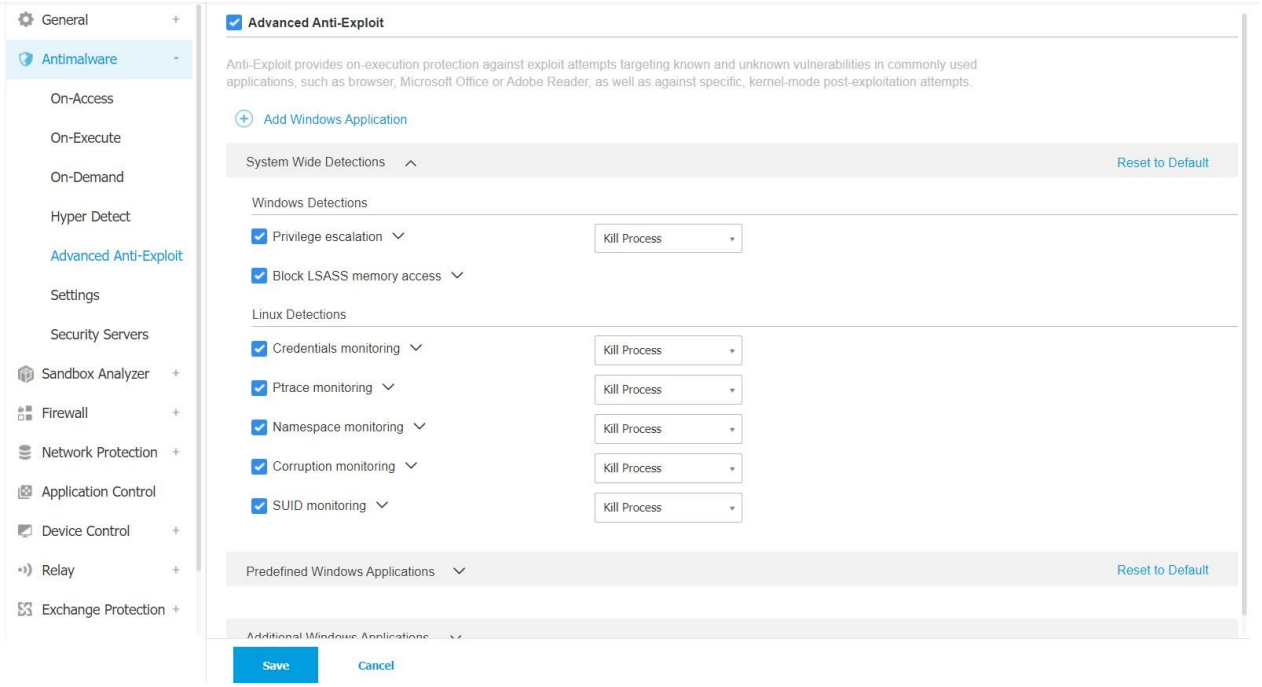


Рис. 3.10. Налаштування виявлення експлойтів у масштабі всієї системи

Sandbox Analyzer налаштований таким чином, щоб він автоматично сканував підозрілі файли в ізольованому середовищі. Під час такого сканування зібрані файли будуть доступні для користувача, але при виявленні загрози переміщатимуться до карантину, а інакше – видалятимуться. Також є попередня фільтрація вмісту, яка сканує файли, аргументи командного рядка, URL-адреси на наявність підозрілої поведінки та передає їх до пісочниці для подальшого дослідження.

Розділ «Firewall» не містить специфічних налаштувань, лише стандартні, оскільки Група компаній має додаткове програмне рішення фаєрволу на мережевих пристроях, які контролюють роботу кінцевих точок. Але все ж таки даний фаєрвол надає ще один рівень захисту – має систему IDS, яка інтегрована з АТС. Але основна його функція – це робота на основі правил дозволу або заборони встановлення з'єднання програм з мережею Інтернет.

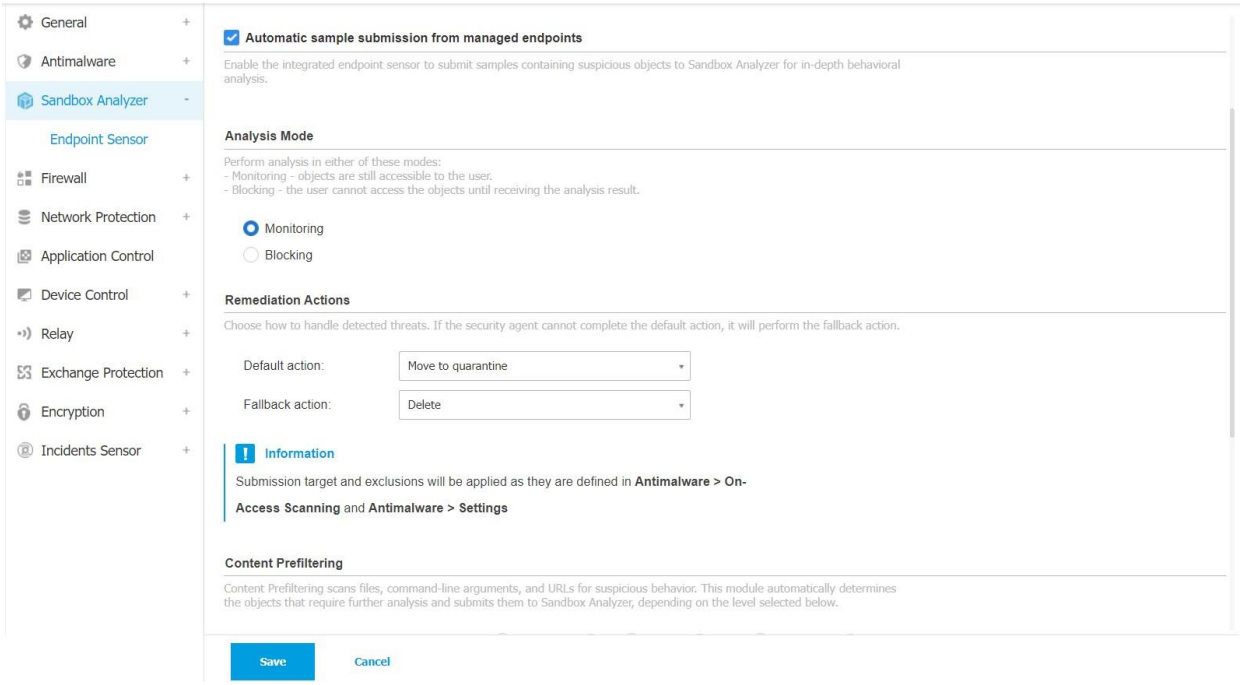


Рис. 3.11. Налаштування Sandbox Analyzer

Розділ «Network Protection» відповідає за фільтрацію вмісту у веб-браузерах під час роботи в мережі Інтернет. В основних налаштуваннях варто виділити функцію сканування на наявність SSL-сертифікату кожного веб-ресурсу, а також список глобальних виключень, тобто тих сайтів, які не будуть перевірятися жодним з модулів «Network Protection».

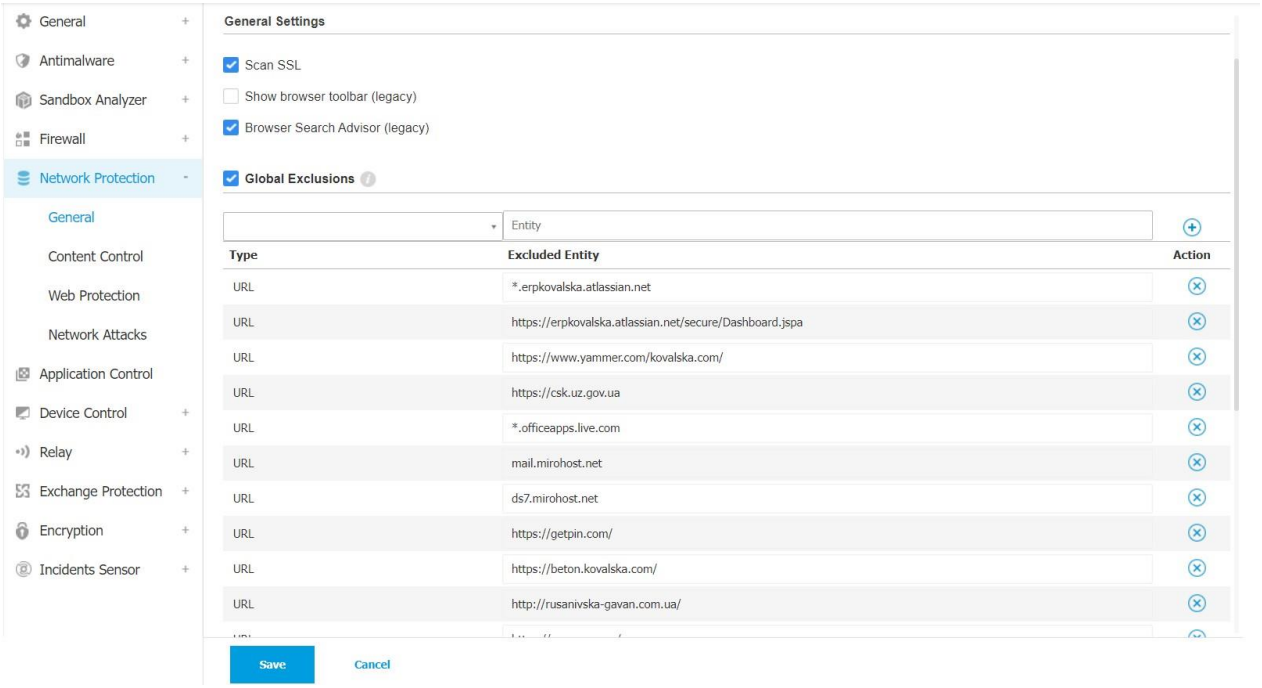


Рис. 3.12. Основні налаштування роботи у мережі Інтернет

У підрозділі «Content Control» зазначений список програм, що заборонені політиками Групи компаній, які неможливо буде завантажити будь-якого браузера. Також важливим нюансом є вимкнення модуля «Web Access Control», оскільки на кінцевих точках користувачів встановлений проксі-агент, який повністю контролює їхню діяльність в мережі Інтернет. При роботі обох виникає колізіція під час блокування веб-ресурсів для користувачів, багато хибних спрацювань та й вцілому некоректна робота модуля «Web Access Control».

«Web Protection» та «Network attack» увімкнені. Перший модуль відповідає за блокування фішингових сайтів, а другий – за виявлення методів мережевих атак, які намагаються отримати доступ до кінцевих точок.

«Application Control» додає ще один рівень захисту від усіх видів шкідливих загроз (вимагачів, атак нульового дня, експлойтів, троянів, шпигунських програм, руткітів, рекламного ПЗ і т. д.) за рахунок блокування запуску неавторизованих додатків та процесів. Можна додати будь-який процес/програму вручну або підтягнути дозволені або заборонені процеси/програми з «Application Inventory».

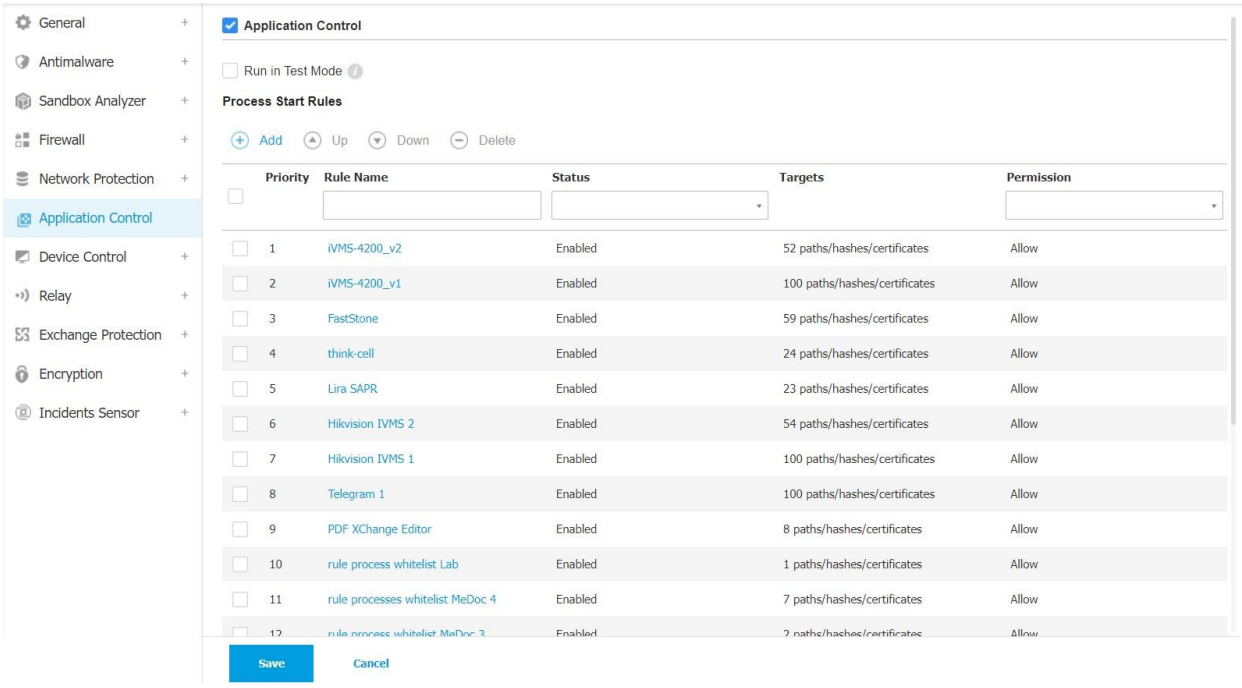


Рис. 3.13. Створення правил для контролю програм та процесів

Глобально усі програми поділені на «whitelist» (дозволені) та «blacklist» (заборонені). Як видно на рисунку, дозволені програми також поділені між собою

згідно алфавіту для полегшеного пошуку необхідних програм та зменшення навантаження на систему GravityZone під час відкриття кожного з листів.

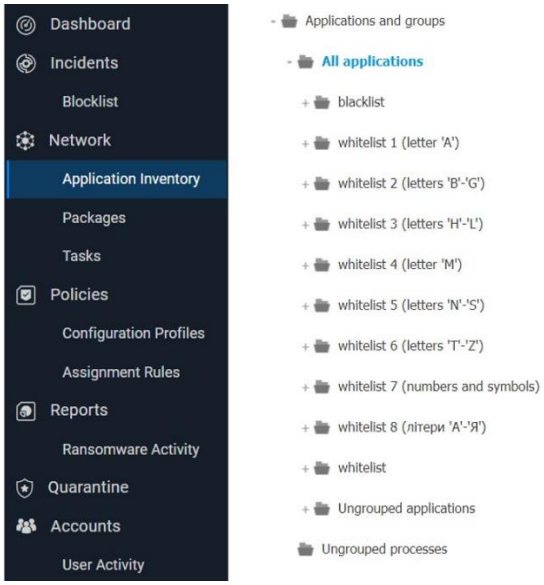


Рис. 3.14. Інвентаризація і структуризація програм та процесів

«Device Control» дозволяє запобігти витоку даних і проникненню шкідливого ПЗ через зовнішні пристрої, що підключаються до кінцевих точок, тому глобально по Групі компаній заборонено використання CD-ROM Drive, дискет, застарілих кабелів передачі даних IEEE 1394, магнітних накопичувачів, завантажувальних флешок, та зовнішніх накопичувачів.

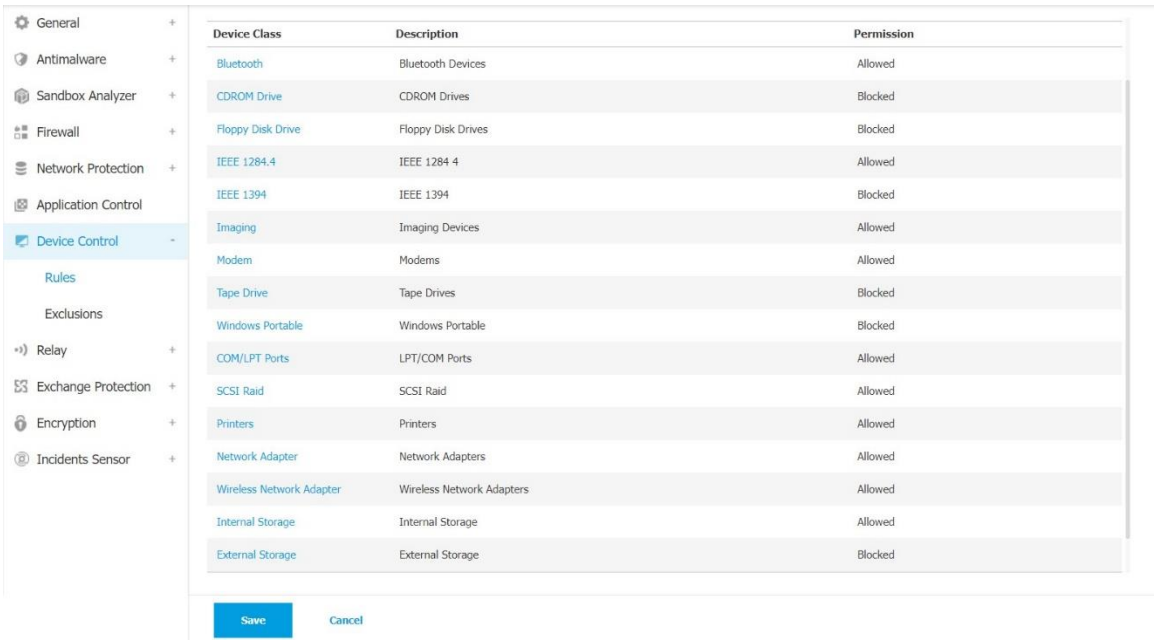


Рис. 3.15. Правила дозволу та блокування для підключених пристроїв

Оскільки заборонене використання власних USB-накопичувачів, є альтернатива – корпоративні USB-накопичувачі (для електронних ключів, креслень тощо), які мають унікальні USB\VID, що внесені у виключення і мають змогу підключатися до кінцевих точок.

«Encryption» вмикає шифрування дисків на кінцевих точках за допомогою BitLocker. Коли ця функція застосована, у користувача на робочому місці з'являється вікно вводу паролю на шифрування. Для того, щоб не налаштовувати BitLocker на кожній з кінцевих точок, використовується управління через GravityZone.

Політики для серверів та промислових машин мінімально відрізняються від політики для користувачів. Зокрема повністю інший набір дозволених та заборонених програм у «Application control», сайтів у «Network Protection», а також правил доступу програм до мережі Інтернет у «Firewall». Всі інші налаштування ідентичні.

Інша справа – поштові сервери. Для їх налаштування виділений окремий розділ в політиці – «Exchange Protection». Тут є багато тонкощів налаштувань.

На вкладці «General» присутні групи користувачів за замовчуванням: адміністратори, гості, користувачі і т.д., але окремо був створений список довірених користувачів «Partner», на які не буде розповсюджуватися сканування модуля «Antimalware», який спричиняє блокування вхідних листів. Це довірені користувачі, які, як правило, використовують застарілі версії поштових серверів, тому GravityZone розцінює листи від цих відправників як потенційно небезпечні та відправляє їх до карантину. Також налаштований і «blacklist» заборонених відправників, які погано зарекомендували себе для організації (масова розсилка, некоректний зміст листів, фішинг тощо).

GravityZone інтегрується із поштовими серверами для сканування всього поштового трафіку, тож було створено правило, яке сканує всю вхідну/вихідну кореспонденцію на наявність шкідливих або потенційно небезпечних вкладень.

Максимальний розмір файлу, який передається поштою та може скануватися – 25 МБ, глибина архівів 25.

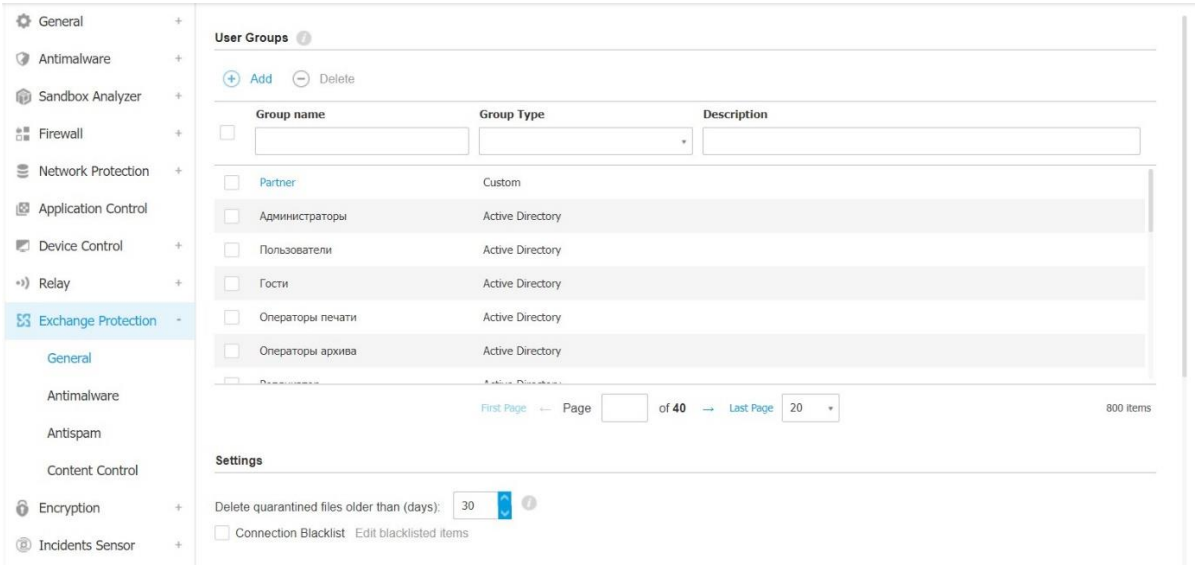


Рис. 3.16. Групування користувачів за списками

Інфіковані вкладення відразу переміщуються до карантину, в іншому випадку – видаляються. Підозрілі файли, або ті, які система не може просканувати також переміщаються до карантину, але як альтернатива – вкладений фацл заміняється на текстовий від Bitdefender.

Для кожного випадку переміщення вкладення до карантину був написаний текст заміщення, який буде відображатися у текстовому файлі, замість вкладеного документу.

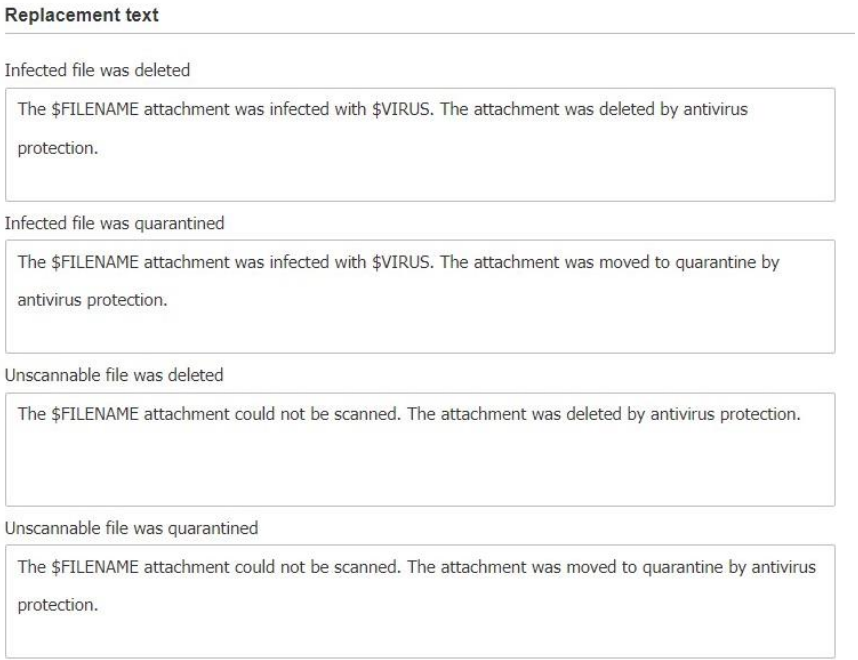


Рис. 3.17. Шаблони тексту для файлів заміщення

Також увімкнений «Antispam filtering», який підключений до загальнодоступних RBL-серверів.

І останнім, але не менш важливим є налаштування фільтрації вмісту листів.

За допомогою «Content filtering» був налаштований певний набір правил для виявлення фішингових листів. Правила налаштовані таким чином, щоб інспектувати текст як і в тілі, так і в темі листа. Також прописані регулярні вирази, які також працюють для блокування листів.

На основі попередніх фішингових листів, які надходили до поштових серверів компанії, був сформований список популярних фраз, які часто зустрічаються у таких листах, а також список посилань, які ведуть на фішингові сайти.

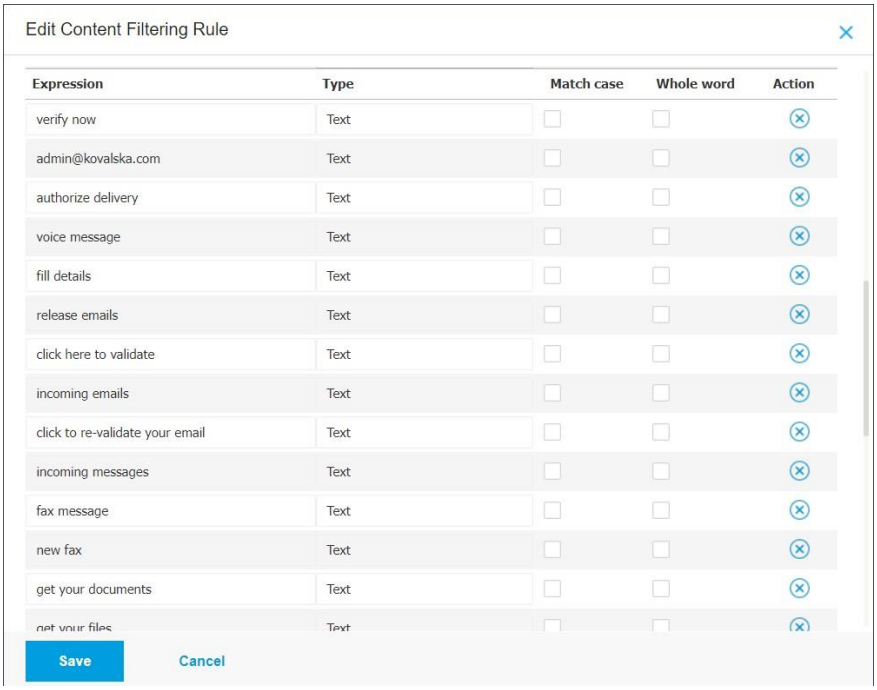


Рис. 3.18. Правило блокування фішингових листів на основі словосполучень

Підготовка до встановлення агентів на кінцеві точки. Створення інсталяційних пакетів.

Для того, щоб кінцеві точки отримали необхідну політику відразу після встановлення агента, необхідно назначити політику на групи AD. Це

відбувається у розділі «Network», де відображаються дані з AD. Дану процедуру необхідно зробити для усіх груп, які були визначені вище.

Наступним кроком необхідно створити інсталяційні пакети. Вони будуть поділені на інші групи: для кінцевих точок з агентом Proxy, без агенту Proxy, а також для поштових серверів.

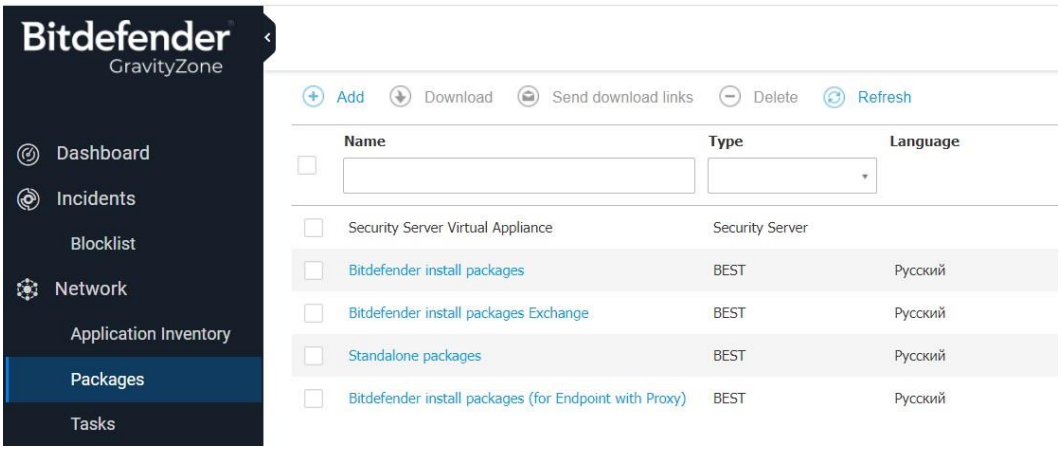


Рис. 3.19. Формування інсталяційних пакетів

Основною відмінністю агентів Bitdefender GravityZone для кінцевих точок з агентом Proxy є вимкнена функція видалення конкурентного ПЗ, оскільки в іншому випадку Bitdefender видалить Proxy з хоста.

Те що стосується поштових серверів – то в даному випадку увімкнене призначення ролі «Exchange Protection».

Встановлення агентів на кінцеві точки.

Для того, щоб встановити агент на усі локальні хости відразу, необхідно створити завдання для віддаленого встановлення пакету. Кінцеві точки обов'язково мають бути активними та в статусі онлайн. Після інсталяції запускається автоматичне сканування кінцевої точки на наявність загроз та формування розгорнутого звіту сканування для подальшого розслідування.

Управління користувачами системи антивірусної безпеки.

Управління користувачами включає створення, редагування, блокування облікових записів користувачів системи і здійснюється адміністратором за допомогою мережевого центру управління [26].

Для кожного облікового запису користувача можна налаштувати доступ до функцій GravityZone або до певних частин мережі, до якої він належить.

Доступні такі ролі користувачів:

Адміністратор компанії – зазвичай, унікальний обліковий запис користувача, з повним доступом до всіх функцій управління рішенням GravityZone. Адміністратор компанії конфігурує налаштування Control Center, керує ліцензійними ключами служб безпеки, керує обліковими записами користувачів тощо.

Адміністратор мережі – з адміністративними привілеями щодо розгортання агентів безпеки у всій компанії або за певними групами кінцевих точок. Мережеві адміністратори відповідають за активне керування налаштуваннями безпеки мережі.

Спеціаліст з безпеки – облікові записи спеціаліста з безпеки доступні лише для читання. Вони дозволяють доступ тільки до даних, звітів та журналів, пов'язаних з безпекою.

Налаштований користувач – ролі користувачів, що включають певну комбінацію прав користувачів, якщо певна роль не відповідає вимогам адміністратора системи.

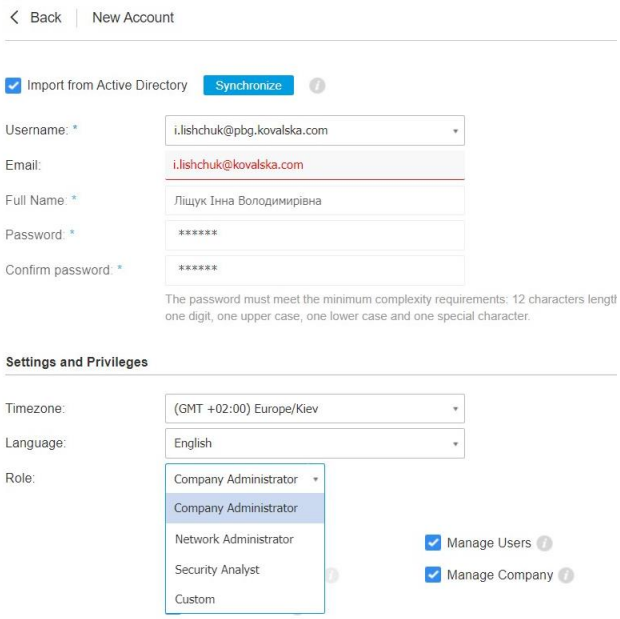


Рис. 3.20. Створення облікового запису користувача

В компанії були задіяні перші три ролі для фахівців з ІБ та ІТ-адміністраторів.

Щоденний моніторинг кінцевих точок та подій.

Процес моніторингу здійснює інформування адміністратора та інших відповідальних осіб про стан системи антивірусної безпеки, про інциденти та події в системі.

Панель Control Center – візуальний дисплей, що налаштовується під кожного користувача та забезпечує швидкий огляд всіх кінцевих точок і статусу мережі. Портлети інформаційної панелі відображають різну інформацію про стан безпеки в реальному часі, використовуючи прості графіки, які дозволяють швидко виявити всі проблеми, які можуть вимагати втручання адміністратора.

В даному випадку були створені два дашборди: перший, який показує статус кінцевих точок і другий – статус модулів політики безпеки.

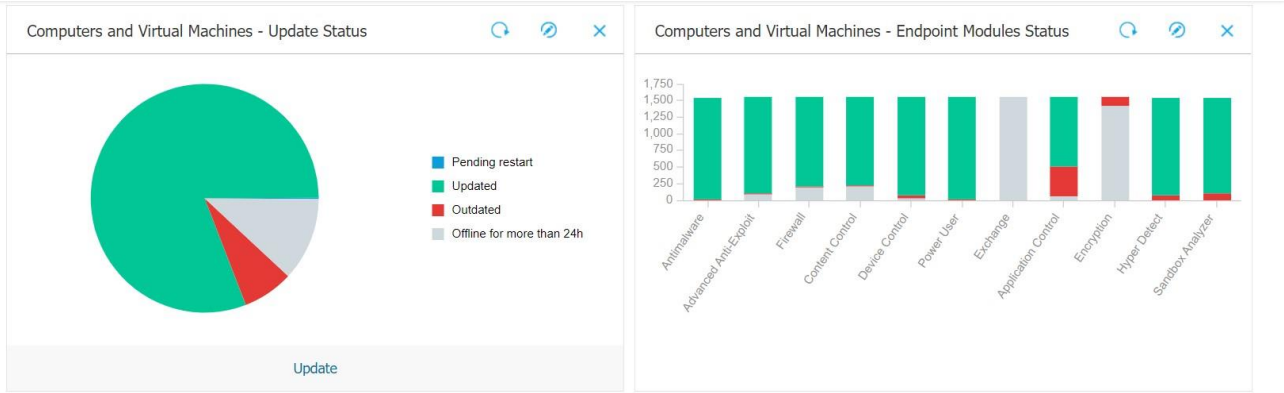


Рис. 3.21. Створення дашбордів моніторингу

Control Center дозволяє створювати та переглядати централізовані звіти про стан безпеки керованих мережевих об'єктів.

Доступно кілька різних типів звітів:

антифішингова активність;

заблоковані програми;

заблоковані веб-сайти;

стан шифрування кінцевих точок;

стан модулів кінцевої точки;

стан активності шкідливого ПЗ;

аудит безпеки;

стан оновлення версії продуктів;

Exchange – активність шкідливого ПЗ тощо.

Отже, можна легко отримати необхідну інформацію, яка представлена в зручних для читання інтерактивних графіках і таблицях, що дозволяє швидко перевірити статус безпеки мережі і виявити будь-які загрози.

Розділ «Quarantine» надає докладну інформацію про файли в карантині з усіх кінцевих точок та Exchange серверів, які знаходяться під керуванням.

Карантин – це зашифрована папка, яка містить потенційно шкідливі файли, такі як: підозріло-шкідливі програми, підозріло-заражені програми або інші небажані файли. Вірус, ізольований у карантинній зоні, не може заподіяти жодної шкоди, тому що його не можна запустити або відкрити для читання.

Сторінка карантину складається із двох панелей:

заражені файли, виявлені безпосередньо у файловій системі кінцевої точки;

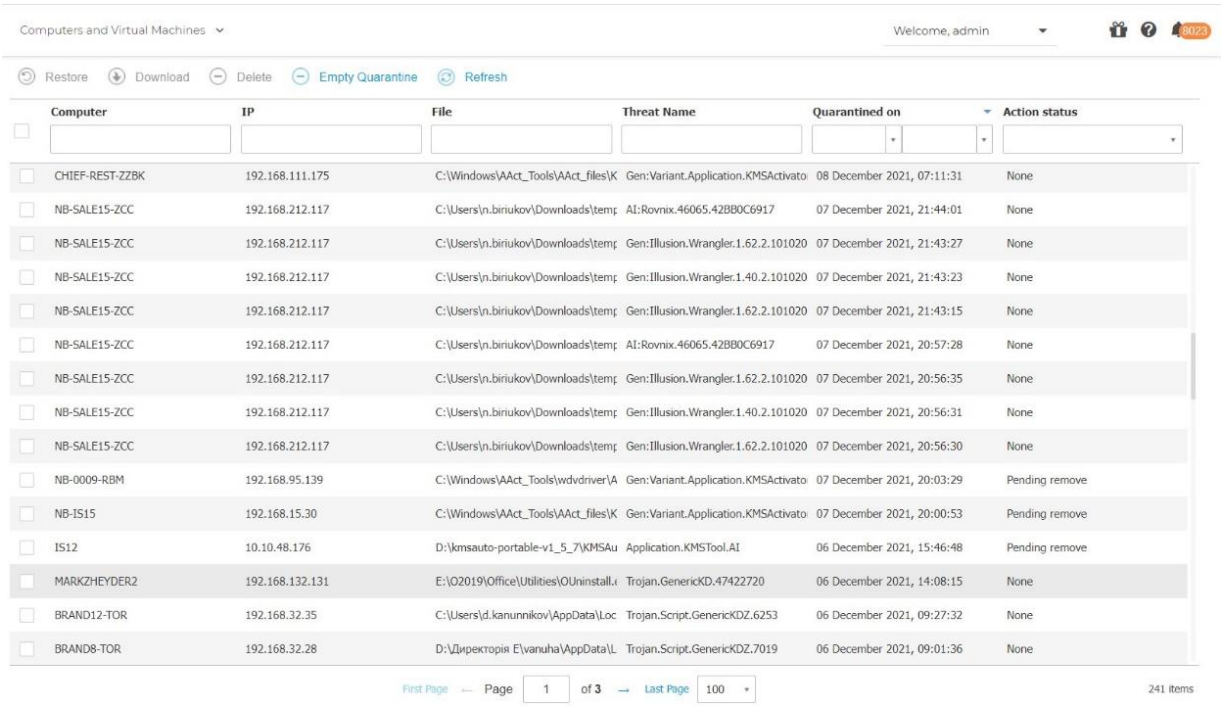


Рис. 3.22. Карантин комп’ютерів та віртуальних машин

інфіковані електронні листи та вкладення, виявлені на серверах Exchange.

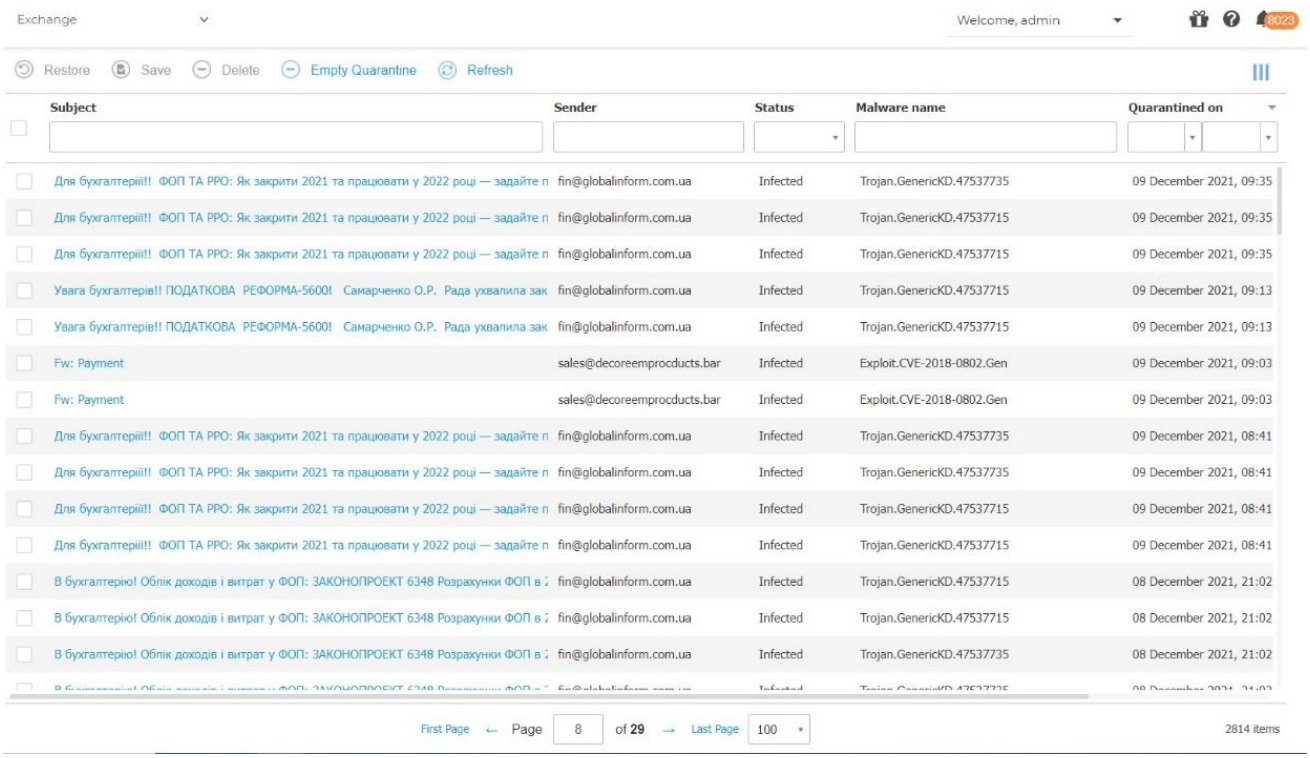


Рис. 3.23. Карантин серверів Exchange

Карантин Exchange містить електронні листи та вкладення. Модуль захисту від шкідливих програм надсилає до карантину вкладення електронної пошти, у той час як антиспам, фільтрація контенту та вкладень, відправляє до карантину весь електронний лист.

Розід «Sandbox Analyzer» є єдиним інтерфейсом для перегляду, фільтрації та пошуку файлів в середовищі пісочниці. Сторінка Sandbox Analyzer складається з двох областей:

область фільтрації дозволяє шукати та фільтрувати матеріали за різними критеріями: ім'я, хеш, дата, результат аналізу, статус, оцінка критичності;

область сканування об’єктів відображає всі заявки у компактному форматі з детальною інформацією.

Як зазначалося вище, підозрілі об’єкти, що знаходяться на кінцевих точках автоматично надсилаються на сканування до пісочниці, але є можливіть

самостійно завантажити файл, аргумент командного рядка або вказати URL-адресу для аналізу на загрози.

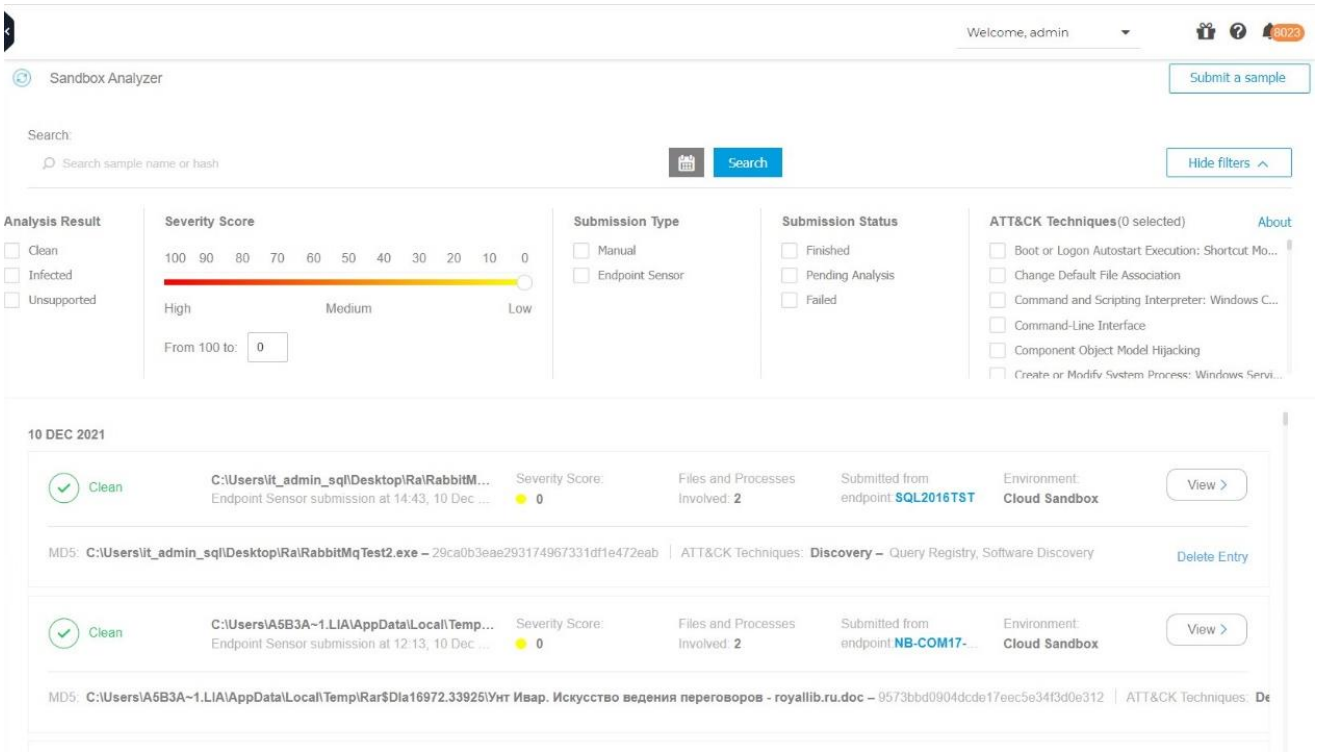


Рис. 3.24. Інтерфейс Sandbox Analyzer

Отже, Bitdefender GravityZone Elite має добре продуману систему керування політиками кінцевих точок, гнучко розгортається та, завдяки своїй структурі, може покрити захистом підприємства будь-якого масштабу. Він виконує усі основні операції безпеки за допомогою власних ресурсів.

3.2 Технологія забезпечення кібербезпеки кінцевих точок на базі рішення Bitdefender GravityZone Elite

Наразі, інформація – це головна зброя в конкурентній боротьбі: знання ситуації, аналіз і контроль для зважених і своєчасних рішень. Витік інформації за межі компанії може завдати непоправної шкоди її репутації, фінансового становища і корпоративній інформаційній системі компанії в цілому. Витік інформації – це цілий спектр неприємностей: починаючи від зриву угод, шкоди

репутації і закінчуючи прямою загрозою бізнесу. Чим більше кінцевих пристроїв підключається до корпоративної мережі, тим більше можливостей для проникнення в цю мережу мають кіберзлочинці.

Зміст технології забезпечення кібербезпеки кінцевих точок корпоративної інформаційної системи на базі Bitdefender GravityZone Elite будуть становити операції безпеки та застосовувані методи і засоби під час їх реалізації (рис. 3.2).

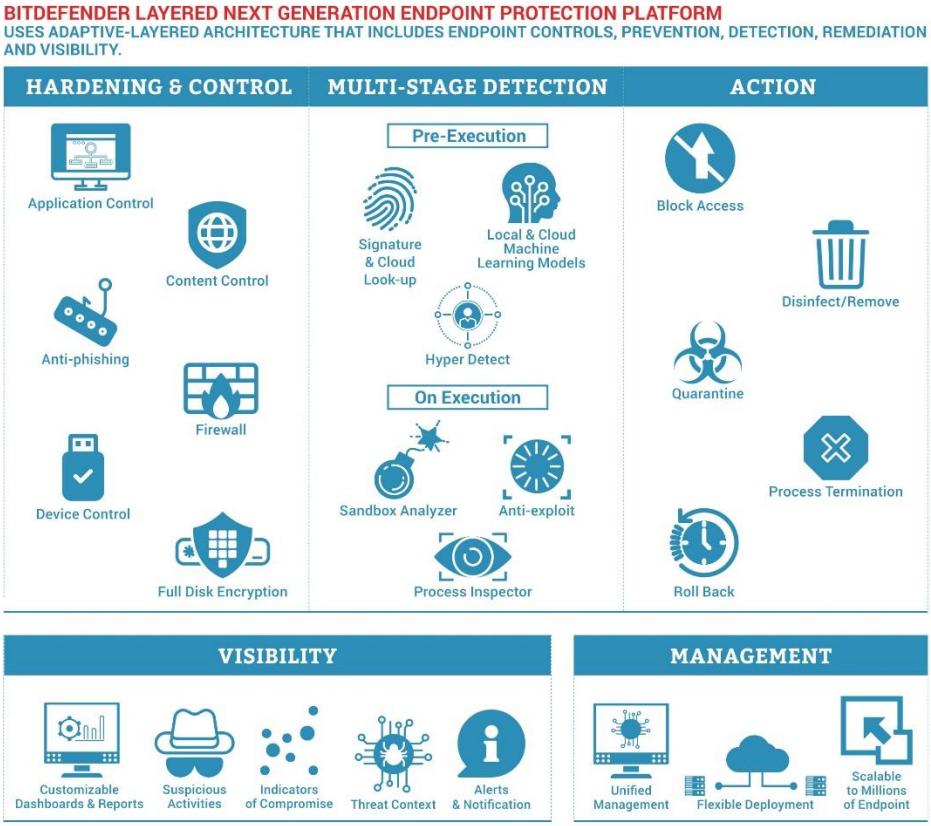


Рис. 3.25. Технологія забезпечення кібербезпеки кінцевих точок корпоративної інформаційної системи на базі Bitdefender GravityZone Elite [25]

Розглянемо основні операції безпеки та застосовувані методи та засоби їх здійснення:

Посилення безпеки та контроль кінцевих точок (Hardening and control).

Дана операція безпеки реалізується за допомогою політик, які в свою чергу містять наступні засоби посилення безпеки на кінцевих точках:

контроль усіх програм, встановлених на АРМ на основі «білих» та «чорних списків»;

контроль веб-вмісту із категоризацією URL-адрес;

фільтрування електронних листів за допомогою правил;

контроль інтернет-з’єданнь за допомогою розподілу мереж;

контроль усіх пристроїв, що підключаються до кінцевої точки із скануванням;

повне шифрування дисків з використанням Windows Bitlocker і Mac FileVault.

Багатоетапне виявлення загроз (Multi-stage detection).

Ділиться на два етапи: до їх виконання (pre-execution) та при виконанні (on execution).

До виконання містить такі засоби виявлення:

пошук об’єктів, які відповідають сигнатурам у БД Bitdefender;

використання локального або хмарного модуля машинного навчання для прогнозування та блокування атак;

моделі машинного навчання та передові технології евристики, навчені виявляти інструменти злому, експлойти та шкідливі програми, щоб заблокувати їх перед виконанням.

При виконанні:

сканування у пісочниці, що глибоко аналізує підозрілі файли, детонує корисне навантаження у закритому віртуальному середовищі, розміщеному на Bitdefender, аналізує поведінку та повідомляє про зловмисний намір об’єкта;

розширені механізми антиексплойту захищають пам'ять і вразливі програми, такі як браузери, засоби зчитування документів, мультимедійні файли та середовище виконання (наприклад, Flash, Java);

інспектор процесів, який працює в режимі нульової довіри та шукає підозрілі дії або аномальну поведінку процесу, а також вживає відповідних дій щодо виправлення, включаючи припинення процесу та скасування внесених процесом змін.

Дії після виявлення загрози (Action).

Основними методами є:

негайне блокування доступу (це може бути припинення процесу або б заборона доступу до ПЗ, пристрою, веб-ресурсу тощо);

лікування або видалення (будь–яку знайдену частину шкідливого коду Bitdefender намагається видалили, але за неможливості – видаляє повністю файл);

переміщення до карантину усіх файлів, що відповідають встановленим налаштуванням у політиці;

припинення процесу при виявленні загрози;

відкат при збої системи або некоректної роботи.

Покращення видимості загроз (Visibility).

Досягається за допомогою наступних засобів:

налаштовуваних дашбордів та звітів, які збирають інформацію згідно до вимог кожного з користувачів системи;

моніторингу підозрілої активності;

індикаторів компромісу, тобто певний пороговий бал, що встановлюються для кожного типу загроз, при перетині якого система сигналізує про небезпеку;

розпізнання контексту загроз та зв’язків;

попередження та сповіщення, що налаштовуються відповідно до потреб.

Управління компонентами (Management).

Основними засобами для продуктивного управління системою є:

єдина точка керування – веб-консоль Control Center;

гнучке розгортання, як хмарне так і локальне;

масштабованість до мільйону кінцевих точок.

3.3 Розроблення рекомендацій щодо застосування технології управління захистом кінцевих точок корпоративної інформаційної системи

Реалізація заходів ефективної кібербезпеки є доволі складним завданням, оскільки сьогодні існує набагато більше пристроїв, ніж людей, а зловмисники стають все більш винахідливими.

Забезпечення інформаційної безпеки сьогодні є нагальною потребою, зневага якої може мати руйнівні наслідки для бізнесу. Широкий набір засобів та рішень, доступних сьогодні захисту інформації, може ускладнювати вибір для підприємства. Забезпечити безпеку IT-інфраструктури дозволяє певний набір інструментів, який необхідно підбирати індивідуально. Це дозволить реалізувати багаторівневу систему захисту, яка забезпечить надійну нейтралізацію актуальних загроз.

Вибір інструментів захисту корпоративної інформації при створенні такої системи має здійснюватися з урахуванням цілого комплексу факторів, таких як:

сфера діяльності компанії;

розмір бізнесу, наявність територіально віддалених підрозділів, а також підрозділів, які потребують особливого інформаційного захисту;

технічна оснащеність компанії – склад та характеристики використовуваного обладнання, рівень зносу тощо;

рівень підготовки та досвіду персоналу, зайнятого обслуговуванням інформаційної інфраструктури [27].

Захист кінцевої точки є однією з найважливіших частин багаторівневого підходу до кібербезпеки. Для того, щоб мати можливість ефективно та комплексно захищати КІС, система захисту кінцевих точок має вирішувати такі завдання:

контроль усіх можливих каналів проникнення вірусів: шлюзи електронної пошти, мережеві протоколи, у тому числі веб-трафік, зовнішні носії інформації, робочі станції користувачів та сервера, мобільні пристрої;

захист від різних видів загроз – вірусів, мережевих та поштових «хробаків», «троянських коней», небажаних програм, руткітів тощо;

безперервний антивірусний моніторинг та періодичне антивірусне сканування всіх підконтрольних об'єктів;

автоматичні звіти та сповіщення при «зараженні», «лікуванні» від вірусів;

контроль дотатків та пристроїв;

централізоване керування всіма компонентами антивірусного захисту;

інтеграція зі сторонніми розробниками такими як Active Directory, IPS/IDS, SIEM тощо;

гнучні варінти розгортання відповідно до потреб організації;

відсутність негативного впливу на продуктивінсть користувачів;

інвентаризація програмного та апаратного забезпечення;

регулярні оновлення та підтримка продукту.

Після встановлення системи безпеки необхідно переконатися, що у продукту є регулярні заплановані оновлення. Шкідливе програмне забезпечення швидко розвивається, і програми безпеки потребують виправлень та оновлень, щоб виявляти будь-які атаки, не залежно від їхніх форм.

Але КІС необхідно захищати не лише з точки зору програм та різних систем захисту. Щоб захистити бізнес від атак зловмисного програмного забезпечення потрібно навчати співробітників, які користуються кінцевими точками в компанії. Дослідження показали, що численні атаки на дані є просто результатом того, що співробітники не можуть ідентифікувати атаку зловмисного програмного забезпечення і, отже, допомагають хакерам у їхніх схемах.

Навчання співробітників розпізнавати потенційні атаки зловмисного програмного забезпечення, такі як фішинг-шахрайство та шкідливі посилання, є надзвичайно корисним кроком у захисті бізнесу та його даних. Тому необхідно регулярно навчати своїх співробітників, а також підтримувтаи їхню обізнаність у сфері загроз інформаційної безпеки [28].

І те, що стосується повністю всієї роботи компанії: на основі висновків IBM Security X-Force у звіті «X-Force Threat Intelligence Index 2021» [13], ефективні способи запобігання загрозам (згідно з еволюційним ландшафтом) – це йти в ногу

із своєчасним аналізом загроз і розбудовувати потужні можливості реагування, не залежно від галузі роботи.

X-Force рекомендує наступні кроки, які необхідно зробити організаціям, щоб краще підготуватися до кіберзагроз у 2021 році:

Працювати на випередження, витрачати більше часу на дослідження загроз, а не на реагування (використовувати розвідку про загрози, щоб краще зрозуміти мотивацію та тактику суб'єктів загроз, щоб визначити пріоритети забезпечення безпеки ресурсів компанії).

Регулярно перевіряти структуру управління виправленням організації (оскільки сканування та експлойти були найпоширенішим вектором зараження минулого року, необхідно зміцнювати свою інфраструктуру та активізувати внутрішнє виявлення, щоб швидко та ефективно знаходити та зупиняти автоматизовані спроби експлуатації).

Створити групу реагування на інциденти в організації (якщо це неможливо, залучити ефективні можливості реагування на інциденти для швидкого реагування на інциденти з високим рівнем впливу).

Впровадити багатофакторну аутентифікацію (MFA) (додавання рівнів захисту до облікових записів співробітників залишається одним із найефективніших пріоритетів безпеки для організацій).

Планувати та вивчати атаки програм-вимагачів (особливо які складаються з комбінованих методів вимагання та крадіжки даних; регулярне дослідження цього плану може змінити те, як організація зреагує в критичний момент).

Пропрацювати захист від внутрішніх загроз (використовувати рішення для запобігання втрати даних, проводити постійний моніторинг, щоб запобігти проникненню ненавмисних або зловмисних інсайдерів в організацію).

Проводити стрес-тестування плану реагування на інциденти організації для розвитку м'язової пам'яті (такі тренування можуть надати команді інформаційної безпеки важливий досвід, щоб покращити час реакції, скоротити час простою та, зрештою, заощадити гроші у разі порушення безпеки).

Створювати резервні копії та зберігати їх в автономному режимі (не тільки наявність резервних копій, але й їхня ефективність має важливе значення в безпеці організації, особливо з урахуванням даних 2020 року, які свідчать про відновлення активності програм-вимагачів).

Питання не в тому, чи є в інфраструктурі тієї чи іншої компанії вразливі місця. Критичні чи некритичні, але вразливості є і будуть, і це об'єктивна даність. Питання в тому, як до цього ставляться самі власники бізнесу та технічні фахівці.

Кінцеві точки – це найважливіший елемент інфраструктури, що потребує підвищеної уваги до питань безпеки. Розвиток сучасних інструментів – продуктів класу EDR, SIEM-систем, DLP-рішень та інших засобів боротьби з кіберзагрозами, – безумовно, підвищує загальний рівень захищеності компанії, але не достатньо вирішує проблеми робочих станцій, багато з яких можуть і зовсім перебувати за периметром безпеки.

За сучасних умов антивірус став абсолютно необхідним для будь-якої компанії, незалежно від її масштабу, але не потрібно забувати, що жодна система не дасть стовідсоткової безпеки, тому для забезпечення безпеки корпоративних інформаційних систем потрібен комплекс рішень, як програмних, так і виховних, що залучають моральні цінності користувачів системи.

ВИСНОВОК

В роботі проведено дослідження та аналіз проблеми забезпечення кінцевих точок корпоративної інформаційної мережі, що базується на звітах Ponemon Institute від 2020 року, компанії Accenture та IBM Security X-Force від 2021 року. Доведено актуальність загроз, які стосуються саме кінцевих точок та зростають в масштабованості з кожним роком.

Проаналізовано призначення, структуру, функції та умови функціонування корпоративних інформаційних систем типу ERP, а також проведено аналіз існуючих технологій управління захистом кінцевих точок КІС на основі даних звіту Gartner від 2021 року «Magic Quadrant for Endpoint Protection Platforms»: ESET Endpoint Security, McAfee Enterprise, Symantec Endpoint Security та Bitdefender GravityZone.

Досліджено призначення та функції Bitdefender GravityZone Elite. Описані основні рівні захисту продукту: захист від шкідливого ПЗ, АТС, виявлення гіпервізора, брандмауер, контроль контенту, додатків та пристроїв, шифрування, захист Exchange, Sandbox Analyzer, безпека для мобільних пристроїв.

Визначено компоненти та архітектуру рішення GravityZone, яке керується з єдиної точки управління – веб-консолі Control Center. Наведено топологію системи управління кінцевими точками. Розглянуті усі ролі, з яких складається Bitdefender GravityZone Elite: база даних, сервер оновлень, веб-консоль, сервер безпеки, комунікаційний сервер, балансувальник, а також описані ролі кінцевих точок.

Окремим пунктом проаналізовано призначення, характеристики та можливості модуля «Policy», оскільки він є ключовим елементом у керуванні кінцевими точками та забезпеченні їхньої безпеки.

Розроблено технологію застосування системи управління захистом кінцевих точок КІС – створено алгоритм впровадження антивірусного захисту

Bitdefender GravityZone Elite, а також власну структуру взаємодії кінцевих точок та компонентів GravityZone.

У роботі показано основні можливості налаштування превентивних засобів у програмному забезпеченні Bitdefender GravityZone Elite: створення політик безпеки, правила сканування пісочниці, правила блокування застосунків, веб-ресурсів, шкідливих електронних листів, несанкціонованих інтернет-з’єднань тощо.

Визначено зміст технології забезпечення кібербезпеки кінцевих точок за допомогою операцій безпеки та методів їх реалізації.

Розроблено рекомендації щодо застосування технології управління захистом кінцевих точок з метою протидії усім типам загроз, наведено поради вибору інструментів антивірусного захисту відповідно до можливостей компанії, а також описані ключові задачі, які має виконувати система захисту кінцевих точок.

Таким чином, правильна реалізація захисту кінцевих точок буде забезпечувати безпечне, повноцінне, безперебійне функціонування корпоративної інформаційної системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Інформаційна безпека підприємства: ключові загрози та засоби захисту [Електронний ресурс] // Smart-Soft Team. – 2020. – Режим доступу до ресурсу: https://www.smart-soft.ru/blog/informatsionnaja-bezopasnost/.

2. Загальні характеристики комп'ютерних вірусів. Антивірусні програми та їх застосування [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: http://informatics.dp.ua/zagalni-harakterystyky-kompyutern/.

3. Саричев Д. В. Защита конечных точек в современных условиях [Електронний ресурс] / Денис В. Саричев. – 2021. – Режим доступу до ресурсу: https://www.anti-malware.ru/analytics/Technology_Analysis/EndPoint-Protection-in-modern-conditions.

4. Endpoint Protection – багаторівневий підхід до захисту від сучасних загроз [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://itbiz.ua/statti-ta-obzori/endpoint-protection-bagatorivnevij-pidxid-do-zaxistu-vid-suchasnix-zagroz/.

5. Глушко С. В. Управлінські інформаційні системи / С. В. Глушко, А. В. Шайкан. – Львів: Магнолія Плюс, 2006. – 320 с.

6. Савінов А. В. Корпоративні інформаційні системи [Електронний ресурс] / А. В. Савінов. – 2004. – Режим доступу до ресурсу: http://kist.ntu.edu.ua/textPhD/.

7. Інформаційні технології автоматизації управління в масштабах корпорації [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://pidru4niki.com/74260/informatika/korporativni_informatsiyni_sistemi.

8. Куровський І. В. ERP – система планування та управління ресурсами підприємства [Електронний ресурс] / І. В. Куровський. – 2013. – Режим доступу до ресурсу: https://system.dss-bi.com.ua/erp.

9. Chang J. Benefits of ERP Software: Examples of Top Solutions Explained [Електронний ресурс] / Jenny Chang – Режим доступу до ресурсу:

https://financesonline.com/benefits-erp-software-examples-top-solutions-explained/.

10. Endpoint security: The key to protecting your enterprise [Електронний ресурс] // Vulnerability Manager Plus. – 2020. – Режим доступу до ресурсу: https://blogs.manageengine.com/desktop-mobile/vulnerability-manager-plus/2020/01/30/endpoint-security-the-key-to-protecting-your-enterprise.html.

11. What Is Endpoint Security? [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.mcafee.com/enterprise/ru-ru/security-awareness/endpoint.html.

12. How aligning security and the business creates cyber resilience [Електронний ресурс] // Accenture. – 2021. – Режим доступу до ресурсу: https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf.

13. X-Force Threat Intelligence Index 2021 [Електронний ресурс] // IBM Corporation. – 2021. – Режим доступу до ресурсу: https://www.cert.hu/sites/default/files/xforce_threat_intelligence_index_2021_90037390usen.pdf.

14. Кондрашин М. Р. Защита конечных точек в современных условиях: инструменты и основные проблемы [Електронний ресурс] / М. Р. Кондрашин. – 2019. – Режим доступу до ресурсу: https://ko.com.ua/zashhita_konechnyh_tochek_v_sovremennyh_usloviyah_instrumenty_i_osnovnye_problemy_129548.

15. What Is Next-Generation Antivirus (NGAV)? [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.sentinelone.com/cybersecurity-101/next-generation-antivirus-ngav/.

16. What Is Next-Gen Antivirus? [Електронний ресурс] // Impact. – 2021. – Режим доступу до ресурсу: https://www.impactmybiz.com/blog/blog-what-is-next-gen-antivirus/.

17. ESET – единственный «Претендент» по платформам для защиты конечных точек у Gartner [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://channel4it.com/publications/ESET-edinstvennyy-Pretendent-po-

platformam-dlya-zashchity-konechnyh-tochek-u-Gartner-29298.html.

18. CROWDSTRIKE has become the leader in the Gartner Magic Quadrant 2021 for the second time among endpoint protection platforms [Електронний ресурс] // Intelligent IT Distribution. – 2021. – Режим доступу до ресурсу: https://iitd.com.ua/en/news/crowdstrike-vdruge-stala-liderom-v-gartner-magic-quadrant-2021-roku-sered-platform-zahistu-kincevih-tochok/.

19. What's Changed: 2021 Gartner Magic Quadrant for Endpoint Protection Platforms (EPP) [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://solutionsreview.com/endpoint-security/whats-changed-2021-gartner-magic-quadrant-for-endpoint-protection-platforms-epp/.

20. Документация для пользователей, подключенных с помощью ESET Remote Administrator [Електронний ресурс] // ESET. – 2019. – Режим доступу до ресурсу: https://help.eset.com/ees/6/ru-RU/index.html?documentation_for_users_connected.htm.

21. Symantec EDR architecture [Електронний ресурс] // Broadcom. – 2021. – Режим доступу до ресурсу: https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-detection-and-response/4-5/introduction-v119804561-d38e3280/architecture-v125228003-d38e2709.html.

22. Witts J. The Top 11 Endpoint Security Solutions For Business [Електронний ресурс] / Joel Witts // Expert Insights. – 2021. – Режим доступу до ресурсу: https://expertinsights.com/insights/the-top-endpoint-security-solutions-for-business/#Bitdefender%20GravityZone.

23. Lord N. What is Endpoint Protection? [Електронний ресурс] / Nate Lord // Digital Guardian. – 2018. – Режим доступу до ресурсу: https://digitalguardian.com/blog/what-endpoint-protection-data-protection-101.

24. Bitdefender GravityZone Руководство администратора [Електронний ресурс] // Bitdefender. – 2020. – Режим доступу до ресурсу: https://bitdefender.ru/wp-content/uploads/Elite-Security-rukovodstvo-administratora.pdf.

25. Bitdefender GravityZone Руководство по установке [Електронний ресурс] // Bitdefender. – 2020. – Режим доступу до ресурсу: https://bitdefender.ru/wp-

content/uploads/GravityZone-Business-Security-GID-po-ustanovke.pdf.

26. Анучин Р. А. Методика управления антивирусной безопасностью в организации [Електронний ресурс] / Р. А. Анучин. – 2018. – Режим доступу до ресурсу: https://elib.pnzgu.ru/files/eb/doc/ii5D4s2QfntL.pdf.

27. Информационная безопасность предприятия: ключевые угрозы и средства защиты [Електронний ресурс] // Smart-Soft Team. – 2020. – Режим доступу до ресурсу: https://www.smart-soft.ru/blog/informatsionnaja-bezopasnost/.

28. How to protect your business from malware attacks [Електронний ресурс] // Copy CEI. – 2021. – Режим доступу до ресурсу: https://www.copycei.com/how-to-protect-your-business-from-malware-attacks/.